Análisis forense a equipos informáticos

Ángel Gabriel Párraga Ganchozo
Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López", ESPAM MFL
angel.parraga@espam.edu.ec
Calceta, Ecuador

Adriana Elizabeth Cedeño Zambrano
Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López", ESPAM MFL
adriana_cedeno_mdw@espam.edu.ec
Calceta, Ecuador

Ligia Elena Zambrano Solórzano
Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López", ESPAM MFL
lzambrano@espam.edu.ec
Calceta, Ecuador

Jessica Johanna Morales Carrillo
Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López", ESPAM MFL
jmorales@espam.edu.ec
Calceta, Ecuador

DOI: https://doi.org/10.56124/encriptar.v8i15.006

Resumen

El propósito de la presente investigación es lograr determinar las causas y medios digitales por las cuales se puede fugar la información de una empresa, mediante herramientas de informática forense se pretende identificar a los posibles infractores y los medios utilizados sin alterar la evidencia digital. Para esto se utilizó la metodología que sigue la norma ISO/IEC 27037:2012, que guía la identificación, recolección y preservación de evidencias digitales, manteniendo su integridad y relevancia. Se obtuvo como resultado la fuga de información mediante correo electrónico a entidades externas, revelando información crítica y confidencial de la empresa.

Palabras clave: Informática forense, evidencia digital, integridad, ISO/IEC 27037.

ABSTRACT

The purpose of this investigation is to determine the causes and digital means by which a company's information can be leaked, using computer forensic tools to identify possible offenders and the means used without altering the digital evidence, for this The methodology that follows the ISO/IEC 27037:2012 standard was used, which guides the identification, collection and preservation of digital evidence, maintaining its integrity and relevance. The result was a leak of information via email to external entities, revealing critical and confidential information of the company.

Keywords: Computer forensics, digital evidence, integrity, ISO/IEC 27037.

1. Introducción

La aplicación de las tecnologías digitales en los procesos de negocio del sector empresarial mundial denota marcados beneficios económicos para estas organizaciones, sin embargo, el uso acelerado de las tecnologías digitales ha ocasionado un crecimiento de los ataques informáticos, los cuales ocupan la octava posición de los fenómenos con mayor impacto económico a nivel mundial; los cuales afectan seriamente a la disponibilidad de los servicios de Tecnología de la información(World Economic Forum, 2020).

La Informática Forense es una disciplina que, permite identificar, adquirir, preservar y analizar evidencias mediante investigación al utilizar modelos y técnicas forenses en áreas específicas de casos penales y civiles, ésta permite que, se resuelvan disputas judiciales ante los tribunales, debido a esto, es necesario que investigadores y peritos posean un conocimiento en áreas técnicas. La Informática Forense permite detectar y recuperar datos e información digital y utilizar la misma como evidencia en el restablecimiento de un hecho y por tanto, ser utilizados como un valor demostrativo (Iorio, y otros, 2017)

En su trabajo de investigación Beltrán (2021) menciona que la Informática Forense aparece como necesidad para la investigación de los diferentes delitos que afectan día a día a la sociedad, esta tiene como propósito comprobar los responsables de los delitos y aclarar el origen de un suceso, mediante la recolección de pruebas digitales para fines investigativos a través de las diferentes técnicas.

Cabe recalcar que el Ecuador existe la Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos la cual busca tipificar los delitos que usan medios digitales y poderlos sentenciar (Pleno del Congreso Nacional de Ecuador, 2010).

El presente trabajo tiene como finalidad determinar el medio tecnológico por el cual está fugando la información para esto se realiza el análisis forense a equipos informáticos, la finalidad es obtener pruebas, o como indica (Ochoa, 2018) obtener evidencia digital que es cualquier información con valor probativo que es almacenada o transmitida en forma digital.

Actualmente, todo dispositivo digital es parte de las actividades de una persona o institución y es capaz de generar información que puede convertirse en evidencia valiosa en caso de presentarse un incidente de seguridad (Molina, F. 2020).

Una vez que se obtiene la información se asegura la cadena de custodia que en general, cuando la evidencia original ha estado sujeta al cambio a través del tiempo, es susceptible a la alteración, la parte que la presenta debe demostrar que ésta no ha sido alterada desde el momento en que fue recolectada hasta su producción en la corte.

2. Metodología (Materiales y métodos)

Durante la implementación de la solución propuesta, el autor considera que es importante que, la información no sea modificada de ninguna manera, para lo cual, es necesario mantener la integridad de la evidencia, por lo que,

es necesario seguir la parte medular una metodología, la norma ISO/IEC 27037:2012 Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence, provee modelos para la identificación, sistematización, recolección, adquisición, y preservación de la información, esta norma se basa en tres elementos: relevancia, confiabilidad y suficiencia (Beltrán, 2021).

Para cada tipo de dispositivo la norma ha determinado un tratamiento de evidencias en tres procesos básicos:

La identificación para localizar información potencial o elementos de prueba en sus posibles estados.

La recolección de los dispositivos y la documentación (incautación y secuestro de estos) que puedan contener la evidencia.

La preservación de las mismas, para garantizar su utilidad y su originalidad para ser consideradas como elementos de prueba íntegros; tres acciones dirigidas a conservar la cadena de custodia e integridad de la información. (Servicio de Acreditación Ecuatoriana, 2018)

3. Resultados (análisis e interpretación de los resultados)

El caso de estudio reside en el análisis a equipos informáticos a una empresa de ventas; que en los últimos meses ha notado que su principal competidor está ganando mercado con mejores precios y los clientes potenciales se están yendo. El análisis forense del presente estudio de caso para supuesta fuga de información.

