DMS LOGISTICS

FORENSIC INVESTIGATION POLICY

Code: POL-TI-013
Revision: 01
Data: 01/03/2023

CONTROLE DE QUALIDADE
APROVADO DMS LOGISTICS
ISO 9001:2015

1. INTRODUCTION

DMS LOGISTICS is responsible for ensuring compliance with ISO 27001, responsible for best information security practices, and the General Law for the Protection of Personal Data (LGPD) and its requirements regarding the collection, storage, recovery and destruction of records of personal data and/or sensitive data ("Personal Data").

This policy is aimed at the investigation of incidents that may lead to leakage, theft, copying or any unauthorized actions in the data and information existing in DMS LOGISTICS. That document was based on NIST.

The objective is to establish clear procedures on forensic investigation, as well as processes for identifying, collecting, acquiring and preserving digital evidence that can ensure the probative value of evidence and investigations, in cases where it proves necessary.

2. GLOSSARY

Acquisition of Digital Proof: Process that involves the creation (image) of the Digital Proof. The end result of this process is the copy of the defined data.

Privacy and Data Protection Area: Area responsible for supporting the DPO (Data Protection Officer).

Notarial Minutes: Written and public faith proof of facts witnessed by the notary in the exercise of his office.

Chain of Custody: Set of all procedures used to maintain and document the chronological history of evidence, to trace its possession and handling from its recognition to its disposal, thus ensuring the preservation of evidentiary value.

Time Carimbo: A time variation parameter that indicates the specific moment that concerns a common time reference.

SubscriberIdentity Module (SIM) and USIM cards: Universal SubscriberIdentity Module.

Cards that are used for communication, the first being for communication on GSM networks and the second for UMTS (3G) networks.

Digital Proof Collection: Process of recalling physical items that contain potential Digital Evidence.

Reliability of Digital Proof: Guarantee that Digital Proof is subject to audit and repeatability by other authorities and employees.

Volatile Data: Data that is prone to change and can be easily modified or lost.

Digital Evidence Specialist (DES): Authorized laborer, trained and qualified to handle digital evidence.

Digital Device: Equipment or resource used to process or store digital data.

Digital Evidence Specialist (DES): Authorized, trained and qualified collaborator to handle digital evidence.

Digital Evidence: Data stored or transmitted in digital form, which may be used as evidence.

Check/ Hash Function: Function used to verify two sets of identical data.

Digital Proof Identification: Process of search, recognition and documentation of the Digital Proof.

Mouse-Jugglers: Feature used to prevent the device from entering standby mode.

Preservation of Digital Proof: Process to maintain and protect the integrity and/or original condition of the Digital Proof.

Digital Proof Acquisition Process: Process in which the duplication of the Digital Proof to another device in the physical environment is performed.

Digital Proof Collection Process: A process in which the device that stores potential digitais evidence is removed from the original environment and taken for copying in another area of the organization.

Relevance of Digital Evidence: Ensuring that the digital evidence is relevant to the investigation of the incident.

Sufficiency of Digital Proof: Ensures That the Digital Evidence collected or acquired is sufficient to allow its proper use.

Attempted Fraud: An attempt to circumvent established guidelines and controls, when found, should be treated as a violation.

Violation: Any activity that disrespects the rules established in this Policy and in complementary documents.

3. FORENSE RESEARCH

Forensic analysis of computers and networks has evolved to ensure the proper presentation of evidentiary data of cyber institutions. Forensic and technical tools are designed in the context of criminal investigations, equipment security, and incident handling – used to respond to an event by investigating suspicious systems, collecting and preserving evidence, reconstructing events, and assessing the current state of an event. However, forensic tools and techniques are also useful for many other types of tasks, such as the following:

Operational troubleshooting. Many forensic tools and techniques can be applied to troubleshoot operational issues, such as finding the virtual and physical location of a host with an incorrect network configuration, resolving a functional problem with an application, and writing and reviewing the current operating system and application settings for a host.

Monitoring of records. Several tools and techniques can assist in monitoring logs, such as analyzing correlated log entries across multiple systems. This can help with incidents of manipulation, identification of policy violations, auditing, and other efforts.

Data recovery. There are dozens of tools that can recover lost data from systems, including data that has been accidentally or purposely deleted or modified. The amount of data that can be recovered varies from case to case.

Data acquisition. Some organizations use forensic tools to acquire data from hosts that are being deployed or retired. For example, when a user leaves an organization, data from the user's workstation can be acquired and stored if needed in the future. The workstation can then be sanitized to remove alldata from the original user.

Due Diligence/Regulatory Compliance. Existing and emerging regulations require many organizations to protect sensitive information and maintain certain records for audit purposes.

In addition, when protected information is exposed to other parties, organizations may be required to notify other agencies or individuals affected. Expertise can help organizations exercise due diligence and comply with such requirements.

Regardless of the situation, the forensic process comprises the following basic phases:

1. Collection. The first phase of the process is to identify, label, record and acquire data from potential relevant data sources, following guidelines and procedures that preserve data integrity. Collection is typically performed in a timely manner due to the likelihood of losing dynamic data, such as current network connections, as well as losing data from battery-powered devices (e.g., tablets, mobile phones).

2. Examination. Examinations involve the forensic processing of large amounts of data collected using a combination of automated and manual methods to evaluate and extract data of interest, while preserving the integrity of the data.

3. Analysis. The next phase of the process is to analyze the test results, using justifiable methods and techniques, to obtain useful information that addresses the issues that drove the collection and test.

4. Communicating. The final phase is to report the results of the analysis, which may include describing the actions used, explaining how the tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, security, identified vulnerabilities, improved existing security) and providing recommendations for improving policies, guidelines, procedures, tools, and other aspects of forensic expertise. The formality of the notification step varies greatly depending on the situation.

5. Lessons Learned. After the investigation, a meeting should be held with the Senior Management of DMS LOGISTICS., the CISO, the Information Security Manager and the Information Security Team to evaluate the results and discuss points of improvement.

4. ROLES AND RESPONSIBILITIES

Forensic Team

To carry out investigations and forensic analysis of computers and networks, it is necessary to have the determination of roles and responsibilities of the professionals involved. Although there is the possibility of adhesion of other roles, according to the concrete scenario, all processes of investigation and collection of digital evidence will involve the

following groups:
CISO: It is responsible for the strategy of forensic analysis, specifies the form of evidence collection and approves the documents, reports and evidence collected.

Information Security Manager: Is responsible for verifying that the guidelines passed by the ICSO are being complied with. Converts strategies into tactical actions and accompanies the Investigator Team in the work.

Data Officer: If the investigation involves personal data, whether of employees or third parties, the Data Controller shall supervise the documents, reports and monitor the adoption of technical protective measures to ensure the confidentiality of the data, communication with the Holders and the National Data Protection Authority and other interested parties, according to the concrete situation.