Para el estudio forense se empleó la ISO/IEC 27037:2012 donde se trabajaron tres etapas que se detallan a continuación.

La Identificación

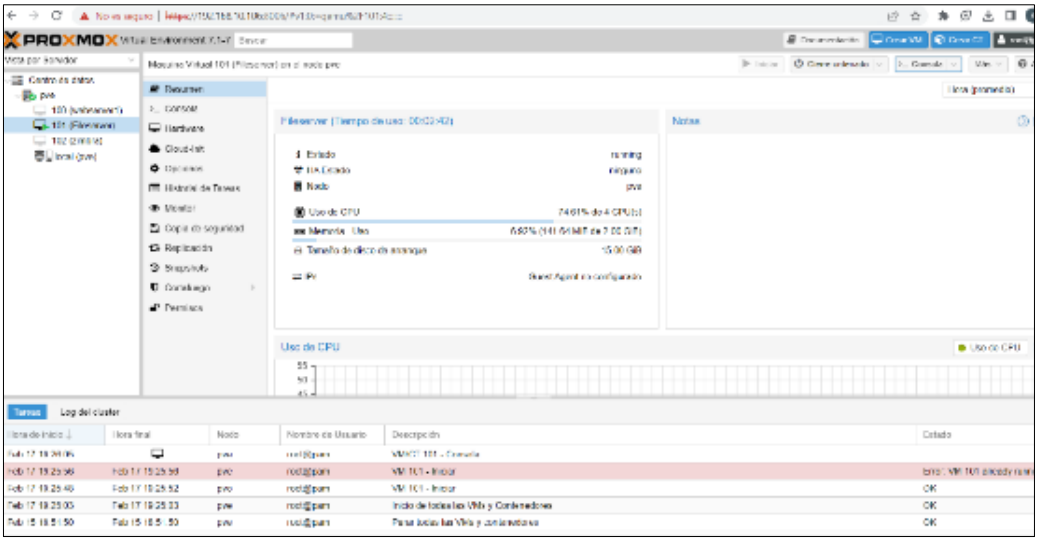
Previo a la evaluación de la infraestructura de tecnología se establece documento de responsabilidades y a qué información se tiene acceso.

Se evalúa la infraestructura de tecnología con la que cuenta la empresa, se encontró que manejan una infraestructura virtualizada con Proxmox 7.1 en la que se tiene lo siguiente (Figura 1):

• 1 servidor de archivos en Samba con acceso a carpetas compartidas puntuales por usuario (Figura 2)

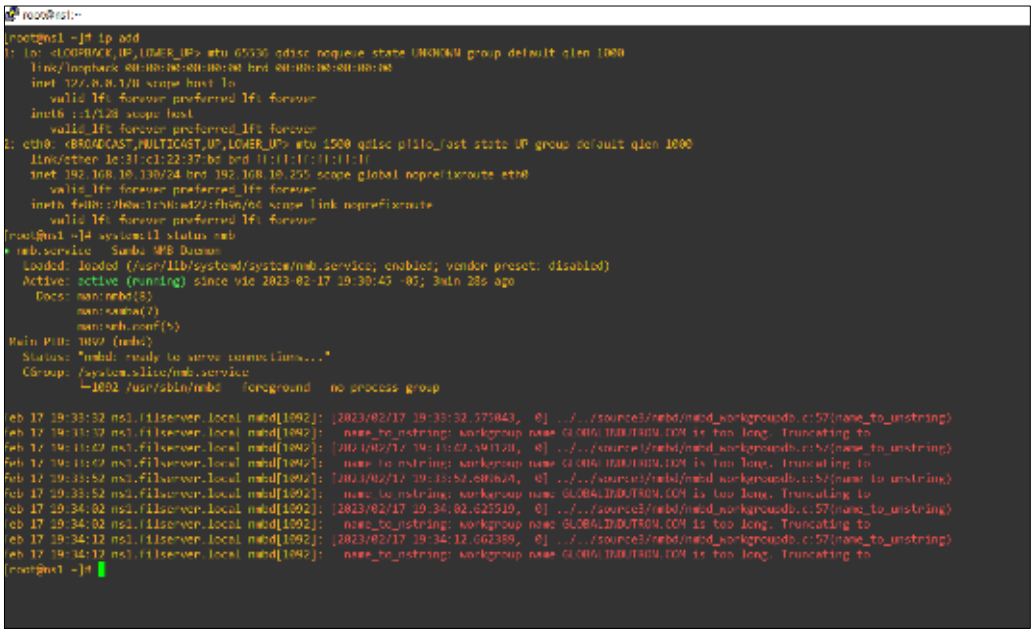
• 1 servidor de correos Zimbra para la comunicación interna y externa (Figura 3, Figura 4).

Figura 1. Servidor Virtual Proxmox 7.1



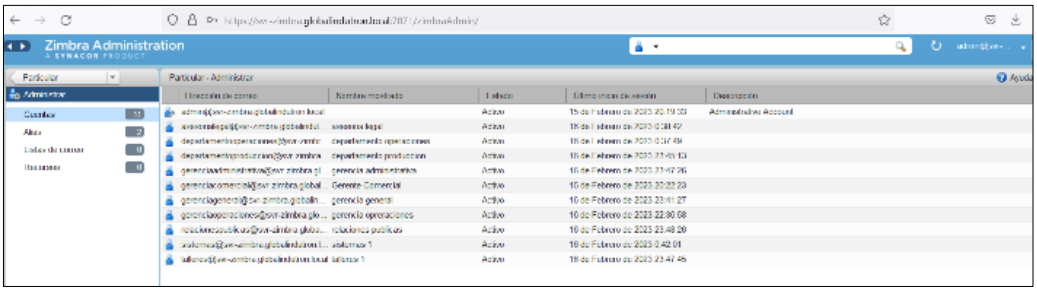
Fuente: Autores (2024).