Lead Investigator: Is responsible for forensic analysis, ensuring that procedures are followed to maintain the integrity of information.

Team of investigators: These are the members, at the operational level, who investigate cases with indications of violations, whether criminal (intentional) or accidental.

They use many forensic techniques and tools. It is composed of other investigators and may include legal advisors, members of the Human Resources department, Finance Department, and the Data Officer (DPO) in case of compromise of personal data. Law enforcement officers and others outside the organization who may conduct criminal investigations are not considered part of the internal group of an investigators' organization.

Information Technology (IT) and Information Security (IS) professionals: This group includes technical support and system, network and security teams, as well as, if necessary, their administrators. They use a small number of forensic techniques and tools specific to their area of expertise, experience and during their routine work (e.g. monitoring, troubleshooting, data recovery).

External Agents: If the concrete situation requires analysts specialized in a certain area of expertise, they may be called to perform forensic expertise, such as sending media physically damaged to a data recovery company for reconstruction, or specially trained law enforcement personnel or consultants collect data from an unusual source (e.g., cell phone). If, in the investigation process, it is necessary to use specialized software, equipment, facilities and technical knowledge that exceed the knowledge of the Investigators' Team, external agents may be called upon to perform specific tasks.

The Forensic Team, in particular the Lead Investigator, the Investigator Team and the Information Technology (IT) and Information Security (IS) Professionals have the following responsibilities:

1. Ensure the auditability, repeatability, reproducibility and justifiability of digital evidence;

2. Examine the physical and logical environment and identify internal and external data sources;

3. Prioritize sources and establish the order in which devices or data should be collected or acquired;

4. Authorize or not the presence of employees in the physical environment of the incident, when the need for handling evidence is originated by incident;

5. Ensure the integrity of the devices during the process of analysis of the physical environment; 6. Determine which employee is responsible for the physical environment;

7. Document the environment and all devices;

8. To ensure, whenever necessary, the authorization or presence of the person responsible for the material or device;

9. Analyze potential digital evidence under this Policy;

10. Carry the necessary resources for the process of collection and acquisition of digital evidence;

11. Request, whenever necessary, technical or legal support;

12. Decide on the collection or acquisition of digital evidence;

13. Collect digital evidence on on, off, or networked devices pursuant to this Policy;

14. Acquire digital evidence on on, off, or networked devices pursuant to this Policy;

15. Analyze the need for partial acquisition of digital evidence, pursuant to this Policy;

16. Carry out the immediate acquisition of mission-critical digital devices in accordance with this Policy;

17. Perform the collection or acquisition of removable digital storage media; 18. Perform the

preservation of digital evidence in a safe place and with restricted access; 19. Enforce The chain of custody of digital evidence;

20. Carry digital evidence securely;

21. Document the entire process of identifying, collecting, acquiring, transporting and preserving digital evidence;

22. Maintain the confidentiality of the entire process of handling and content of digital evidence.

5. GENERAL GUIDELINES

The proper handling of digital evidence is essential to ensure its auditability, repeatability, reproducibility and justifiability, which will contribute to the admissibility of digital evidence in judicial, administrative or disciplinary proceedings.

Digital evidence can originate from different types of digital devices and environments, such as networks, databases, the Internet, hard drives, mobile devices, and even systems.

To ensure the reliability of digital evidence, identification, collection, acquisition and preservation procedures must rely on:

1. Application of the procedures described in this document;

2. Documentation of all actions performed;

3. Indication of qualified DES during the process of handling the digital evidence. The handling of digital evidence must be carried out in accordance with national laws and regulations. In addition, DES should consider its relevance, reliability and sufficiency for DMS LOGISTICS.

If an incident/breach is identified that causes personal data leakage, the Data Officer (DPO), the Privacy team and those responsible for Information Security and Incident Response must be immediately activated and initiate the containment, preservation, recovery and investigation plan for what happened.

The remaining steps will follow the following procedures.

6. PRIOR OPERATING PROCEDURES

If suspicious activity is identified, it should be immediately reported to the Information

Security Manager and the CISO. The Information Security Manager will check if the case requires a forensic investigation. If deemed necessary, it will send an e-mail communication to the CISO, requesting the opening of an investigation. The Information Security Manager will determine, according to the concrete situation, the collection of the equipment potentially involved in the situation and will keep it in a safe place.

If the CISO approves the investigation, he will give the directions to summon the Forensic Team. The investigation shall be deemed to have commenced upon such call.

The Forensic Team should make a prior analysis to see if it is necessary to continue with the investigation or if it is a false alert.

Once the investigation has been decided, the Forensic Team will establish a timeline of actions and determine which methods, tools, devices and systems will be investigated. From there, the chain of custody is created, best described in a topic specified in another section of this document.

All evidence will be stored at a specific location, designated at the opening of the investigation.

An inventory will be kept with all the evidence collected, under the responsibility of the Information Security team and the Information Security Manager.

We then move on to the phases of collection, analysis, reporting and lessons learned, described below.

7. RESPONSE TIME

The forensic investigation process must be initiated within a maximum of 24 hours from the knowledge of the violation.

8. DATA SENSITIVITY

If the existence of personal data, whether sensitive or not, or other issues involving privacy, sensitivity of information and trade or industrial secrets is observed, there may be restrictions on the participation of external agents in the investigation.

In these cases, it will be preferable to keep this data, information, equipment or systems under your own control to protect the privacy of the data.

Guiding principles of forensic investigation

During the handling of digital evidence, the Lead Investigator, the Investigator Team and DES shall ensure:

1. Auditability: ensuring that the activities carried out during the collection procedure or acquisition may be evaluated (audited) by an authorized third party;

2. Repeatability: ensuring that the collection or acquisition procedure can be repeated, under the same conditions and tools, in order to achieve the same result. If the conditions do not allow the repeatability of the test, for example, in case of volatile memory, this fact must be documented in the chain of custody;

3. Reproducibility: guarantee that, when under different conditions and tools, the result obtained by the collection or acquisition of digital evidence can be reproduced;

4. Justifiability: ensuring that the person responsible for the collection or acquisition is able to justify all actions and methods used for the treatment of digital evidence.

9. RESEARCH FORENSE

The goal, when performing a forensic examination, is to gain a better understanding of an event of interest to find and analyze the facts related to that event.

It can be required in many different situations, such as collecting evidence for lawsuits, disciplinary actions, handling malware incidents, and problems.

Unusual operations. The expertise should be carried out using the process of four phases: collection, examination, analysis and reporting with conclusions, which will be addressed during the policy.

This section describes the basic phases of the forensic process: collection, examination, analysis, and communicating.

The research should be guided by the following questions:

1. What is the objective/purpose of the investigation?

2. What is the focus of the investigation?

3. What issues will be investigated?

4. What answers can be obtained with the investigation?

5. What is the relevant data to get these answers?

During collection, data related to a specific event is identified, labeled, recorded and collected, and its integrity is preserved.

In the second phase, the examination is done, with the use of forensic tools and techniques appropriate to the types of data that were collected to identify and extract the information from the collected data, protecting its integrity. The exam can use a combination of automated tools and manual processes.

The next phase, analysis, involves analyzing the results of the exam to obtain useful information that addresses the questions that were the impetus to perform the collection and examination.

The final phase involves reporting the results of the analysis, which may include describing the actions performed, determining what other actions need to be performed, and recommending improvements in policies, guidelines, procedures, tools, and other aspects of the forensic process.

10. DIGITAL PROOF HANDLING

The digital proof can be altered, altered or destroyed by improper handling, making it unusable. Therefore, it is essential that:

1. The original device or data, as well as the material collected or acquired, are handled as little as possible and only by designated persons;

2. All actions taken are documented;

3. All persons who have had access to digital evidence and location are identified and recorded.

11. IDENTIFICATION OF DIGITAL EVIDENCE

Digital evidence can be represented in the following ways:

1. Physics, for example: the desktop computer or mobile devices;

2. Logic, for example: the data or applications on a device.

To identify digital evidence, the designated officer (Lead Investigator/DES) must become aware of the incident, perform the recognition of the physical and logical environment and possible sources of data, whether internal or external.

It is essential that, before starting the digital evidence identification procedure, the Lead Investigator /DES has details about the incident that required his activity.

Thus, when examining the physical and logical environment where digital evidence will be collected or acquired, the Lead Investigator/DES must identify internal data sources, such as:

1. Desktop computers;

2. Servers;

3. Networked storage devices;

4. Notebooks, mobile phones, smartphones and tablets;

5. Pen drives, CDs, DVDs and USB ports;

6. Flash memory cards;

7. Printers;

8. Backup Media;

9. Systems.

External sources of data can also be identified, such as:

1. Activities carried out via the Web;

2. Cloud computing;

3. Personal or third-party devices.

The identification should prioritize the sources and establish the order that the devices will be collected or the data acquired, considering:

1. Value of the data;

2. Data volatility;

3. Amount of effort required (time spent, cost of equipment and services).

At this stage, the Lead Investigator/DES must ensure that the devices remain in the state they are in, i.e. if they are turned on, they will remain on; if they are turned off, they will remain off.

The Lead Investigator/DES should evaluate and battery-powered devices need to be charged to the power source to ensure that data is not lost.

12. ANALYSIS OF THE PHYSICAL ENVIRONMENT OF THE INCIDENT

The physical environment of the digital evidence must be preserved and accessed only by the Lead Investigator / DES and by the collaborators authorized by him.

Before commencing the collection or acquisition of digital evidence, the Lead Investigator/DES must:

1. Ensure and take control of the physical environment where the devices are;

2. Determine which employee will be responsible for the physical environment;

3. Ensure that employees are away from devices and power sources;

4. Document any employee who has access to the environment or may be involved with the incident/;

5. Document the scene and all its devices (photograph or take notes);

6. Search for items such as notes, drafts, calendars, papers, notes, and mobile devices in the environment;

7. Disable bluetooth connections and wireless networks of employees' mobile devices;

8. Use, if necessary, wireless signal detector.

13. PRESENCE OF THOSE RESPONSIBLE

If the digital evidence collected or acquired is not the property of DMS LOGISTICS., the Lead

Investigator/DES must ensure that the person responsible for the device is authorized and present.

14. ANALYSIS OF POTENTIAL DIGITAL EVIDENCE

For analysis of potential digital evidence, the Lead Investigator/DES should consider the following aspects before commencing any activity:

1. Which method of collection or acquisition will be applied in the case;

2. What is the level of volatility of the data related to the potential digital evidence; 3. What resources will be needed;

4. Whether it is possible to identify the existence of any remote connection to the device and whether this poses any threat to the integrity of potential digital evidence;

5. What to do if the device or data is damaged or compromised;

6. What you do and any device is configured to destroy or obfuscate a piece of data if turned off or accessed in an uncontrolled manner.

In addition, the Lead Investigator/DES should consider the following circumstances:

1. If there is legal permission or formal authorization from the person responsible for the device to carry out its collection if the device is not owned by DMS LOGISTICS.;

2. If there is a need to draw up notarial minutes, in order to authenticate and understand the truth of facts or state of the data;

3. Whether there is a need to use another method for acquiring evidence;

4. Mandatory acquisition or collection occurs in secrecy. Whenever possible this activity should occur at times and days that have the lowest concentration of people;

5. If the device is mission critical, what is the grace period to perform any activity.

For the process of collecting or acquiring digital evidence, the Lead Investigator/DES must have the following resources:

1. Workstation Forense;

2. Devices for data storage;

3. Blank media;

4. Material for handling and recording evidence, for example, sealed bags for storing evidence, notebooks, labels and cameras;

5. Physical protection of the physical environment, if necessary.

The Lead Investigator / DES must request technical or legal support, whenever necessary, from the other areas of DMS LOGISTICS. or outsourced companies.

To acquire or collect data from external or intrusive sources, the Lead Investigator / DES must contact and involve the Legal Department, as it may depend on lawsuits, extrajudicial, contractual clauses or internal regulations.

15. DECISION-MAKING PROCESS: COLLECTING OR ACQUIRING DIGITAL EVIDENCE

For the Lead Investigator/DES to decide on the collection or acquisition of digital evidence, it should note:

1. Data volatility;

2. Legal permission or authorization to perform the collection of the device or acquisition of evidence, if not from DMS LOGISTICS;

3. Confidentiality of collection or acquisition;

4. Criticality of the system or device;

5. Existence of complete disk encryption, or of volumes on which keys and passwords may reside as volatile data;

6. Resources, such as the size of the other device for acquiring evidence or the availability (time) of the DES;

7. Need to maintain or re-establish the activity or service of DMS LOGISTICS.

Below is a flow for decision making in collecting or acquiring digital evidence:

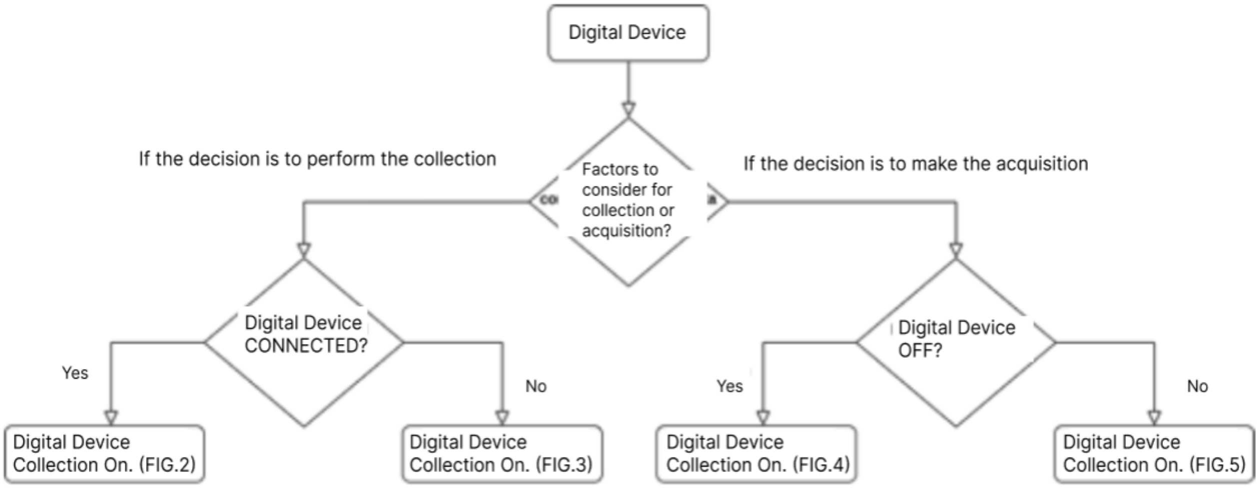

Digital Device
If the decision is to perform the collection
Factors to consider for collection or acquisition?
If the decision is to make the acquisition
Digital Device CONNECTED?
Yes
No
Digital Device OFF?
Yes
No
Digital Device Collection On. (FIG.2)
Digital Device Collection On. (FIG.3)
Digital Device Collection On. (FIG.4)
Digital Device Collection On. (FIG.5)

Figure 1 - Flow for decision making. Source: ABNT NBR ISO/IEC 27037:2013

After defining by the collection or acquisition of digital evidence, the Lead Investigator / DES must formalize what motivated his decision and define when the action will be carried out.

If you assess that certain digital evidence should not be collected or acquired, your decision should also be documented and justified.

16. DATA COLLECTION: CONNECTED DEVICES

The first step in the forensic investigation process is to identify potential sources of data and acquire data from them. In this phase, the data are identified, collected and inventoried. Researchers should think about possible data sources located elsewhere, in addition to the variety of data sources available.

The Forensic Team collected relevant data from the devices and systems under suspicion of breach. The goal is to provide a detailed analysis of the information found. The data will be identified, labeled, recorded and collected.

If necessary,the device or system may be isolated, turned off or other procedures specific to the situation.

If the Forensic Team identifies this need, corporate emails may be the subject of evidence collection and investigation. In this case, the emails must be exported and saved in the storage location designated for the case under analysis. They should be identified: who exported the emails, how and when this was done and where the messages were transferred and stored. This information will be documented in order to be consulted and tracked if necessary.

In addition, the team responsible for the investigation should discuss the considerations of incident response, emphasizing the need to calculate the value of those collected, in relation to the costs and impact for the organization of the collection of the process.

For the process of collecting digital evidence on connected devices, the Lead Investigator/DES should consider:

1. Acquisition of volatile data, before shutting down the system or removing the power source;

2. Check for encryption keys and other crucial data in active or inactive memory;

3. Verify the possibility of carrying out the acquisition of evidence when there is suspicion of the use of encryption, with the use of portable power supplies so as not to interrupt the power of the device or mouse-jugglers to prevent the activation of the screen protector;

4. Check the reliability or not of the system;

5. Check the configuration of the device in order to determine whether it will be turned off through normal procedures or removed from the power source. If the decision is to remove the power supply, the Investigator/DES must first remove the end of the cable connected to the device;

6. Carefully pack the device and label;

7. Establish the chain of custody.

Below is the flow for digital evidence collection on connected devices:

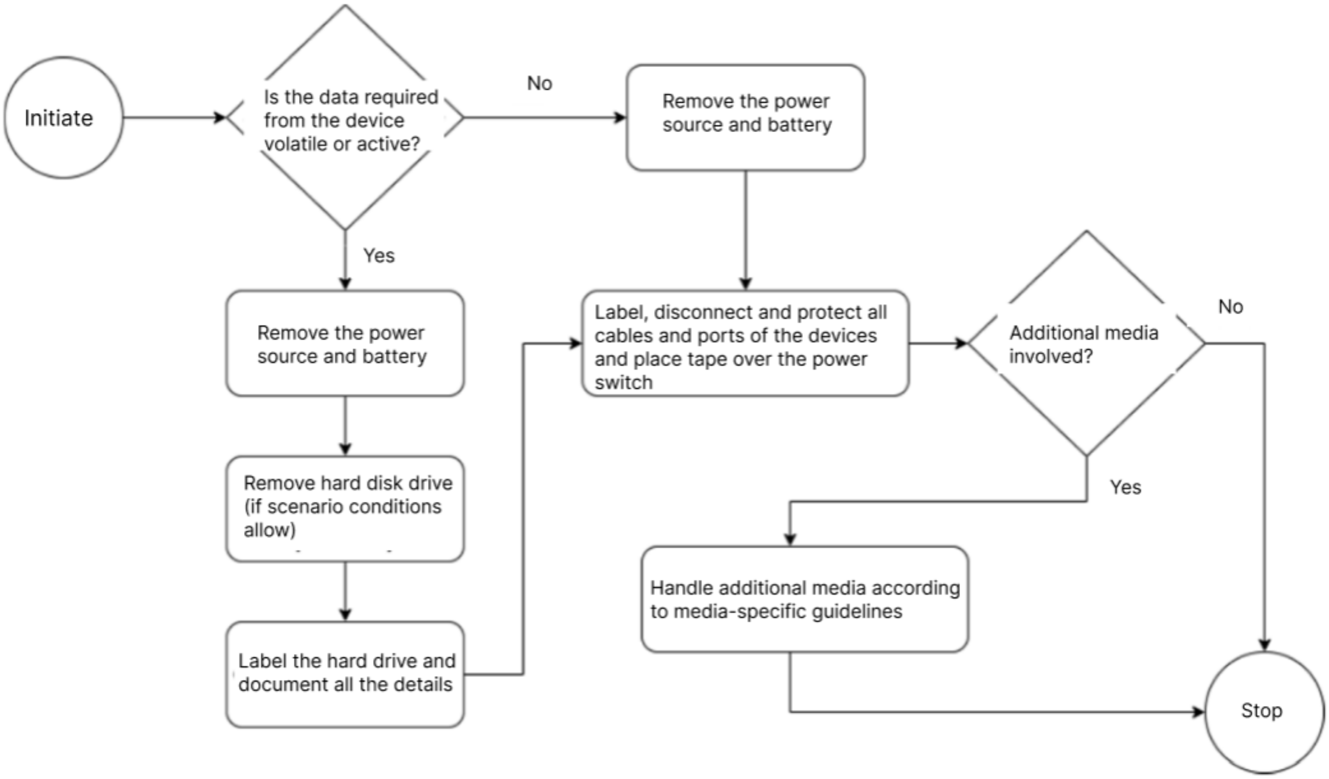

Initiate
Is the data required from the device volatile or active?
No
Remove the power source and battery
Yes
Remove the power source and battery
Label, disconnect and protect all cables and ports of the devices and place tape over the power switch
Additional media involved?
No
Remove hard disk drive (if scenario conditions allow)
Yes
Handle additional media according to media-specific guidelines
Label the hard drive and document all the details
Stop

Figure 2 - Collection of digital evidence on connected devices. Source: ABNT NBR ISO/IEC 27037:2013

17. COLLECTION: DEVICES TURNED OFF

Before beginning the process of collecting devices turned off, the Investigator/DES should make sure that they are effectively turned off, and not in standby mode.