Figura 2. Servidor de Archivos Samba



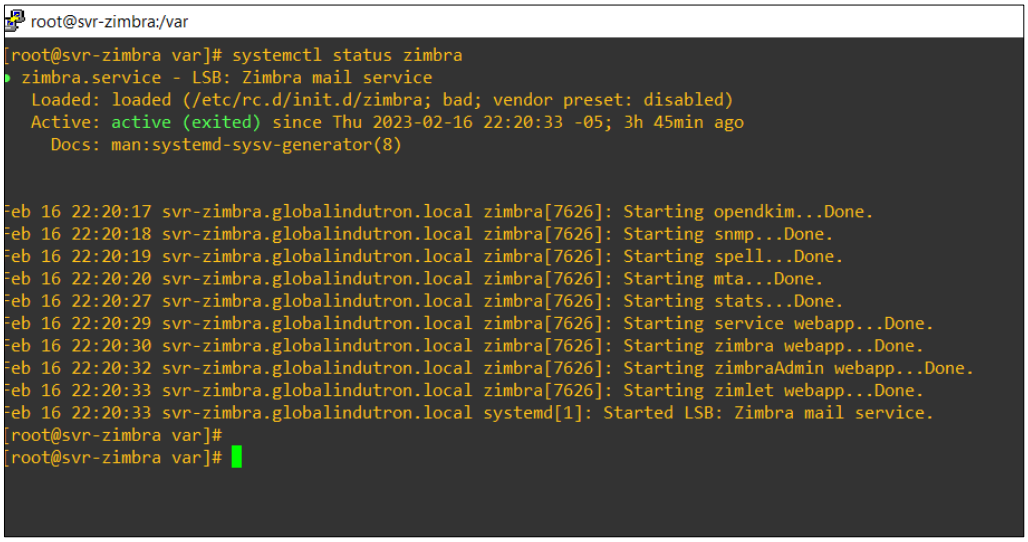
Fuente: Autores (2024).

Figura 3. Servidor de Correos Zimbra con las cuentas de Usuario Existentes



Fuente: Autores (2024).

Figura 4. Servicio de Correos Zimbra activo



Fuente: Autores (2024).

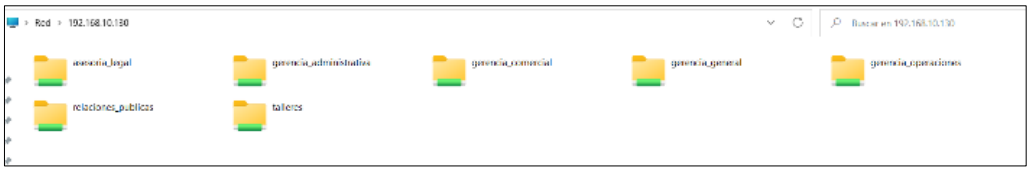
Se logra identificar que cada usuario tiene acceso a una carpeta del servidor de Archivos con información sensible (Figura 5).

Se puede observar que la información de clientes y proveedores la maneja el gerente comercial, por tal motivo la investigación se centra en el gerente comercial y se revisa su carpeta gerencia_comercial (Figura 6).

Se cambia la contraseña del correo electrónico gerentecomercial@svr-zimbra.xxxx.local para evitar modificación de la evidencia (Figura 7).

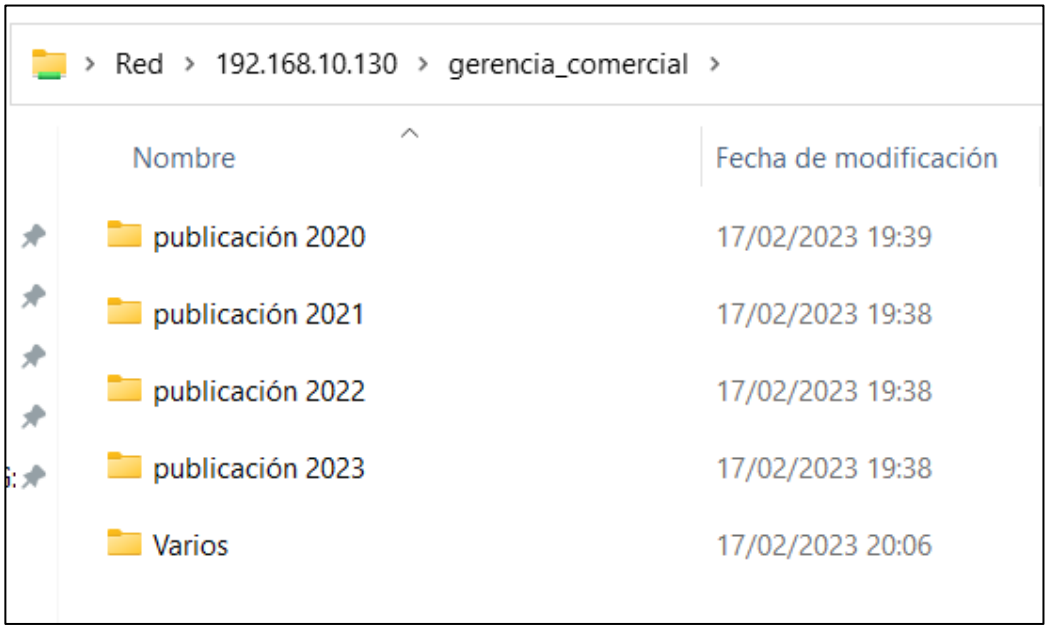
Se pudo detectar que la empresa cuenta con un respaldo diario de todos los buzones de correo incremental y total, de esta forma se puede extraer la imagen del último respaldo del gerente comercial (Figura 8).

Figura 5. Carpetas del servidor de Archivos



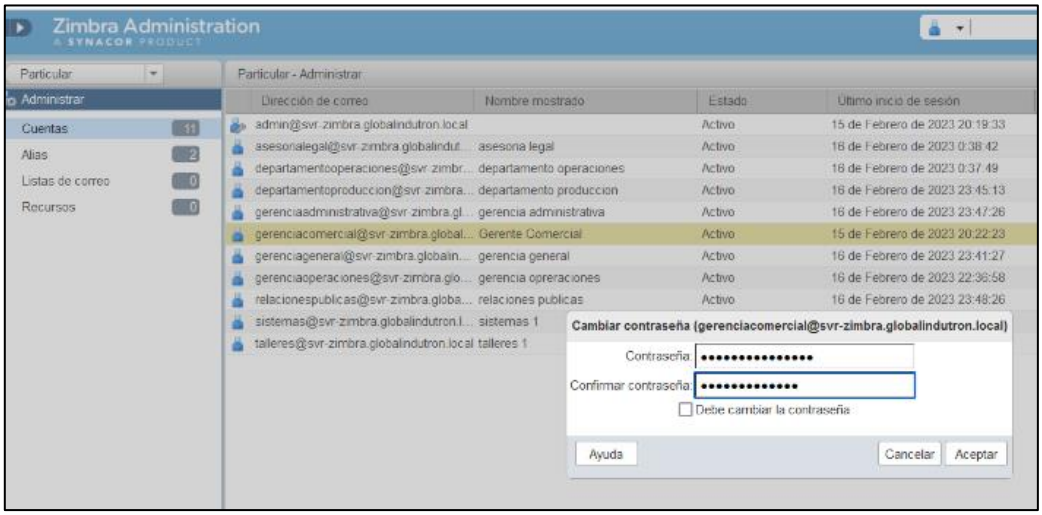
Fuente: Autores (2024).

Figura 6. Carpeta gerencia_comercial



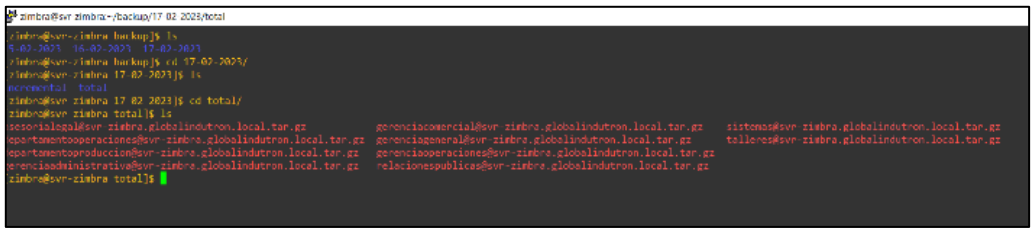
Fuente: Autores (2024).

Figura 7. Cambio de Contraseña de correo sospechoso para evitar alteración de la información.



Fuente: Autores (2024).

Figura 8. Respaldos diarios de buzón de correo.



Fuente: Autores (2024).

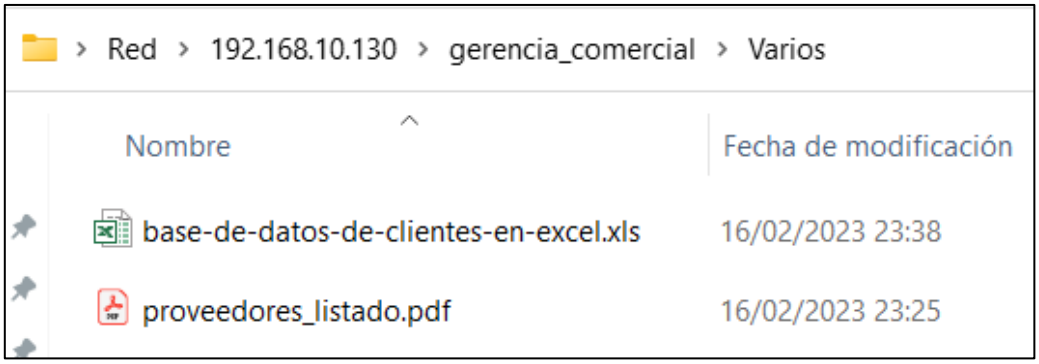
La Recolección y/o Adquisición

Una vez identificado el posible infractor se procede a recolectar la evidencia, se toma la información que probablemente está fugando, se toman 2 archivos del servidor de archivos que contiene información de clientes y proveedores (Figura 9).

Se toma el último respaldo del buzón de correo de gerentecomercial@svr-zimbra.xxxx.local y se procede a copiar la información desde el servidor a otra unidad externa (Figura 10).

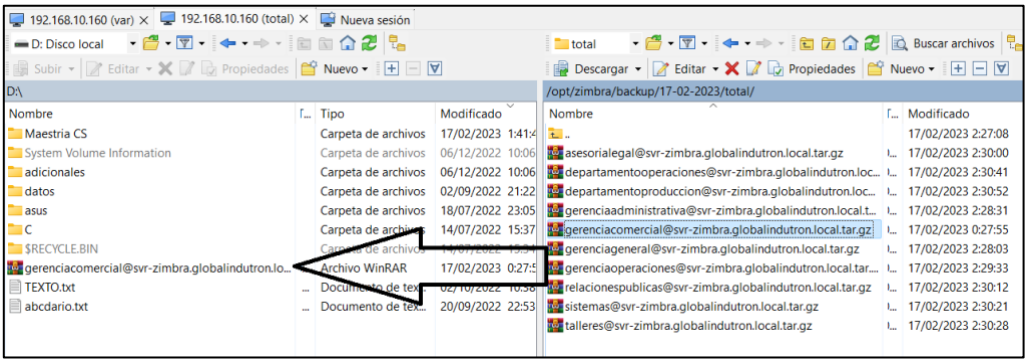
Para fortalecer la disponibilidad y confidencialidad se encripta la información en un archivo .zip con contraseña (Figura 11).