For the process of collecting digital evidence on switched-off devices, the Investigator/DES must:

1. Remove the power source, first removing the end connected to the device; 2. Make sure that the CD and DVD trays are empty and retracted properly; 3. Disconnect and protect all cables from the device and etquetar the connection ports; 4. Place tape over the power

switch if necessary;

5. Carefully pack the device and label;

6. Establish the chain of custody.

Additional media involved should be removed from the device and handled as supplemental evidence . It is important to identify which port the media is connected to on the device.

Below is the flow for digital evidence collection on devices turned off:

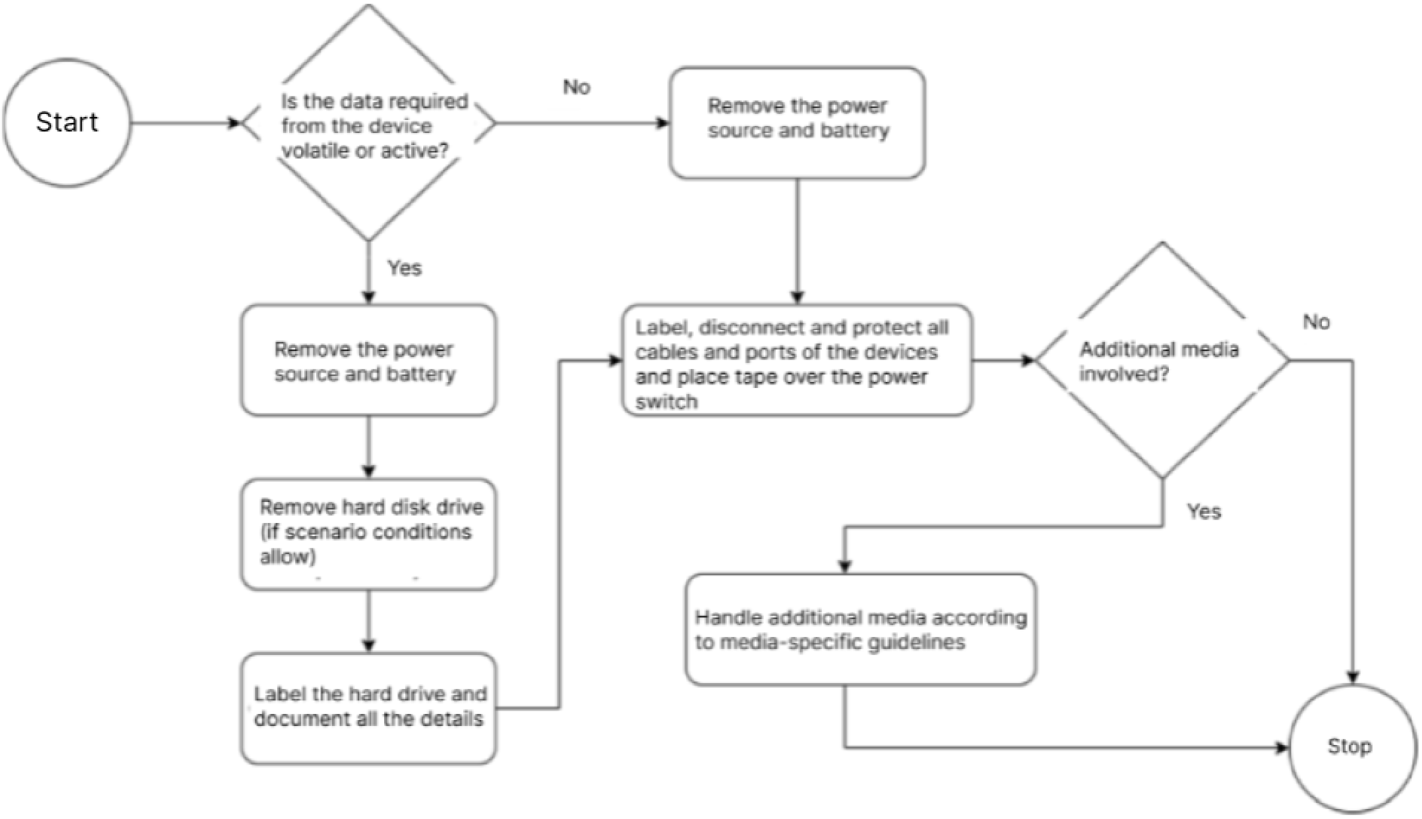

Start
Is the data required from the device volatile or active?
No
Remove the power source and battery
Yes
Remove the power source and battery
Remove hard disk drive (if scenario conditions allow)
Label the hard drive and document all the details
Label, disconnect and protect all cables and ports of the devices and place tape over the power switch
Additional media involved?
No
Yes
Handle additional media according to media-specific guidelines
Stop

Figure 3 - Collection of digital evidence on switched off devices. Source: ABNT NBR ISO/IEC 27037:2013

18. COLLECTION: NETWORKED DEVICES

For the network device collection process, the Investigator/DES must:

1. Disconnect the device only after making sure that no digital evidence will be lost as per the data volatility;

2. Identify communication services, such as wireless or bluetooth networking, in order to protect digital evidence from destruction;

3. Before disconnecting the device from wired networks, trace the connections to the devices and identify the ports for future reconstruction of the network;

4. Check if it is necessary to connect it to a power source;

5. Check if it is necessary to turn off the device at the time of collection to prevent the data from being altered;

6. If the device is turned off, keep it off;

7. Carefully pack the device and label;

8. Establish the chain of custody.

19. EXAMINATION OF DATA

After data collection, the next phase is to examine the data, which involves evaluating and extracting the relevant information from the collected data. She will seek to answer questions arising from suspected rape.

This phase may also involve circumventing or mitigating operating system or application features that obscure data and code, such as data compression, encryption, and access control mechanisms. An acquired hard drive can contain hundreds of thousands of data files; it provides data files that contain information of interest, including information hidden through file compression and access control. In addition, data files of interest may contain extraneous information that must be filed, that is, only information related to the event under investigation should be analyzed.