Figura 9. Posible prueba del servidor de Archivos.



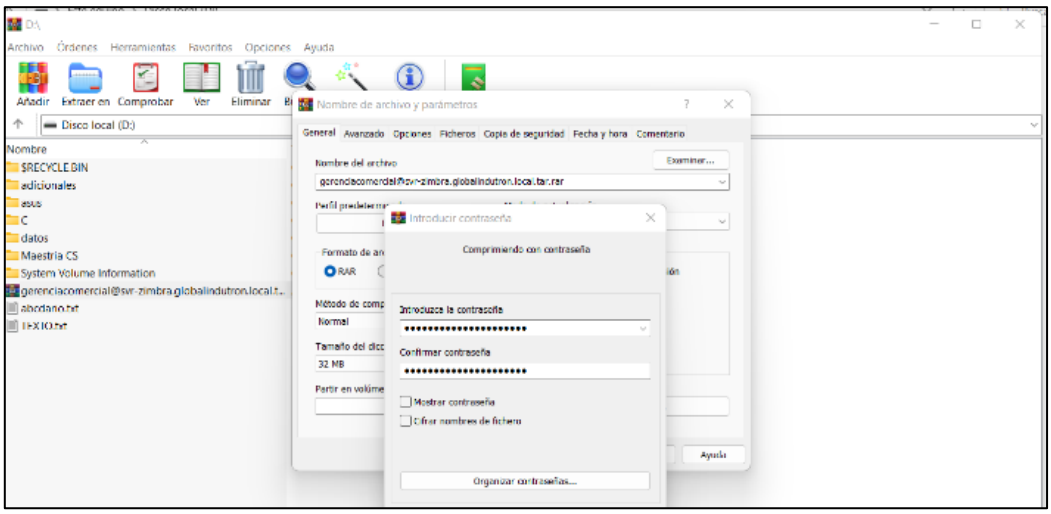
Fuente: Autores (2024).

Figura 10. Copia de último respaldo del Buzón de correo gerentecomercial@svr-zimbra_xxxx.local.



Fuente: Autores (2024).

Figura 11. Cifrar información con Contraseña .zip



Fuente: Autores (2024).

La Conservación/Preservación

En esta etapa se procede a crear un hash de toda la información extraída para que de esta forma se pueda garantizar la integridad de esta, se utiliza la herramienta Hashmyfiles (Figura 12).

Luego se analiza la información para determinar responsabilidades sobre la fuga de información, para ello se analiza el buzón de correo con SysTools MBOX Viewer, cabe indicar que este es un software forense que al analizar los datos no altera su contenido (Figura 13).

Se pudo observar que la información clientes y proveedores ha sido enviada a correos externos, todo esto se logró determinar con el análisis de los correos desde su cabecera y todo su contenido (Figura 14).

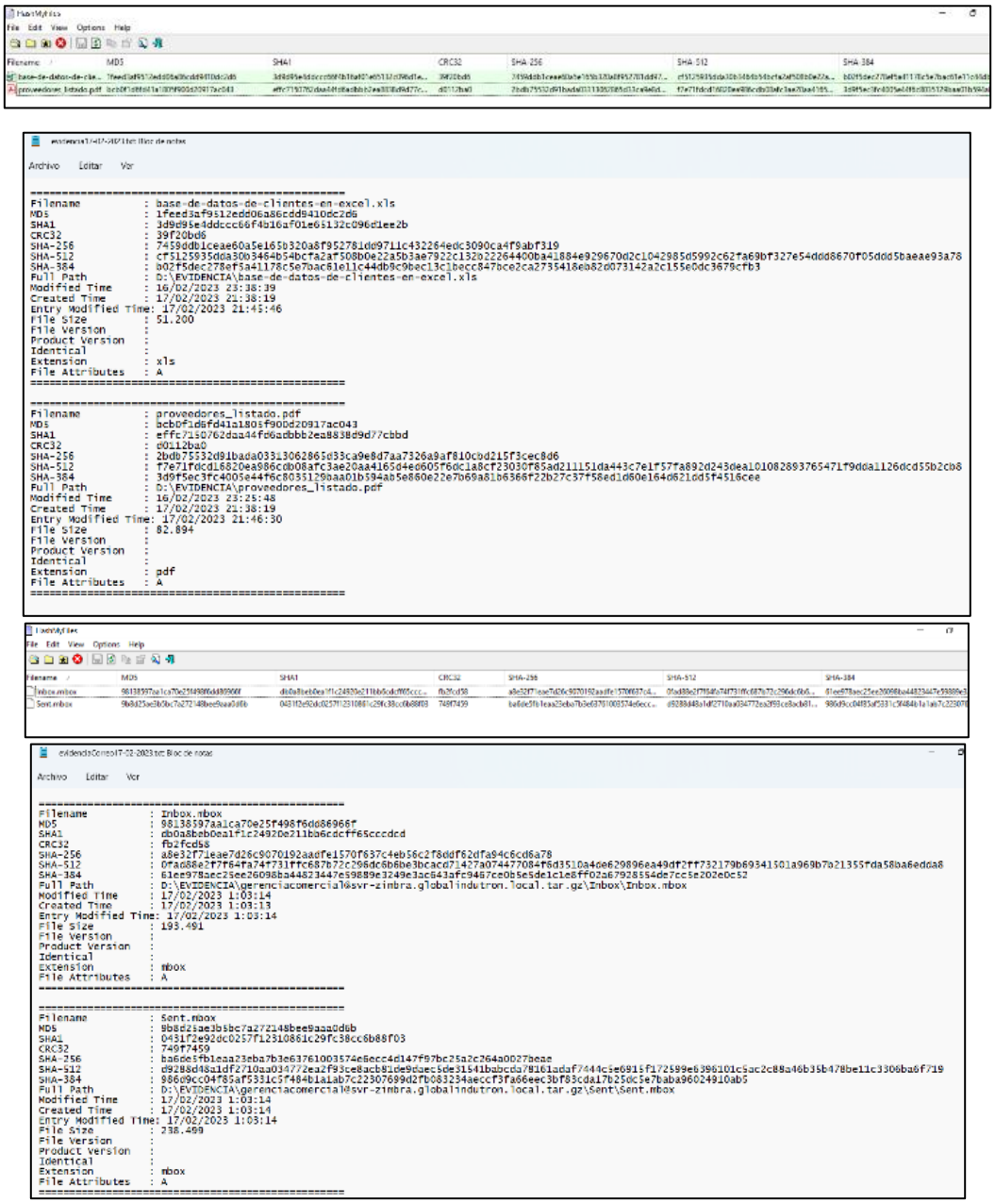
Finalizando el análisis de la información se ubica la información en una unidad extraíble nueva para poder entregar la información al gerente de la empresa se emite un informe forense con todas las novedades encontradas para la toma de decisiones y asumir responsabilidades del daño causado a la empresa.

Se pudo determinar que el medio por el cual estaba fugando la información era el correo electrónico empresarial, adjuntando información sensible de clientes y proveedores siendo enviado a correos personales, desde la cuenta del gerente comercial.

Según Granda, (2015) el mantenimiento de la integridad de la evidencia recolectada es una de las características primordiales en una investigación forense, por lo que el presente trabajo se hace énfasis en la verificación y preservación de la integridad recomendando herramientas y procesos para esta tarea.

El autor del presente trabajo concuerda con Granda ya que la evidencia recolectada es de relevancia por ello es importante mantener la integridad de la misma, para ello se utilizó hashmyfiles para extraer el hash de la información para comparar al final del día y evidenciar que la información no haya sido alterada.

Figura 12. Posible prueba del servidor de Archivos y Servidor de Correo (hash)



```
Archivo   Editar   Ver

==========
Filename          : base-de-datos-de-clientes-en-excel.xls
MD5               : 1feed3af9512edd06a86cdd9410dc2d6
SHA1              : 3d9d95e4ddccc66f4b16af01e65132c096d1ee2b
CRC32             : 39f20bd6
SHA-256           : 7458ddb1ceae60a5e165b320a8f952781d0971lc432264edc3090ca4f9abf319
SHA-512           : cf5125935dda30b3464b54bcfa2af508b0e22a5b3ae7922c132b22264400ba41884e929670d2c1042985d5992c62fa69bf327e54ddd8670f05ddd5baeae93a78
SHA-384           : b02f5dec278ef5a41178c5e7bac81e11c44db9c9bec13c1becc847bce2ca2735418eb82d073142a2c155e0dc3679cfb3
Full Path         : D:\EVIDENCIA\base-de-datos-de-clientes-en-excel.xls
Modified Time     : 16/02/2023 23:38:19
Created Time      : 17/02/2023 21:38:19
Entry Modified Time: 17/02/2023 21:45:46
File Size         : 51.200
File Version      :
Product Version   :
Identical         :
Extension         : xls
File Attributes   : A
==========

==========
Filename          : proveedores_listado.pdf
MD5               : bcbdf1d8fd41a1805f90dd20917ac043
SHA1              : effc71507624aa44fd6adbbb2ea883d9d77cbbd
CRC32             : e0112ba0
SHA-256           : 2bdb75532d91bada0331306286fd33ca9e8d7aa7326a9af810c0d215f3cec8d6
SHA-512           : f7e71fdcd16820ea986cdb08afc3ae20aa4165d4ed605f6dc1a8cf23030f85ad211151da443c7e1f57fa892d243dea101082893765471f9dda1126dcd55b2cb8
SHA-384           : 3d9f5ec3fc4005e44f6c8035129aa01b594ab5e880e22e7b69a81b6366f22b27c37f58ed1d60e164d621dd5f4516cee
Full Path         : D:\EVIDENCIA\proveedores_listado.pdf
Modified Time     : 16/02/2023 23:25:48
Created Time      : 17/02/2023 21:38:19
Entry Modified Time: 17/02/2023 21:46:30
File Size         : 82.894
File Version      :
Product Version   :
Identical         :
Extension         : pdf
File Attributes   : A
==========
```