The Forensic Team will be able to use a variety of tools and techniques to investigate, interpret, filter, and reduce the amount of data that needs to be brought. Text and pattern searches can be used to identify pertinent data, such as finding documents that mention a particular subject or person, or identifying email log entries for a specific email address. Another technique that can be used is to use a tool that can determine the content type of each data file, such as text, graphics, music, or a compressed file. Knowledge of data file types can be used to identify files that deserve further study, as well as to exclude files that are of no interest to the examination. The same can be applied to databases containing information about known files, which can also be used to include or exclude files for further consideration.

The Team should make a detailed schedule of events, with analysis of devices and systems and prepare a report, which will be forwarded to the CISO.

20. ACQUISITION OF DIGITAL PROOF

The Digital evidence acquisition procedure should use validated and reliable tools in order to avoid unwanted or unforeseen effects on the system.

The DES must define, according to the criticality, whether there is a need to draw up Notarial Minutes of the process of the acquisition of digital evidence (for example, of the process that generated the identical copy of the data) or of the evidence acquired (such as an Internet page, publication on a website).

The acquisition of digital evidence should generate a bit-by-bit duplication of the original data or devices. The original source and the copy of the digital evidence must produce the same hash function result.

DES should preferably perform a bit-by-bit duplication of what is on the digital device. If this is not possible, copies of specific data may be made.

For the process of acquiring digital evidence on connected devices, DES shallco-ordinate:

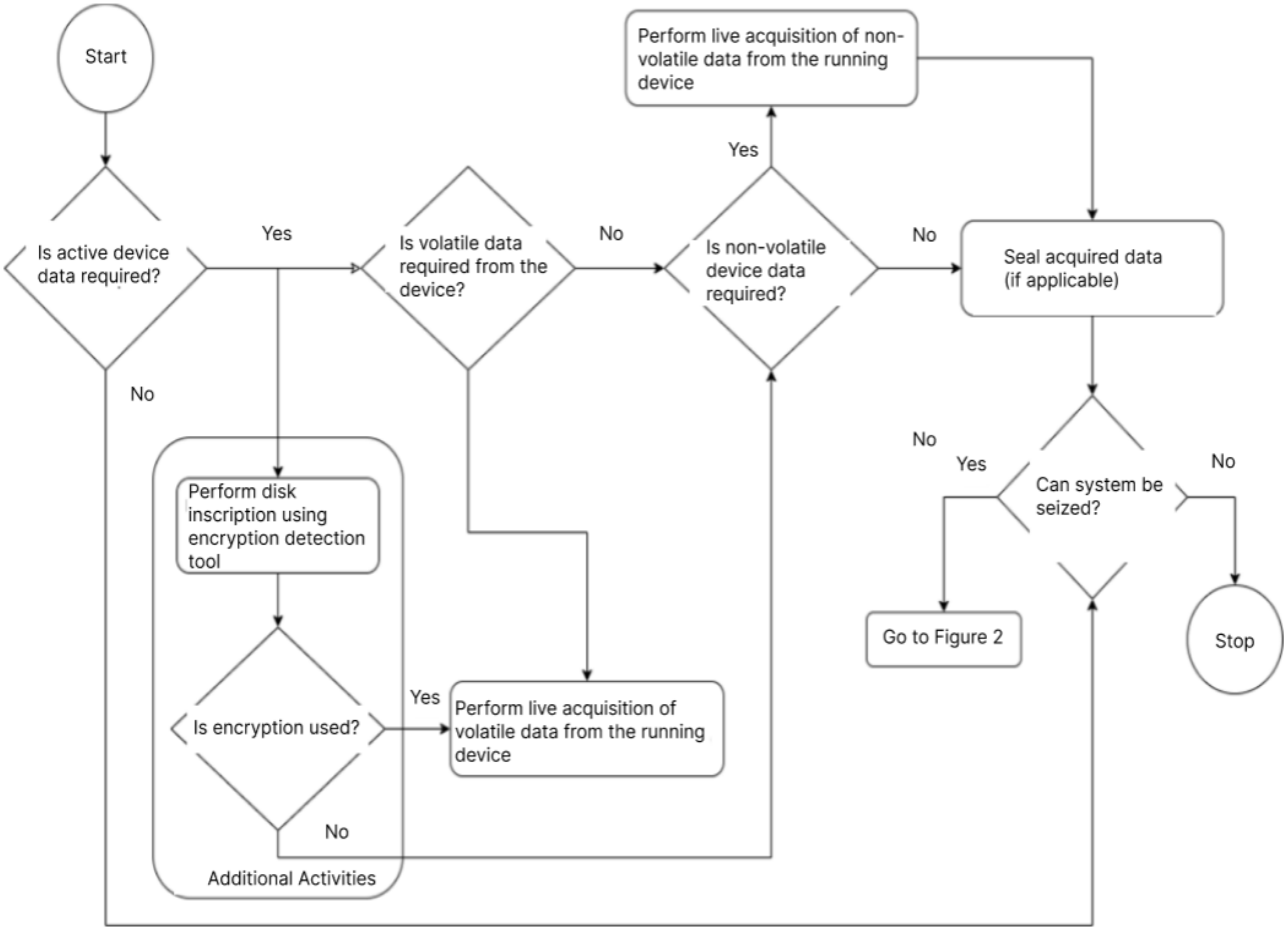
1. Possibility for the digital device to turn off, or for the connected system to go into screensaver mode or automatic locking;

2. Realization of the initial acquisition of volatile data, such as stored in RAM, running processes, network connections and date and time settings;

3. Possibility of the acquisition being carried out in person or remotely;

4. Possibility of using tools for encryption detection.

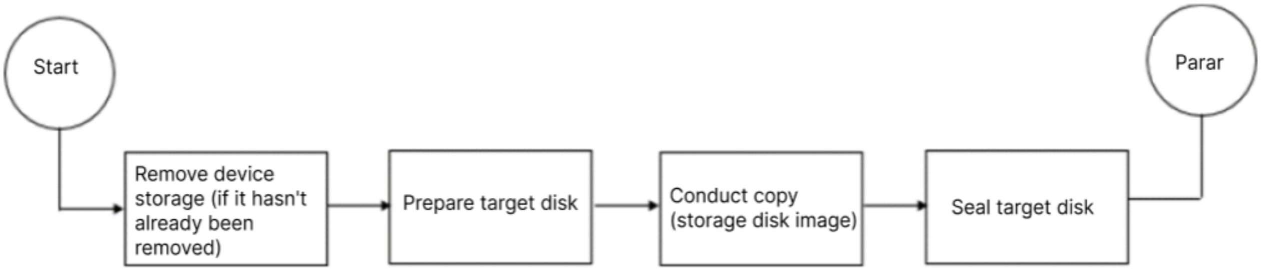
Below is the flow for digital evidence acquisition on connected devices:


Start
Is active device data required?
Yes
No
Is volatile data required from the device?
No
Is non-volatile device data required?
Yes
Perform live acquisition of non-volatile data from the running device
No
Seal acquired data (if applicable)
Perform disk inscription using encryption detection tool
Is encryption used?
Yes
Perform live acquisition of volatile data from the running device
No
Additional Activities
No
Yes
Can system be seized?
No
Go to Figure 2
Stop

Before starting the process of purchasing devices turned off, DES should make sure that they are effectively turned off, and not in standby mode.

For the process of acquiring digital evidence on disconnected devices, DES must remove the storage media (e.g., hard drive) from the device and document all details such as model, manufacture, serial number, and size.

Below is the flow for digital evidence acquisition on switched-off devices:


Start
Remove device storage (if it hasn't already been removed)
Prepare target disk
Conduct copy (storage disk image)
Seal target disk
Parar

DES may opt for partial acquisition of digital evidence when:

- The storage system is too large to be purchased - for example, database server ;

- The system is crucial to DMS LOGISTICS' business and cannot be shut down; ● Only selected data can contain digital evidence;

- Due to a court order that limits the scope of the acquisition.

When DES opts for partial acquisition, all relevant folders, data, and files must be identified.

In some cases, devices may be connected to more than one physical or logical network. Thus, before disconnecting the device from the network, DES must acquire the connection-related data - for example, IP configuration and routing tables.

For networked devices that need to be constantly turned on, DES must prevent it from interacting with a wireless radio network through isolation methods.

For the process of acquiring networked digital devices, DES shall:

- Use a protected desktop;

- Use a SIM or USIM card that simulates the identity of the original device and prevents access to the work network by the device, whenever necessary;

- To acquire the digital evidence, before removing the battery.

- When it is not possible for digital devices to be turned off due to their criticality, because if they are interrupted, they may affect the continuity of DMS LOGISTICS' activities.

LOGISTICS, the Digital Proof Specialist Collaborator (DES) must carry out the immediate acquisition of the digital or partial evidence, according to items 17 and 19.

When collecting or purchasing removable digital storage media, the Digital Proof Specialist Contributor (DES) must:

- Document your location (e.g. CD/DVD input trays or USB port), manufacturer, make, model and serial number;

- Label so that labels are not inserted directly on the mechanical parts of the media, nor hide important information, such as the serial number, part or model;

- Be aware of the maximum retention capacity of digital media.

21. PRESERVATION OF DIGITAL EVIDENCE

Digital evidence and the devices containing it should be stored in a secure location and with restricted access only to Investigators/DES and the collaborators responsible for their custody, in order to maintain the integrity and reliability of the evidence.

The Lead Investigator/DES is responsible for recording the chain of custody of evidence and devices until their disposal or reuse. It must:

1. Use a hash function in order to show that the copied data are equivalent to the originals;

2. Label digital evidence and devices;

3. Check periodically the devices connected to the battery, so that they have sufficient power;

4. Properly package the devices in order to prevent damage from shocks, vibrations, heat, humidity and exposure to radio frequency;

5. Airmaze digital evidence in formatted or new media;

6. Store magnetic storage media in magnetically inert, antistatic and particle-free packaging;7. Use particle-free gloves during evidence packaging ;

8. Protect devices from the influence of electromagnetic sources.

22. TRANSPORT OF DIGITAL PROOF

Digital evidence must:

1. Preferably, be transported only by the DES, and should not be left unaccompanied at any time;

2. Be encrypted, if necessary;

3. Be packed in an appropriate and safe place, to prevent damage, humidity and inadequate temperatures.

The entire transportation process, including the person responsible for carrying it out, must be documented in the chain of custody.

23. DOCUMENTATION

All activity carried out during the process of identification, collection, acquisition, transportation and preservation of digital evidence must be documented by the DES, including identifying:

1. Date and time of the devices that are connected, compared to the time source established by DMS LOGISTICS;

2. Data visible on screens on the digital device, active systems and open documents, for example;

3. Device data, such as serial number, make, model and manufacture;

4. Decisions taken and actions taken;

5. Manners performed.

A single time source should be used and the time of each action should be documented.

24. DATA ANALYSIS

Once the relevant information has been extracted, the analyst must study and analyze the data in order to draw conclusions from it.

A methodical approach should be used to reach conclusions based on the available data or to determine that no conclusions can yet be drawn.

The analysis should include identifying people, places, items, and events, and determining how these elements are related so that a conclusion can be reached. Often, this effort includes data correlated across multiple sources. For example, a Network Intrusion Detection System (IDS) log can link an event to a host, host audit logs can link the event to a specific user account, and the host IDS log can indicate what actions that user has taken. Tools such as centralized logging and security event management, the software can facilitate this process by automatically gathering and correlating data. Comparing system characteristics to known baselines can identify various types of changes made to the system.

If evidence is needed for legal or internal disciplinary action, analysts should carefully document the findings and all steps taken.

25. INVESTIGATION REPORT

The final stage of the forensic investigation is the report, where the processes of preparation and presentation of the information resulting from the analysis phase are found. The results and methodologies used are described in the report, including the following:

Alternative explanations. At the moment when the information relating to an event is incomplete, it may not be possible to arrive at a definitive explanation of what occurred. When a

The event has two or more plausible explanations, each of which should be given due consideration in the reporting process. Responsible analysts should use a methodical approach in an attempt to prove or disprove every possible explanation that is proposed. Some forensic process methodologies have a separate analysis phase after the exam phase. For the sake of simplicity, this publication presents the analysis as part of the examination phase. Typically, an analyst examines the data and performs analysis of that data, and then performs additional examinations and analyses based on the results of the initial analysis.

Consideration of the Public. Knowing the audience to which the data or information will be shown is important. An incident that requires the involvement of law enforcement, such as the LGPD, for example, requires highly detailed reporting of all information collected, and may also require copies of all evidentiary data obtained. A system administrator may want to see network traffic and related statistics in great detail. Top management can simply provide a high-level overview of what happened, through a simplified visual representation, reporting how the attack occurred and what should be done to prevent similar incidents.

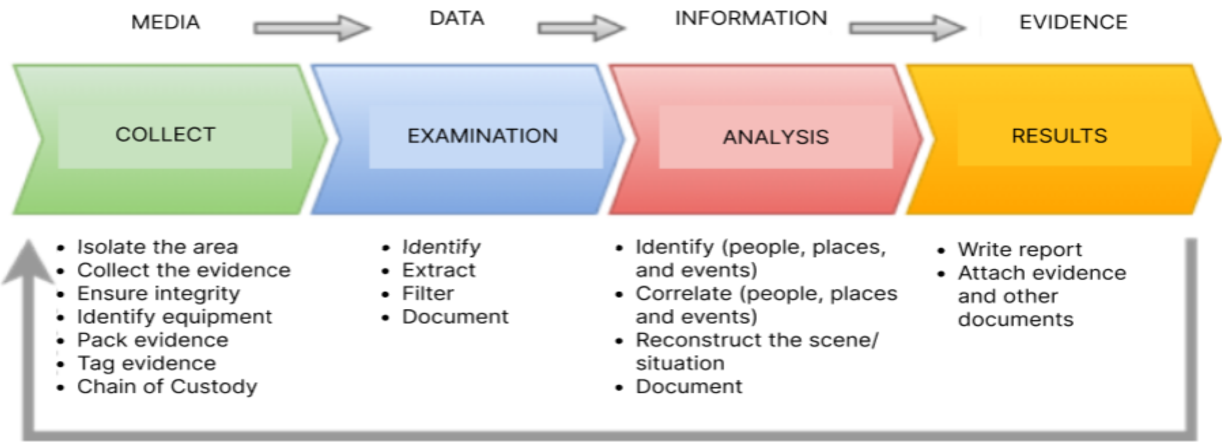
Actionable information. The report also includes identifying actionable information, gleaned from data that can allow an analyst to collect new sources of information. For example, a contact list can be developed from data that can lead to additional information about an incident or crime. In addition, information can be obtained that can prevent future events, such as a backdoor on a system that can be used for future attacks, a crime that is being planned, a worm that is scheduled to start spreading at a certain time, or a vulnerability that can be exploited.

Documentation. All activity carried out during the process of identifying, collecting, acquiring, transporting and preserving digital evidence must be documented by the analyst, identifying, including the date and time of the devices that are connected, comparing with the time source established by DMS LOGISTICS, the data visible on the screens on the digital device, active systems and open documents, for example, the data of the devices, such as serial number, make, model and manufacture, the decisions taken and actions taken and the handling and procedures performed. The analyst should use a single time source and document the timing of each action.

The report shall contain the facts which can be proved by the evidence collected and examined. If the data do not provide a clear answer, it should be noted that the

evidence is not conclusive. The investigator will be able to describe the plausible hypotheses, emphasizing, however, that these hypotheses cannot be corroborated by the evidence.

In conclusion, if possible in the specific case, recommendations for improvement should be presented.



26. LESSONS LEARNED

After the presentation of the report to the CISO, the outcome of the investigation should be discussed between the Senior Management of DMS LOGISTICS, the CISO, the Information Security Manager and the Information Security Team.

They should check improvement processes to prevent further violations, evaluate changes in company policies, review procedures or tool performance,

evaluating the replacement, hiring new technologies or staying in the same situation , depending on each situation.

The lessons learned and the completion of the process should be recorded and stored in its own document.

27. CHAIN OF CUSTODY

The chain of custody has the function of promoting the integrity of the evidence, and the possibility of tracing traces associated with the criminal act, as a way to ensure and preserve the reliability and transparency of the crime investigation process. The chain of custody contributes to maintaining and documenting the chronological history of the evidence, to trace the possession and handling of the sample, from the preparation of the collecting container, from collection, transport to the controlled environment, from receipt, analysis and storage. It includes the entire sequence of possession.

To ensure that the chain of custody is as authentic as possible, a series of steps must be followed. It is important to note that the more information a forensic expert obtains about the pagesat hand, the more authentic the chain of custody created. Because of this, it's important to get information from the administrator about the evidence: for example, the administrative log, date and file information, and who accessed the files.

The chain of custody must record it:

1. The location of collection of the device and data;

2. Responsible for the collection or acquisition of data;

3. Details of the device collected, or details of the data that was the target of acquisition; 4. Details of the acquired data (duplicates);
5. Methodology used;

6. Tools used;
7. Verification of the integrity of the images (hash);

8. The custodian responsible for the evidence;

9. Who had access, when, where and for what reason.

The chain of custody record and digital evidence shall be kept for as long as necessary for use in judicial, administrative, and disciplinary proceedings in the following procedure, assembled in accordance with the chain of custody for electronic evidence:

1. Save the original materials: Always work on copies of the digital evidence as opposed to

the original. This ensures that you can compare your work products with the preserved original without modifications.

2. Take photos of physical evidence: Photos of physical (electronic) evidence establish the chain of custody and make it more authentic.

3. Take screenshots of digital evidence content: In cases where the evidence is intangible, taking screenshots is an effective way to establish the chain of custody.

4. Date, time and any other information of receipt of the document. Recording the timestamps of who had the evidence allows investigators to construct a reliable timeline of where the evidence was before it was obtained. In the event that there is a hole in the timeline, further investigation may be necessary.

5. Inject a bitwise clone of digital evidence content into forensic computers. This ensures that we get a complete duplicate of the digital evidence in question.

6. Run a hash test analysis to further authenticate the working clone. Performing a hash test ensures that the data obtained from the previous bi t to bit copy procedure is not corrupted and reflects the true nature of the original evidence. If this is not the case, then forensic analysis can be flawed and can result in problems, rendering the copy inauthentic.

7. Access analysis. The analysis should bring information from who had access, when, where and for what reason, thus using a 5W2H's methodology to chronologically describe the collection of evidence for the investigation.

The chain of custody procedure may be different,depending on the jurisdiction in which the evidence resides; however, the steps are basically identical to those described above.

28. FINAL PROVISIONS

All collaborators involved in the handling of digital evidence and forensic investigation must maintain confidentiality of the process and content.

Any activity that disrespects the provisions established in the DMS LOGISTICS Policies or in Brazilian legislation will be considered a violation and treated in order to ascertain the responsibilities of those involved, aiming at the application of appropriate sanctions provided for in contractual clauses and in the current legislation.

Violations, even if by mere omission, negligence, recklessness or unconsummated attempt to violate the DMS LOGISTICS Policies, as well as other rules and procedures, will be subject to disciplinary action.

If a violation of Brazilian laws, whether criminal, civil or administrative, is found, the evidence, evidence, devices, documents and reports obtained in the forensic investigation may, if necessary, be forwarded to the security or judicial authorities. The same can occur if the information obtained by the forensic investigation is requested by the Judiciary.

29. IMPLEMENTATION AND UPDATE

The Forensic Investigation Policy of DMS LOGISTICS must be updated whenever necessary or at an interval not exceeding 01 (one) year.

30. REVISION HISTORY

Revision	Data	Description
00	09/02/2023	Document creation.
01	27/02/2023	Review and standardization of the entire document.

31. APPROVAL AND CLASSIFICATION OF INFORMATION

Prepared by:	CyberSecurity Team
Reviewed by:	Leonardo Sabbadim
Approved by:	Victor Gonzaga

Level of Confidentiality:	**X**	**Public Information**
		Internal Information
		Confidential Information
		Confidential Information

DMS
LOGISTICS

WE NEVER PUT QUALITY OR ETHICS AT RISK IN BUSINESS

WE NEVER COMPROMISE ON QUALITY AND BUSINESS ETHICS

WWW.DMSLOG.COM