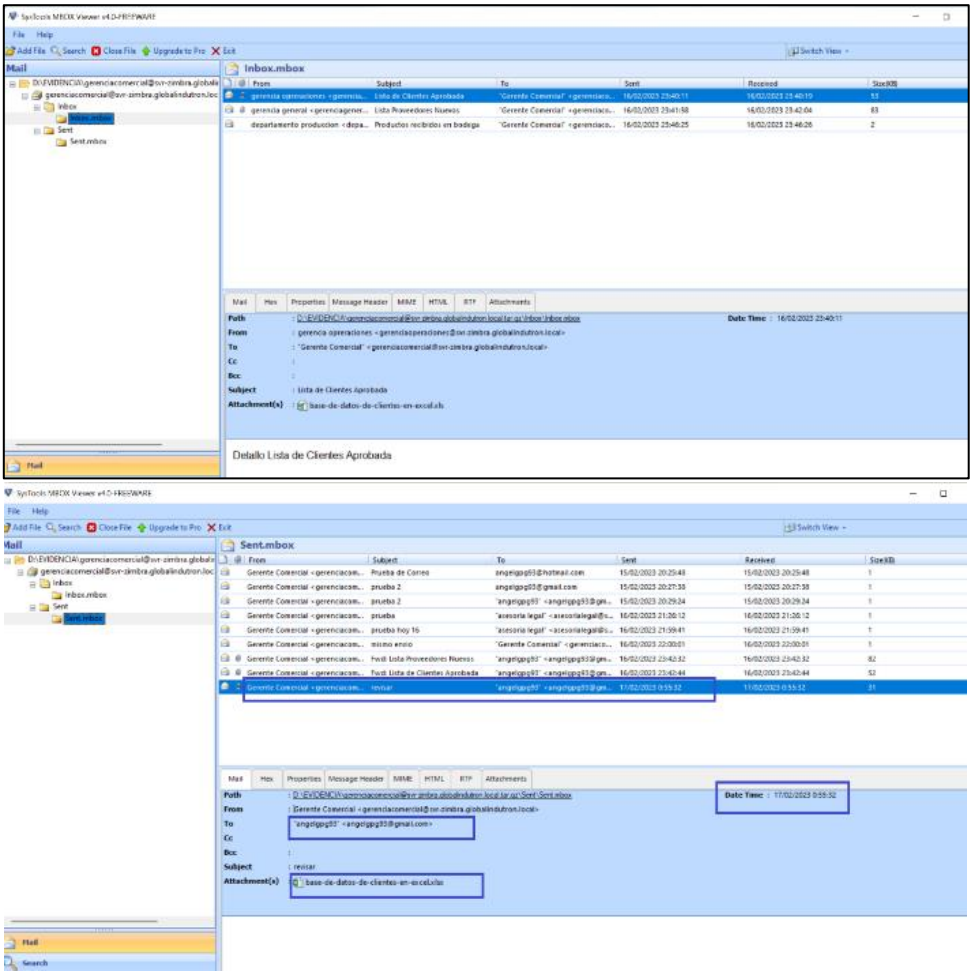
```
Archivo   Editar   Ver

==========
Filename          : Inbox.mbox
MD5               : 98138597aa1ca70e25f498f6dd86966f
SHA1              : db0a8bebbea1f1c2492be211ba6cdcff65cccdcd
CRC32             : fb2fcd58
SHA-256           : a8e32f71eae7d26c9070192aadfe1570f637c4eb56c2f8ddf62dfa94c6cd6a78
SHA-512           : 0fa688e2f7ff64fa74f731ffc687b72c298dc6b6be3bcacd71427a07447708df6d3510a4de629896ea49df2ff732179b69341501a969b7b21355fda58ba6edda8
SHA-384           : 61ee978aec25ee26098ba44823447e59889e3249e3ac643afc9487ce0b5e5de1c1e8ff0fa67928554de7cc5e202e0c52
Full Path         : D:\EVIDENCIA\gerenciacomercial@svr-zimbra.globalindutron.local.tar.gz\Inbox\Inbox.mbox
Modified Time     : 17/02/2023 1:03:14
Created Time      : 17/02/2023 1:03:13
Entry Modified Time: 17/02/2023 1:03:14
File Size         : 193.491
File Version      :
Product Version   :
Identical         :
Extension         : mbox
File Attributes   : A
==========

==========
Filename          : Sent.mbox
MD5               : 9b8d23ae3b35bc7a272148bee9aaa0d6b
SHA1              : 0431f2e92dc0257f12510861c29fc38cc6b88f03
CRC32             : 749f7459
SHA-256           : ba6de5fb1eaa23eba7b3e63761003574e6ecc4d147f87bc25a2c264a0027eeae
SHA-512           : d9288d48a1df2710aa034772ea2f93ce8acb81de9daec5de31541babcda78161adaf7444c5e6918f172599e6396101c5ac2c88a46b35b478be11c3306ba6f719
SHA-384           : 986e9cc04f85af5331c5f484b1a1ab7c22307699d2fb083234aeccf3fa66eec3bf83cda17b25dc5e7baba96024910ab5
Full Path         : D:\EVIDENCIA\gerenciacomercial@svr-zimbra.globalindutron.local.tar.gz\Sent\Sent.mbox
Modified Time     : 17/02/2023 1:03:14
Created Time      : 17/02/2023 1:03:14
Entry Modified Time: 17/02/2023 1:03:14
File Size         : 238.499
File Version      :
Product Version   :
Identical         :
Extension         : mbox
File Attributes   : A
==========
```

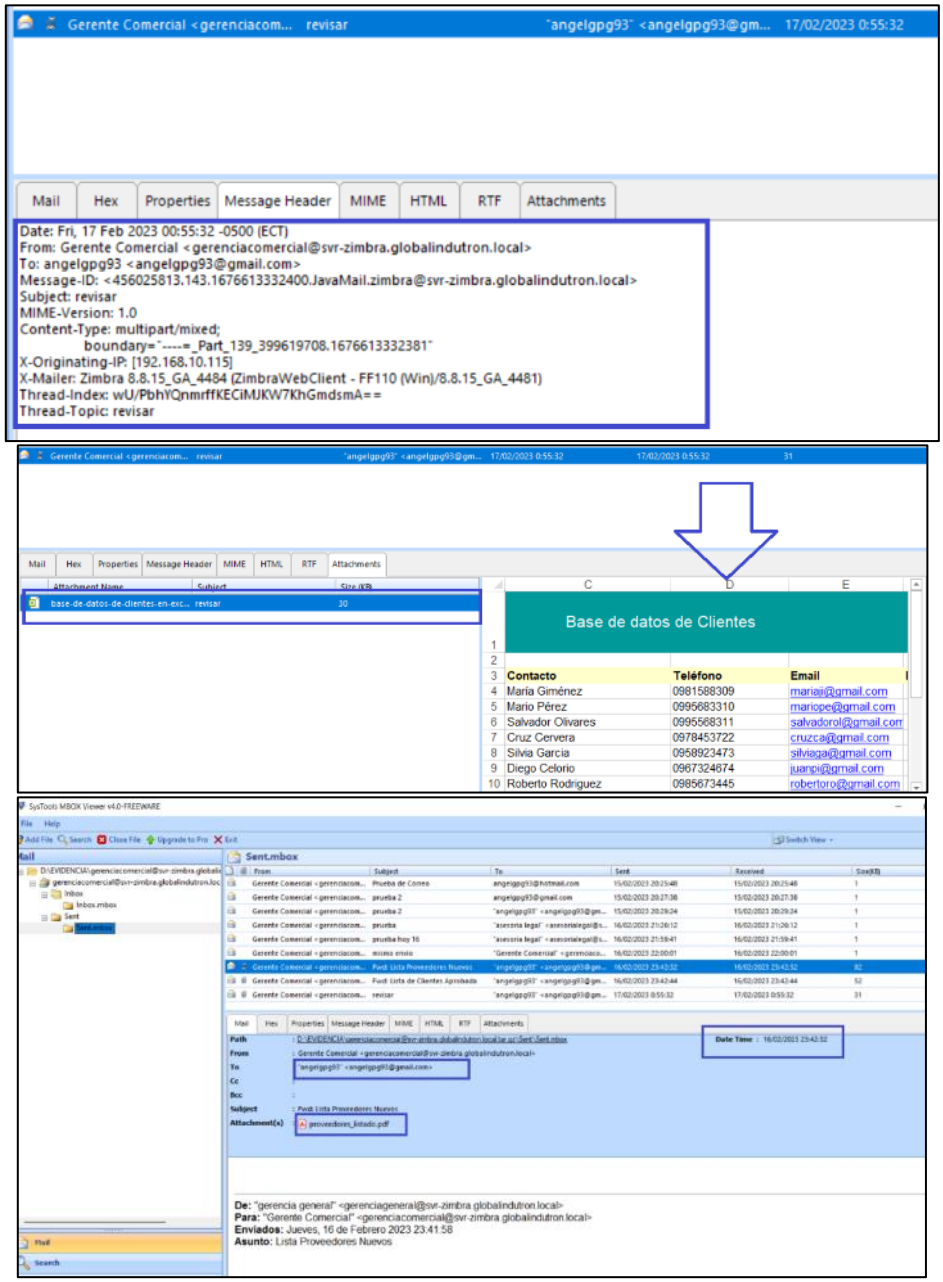
Fuente: Autores (2024).

Figura 13. Análisis del Buzón de correo con SysTools MBOX Viewer



Fuente: Autores (2024).

Figura 14. Hash del buzón de correo del posible infractor



Fuente: Autores (2024).

4. Conclusiones

Como resultado de la investigación forense efectuada en la

infraestructura tecnológica, se logró determinar que la información sensible de lista de proveedores y clientes estaba siendo enviada a correos personales desde la cuenta de correo de gerentecomercial@svr-zimbra_xxxx.local, para esto realizó el análisis forense del buzón de esta cuenta. La información extraída se le aplicó un hash para comprobar la integridad en las diferentes etapas del proceso. En este sentido, se hace hincapié en la verificación y preservación de la integridad de la evidencia, lo que implica el uso de herramientas y procesos adecuados.

La implementación rigurosa de estos procedimientos no solo ayuda a prevenir la contaminación o manipulación de la evidencia, sino que también proporciona transparencia y confianza en el proceso investigativo. Además, al resguardar la integridad de la evidencia, se fortalece la base sobre la cual se toman decisiones judiciales y se establece la verdad de los hechos.

5. Referencias

Beltrán, K. 2021. Modelo para análisis forense en dispositivos móviles con Sistema operativo Android. Disponible en: https://repositorio.pucesa.edu.ec/bitstream/123456789/3293/1/77448.pdf

Granda, G. 2015. Metodología para el análisis forense de datos e imágenes de acuerdo a las leyes del Ecuador. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/8943/1/UPS-CT005203.pdf

Iorio, D., H., A., Castellote, M. A., B., C., H., C., J., W., . . . I., I. J. 2017. El rastro digital del delito: Aspectos técnicos, legales y estratégicos de la Informática Forense.

Molina, F. 2020. Modelo de preservación de la evidencia digital. Disponible en: https://libros.cidepro.org/index.php/cidepro/catalog/download/9/9/30-1?inline=1

Ochoa, P. 2018. El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. Disponible en: https://www.redalyc.org/journal/5711/571167817003/571167817003.pdf

Pleno del Congreso Nacional de Ecuador. 2010. Ley de Comercio Electrónico, firmas electrónicas y mensajes de Datos. Disponible en: http://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf

Rios, J. 2016. Admisibilidad de la evidencia digital en un caso de fraude. Disponible en: https://www.auditool.org/blog/fraude/admisibilidad-de-la-evidencia-digital-en-un-caso-de-fraude

Servicio de Acreditación Ecuatoriana. (2018). Norma para recopilación de evidencias. Disponible en: https://www.acreditacion.gob.ec/norma-para-recopilacion-de-evidencias/

World Economic Forum. (2020). The Global Risks Report 2020 (15th ed.) Disponible en: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf