# Informe forense pericial

*Expediente 202505/06*

*09/07/2025*

- CONFIDENCIAL -

EXPEDIENTE: 202505/06

- FECHA DE INICIO: 19/05/2025
- FECHA DE FINALIZACIÓN: 09/07/2025

## CONTRATANTE

- NOMBRE: Inverfin Holding S.A.
- DIRECCIÓN: C/Amanecer de África s/n. Malabo (Guinea Equatorial)
- CONTRATO: REF-1742812592

## LEGITIMACIÓN

- NOMBRE: Roberto Nsue
- ROL: CEO y apoderado

## DE UNA PARTE:

Grupo Zerolynx (Zerolynx S.L.), representada por su Director General y Apoderado, D. Juan A. Calles.

## MANIFIESTA:

Que requerido por D. Roberto Nsue, en calidad de CEO y Apoderado de Inverfin Holding S.A.

## LE HA SIDO SOLICITADO:

Clonación de servidor Windows para puesta en custodia y posterior análisis forense pericial para la ratificación de la existencia y autenticidad de una serie de logs o trazas de auditoría que pudiesen contener indicadores de mal funcionamiento o anomalías sobre el comportamiento habitual de las aplicaciones de gestión del Instituto de Seguridad Social (INSESO) de Guinea Ecuatorial. Concretamente, es del interés del contratante la revisión de logs del software Agresso, donde se encontrarían las trazas core del sistema que gestiona la institución.

De forma añadida, el contratante solicita al equipo de Zerolynx evaluar el estado actual de ciberseguridad de los sistemas auditados, utilizando como base de comparación un estándar de ciberseguridad recomendado por el propio equipo auditor.

Asimismo, y debido a una incidencia acontecida durante el proyecto, el cliente requiere al equipo de Zerolynx ampliar el alcance para incluir los siguientes requerimientos:

- Extracción de los objetos del Directorio Activo de INSESO.
- Revocación de privilegios en el Directorio Activo de INSESO.
- Análisis de logs de la máquina afectada por la incidencia.

# ACEPTACIÓN

La realización del presente estudio ha sido aceptada por los peritos forenses de Zerolynx, D. Juan A. Calles, como máximo responsable del equipo de forense de Zerolynx y D. Daniel Puente y D. José L. González, peritos expertos, con el fin de: "Obtener y aportar información y pruebas sobre posibles malos funcionamientos o anomalías en el comportamiento de las aplicaciones de la entidad INSESO de Guinea Ecuatorial".

El presente INFORME se emite con carácter estrictamente CONFIDENCIAL y RESERVADO, se señala expresamente la AUSENCIA DE TODO ÁNIMO INJURIOSO, siendo el único ánimo de este informar de los hechos que se analizan con absoluta objetividad y veracidad.

Se advierte expresamente a los efectos previstos en la Ley Orgánica 3/2018, de 5 de diciembre de ESPAÑA, que de este INFORME NO QUEDA CONSTANCIA EN SOPORTE FÍSICO ALGUNO SUSCEPTIBLE DE TRATAMIENTO AUTOMATIZADO.

Se entrega TODA LA DOCUMENTACIÓN – todas las copias en formato digital de las evidencias, informes, y cualquier información recabada de los sistemas de INSESO – mediante un dispositivo de almacenamiento externo, tal y como queda reflejado en la última cadena de custodia, TODOS LOS DÍAS SE REALIZA CADENA DE CUSTODIA, quedando el dispositivo salvaguardado en la sede de INSESO.

# Índice

# 1. Confidencialidad

Toda la información y documentación facilitadas o entregadas a los peritos, para la prestación de este servicio, se considera confidencial. Los peritos se comprometen a no divulgarla, ni suministrarla, total o parcialmente, a terceros. La adquisición de evidencias que ha tenido lugar en el desarrollo del análisis forense mantiene los preceptos de mantenimiento según los criterios de cadena de custodia.

# 2. Introducción

La fiabilidad de los sistemas informáticos en entornos críticos depende en gran medida de su diseño, mantenimiento, capacidad de auditoría y actualización tecnológica continua. Cuando estas condiciones no se cumplen, el riesgo de fallos operativos, pérdida de trazabilidad o aparición de comportamientos anómalos se incrementa significativamente. En este contexto, el presente trabajo forense se enmarca en una intervención técnica orientada a identificar y documentar posibles indicios de mal funcionamiento e inconsistencias operativas en uno de los entornos clave del Instituto de Seguridad Social (INSESO) de Guinea Ecuatorial, sobre una plataforma Microsoft Windows en producción.

El trabajo en cuestión viene requerido por la entidad Inverfin Holding S.A. a petición de INSESO, quien manifiesta como antecedente a los peritos que, el Delegado Nacional del Instituto de Seguridad Social (INSESO) compareció ante el Pleno de la Cámara de los Diputados en la jornada del lunes 14 de abril, con el fin de dar detalles acerca de las limitaciones en el sistema de gestión informática, incluyendo la obsolescencia tecnológica y la falta de un plan director de sistemas de información.

Tal y como el contratante informa a los peritos, la infraestructura objeto de análisis presentaría, por tanto, indicios de obsolescencia tecnológica, tanto a nivel de hardware como de software, junto a deficiencias en la implementación de mecanismos de auditoría y continuidad operativa. La ausencia de un plan director de sistemas, la dependencia de recursos no redundados y la falta de respaldo estructurado para los datos críticos son elementos que podrían estar agravando el riesgo inherente al entorno. Frente a esta situación, se ha solicitado la realización de una clonación forense del servidor Windows, con el objetivo de preservar el estado actual del sistema para su análisis posterior, manteniendo la integridad de la evidencia y permitiendo su estudio bajo condiciones controladas.

Este trabajo no pretende evaluar aspectos organizativos, normativos o de gobernanza institucional, sino centrarse exclusivamente en el diagnóstico técnico del entorno Windows analizado, desde una perspectiva objetiva, empírica y basada en evidencia digital; debido a las incidencias, se han realizado los trabajos de análisis forense de la incidencia ocurrida. El objetivo es generar un informe técnico que sirva como base para identificar deficiencias a nivel de auditoría forense, validar la autenticidad de los registros de actividad y proponer recomendaciones de mejora desde el punto de vista de la arquitectura informática, la seguridad operativa y la resiliencia del entorno; quedando

entregado el informe técnico con las evidencias a fecha 23/05 (recogido en cadena de custodia) incluida en este informe, y siendo entregado en fecha futura el informe de recomendaciones.

La creciente necesidad de disponer de sistemas trazables, auditables y técnicamente coherentes exige adoptar un enfoque forense no sólo reactivo, sino también preventivo, especialmente en entornos donde la continuidad de servicios y la precisión de los registros son fundamentales para la operativa institucional. El presente análisis se sitúa en ese marco técnico, orientado a la obtención de conclusiones claras, fundamentadas y técnicamente reproducibles.

# 3. Presentación de evidencias

## Evidencias recibidas

Para la realización del informe forense, INSESO ha facilitado a los peritos el usuario y contraseña de la cuenta de administración del sistema "INSESOBCK02". Este sistema, por razones de negocio, no puede ser apagado, motivo por el que los peritos deciden realizar una clonación forense del sistema en vivo, extrayendo cada una de las particiones, bit a bit, en formato de imagen de disco.

Una vez recibidas las credenciales de acceso, los peritos comienzan con el proceso de extracción forense, el cual es descrito en el siguiente apartado.

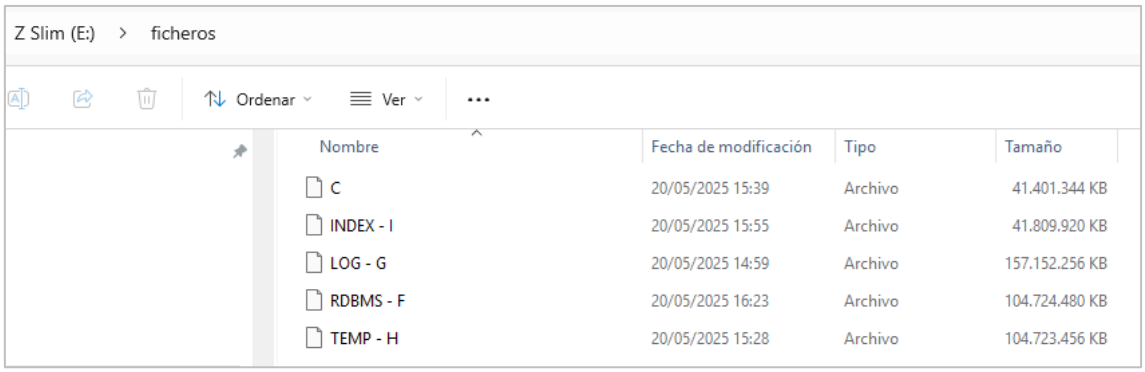
## Validez técnica de las evidencias

La labor de adquisición de evidencias y de análisis forense posterior han sido realizadas tomando como base las normas españolas e internacionales "UNE 71506: Metodología para el análisis forense de las evidencias electrónicas" y "UNE-EN ISO/IEC 27037:2016".

Este informe sigue las directrices marcadas en la norma española "UNE 197001:2019", bajo la que se define la estructura formal que deben seguir los informes periciales.

En primer lugar, una vez recibidas las credenciales de administración, los peritos llevan a cabo la clonación de las particiones de disco objeto de la pericia. Esta clonación, por incidencias técnicas del entorno, se realiza de forma parcial, sin embargo, ello no impide la obtención de material suficiente para la realización de un estudio técnico y la emisión de diferentes conclusiones que puedan dar respuesta a los requerimientos del contratante.

Para la realización de la clonación forense de las unidades de almacenamiento, se ha utilizado el software HxD, en su última versión disponible, la versión 2.5.0.0 (publicada el 11 de febrero de 2021). La herramienta es reconocida en el ámbito pericial por su capacidad de efectuar **copias bit a bit**, lo que **garantiza la integridad de los datos originales** y su idoneidad como prueba. El proceso de clonación se ha realizado unidad por unidad, almacenando las imágenes generadas en una unidad USB externa dedicada a tal efecto. Este procedimiento permite conservar la cadena de custodia y asegurar la fidelidad de la información extraída, cumpliendo con los principios de inalterabilidad y reproducibilidad exigidos en el ámbito judicial.




*Proceso resultante de la clonación parcial (imagen extraída de la unidad entregada como evidencia)*

A continuación, los peritos obtienen las correspondientes firmas digitales en formato hash SHA256 que garantizan la inalterabilidad y no repudio de los medios clonados, cuyos detalles pueden ser comprobados en la tabla inferior.

Posteriormente, y tal y como se informó en la SOLICITUD del presente informe, debido a lo que a todas luces pudo ser un posible incidente de seguridad acontecido mientras los peritos realizaban las labores solicitadas, se requiere a estos de forma urgente la revocación de todos los privilegios de los usuarios del dominio, a excepción de dos personas, el usuario del Sr. Delegado Nacional, y del Sr. Rosendo (Jefe Adjunto de Servicio de Informática de INSESO), labor que realizan de forma inmediata. Con objeto de preservar la evidencia del estado del Directorio Activo previa revocación de privilegios, en presencia de los auditores, el Sr. Rosendo realiza una extracción de los objetos del Directorio Activo, facilitando dos archivos a los peritos con los resultados de la extracción.

Como resultado de la extracción, los peritos obtienen 2 copias inmutables de los ficheros extraídos, cuyas firmas digitales en formato hash SHA256 pueden ser comprobadas en la tabla inferior correspondiente al Directorio Activo.

Con el fin de analizar el posible incidente, y las trazas que hayan podido quedar en los sistemas, el equipo técnico de INSESO extrae los logs del clúster donde se encuentran alojados los sistemas virtuales, recuperando únicamente logs del sistema operativo – Windows Server 2012. Se facilitan los logs para su análisis a los peritos.

Resultado de la extracción, los peritos obtienen una copia inmutable de los logs extraídos, cuyas firmas digitales en formato hash SHA256 pueden ser comprobadas en la tabla inferior.

| Partition name | Hash SHA256 |
|---|---|
| C | 12c1eb545126a540e35987b2a5acbb10e5c5c6984ad2ccd375d15383b47cfca7 |
| INDEX - I | d03bccb17039478b441b3b2b81b8301431d4232ff7caffbc9eb82c52ad0e93cf |
| LOG - G | f3a588eb37f2fdf9bf60b422a24f9cb7235b0a3772aac67850dc4823cb956b7a |
| RDBMS - F | 2e7695860b6e6813252682f27f367f461b8b14b9c91daea165b8abf75d323d7f |
| TEMP - H | 3acd6eda2094f91e98801f2f3022435794745393c60b1d3e342f78b7518534bc |

| Directorio Activo | Hash SHA256 |
|---|---|
| ESTRACCION DA.dat | 8b7f0fd2d278b8aa7ad205f3ba8652ed00f3b6e8fd18f173b26270b9e71a8603 |
| ESTRACCION DA1.dat | 06fc7b7337114b02134922f536e55c671a0c38efc7a63a7173a6b7030ed7cf6d |

| Ficheros de log | Hash SHA256 |
|---|---|
| logs de windows.zip | 32773acbf94f76ca95bd81bea76dcb16dcd2efe31d346672610be1f63a60d32b |

Por requerimiento del contratante, se informa a las partes interesadas de que los peritos, a la conclusión del presente informe, le entregan todas las copias forenses realizadas para su posterior proceso de custodia.

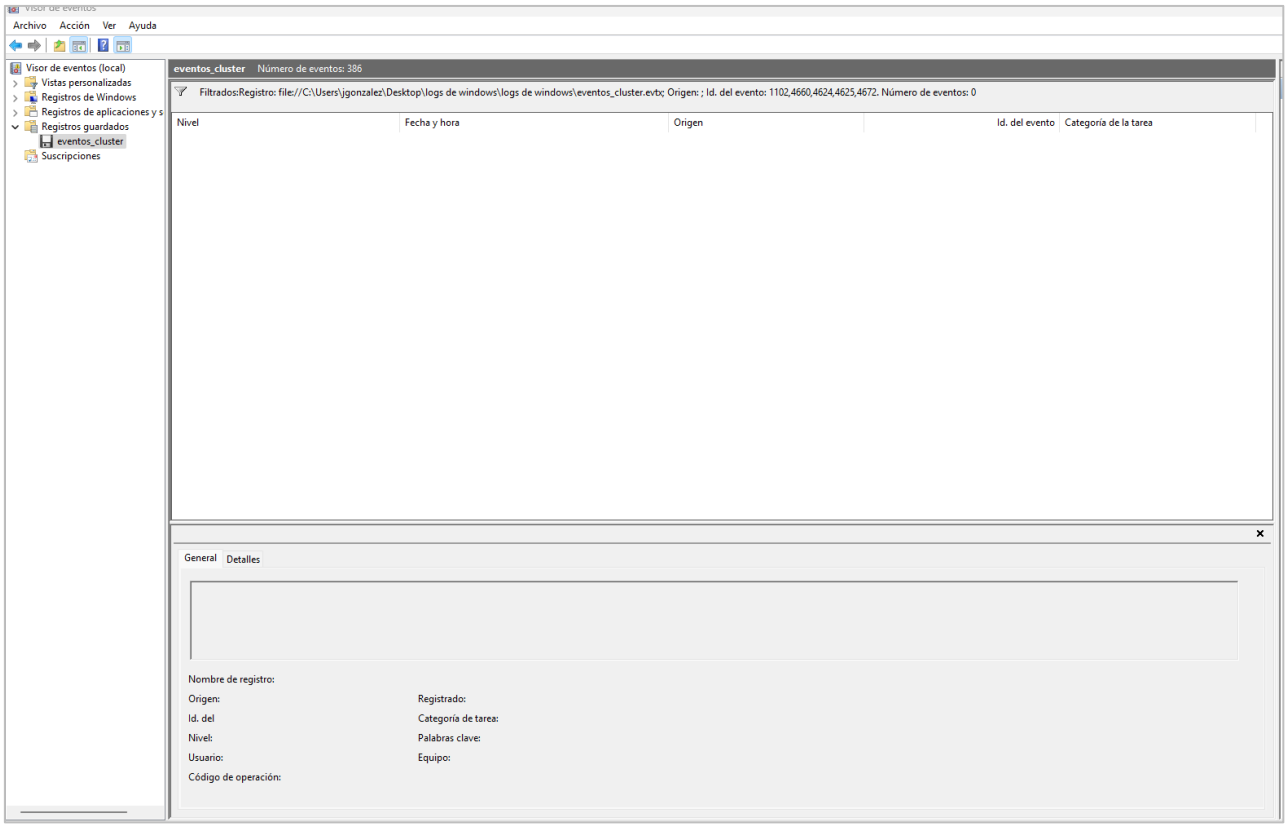
# 4. Auditoría de logs

El cliente, Inverfin, dada la situación que ha surgido durante el transcurso de la auditoría forense, solicita a los peritos el análisis extra de las trazas de log que se puedan recuperar del nodo “insesonodo03”.

El técnico de INSESO facilita la información recabada a modo de evidencia para que los técnicos de Zerolynx la analicen. A continuación, se presentan las evidencias obtenidas de cada uno de los ficheros facilitados.

*eventos cluster.evtx*

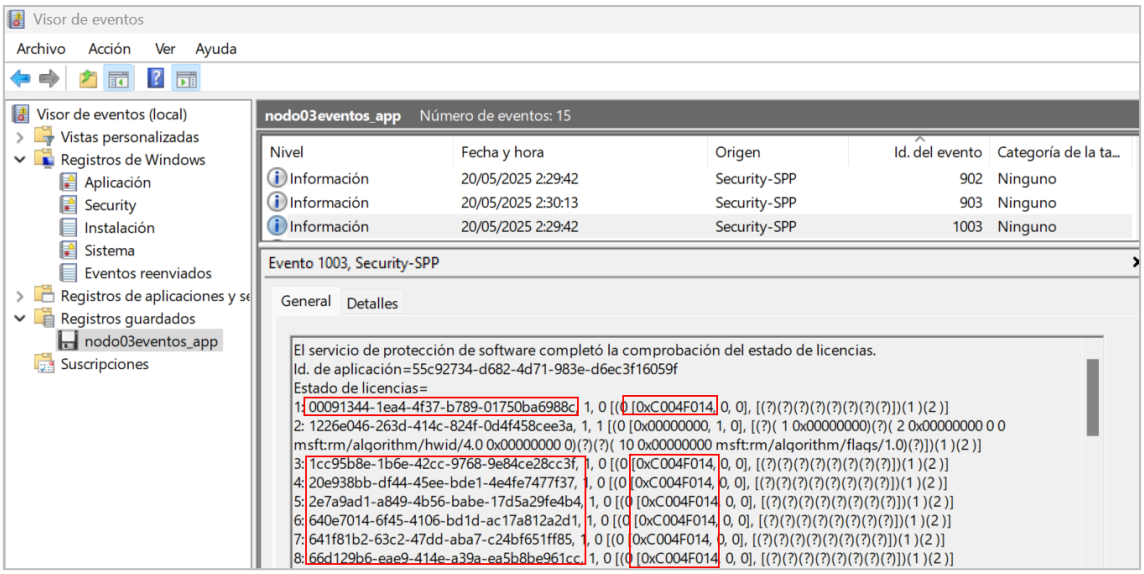
- Se identifican logs en el rango acontecido desde el 21/05/2025 a las 11:38:08 hasta el 22/05/2025 a las 10:44:55. Este periodo se encuentra fuera de las horas en las que acontece el incidente de seguridad anteriormente indicado, a pesar de ello, se decide realizar un análisis por si pudiera contener información de interés.
- Se identifican los siguientes errores relevantes:
    - ID 1069 – Indica que un recurso del clúster ha intentado inicializar y no ha sido capaz. El recurso puede ser un disco, una interfaz de red, un servicio, etc. – Nombre de recurso “SCVMM INSESODB” y “SCVMM INSESODB Configuration”.
    - ID 1127 – Error en la operación de disco mientras se tenía acceso al disco duro, incluso después de varios intentos – Nombre de la interfaz de red “insesonod0- Ethernet 4”.
    - ID 1130 – No hay suficientes recursos de memoria del servidor disponibles para procesar este comando – Nombre de red “Red de clústeres 3”.
    - ID 1205 – Un recurso del clúster no se ha podido inicializar completamente, o apagar completamente – Grupo de Recursos: “SCVMM INSESODB Resources”.
    - ID 1254 – Un rol del clúster, ha superado el límite de fallos permitidos – Grupo de Recursos: “SCVMM INSESODB Resources”.
- Asimismo, se analiza el fichero de logs al completo, independientemente de las fechas de los eventos, y no se identifica ningún registro de log de seguridad relativo a inicios de sesión, rotación de logs, borrado de eventos, etc.
- En conclusión, no se recupera ningún evento de Windows relacionado con la búsqueda en cuestión.




*Resultado de filtrar por los principales identificadores de eventos de Windows en eventos_cluster*

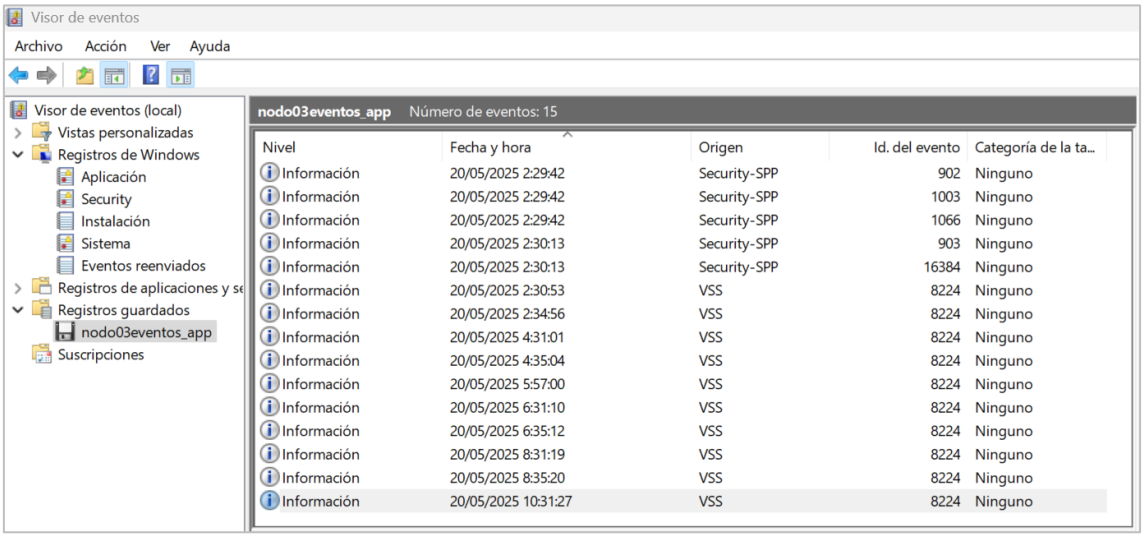
### *nodo03eventos_app.evtx*

- Se identifican logs desde el 20/05/2025 a las 02:29:42 hasta el 20/05/2025 a las 10:31:27.
- Los logs contenidos en el fichero tampoco son compatibles con las horas en las que acontece el incidente de seguridad, a pesar de ello, son objeto de estudio por si pudieran contener información de interés.
- Todos los logs registrados son de categoría informativa, se analizan por si pudieran contener información relevante.
    - ID 902 – Se inició el servicio de protección de software – Datos del evento “6.3.9600.19101”.
    - ID 903 – Se detuvo el servicio de protección de software.
    - ID 1003 – Se completa el servicio de comprobación de licencias. 24 licencias comprobadas reportan el error “0xC04F014” el cual implica que el servicio no ha podido validar satisfactoriamente la licencia.




*Registro de errores arrojado por el evento 1003*

- ID 1066 – Reporte de estado de inicialización para objetos de servicio.
- ID 8224 – Cierre del servicio VSS por inactividad.
- ID 16384 – El servicio de protección de software se programó correctamente para reiniciarse a las 2125.04.26T00:30:13Z. "Motivo: RulesEngine".

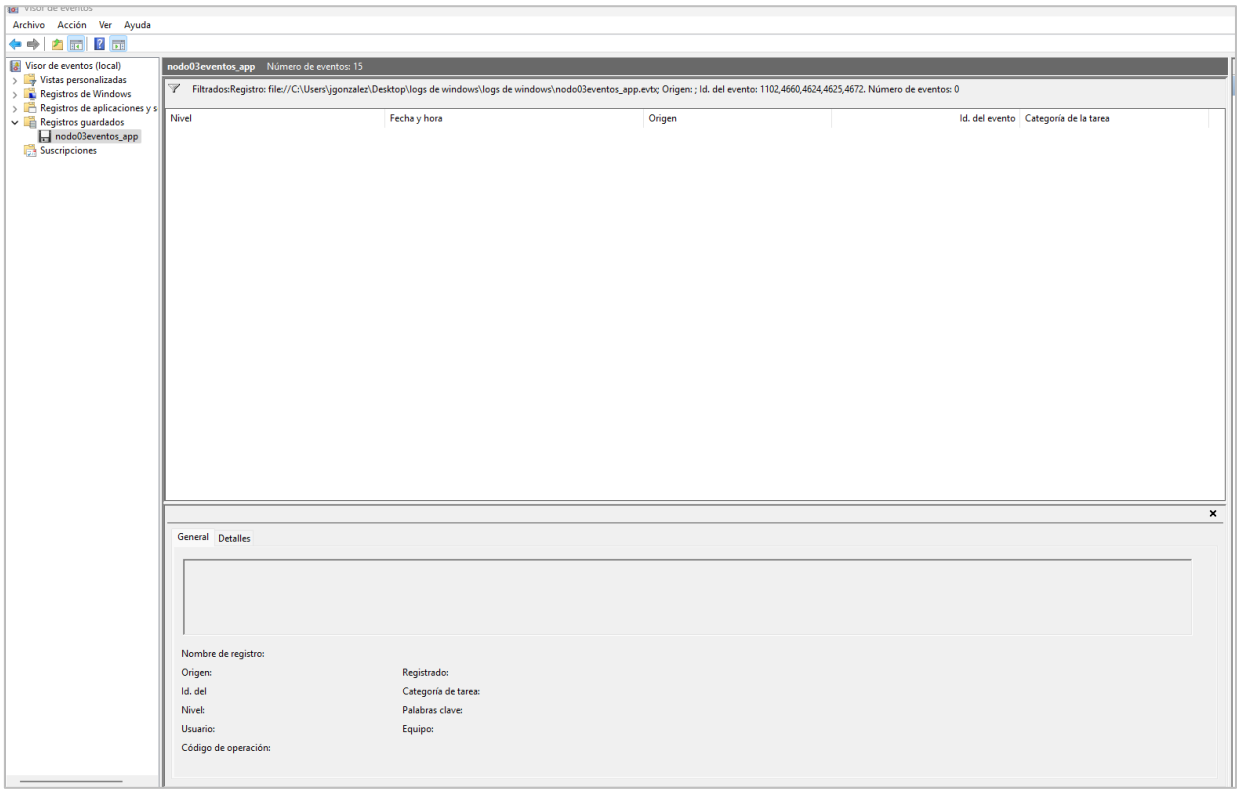



*Todos los registros disponibles para análisis en "nodo03eventos_app.evtx"*

- ID 1069 – Indica que un recurso del clúster ha intentado inicializar y no ha sido capaz. El recurso puede ser un disco, una interfaz de red, un servicio,

etc. – Nombre de recurso “SCVMM INSESODB” y “SCVMM INSESODB Configuration”.

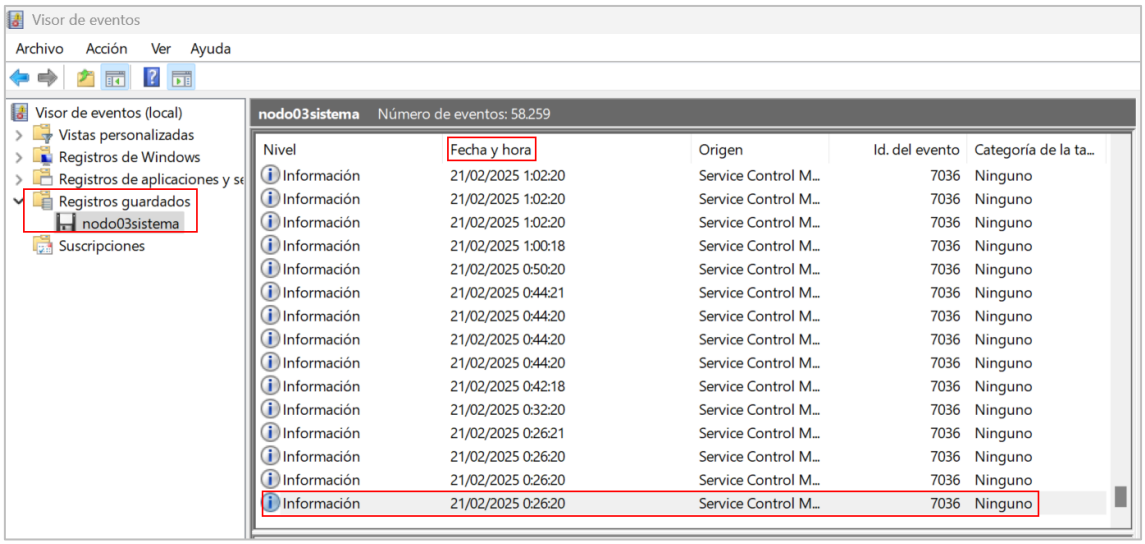
- Para que quede constancia, se realiza filtrado por los principales identificadores de eventos de Windows, relativos a seguridad, autenticaciones exitosas y fallidas, borrado de registros o eventos, etc. No identificándose ningún registro al respecto.




*Resultado de filtrar por los principales identificadores de eventos de Windows en nodo03eventos_app*

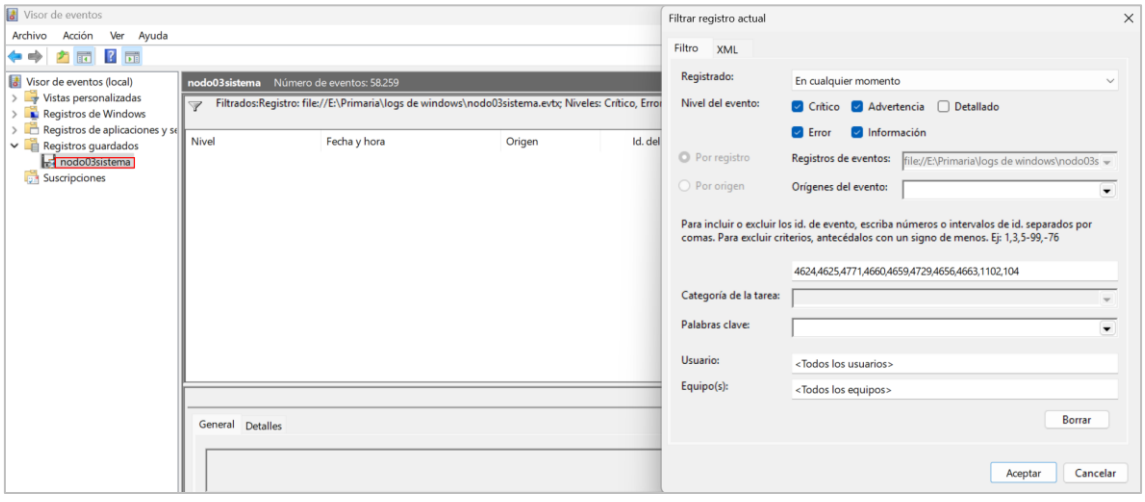
### *nodo03sistema.evtx*

- Se identifican logs desde el 21/02/2025 00:26:20 hasta el 22/05/2025 10:43:11.
- El rango temporal es **excesivamente** amplio, quedando acotado el intervalo de estudio al solapado con el incidente reportado, dado que se notificó que la fecha y hora aproximada era el 20/05/2025 a las 23:30:00.




*El registro más antiguo de la muestra facilitada reporta la fecha y hora 21/05/2025 00:26:20*

- Se analiza el fichero de eventos, arrojando la siguiente información relevante:
    - Se analizan los principales eventos de Windows relacionados con acciones sospechosas o malintencionadas, no reportando ningún evento **en el rango temporal de estudio facilitado** a los auditores.

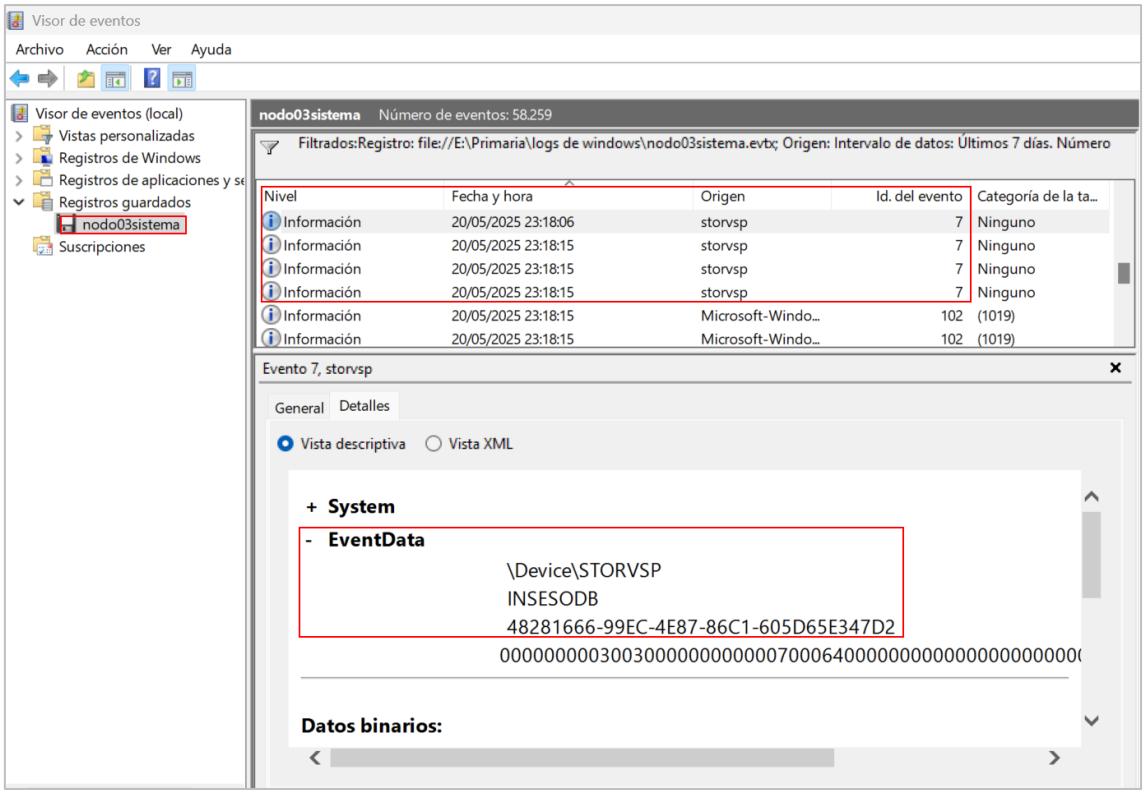



*No se recuperan registros para el filtrado de ventos por los identificadores de seguridad principales*

- ID 1 – Error inesperado – El sistema arroja el primer error en fecha y hora 20/05/2025 a las 20:01:42. – Reporta el código de error “48F@01000003”.

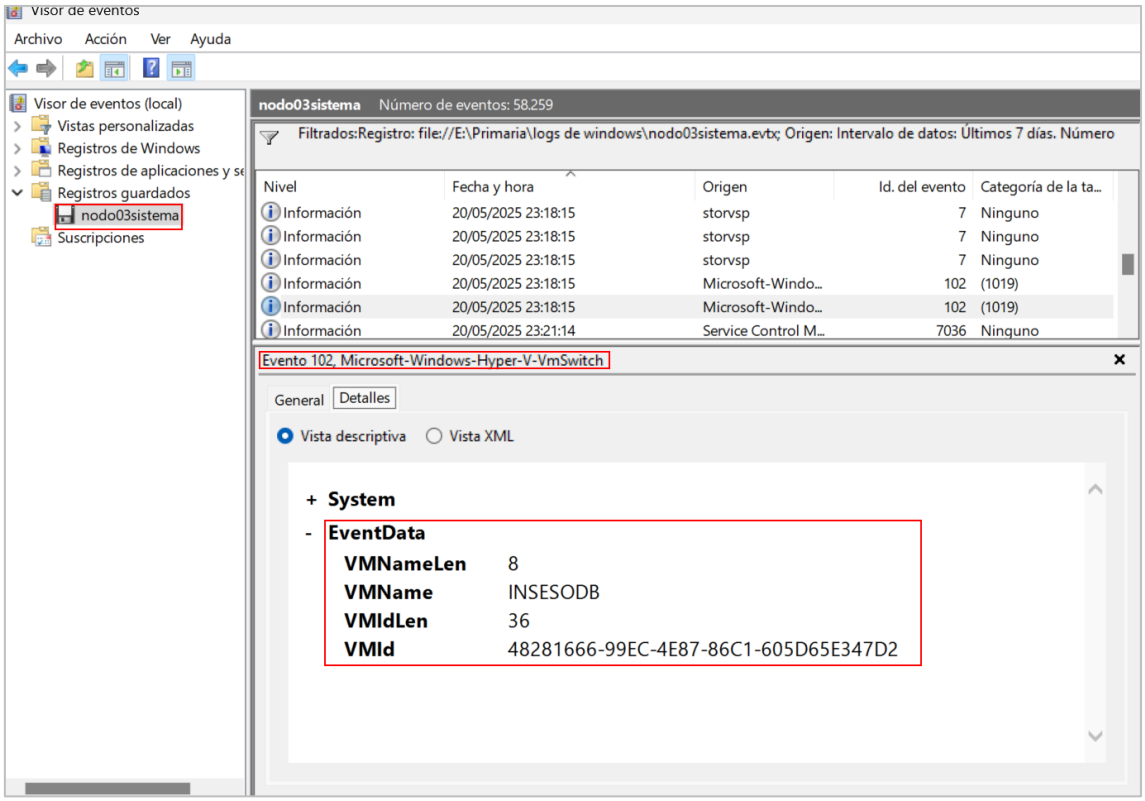
El error indica que se ha intentado ejecutar el backup del servidor y ha fallado, debido a que el CSV no se encuentra disponible en el momento de la ejecución.

- ID 7 – STOPVSP – Se detiene la máquina virtual, generándose 4 eventos en el registro de Windows. No se puede determinar con los datos facilitados por los técnicos de INSESO, si la causa raíz de la detención de la máquina virtual es ocasionada por un agente externo o no.



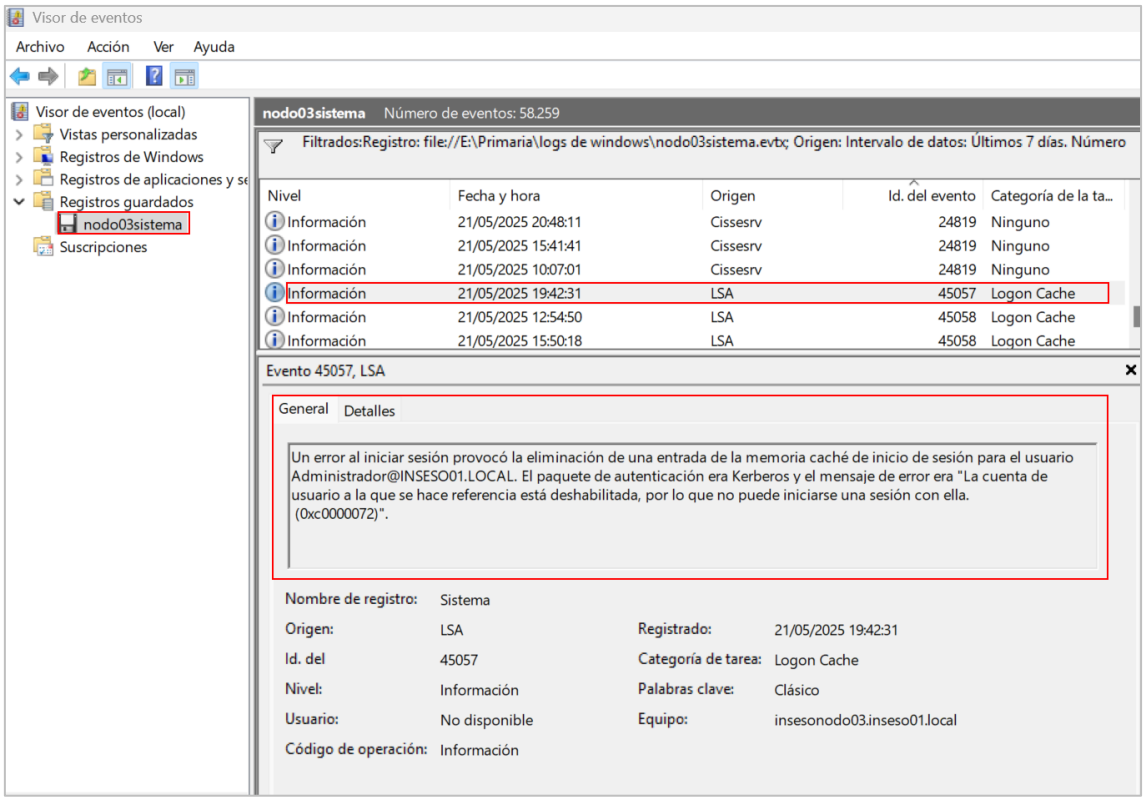

*Eventos de registro con ID 7, indican parada de la máquina virtual INSESODB*

- ID 102 – Microsoft-Windows-Hyper-V-VmSwitch – El error sucede en ocasiones debido a fallos de replicación en entornos de Hyper-V, cuando la máquina primaria y secundaria se encuentran en estado de replicación y una de ellas, además, se encuentra en estado de generación de backup.




*Eventos de registro con ID 102, indicando fallo Microsoft-Windows-Hyper-V-VmSwitch*

- ID 45057 – LSA – Se reporta un inicio sesión fallido para el usuario "Administrador@INSESO01.local", este error sucede **después** de que se realizara la eliminación de privilegios de todos los usuarios del dominio y de deshabilitar la cuenta de Administrador del dominio, esa misma tarde.



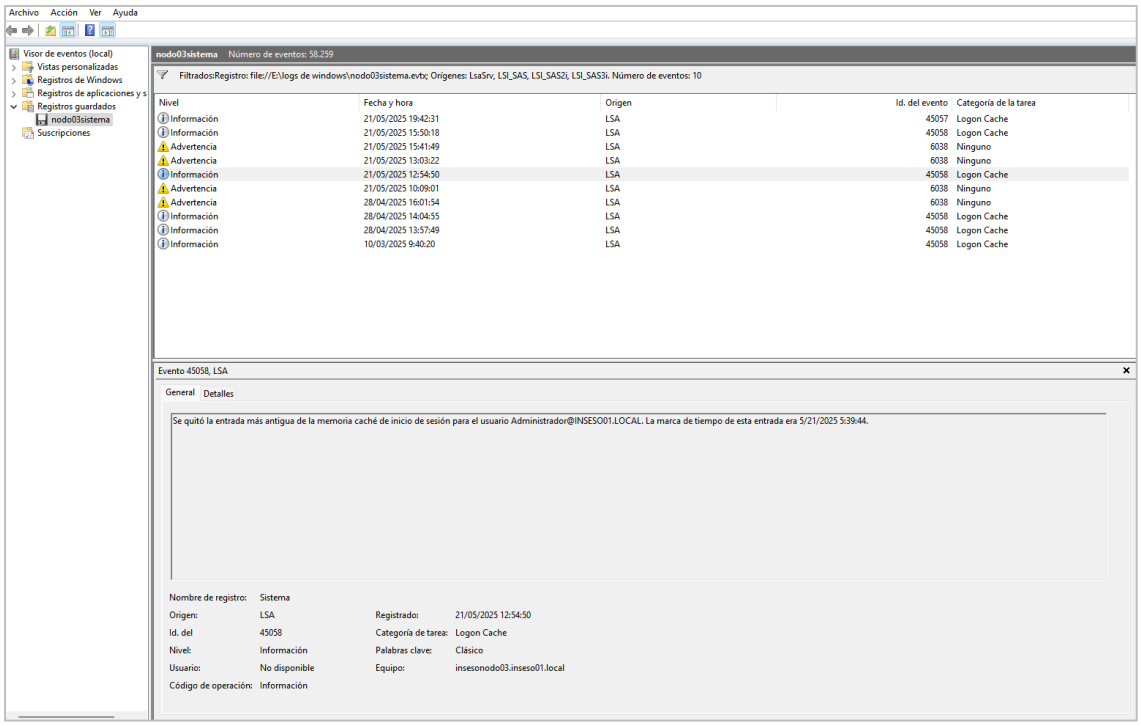

*Se detecta un intento de inicio de sesión con el usuario Administrador después de que se haya deshabilitado*

En una segunda instancia se analiza al completo el fichero de logs, **facilitado por el personal técnico de INSESO a los auditores de Zerolynx**, en este segundo análisis se han analizado **todos los registros** exportados, independientemente de cuando ocurrieron.

La siguiente evidencia muestra todos los eventos registrados en el nodo 3 – nodo03sistema – referidos al módulo LSA.

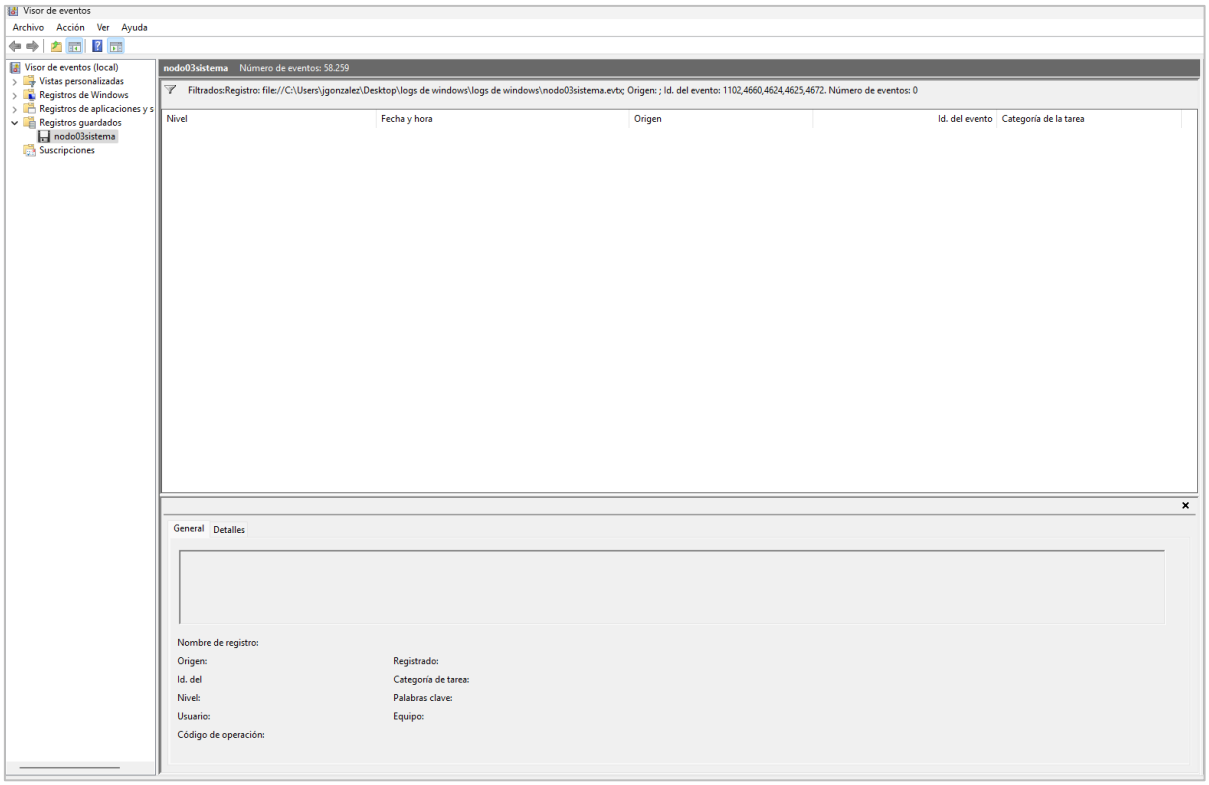
A partir de los resultados evidenciados, se pueden identificar diferentes inicios de sesión desde el 10 de marzo de 2025, fecha en la cual el registro de logs facilitado a los auditores posee el primer inicio de sesión en el nodo.

Se debe remarcar que los eventos de categoría “Logon Cache” representan un inicio de sesión satisfactorio, puesto que el sistema es capaz de autenticar al usuario y almacenar en caché la última versión de sus credenciales del dominio.




*Eventos de LSA registrados en nodo03sistema*

- Se realiza filtrado por los principales identificadores de eventos de Windows, relativos a seguridad, autenticaciones exitosas y fallidas, borrado de registros o eventos, etc. No se identifica ningún registro de seguridad.




*Resultado de filtrar los logs facilitados por los principales eventos de Windows relacionados con el trabajo en curso – en nodo03sistema*

## *Cronología de Eventos registrados a través del Visor de Eventos de Windows*

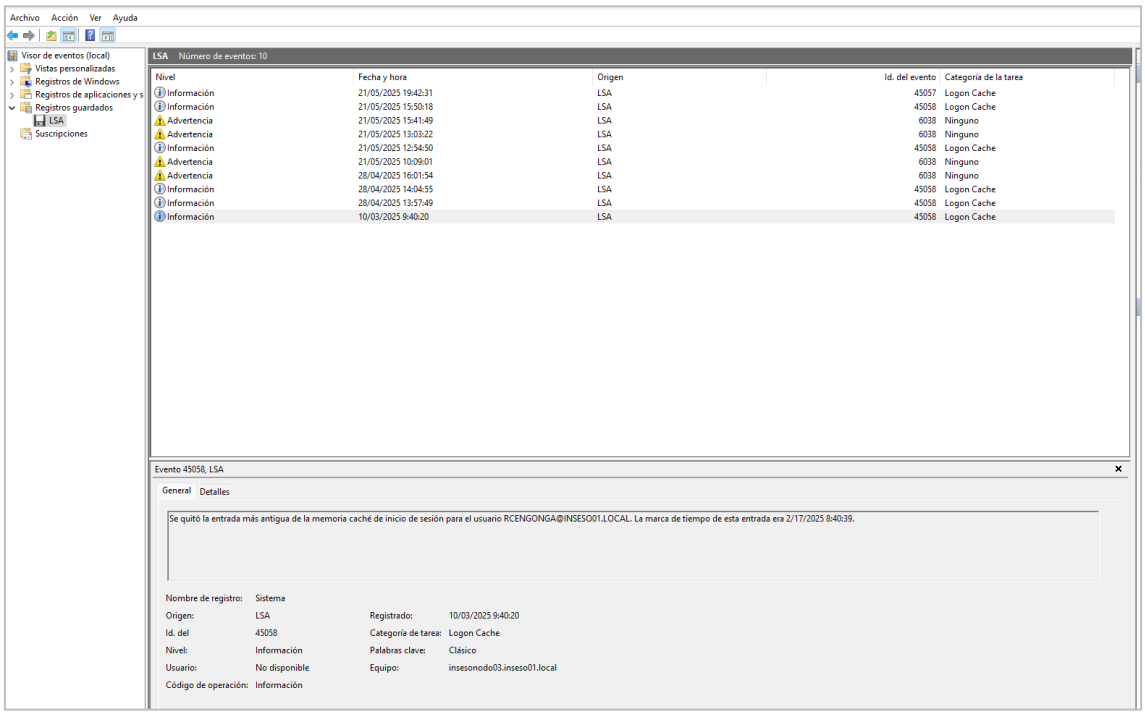
Tras el análisis forense de los registros de eventos proporcionados por el sistema operativo Windows del nodo identificado como nodo03sistema, y en base a la información extraída directamente desde el Visor de Eventos (Event Viewer), se ha reconstruido la siguiente cronología de actividad de autenticación relevante en el sistema:

1. *Evento de inicio de sesión exitoso – Usuario* RCENGONGA@INSESO01.LOCAL

Fecha y hora: 10 de marzo de 2025, a las 09:40:20

Se constata un inicio de sesión satisfactorio por parte del usuario RCENGONGA@INSESO01.LOCAL. Este evento conlleva la eliminación automática de la entrada más antigua del historial de autenticaciones exitosas almacenadas en caché por el sistema, la cual corresponde al 17 de febrero de 2025.

Por defecto, el sistema Windows conserva las últimas diez entradas de autenticación válidas. Sin embargo, no se ha aportado a los técnicos forenses evidencia que permita confirmar o refutar si dicha configuración permanecía sin alteraciones respecto al valor predeterminado.

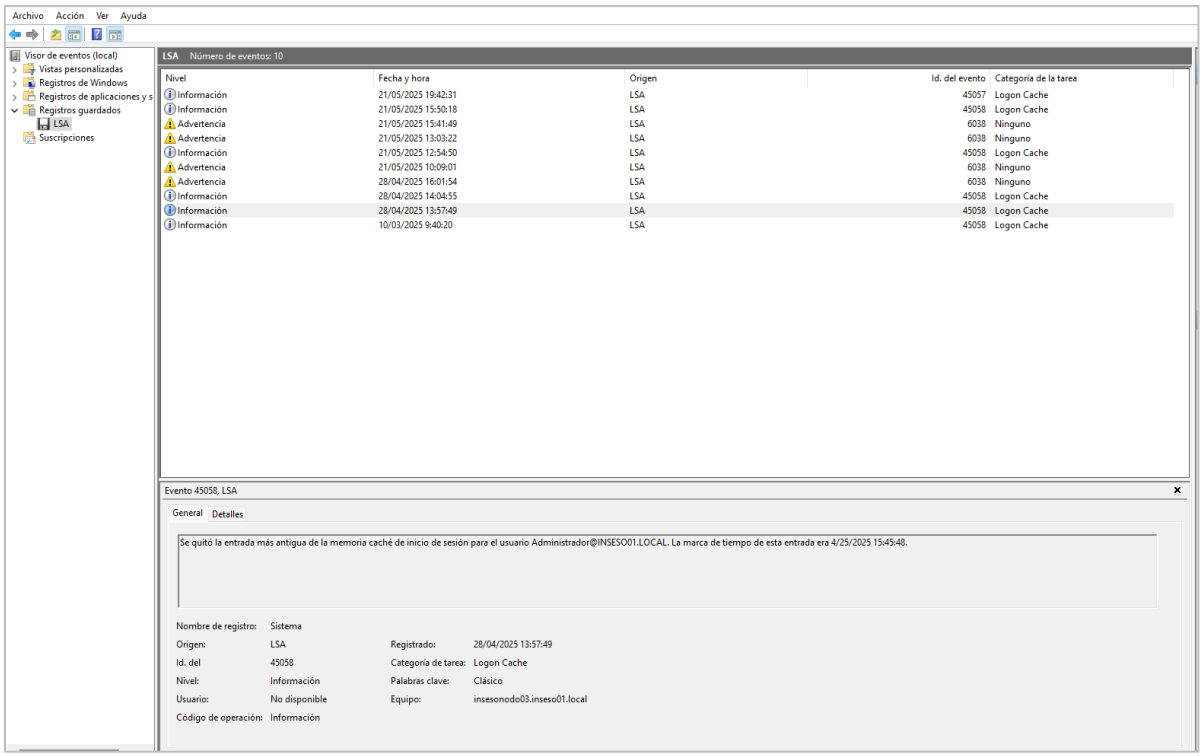



*Detalle información fecha 10/03/2025 9:40:20*

## *2. Evento de inicio de sesión exitoso – Usuario* Administrador@INSESO01.LOCAL

Fecha y hora: 28 de abril de 2025, a las 13:57:49

El usuario Administrador@INSESO01.LOCAL efectúa un inicio de sesión válido. De forma análoga al caso anterior, el sistema procede a eliminar la décima entrada cacheada correspondiente a una autenticación previa realizada el 25 de abril de 2025.

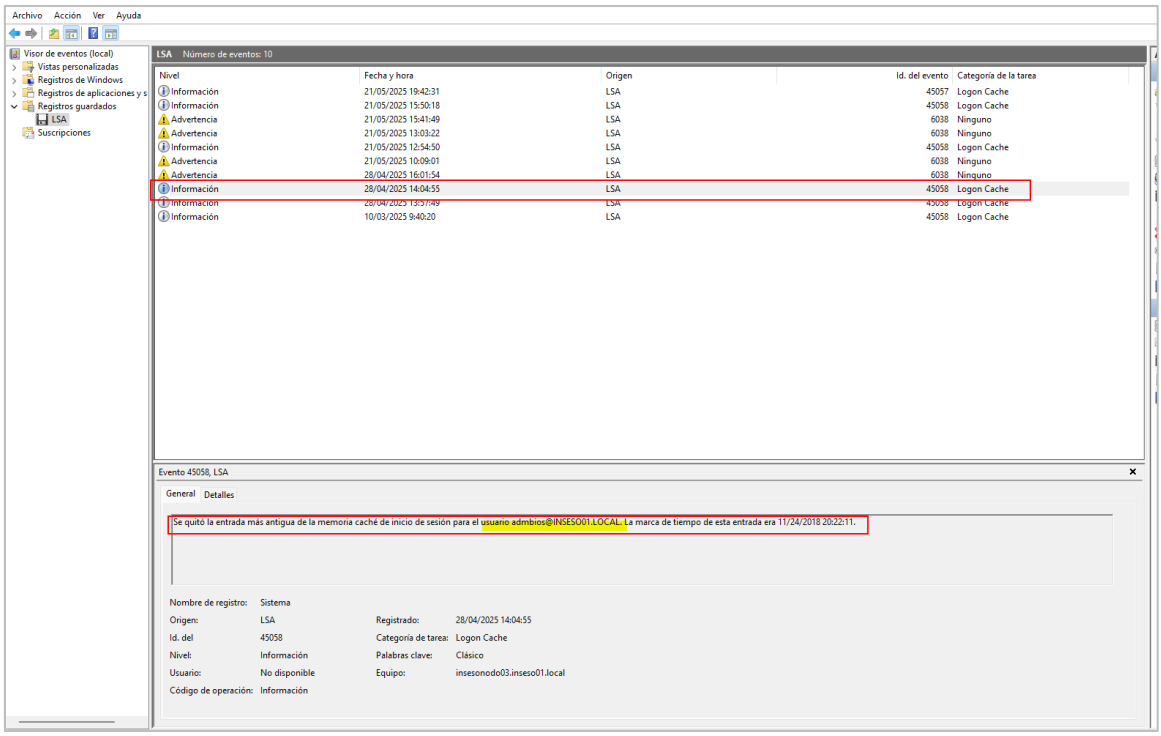



*Evidencia 1: Detalle información fecha 28/04/2025 13:57:49*

### 3. *Evento de inicio de sesión exitoso – Usuario* admbios@INSESO01.LOCAL

Fecha y hora: 28 de abril de 2025, a las 14:04:55

Pocos minutos después del acceso anterior, se identifica un nuevo inicio de sesión satisfactorio, esta vez correspondiente al usuario admbios@INSESO01.LOCAL. La entrada más antigua registrada en la caché de autenticación de este usuario data del 24 de noviembre de 2018, lo cual indica un uso histórico prolongado del perfil en el sistema.

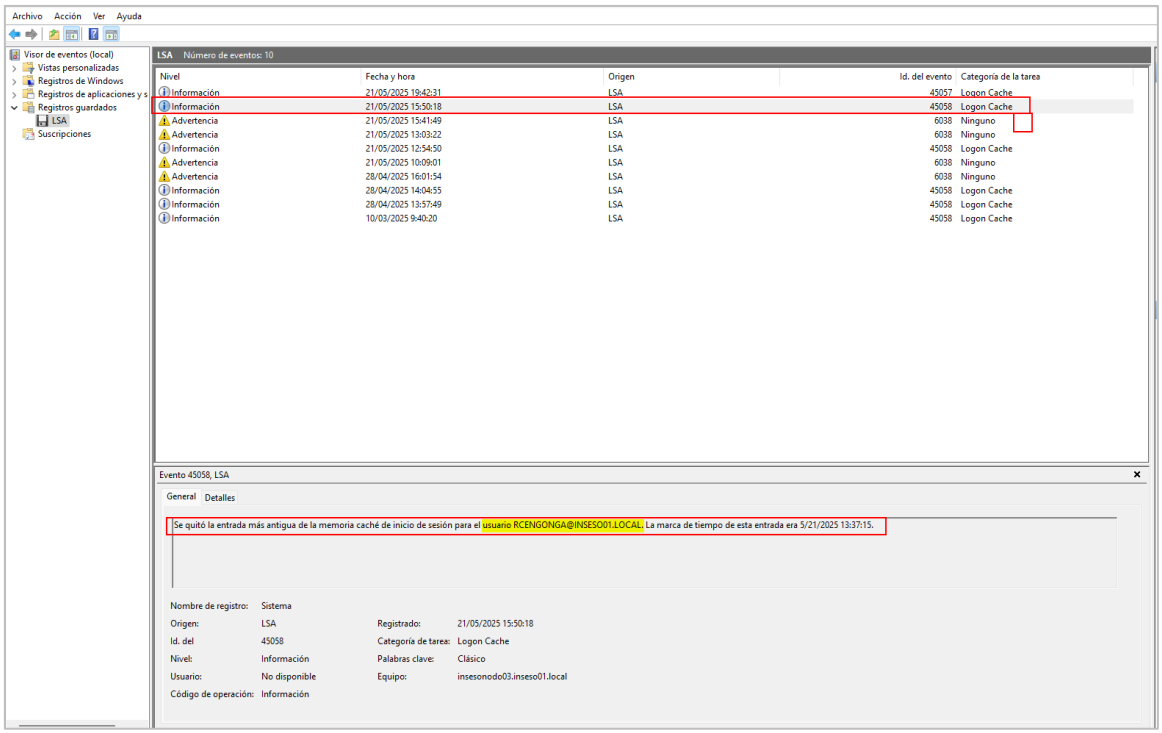



*Evidencia 2: Detalle información fecha 28/04/2025 14:04:55*

### *4. Evento de inicio de sesión exitoso – Usuario* RCENGONGA@INSESO01.LOCAL

Fecha y hora: 21 de mayo de 2025, a las 15:50:18

Se documenta un nuevo acceso exitoso por parte del usuario RCENGONGA@INSESO01.LOCAL, sin indicios de error en la autenticación.



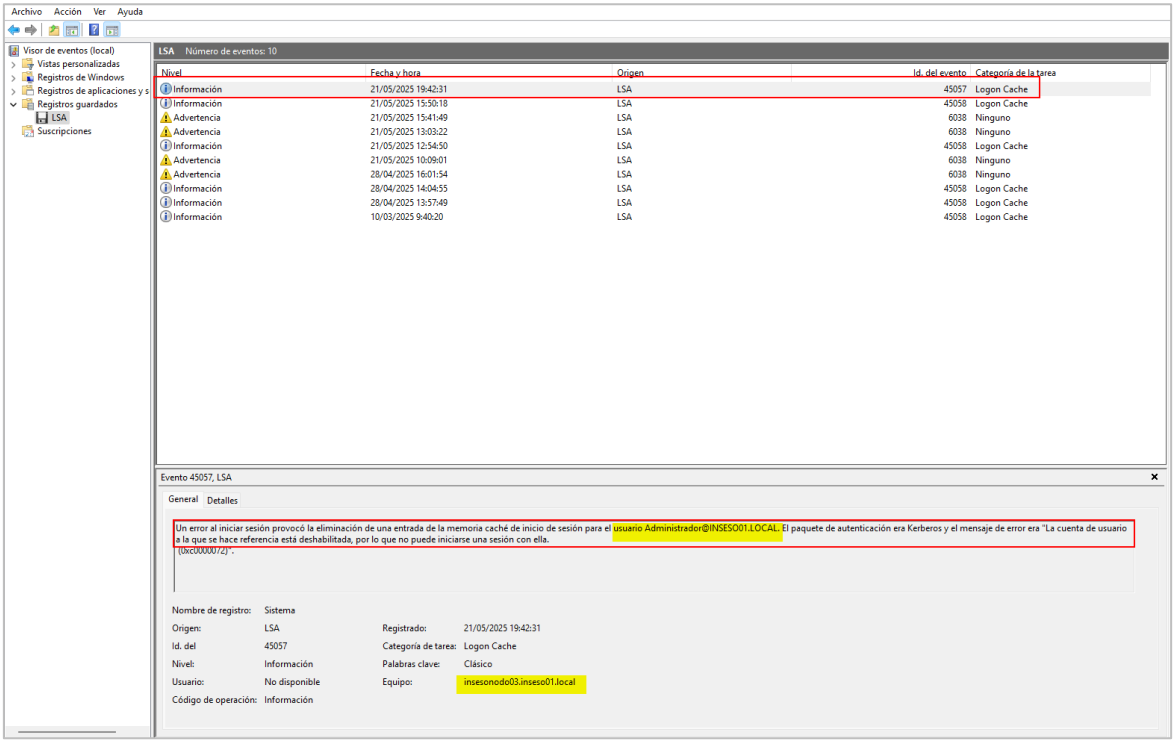

*Evidencia 3: Detalle información fecha 21/05/2025 15:50:18*

### 5. *Evento de inicio de sesión fallido – Usuario* Administrador@INSESO01.LOCAL

Fecha y hora: 21 de mayo de 2025, a las 19:42:31

Se registra un intento de inicio de sesión fallido por parte del usuario Administrador@INSESO01.LOCAL. Este intento ocurre horas después de que la cuenta en cuestión fuese deshabilitada y sus privilegios de administración fuesen revocados en el dominio INSESO01.LOCAL.

Este evento permite inferir la existencia de intentos de acceso persistentes con una cuenta de alto privilegio, previamente válida, pero ya desactivada en el sistema.




*Evidencia 4: Detalle información fecha 21/05/2025 19:42:31*

# 5. Análisis forense de las particiones

En conformidad con lo establecido en el apartado *Presentación de evidencias*, se procede al análisis forense de las particiones extraídas del sistema identificado como *INSESODB*, correspondiente al entorno objeto de esta investigación.

El estudio ha sido efectuado mediante la herramienta **Autopsy**, en su última versión estable disponible a la fecha de redacción del presente informe, concretamente la **versión 4.22.1**. Esta herramienta está reconocida en el ámbito de la informática forense por su capacidad de análisis detallado de sistemas de archivos, metadatos, artefactos del sistema operativo y otras evidencias digitales.

El análisis se realiza sobre las particiones clonadas y presentadas en el apartado 3 del actual informe. Para facilitar su lectura, se replica de nuevo su información a continuación.

| Partition name | Hash SHA256 |
|---|---|
| C | 12c1eb545126a540e35987b2a5acbb10e5c5c6984ad2ccd375d15383b47cfca7 |
| INDEX - I | d03bccb17039478b441b3b2b81b8301431d4232ff7caffbc9eb82c52ad0e93cf |
| LOG - G | f3a588eb37f2fdf9bf60b422a24f9cb7235b0a3772aac67850dc4823cb956b7a |
| RDBMS - F | 2e7695860b6e6813252682f27f367f461b8b14b9c91daea165b8abf75d323d7f |
| TEMP - H | 3acd6eda2094f91e98801f2f3022435794745393c60b1d3e342f78b7518534bc |

## Análisis de ficheros eliminados

Durante el proceso de análisis forense y en un primer envite, los peritos deciden analizar posibles archivos eliminados sobre la raíz del sistema operativo (C:). En este sentido, los peritos llevaron a cabo un estudio detallado de los archivos eliminados, empleando para ello herramientas especializadas en recuperación y examen de evidencias digitales.

El primer hallazgo de relevancia es la identificación de una discontinuidad temporal significativa en el conjunto de ficheros recuperados. Se observa que los

últimos registros con fecha datada corresponden al 20 de mayo de 2025, los cuales coincidente con la fecha en la que se procedió al clonado forense de la unidad de almacenamiento, lo cual es obvio. Sin embargo, el anterior bloque de archivos datados retrocede hasta el 16 de febrero de 2024, sin que exista rastro de actividad o archivos con metadatos temporales comprendidos entre ambas fechas.

Para la detección de esta anomalía, todos los archivos eliminados recuperables fueron ordenados de forma descendente atendiendo a sus marcas temporales – fecha de creación, última modificación y último acceso – sin importar su tipo o extensión. Esta estrategia ha permitido evidenciar un vacío temporal de más de un año, hecho que resulta técnicamente atípico en entornos operativos activos y que puede ser indicativo de una posible acción de borrado selectivo, reinstalación del sistema, limpieza de logs o empleo de herramientas de eliminación segura de datos.

El sistema operativo, en su operativa habitual, genera y elimina archivos de forma continua (tales como archivos de sistema, temporales, de actualización, entre otros). Dichos archivos suelen conservar trazabilidad temporal identificable mediante sus metadatos. La ausencia total de esta trazabilidad durante un intervalo tan prolongado refuerza la hipótesis de una posible manipulación o intervención sobre la unidad.

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size |
|---|---|---|---|---|---|---|---|---|
| inf_4660_3 | | | | 2025-05-20 14:27:31 ... | 2025-05-20 14:27:31 ... | 2025-05-20 14:27:06 ... | 2025-05-20 14:27:06 ... | 32 |
| inf_4660_4 | | | | 2025-05-20 14:27:31 ... | 2025-05-20 14:27:31 ... | 2025-05-20 14:27:06 ... | 2025-05-20 14:27:06 ... | 1168 |
| cab_4660_9 | | | | 2025-05-20 14:27:31 ... | 2025-05-20 14:27:31 ... | 2025-05-20 14:27:06 ... | 2025-05-20 14:27:06 ... | 8 |
| 590aee7bdd69b59b.customDestinations-ms~RF71 | | | | 2025-05-20 14:06:35 ... | 2025-05-20 14:21:36 ... | 2025-05-20 14:06:35 ... | 2025-05-20 14:06:35 ... | 5235 |
| [parent folder] | | | | 2025-05-20 15:16:24 ... | 2025-05-20 15:16:24 ... | 2025-05-20 15:16:24 ... | 2025-05-20 12:12:51 ... | 56 |
| [parent folder] | | | | 2025-05-20 15:16:24 ... | 2025-05-20 15:16:24 ... | 2025-05-20 15:16:24 ... | 2025-05-20 12:12:51 ... | 56 |
| [parent folder] | | | | 2025-05-20 14:28:31 ... | 2025-05-20 14:28:31 ... | 2025-05-20 14:28:31 ... | 2025-05-20 12:12:49 ... | 56 |
| [parent folder] | | | | 2025-05-20 14:28:31 ... | 2025-05-20 14:28:31 ... | 2025-05-20 14:28:31 ... | 2025-05-20 12:12:49 ... | 56 |
| 0000000000022319 | | | | 2024-02-16 10:26:02 ... | 2024-03-18 10:31:08 ... | 2024-02-16 10:26:02 ... | 2024-03-18 10:31:08 ... | 1450496 |
| 000000000002231D | | | | 2024-02-16 10:26:02 ... | 2024-03-18 10:31:08 ... | 2024-02-16 10:26:02 ... | 2024-03-18 10:31:08 ... | 1670280 |
| 0000000000022321 | | | | 2024-02-16 10:26:02 ... | 2024-03-18 10:31:08 ... | 2024-02-16 10:26:02 ... | 2024-03-18 10:31:08 ... | 805376 |
| 0000000000022325 | | | | 2024-02-16 10:26:02 ... | 2024-03-18 10:31:08 ... | 2024-02-16 10:26:02 ... | 2024-03-18 10:31:08 ... | 860672 |
| 0000000000022329 | | | | 2024-02-16 10:26:02 ... | 2024-03-18 10:31:08 ... | 2024-02-16 10:26:02 ... | 2024-03-18 10:31:08 ... | 12927 |
| 000000000002232B | | | | 2024-02-16 10:26:02 ... | 2024-03-18 10:31:08 ... | 2024-02-16 10:26:02 ... | 2024-03-18 10:31:08 ... | 14982 |

*Salto temporal en los ficheros eliminados del sistema*

Adicionalmente, el análisis permitió identificar un total de 74.076 archivos eliminados para los que no consta ninguna marca temporal asociada, es decir, sin fecha de creación, acceso o modificación registrada. Esta carencia de metadatos temporales impide llevar a cabo un análisis cronológico sobre dichos elementos, limitando su valor forense individual, aunque su volumen y contexto siguen siendo relevantes para el análisis global del sistema.

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time |
|---|---|---|---|---|---|---|---|
| RegSvcs.exe | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| regsvcs.exe.config | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| ShFusRes.dll | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| SOS.dll | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| sysglobl.dll | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| System.Data.dll | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| System.Data.OracleClient.dll | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| System.Data.SqlXml.dll | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| webengine.dll | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Microsoft.VisualBasic.dll | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Microsoft.Vsa.dll | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |
| Microsoft.Vsa.tlb | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |

*Extracto de ficheros eliminados en la imagen "C" para los que no constan datos temporales*

## Exportación de bases de datos

Durante el análisis forense del sistema identificado como INSESODB, se examinó el historial de ficheros abiertos recientemente con el objetivo de identificar actividades relevantes vinculadas al uso y manipulación de información sensible.

Como resultado de dicho análisis, se detectó la presencia de copias de información de bases de datos alojadas en una unidad externa identificada con la letra “H:”. De ellas se hablará en posteriores apartados.

| | | |
|---|---|---|
| H:\exportDBinseso\DB_DATABLOBDOC_J.txt | 0000-00-00 00:00:00 | /img_C/Users/Administrador.INSESO01/ |
| H:\exportDBinseso\DB_INDEX_I.txt | 0000-00-00 00:00:00 | /img_C/Users/Administrador.INSESO01/ |
| H:\exportDBinseso\DB_LOG_G.txt | 0000-00-00 00:00:00 | /img_C/Users/Administrador.INSESO01/ |
| H:\exportDBinseso\DB_RDBMS_F.txt | 0000-00-00 00:00:00 | /img_C/Users/Administrador.INSESO01/ |
| H:\exportDBinseso\DB_TEMP_H.txt | 0000-00-00 00:00:00 | /img_C/Users/Administrador.INSESO01/ |

*Ficheros recientes de copia de base de datos en el sistema INSESODB con referencias al usuario administrador*

## Identificación de acceso de usuarios a través de marcas temporales en ficheros y cookies

Durante el análisis forense de la imagen del sistema, se ha identificado actividad reciente atribuida al usuario “Antonio Sánchez”, persona de interés en el presente procedimiento, tal y como fue señalado a los auditores por parte del personal entrevistado.

Concretamente, se ha constatado la apertura de múltiples ficheros entre los meses de febrero y marzo de 2025 por parte del mencionado usuario. Dichos

ficheros, atendiendo a la semántica de sus nombres, se encuentran relacionados con la base de datos del sistema Agresso, información que ha sido confirmada por el equipo técnico de INSESO.

| Source Name | S | C | O | URL | Date Accessed | Program Name | Domain | Username |
|---|---|---|---|---|---|---|---|---|
| WebCacheV01.dat | | | | file:///H:/exportDBinseso/Logs_Robocopy/Log_INSESOAPP05_64... | 2025-03-04 13:27:55 CET | Microsoft Edge Analyzer | | AntonioSanchez |
| WebCacheV01.dat | | | | file:///H:/exportDBinseso/Logs_Robocopy/DB_DATABLOBDOC_... | 2025-03-04 13:27:37 CET | Microsoft Edge Analyzer | | AntonioSanchez |
| WebCacheV01.dat | | | | file:///H:/exportDBinseso/Logs_Robocopy/DB_LOG_G.txt | 2025-03-04 13:27:00 CET | Microsoft Edge Analyzer | | AntonioSanchez |
| WebCacheV01.dat | | | | file:///H:/exportDBinseso/exportcomp.log | 2025-02-20 09:42:03 CET | Microsoft Edge Analyzer | | AntonioSanchez |
| WebCacheV01.dat | | | | file:///F:/app/Oracle/product/12.1.0/dbhome_1/BIN/detener_bd.s... | 2025-02-19 13:01:34 CET | Microsoft Edge Analyzer | | AntonioSanchez |
| WebCacheV01.dat | | | | file://insesobck02/robocopy/Data/EXPORTDB/Logs_Robocopy/L... | 2025-02-19 12:58:08 CET | Microsoft Edge Analyzer | | AntonioSanchez |
| WebCacheV01.dat | | | | file:///H:/exportDBinseso/Logs_Robocopy/Log_INSESODB_H.txt | 2025-02-19 12:45:54 CET | Microsoft Edge Analyzer | | AntonioSanchez |
| WebCacheV01.dat | | | | file:///H:/results.txt | 2024-05-14 20:40:06 CEST | Microsoft Edge Analyzer | | carlossanchez |
| WebCacheV01.dat | | | 1 | https://stackoverflow.com/questions/43557776/how-to-connect-... | 2024-02-13 09:10:26 CET | Microsoft Edge Analyzer | stackoverflow.com | AntonioSanchez |
| WebCacheV01.dat | | | | res://iesetup.dll/HardAdmin.htm | 2024-02-13 09:09:05 CET | Microsoft Edge Analyzer | | AntonioSanchez |
| WebCacheV01.dat | | | | res://C:\Windows\system32\mmcndmgr.dll/views.htm | 2019-04-02 08:34:34 CEST | Microsoft Edge Analyzer | | Administrador |
| WebCacheV01.dat | | | | res://C:\Windows\system32\mmcndmgr.dll/views.htm | 2018-11-12 17:58:22 CET | Microsoft Edge Analyzer | | remotebios |
| WebCacheV01.dat | | | | file://insesofs/IntercambioMalaboBata/DN-SOCIEDAD%20GUINE... | 2018-10-09 10:51:49 CEST | Microsoft Edge Analyzer | | Administrador |

*Registro de accesos a ficheros por parte del usuario Antonio Sánchez en febrero y marzo de 2025*

Entre los elementos técnicos analizados se identifica la referencia a la herramienta Robocopy, ampliamente utilizada en entornos técnicos para la transferencia de ficheros entre distintos directorios o servidores, lo que podría indicar acciones orientadas al movimiento o respaldo de la información.

De forma complementaria, el análisis de las cookies almacenadas en el sistema ha permitido constatar la creación de seis cookies de sesión asociadas al usuario Antonio Sánchez el 20 de mayo de 2025 a las 13:51:18.

Web Cookies — 26 Results

Table | Thumbnail | Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

| Source Name | S | C | O | URL | Date Created | Name | Value | Program Name |
|---|---|---|---|---|---|---|---|---|
| 3MPQDZLO.txt | | | 1 | www.bing.com/ | 2025-05-20 13:51:18 CEST | MUIDB | 39A44C57993E66E33AC9587398C467A7 | Internet Explorer Analyzer |
| 0P5VMYVM.txt | | | 1 | ieonline.microsoft.com/ | 2025-05-20 13:51:18 CEST | MUIDB | 18096F7876E3674E0DE07B5C77086677 | Internet Explorer Analyzer |
| LV133RWR.txt | | | 1 | sstatic.net/ | 2025-05-20 13:51:18 CEST | __cf_bm | ryjB00DjAIwS6TUDfEK61MfVj_0kOsID_p55RMyEqWg-1... | Internet Explorer Analyzer |
| TFDQV263.txt | | | 1 | stackoverflow.com/ | 2025-05-20 13:51:18 CEST | prov | 3a8f893b-4a45-4e42-a3c3-c93dbe34b1ec | Internet Explorer Analyzer |
| 6RQENG3I.txt | | | 1 | microsoft.com/ | 2025-05-20 13:51:18 CEST | MUID | 18096F7876E3674E0DE07B5C77086677 | Internet Explorer Analyzer |
| MDS99S1N.txt | | | 1 | bing.com/ | 2025-05-20 13:51:18 CEST | MUID | 39A44C57993E66E33AC9587398C467A7 | Internet Explorer Analyzer |

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 1 of 1 Result — Web Cookies

**Cookie Details**

Domain: bing.com
URL: www.bing.com/
Name: MUIDB
Value: 39A44C57993E66E33AC9587398C467A7
Program Name: Internet Explorer Analyzer

**Dates**

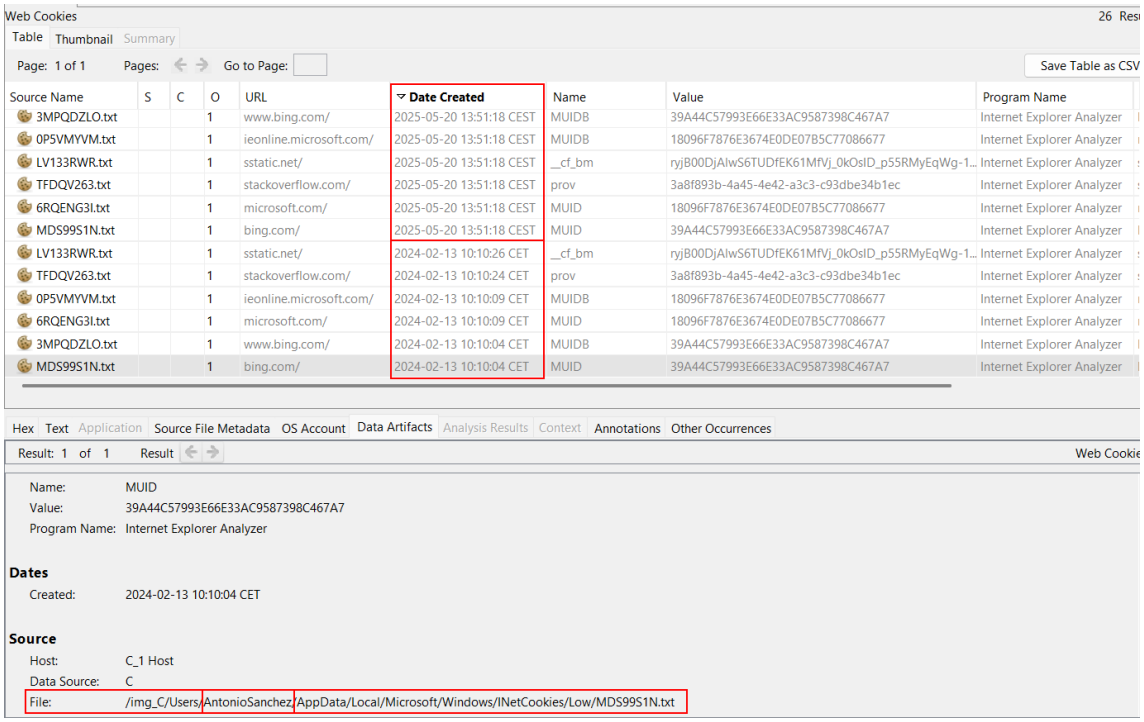
Created: 2025-05-20 13:51:18 CEST

**Source**

Host: C_1 Host
Data Source: C
File: /img_C/$OrphanFiles/Usuarios/AntonioSanchez/Navegadores/IE/Cookies/Low/3MPQDZLO.txt

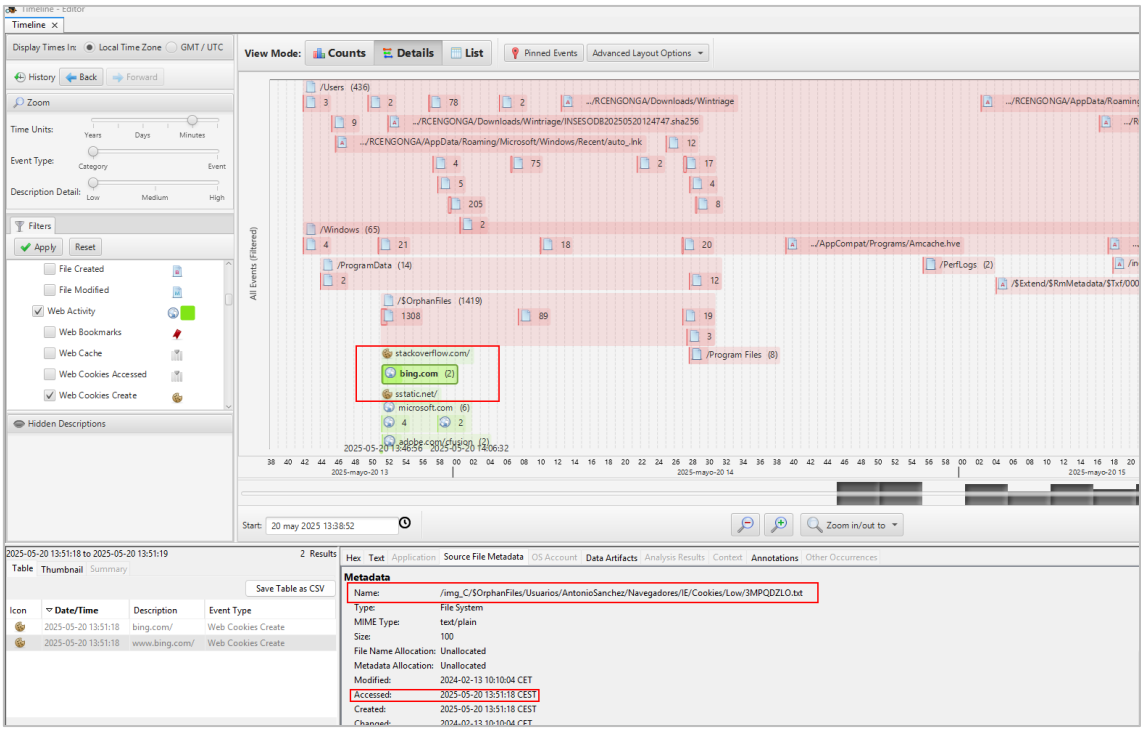
*Cookies de sesión del usuario Antonio Sánchez generadas en mayo de 2025*

Asimismo, se identifican seis cookies adicionales vinculadas al mismo usuario con fecha de 13 de febrero de 2024, observándose que accede a los mismos recursos digitales en ambas fechas, lo que refuerza la correlación entre las sesiones analizadas y su actividad previa.



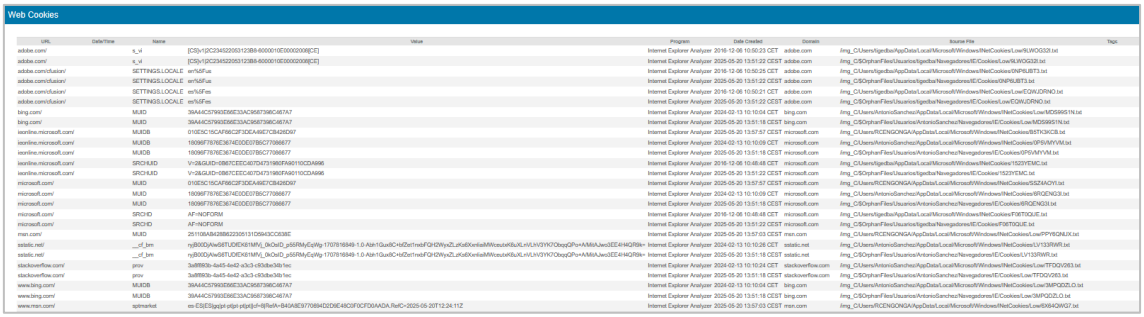

*Cookies del usuario Antonio Sánchez correspondientes a febrero de 2024*

El análisis temporal de eventos correspondiente al día 20 de mayo de 2025 permite observar de manera gráfica la actividad generada, incluyendo el momento exacto de creación de las cookies previamente mencionadas.



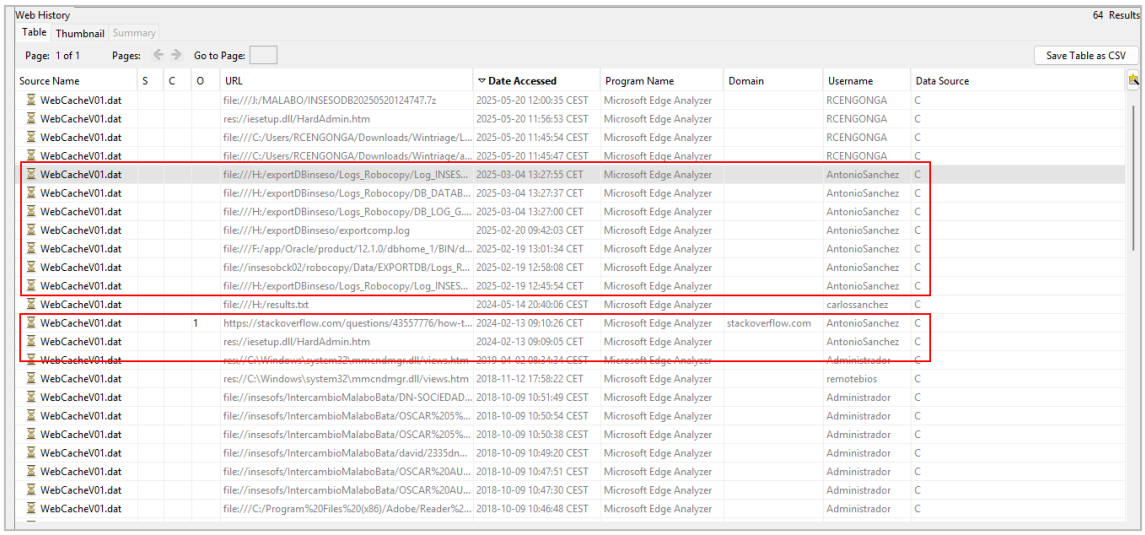
*Línea de tiempo detallada de los eventos relacionados con Antonio Sánchez el 20 de mayo de 2025*

A efectos de exhaustividad, se ha consolidado la información relativa al conjunto completo de cookies de sesión recuperadas a partir de las particiones clonadas, resultando en un total de 26 cookies, datadas entre el 6 de diciembre de 2016 y el 20 de mayo de 2025, lo que permite establecer un marco cronológico amplio de actividad del sistema.

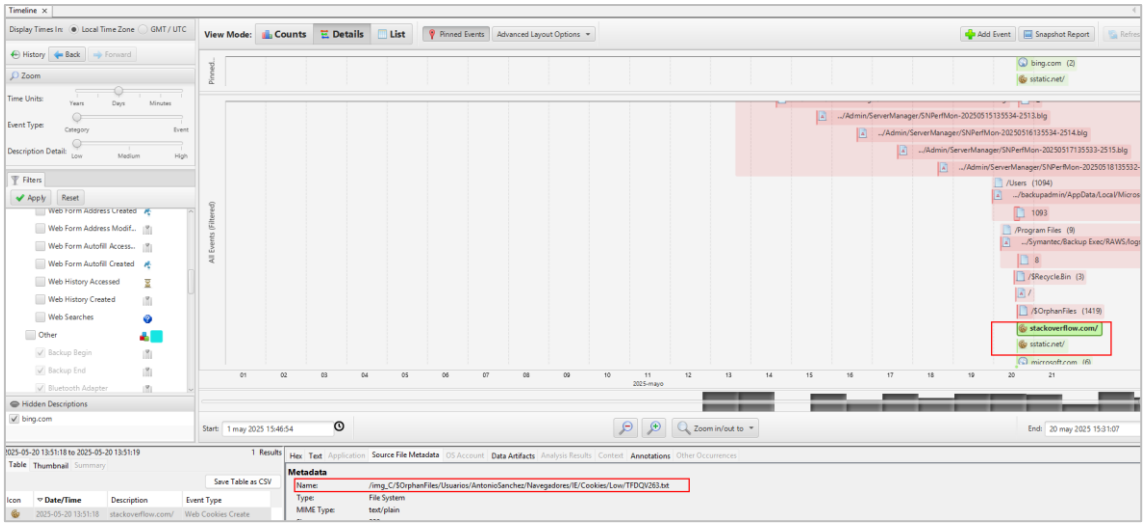


*Relación de la totalidad de cookies de sesión identificadas a lo largo del análisis*

Con el fin de verificar y contextualizar la información obtenida, se ha llevado a cabo un análisis adicional mediante la herramienta forense empleada, utilizando el visor de Historial Web y la función de línea temporal, con lo que se han podido corroborar accesos a recursos web por parte del usuario Antonio Sánchez durante el periodo evaluado.



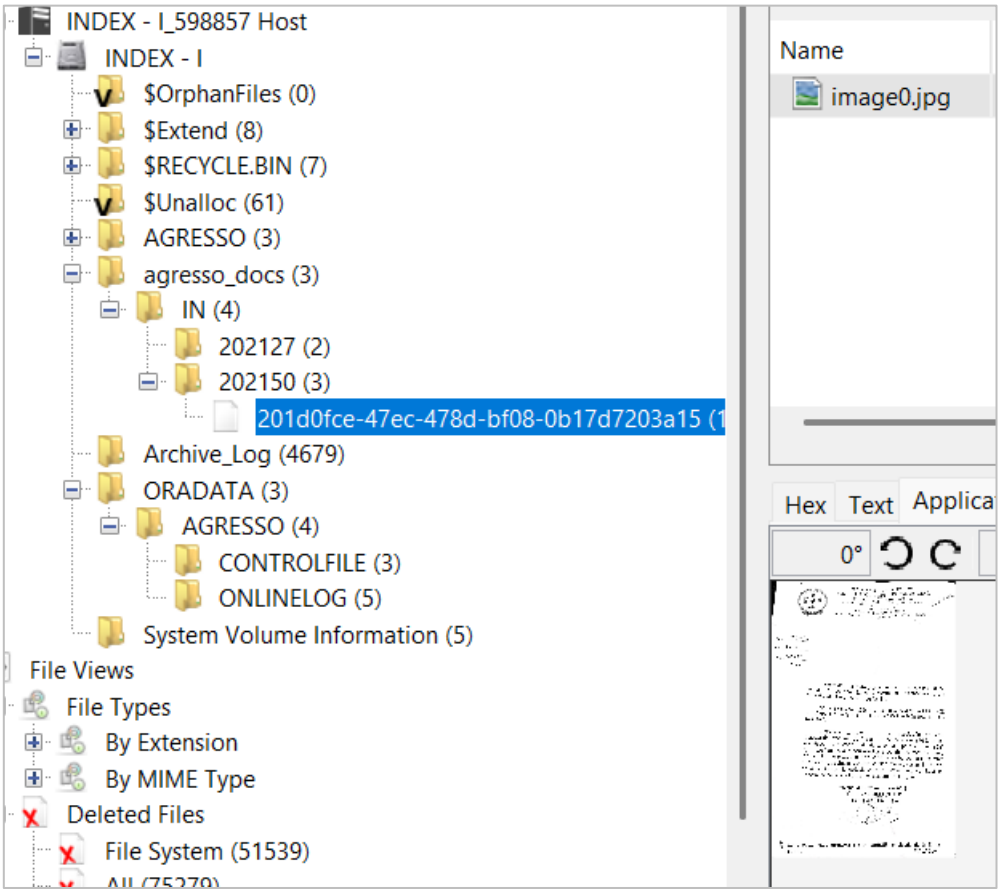

*Ficheros web accedidos por Antonio Sánchez*




*Línea temporal de eventos correspondiente a mayo de 2025, destacando la actividad web del usuario*

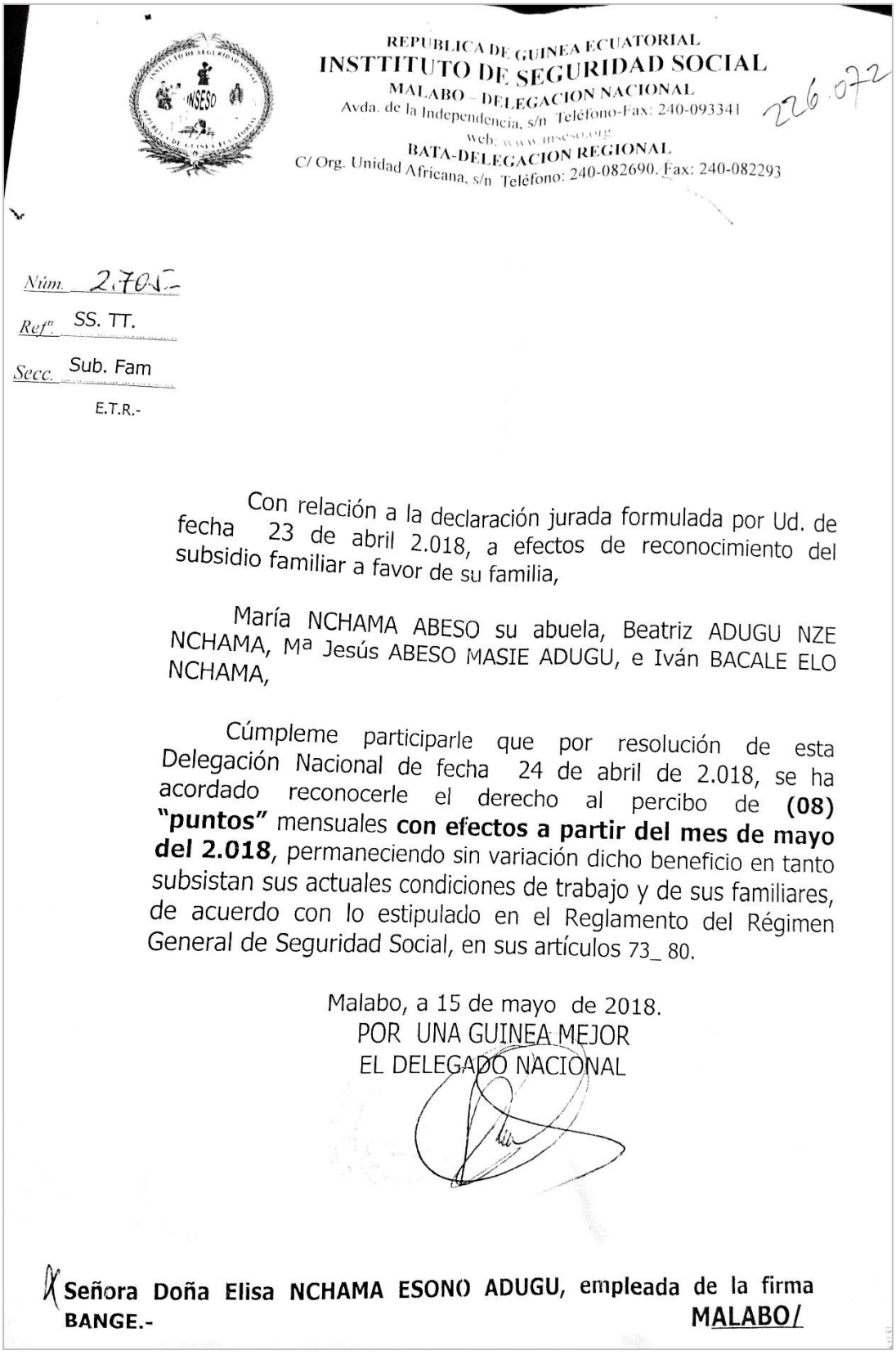
## Imágenes relevantes identificadas

Durante el análisis de la partición identificada como “INDEX – I”, se ha localizado un archivo gráfico de especial relevancia dentro del contexto del análisis pericial. Concretamente, se trata de una imagen digitalizada de una carta oficial, correspondiente a una respuesta emitida por la Delegación Nacional del INSESO en el año 2018, y dirigida a la Sra. María NCHAMA ABESO.




*Ubicación exacta del fichero identificado en la partición “INDEX – I”*

El hallazgo de esta imagen refuerza la existencia de información histórica de carácter institucional y sensible almacenada en el sistema analizado, así como la persistencia de documentos oficiales anteriores a los periodos más recientes de actividad ya descritos.



REPUBLICA DE GUINEA ECUATORIAL
INSTTITUTO DE SEGURIDAD SOCIAL
MALABO – DELEGACION NACIONAL
Avda. de la Independencia, s/n Teléfono-Fax: 240-093341
Web: www.inseso.org
BATA-DELEGACION REGIONAL
C/ Org. Unidad Africana, s/n Teléfono: 240-082690. Fax: 240-082293

226.072

Núm. 2.705
Refª SS. TT.
Secc. Sub. Fam
E.T.R.-

Con relación a la declaración jurada formulada por Ud. de fecha 23 de abril 2.018, a efectos de reconocimiento del subsidio familiar a favor de su familia,

María NCHAMA ABESO su abuela, Beatriz ADUGU NZE NCHAMA, Mª Jesús ABESO MASIE ADUGU, e Iván BACALE ELO NCHAMA,

Cúmpleme participarle que por resolución de esta Delegación Nacional de fecha 24 de abril de 2.018, se ha acordado reconocerle el derecho al percibo de **(08) "puntos"** mensuales **con efectos a partir del mes de mayo del 2.018**, permaneciendo sin variación dicho beneficio en tanto subsistan sus actuales condiciones de trabajo y de sus familiares, de acuerdo con lo estipulado en el Reglamento del Régimen General de Seguridad Social, en sus artículos 73_ 80.

Malabo, a 15 de mayo de 2018.
POR UNA GUINEA MEJOR
EL DELEGADO NACIONAL

**Señora Doña Elisa NCHAMA ESONO ADUGU, empleada de la firma BANGE.-**

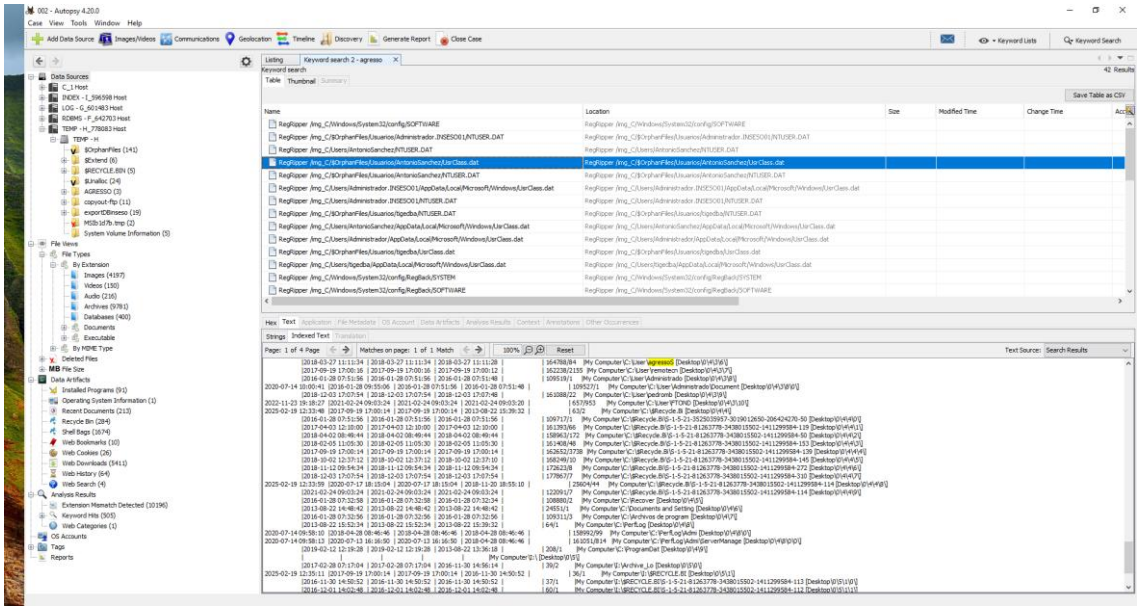
**MALABO/**

*Carta recuperada de la unidad analizada*

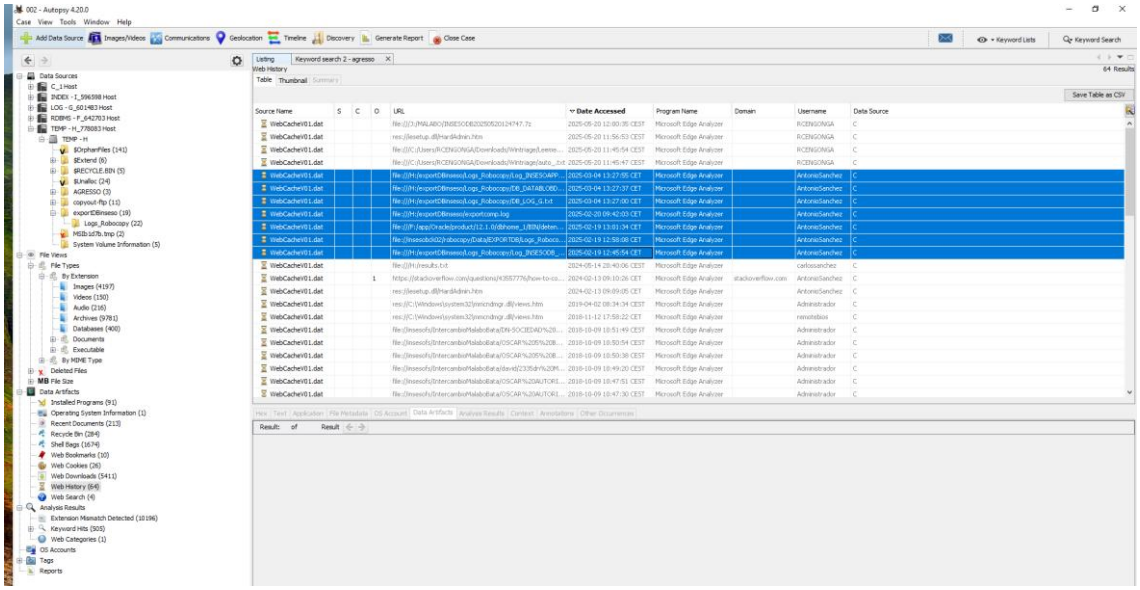
## Revisión de Agresso

Como parte del análisis forense de las evidencias digitales, se ha llevado a cabo una revisión detallada en busca de elementos relacionados con el sistema de gestión empresarial Agresso (actualmente Unit4 ERP). Esta revisión ha abarcado todas las particiones disponibles, rutas de usuario, archivos recientes y estructuras de directorio típicas asociadas al uso de este software en entornos corporativos.

Durante la investigación se han identificado un total de 42 artefactos, es decir, 42 apariciones del texto “agresso” sobre las particiones investigadas:

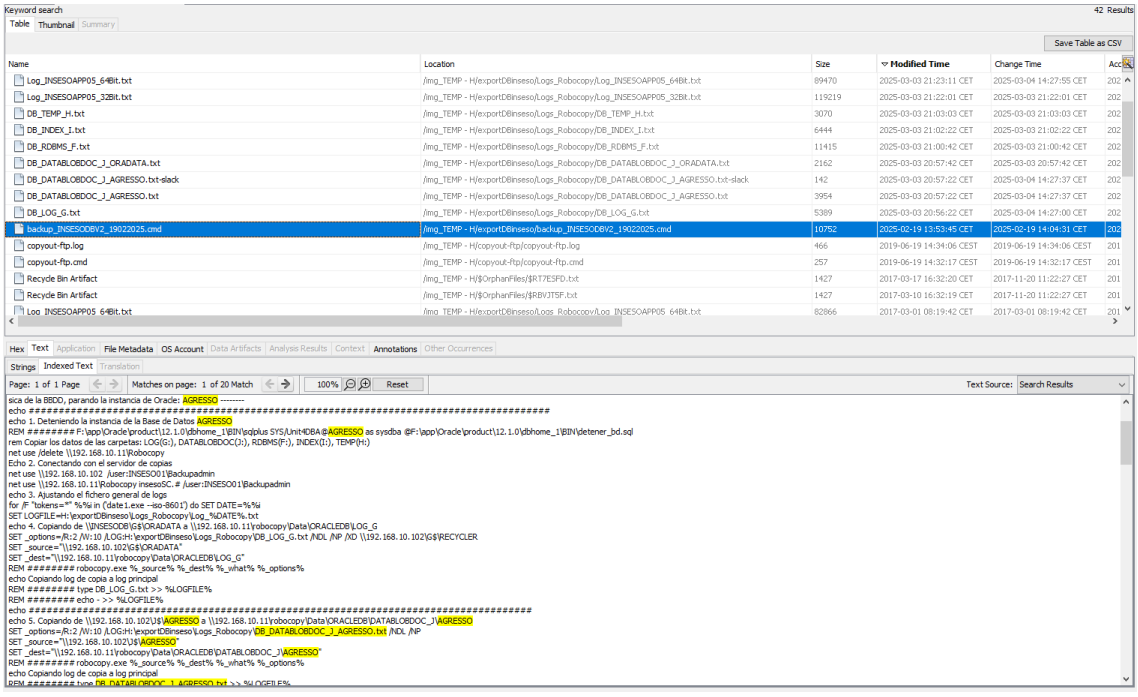


Estas apariciones encajan con las revisadas ya en el historial de webcache, donde se apreciaba un comportamiento inusual entre el 19 de febrero y el 4 de marzo de 2025. Los peritos lo consideran inusual, pues el sistema no manifestaba un uso aparente desde hacía mas de un año y, con anterioridad a ese año, desde hacía 5 años mas.

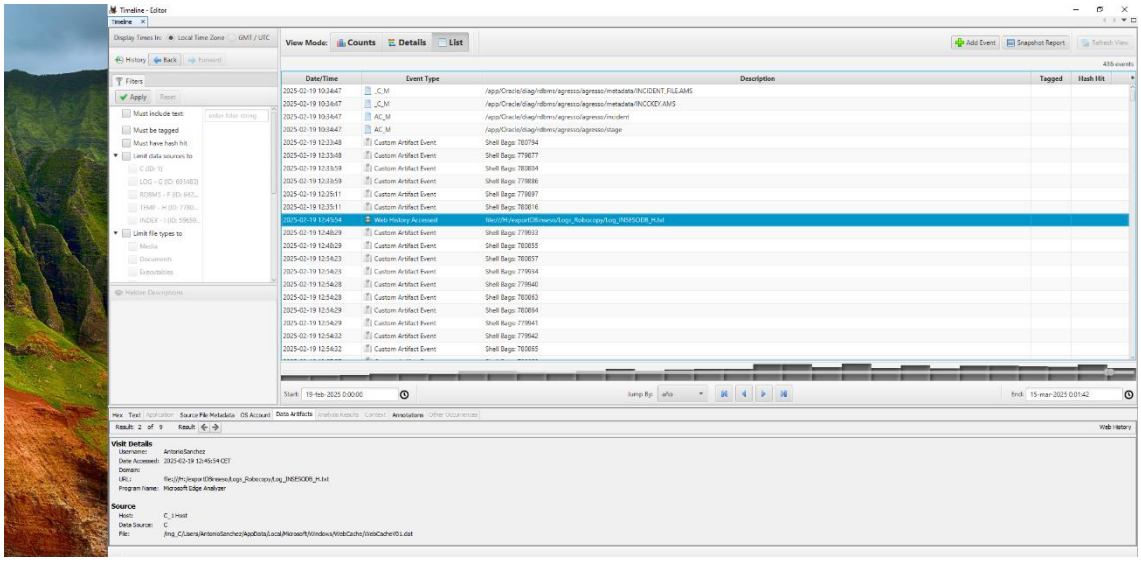


Tal y como se advertía con anterioridad, muchas de las apariciones se corresponden con acciones realizadas por el usuario “Antonio Sánchez” sobre diferentes archivos del sistema Agresso.

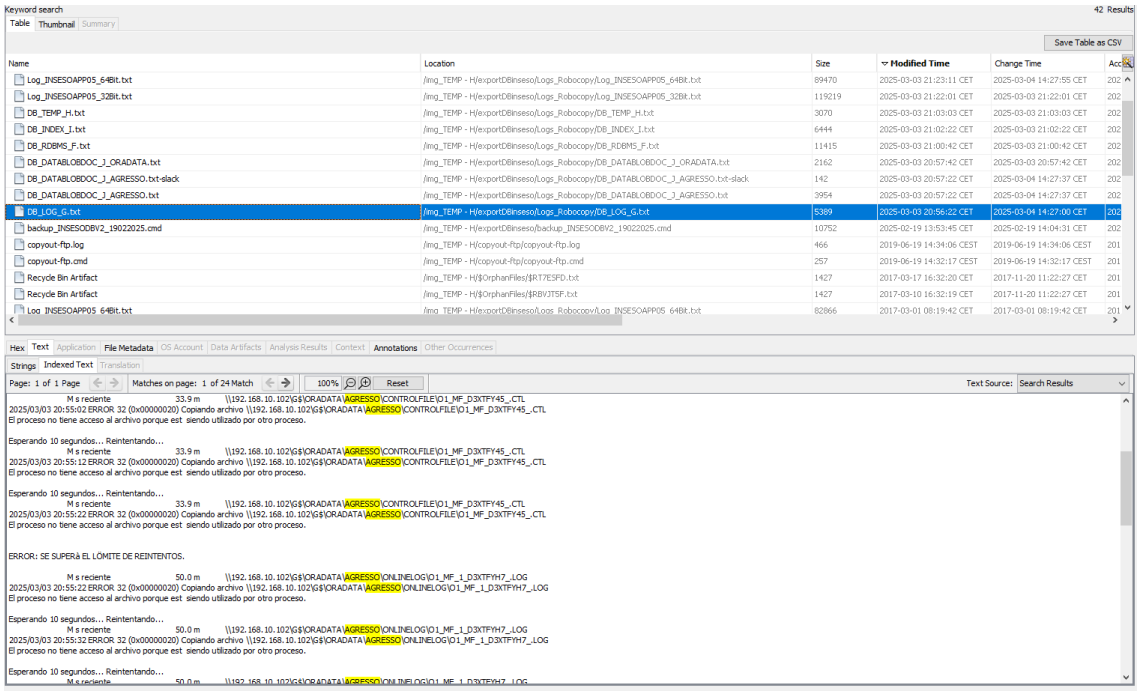
Una particularmente interesante es la acontecida el día 19 de febrero de 2025 a las 13:53h CET, momento en el que el usuario parece solicitar una copia de seguridad de la base de datos del sistema Agresso a través del software Robocopy, anteriormente mencionado.

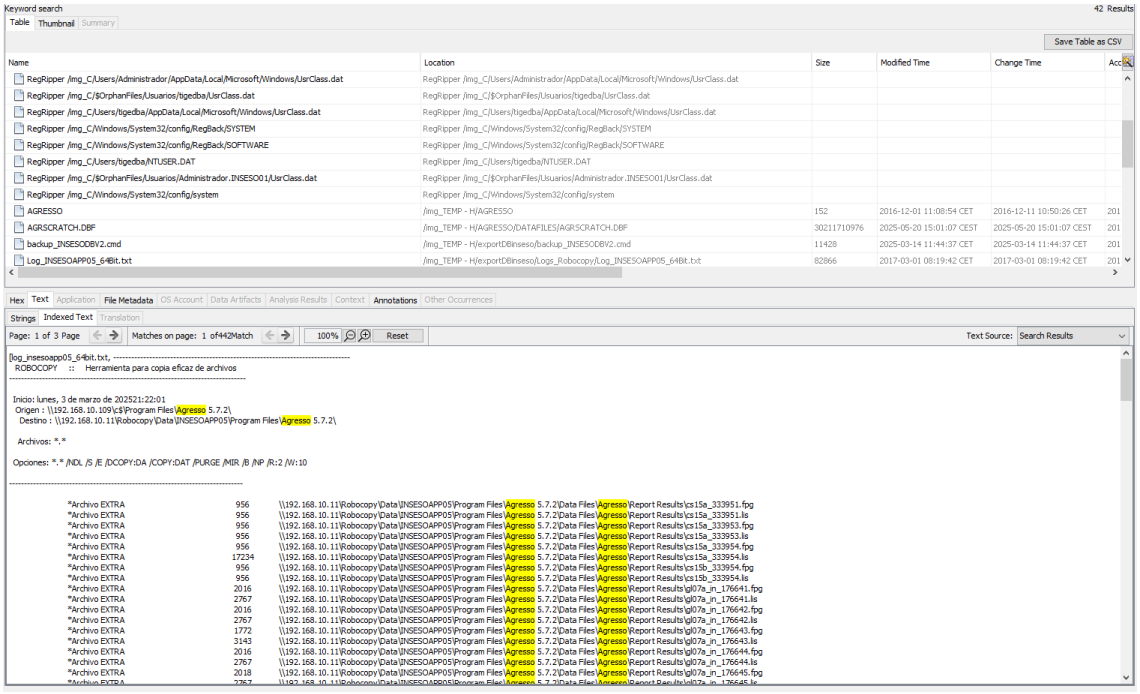


Este comportamiento cuadra con el observado en la línea temporal, donde se aprecia actividad desde la mañana del 19 de febrero de 2025.

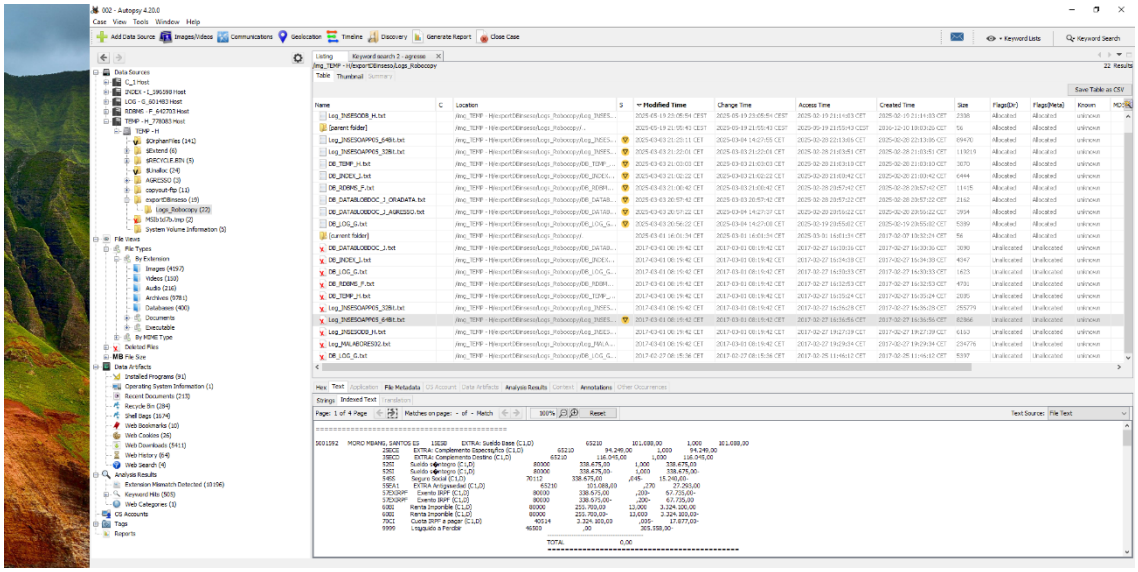


Unos 15 días más tarde, el 3 de marzo de 2025, el sistema vuelve a presentar actividad a última hora de la tarde, a partir de las 20:56h CET.





Como se ha podido verificar a través de archivos antiguos y eliminados pero que han podido recuperarse del proceso de borrado, el sistema contendría los datos relativos al sistema de pensiones, tal y como se puede ver en la siguiente evidencia.



# 6. Análisis GAP frente a estándar

Además del requerimiento forense, el contratante solicitó a los auditores una evaluación inicial, basada en su experiencia y conocimientos especializados en informática y ciberseguridad, con el objetivo de conocer el estado real de la infraestructura analizada. Para realizar esta tarea, se decidió emplear como referencia la metodología *CIS Critical Security Controls*, garantizando así un análisis estructurado y alineado con buenas prácticas reconocidas internacionalmente, basándose únicamente, por las necesidades del proyecto, en la observación, como medio para la toma de información.

Los *CIS Critical Security Controls* son un conjunto de buenas prácticas priorizadas de ciberseguridad diseñadas para proteger sistemas y datos frente a los ciberataques más comunes. Desarrollados por el *Center for Internet Security (CIS)* de Estados Unidos, CIS Controls se estructura en 18 controles agrupados sobre 153 salvaguardas priorizadas según niveles de implementación denominados *Implementation Groups (IG1, IG2 e IG3)*.


El IG1 se centra en medidas esenciales aplicables a PYMES y organizaciones con recursos limitados, IG2 amplía el control en entornos con equipos de TI dedicados y estructuras más complejas, mientras que IG3 incorpora medidas

avanzadas para proteger datos críticos y entornos de alta exposición frente a amenazas sofisticadas. Este es el caso de INSESO, por tratarse de una Administración Pública que opera con datos de índole sanitario/laboral.

Los 18 controles cubren todo el ciclo de protección de la organización: desde la identificación y gestión de activos físicos y software autorizado, la protección de datos en reposo y en tránsito, la configuración segura de sistemas, la gestión de cuentas y privilegios, y la aplicación de parches y gestión de vulnerabilidades de forma continua, hasta la configuración segura de navegadores y correo electrónico, la protección frente a malware, la disponibilidad de copias de seguridad, la segmentación y control de redes, la formación de empleados en seguridad, la gestión de proveedores de servicios, la seguridad en el desarrollo de software, la planificación y ensayo de la respuesta ante incidentes y las pruebas de penetración, incluyendo también la protección de entornos cloud. Este enfoque integral ayuda a las organizaciones a construir una defensa en profundidad, protegiendo capas críticas de su infraestructura de forma ordenada y priorizada.

## Resumen de resultados

El presente apartado detalla los resultados del análisis de brechas de ciberseguridad (análisis GAP) realizado en el Instituto Nacional de Seguridad Social (INSESO) mediante el modelo CIS Controls. Dado que INSESO maneja datos sanitarios altamente sensibles (expedientes médico-laborales y datos personales de ciudadanos), se considera que debe adherirse al Grupo de Implementación 3 (IG3), el nivel más exigente de los controles CIS, lo que implica implementar todos los controles de los grupos IG1, IG2 e IG3

En entornos IG3, que incluyen a las Administraciones Públicas en general, y a las organizaciones del sector salud y social, que manejan información crítica, en particular, los ataques exitosos pueden causar un perjuicio significativo al bienestar público, subrayando la importancia de alcanzar un nivel de seguridad robusto. Actualmente, la situación de ciberseguridad en INSESO es alarmante. Los sistemas tecnológicos son obsoletos, carecen de mantenimiento adecuado y el personal con el que se han mantenido diferentes entrevistas no cuenta con capacitación ni conocimientos en seguridad, probablemente, por no ser este su cometido. Esta situación conlleva un incumplimiento casi total de los controles CIS. Si bien no es un caso aislado, dado que la media de incumplimiento en el sector, que aún sigue contando con sistemas legacy, se eleva al 73%, la situación de INSESO es particularmente preocupante y requiere de acciones tajantes e inmediatas.

En consecuencia, la falta de controles básicos en INSESO lo deja expuesto a potenciales incidentes graves, como filtraciones de datos de ciudadanos, interrupciones de servicio o ataques de ransomware que podrían paralizar los servicios del país. Este hecho fue comprobado in-situ durante el proceso de auditoría, cuando por un ciberataque sufrido en directo, los sistemas cayeron y no pudieron ser restablecidos hasta pasados varios días.

A continuación, se presenta el análisis detallado por cada uno de los 18 Controles CIS, describiendo la situación encontrada (brechas o deficiencias identificadas) y las recomendaciones para remediarlas. El objetivo es brindar a INSESO un plan de acción priorizado para elevar su nivel de ciberseguridad desde un estado actual deficiente hasta un cumplimiento adecuado de las mejores prácticas internacionales.

## Evaluación frente a CIS Controls

### *Control 1: Inventario y control de activos empresariales*

Con la información compartida con el equipo auditor se puede apreciar que INSESO no dispone de un inventario completo y actualizado de sus activos tecnológicos (equipos, dispositivos, servidores, dispositivos de red, etc.). Se han identificado equipos antiguos y no registrados oficialmente, se ha comprobado que no recibieron actualizaciones, ni mantenimiento, en años. Esta falta de visibilidad impide saber con certeza qué dispositivos están conectados a la red y si son autorizados o seguros. Este incumplimiento es crítico, pues “no se puede proteger lo que no se conoce”. Sin un inventario confiable, muchos activos podrían quedar fuera de las medidas de seguridad, sirviendo como puerta de entrada para atacantes o propagando malware inadvertidamente.

Se recomienda establecer de inmediato un inventario centralizado de todos los activos de TI. Esto implica identificar, registrar y etiquetar cada dispositivo físico o virtual de la red, incluyendo sus características (modelo, sistema operativo, ubicación, propietario responsable). El inventario debe mantenerse actualizado de forma continua, añadiendo nuevos activos cuando se incorporen y dando de baja los que se retiren. Asimismo, se recomienda implementar herramientas automatizadas de descubrimiento de activos para detectar cualquier dispositivo conectado no autorizado y tomar acción al respecto. Con un inventario robusto, INSESO podrá monitorizar y gestionar sus activos efectivamente, y eliminar o aislar aquellos dispositivos obsoletos o no autorizados que representen un riesgo inmediato.

### *Control 2: Inventario y control de activos de software*

No existe tampoco un inventario integral del software en uso. En la actualidad, y por las pesquisas recabadas durante los trabajos, se aprecia que el personal instala y utiliza diversas aplicaciones sin medidas específicas de control. Es mas, el equipo auditor pudo comprobar cómo era posible instalar aplicaciones sin necesidad de disponer de permisos especiales. Hay sistemas operativos Windows obsoletos y aplicaciones sin parches, así como programas no autorizados ejecutándose en equipos del entorno. Esta falta de control de software facilita la presencia de software desactualizado con vulnerabilidades conocidas y la instalación de aplicaciones maliciosas o piratas. Solo el personal local conoce qué programas utilizan, lo que dificulta garantizar que solo software aprobado y seguro esté presente.

Se recomienda realizar un inventario de software en todos los equipos, listando los sistemas operativos y aplicaciones instaladas. A partir de este inventario, definir un catálogo de software autorizado para las funciones de la institución sanitaria. Se deben desinstalar o bloquear los programas que no estén en la lista aprobada o que resulten obsoletos/inseguros. Adicionalmente, implementar políticas de control de instalaciones: por ejemplo, restringir permisos de instalación solo al área de TI o usar herramientas de gestión de parches y distribución de software para asegurar que todos los sistemas ejecuten solo versiones aprobadas. Este control ayudará a identificar software no gestionado o malicioso a tiempo, previniendo su ejecución no autorizada.

### *Control 3: Protección de datos*

INSESO maneja volúmenes significativos de datos sensibles de la ciudadanía. En los resultados de los análisis realizados se ha podido acceder a documentos personales relacionados con las pensiones de ciudadanos del país, tal y como se ha evidenciado en apartados anteriores, sin embargo, carece de políticas y mecanismos adecuados para proteger dichos datos. No existe una clasificación de la información por nivel de sensibilidad; muchos datos confidenciales se almacenan sin cifrado en servidores antiguos o incluso en PCs locales. Asimismo, no hay controles para limitar el acceso a la información según roles: personal no autorizado podría potencialmente acceder a expedientes debido a configuraciones permisivas o uso compartido de cuentas. Tampoco se han definido procedimientos claros de retención y eliminación segura de datos (por ejemplo, historiales antiguos podrían conservarse indefinidamente en sistemas sin medidas de protección).

Se recomienda desarrollar una política integral de protección de la información. Como primer paso, clasificar los datos en categorías (por ejemplo: público, interno, confidencial, altamente confidencial) según su criticidad y sensibilidad, priorizando los datos de pacientes como altamente confidenciales. En base a esta clasificación, implementar medidas adecuadas: cifrado de datos sensibles tanto en reposo (en discos, bases de datos) como en tránsito (comunicaciones internas y externas), controles de acceso estrictos (ver Control 6) para que solo el personal autorizado según su rol pueda ver información médica, y registro de accesos a datos sensibles para auditoría. Además, establecer políticas de retención y eliminación segura de datos: definir cuánto tiempo conservar distintos tipos de información sanitaria y asegurarse de borrar o anonimizar datos cuando ya no se necesiten, cumpliendo con normativas de privacidad. Por último, concienciar al personal sobre la importancia de proteger la confidencialidad de la información de la ciudadanía y establecer sanciones o medidas disciplinarias ante accesos o divulgaciones indebidas.

### *Control 4: Configuración segura de activos y software de la empresa*

Los sistemas operativos y aplicaciones en INSESO no siguen configuraciones de seguridad estándares. Los sistemas analizados mantienen configuraciones predeterminadas de fábrica o presentan ajustes inseguros. Por ejemplo, se han hallado contraseñas por defecto, servicios innecesarios corriendo en servidores, y ausencia de directivas de endurecimiento (hardening). La falta de una configuración segura y consistente significa que los sistemas son más vulnerables a explotación: servicios abiertos pueden ser aprovechados por atacantes, y configuraciones débiles (p.ej., protocolos obsoletos habilitados, puertos abiertos sin control) amplían la superficie de ataque. En la situación actual, no se aplican guías de mejores prácticas ni estándares tipo CIS Benchmarks o similares para asegurar la configuración de la infraestructura.

Se recomienda adoptar estándares de configuración segura para todos los activos. Se sugiere utilizar guías reconocidas (como los CIS Benchmarks específicos para Windows, Linux, dispositivos de red, bases de datos, etc.) y adaptar sus recomendaciones a la realidad de INSESO. Con base en ello, configurar cada sistema de forma segura: deshabilitar o desinstalar servicios y software innecesarios, cerrar puertos no requeridos, establecer contraseñas robustas y únicas para cuentas de administración en dispositivos, aplicar políticas estrictas de bloqueo de pantalla, reglas de firewall local, etc. Es importante mantener un procedimiento documentado de hardening para nuevos sistemas antes de ponerlos en producción, así como revisar periódicamente la configuración de sistemas existentes para corregir desviaciones. Asimismo,

implementar un proceso de gestión de cambios para que cualquier modificación significativa en la configuración pase por revisión y aprobación del área de seguridad. Con estos pasos, los activos de la organización estarán menos expuestos y más resistentes frente a ataques comunes que explotan configuraciones débiles o por defecto.

### *Control 5: Gestión de cuentas (identidades y credenciales)*

La administración de cuentas de usuario en INSESO es deficiente. Si bien existe un Directorio Activo, no se utiliza ningún Sistema de Gestión de Identidades tipo Cyberark, Ironchip o similar, para el aprovisionamiento o baja de cuentas que, en cascada, retiren permisos sobre todos los sistemas y aplicaciones. Se observaron casos de cuentas compartidas (varias personas utilizando la misma cuenta genérica, incluso cuentas con privilegios administrativos), lo cual dificulta la trazabilidad y aumenta el riesgo de usos indebidos. Asimismo, hay cuentas antiguas de empleados que ya no trabajan allí, pero siguen activas en los sistemas, representando potenciales brechas si sus credenciales son aprovechadas por terceros. Este hecho provocó un incidente durante la presencia de los auditores, quienes tuvieron que intervenir dando apoyo al personal local para retirar los permisos de acceso remoto a un antiguo empleado que logró conectarse desde fuera de la red para eliminar, aparentemente, evidencias del sistema.

A grandes rasgos, no se emplean principios de mínimo privilegio a la hora de crear cuentas: algunos usuarios tienen más permisos de los necesarios para sus funciones.

Se recomienda implementar una política de gestión de identidades. Esto incluye procedimientos para la creación, modificación y eliminación oportuna de cuentas de usuario. Cada cuenta debe estar asociada a una persona específica (evitar cuentas genéricas compartidas) y asignar únicamente los privilegios necesarios para su rol. Se recomienda actualizar y afinar el Active Directory actual.

Asimismo, se recomienda establecer un proceso de revocación. Cuando un empleado deje la organización o cambie de puesto, sus cuentas deben deshabilitarse o ajustarse inmediatamente. Realizar auditorías periódicas de cuentas para detectar y eliminar cuentas inactivas o huérfanas. Todas las cuentas administrativas deben ser cuidadosamente gestionadas, idealmente separando las cuentas de uso diario de las cuentas con privilegios elevados (cada administrador debería tener su cuenta normal y otra distinta para tareas administrativas). Estas medidas aseguran que solo personas autorizadas tengan

acceso a los sistemas y se reduce el riesgo de acceso indebido mediante cuentas abandonadas o mal gestionadas.

### *Control 6: Gestión de control de accesos (credenciales y privilegios)*

INSESO carece de un control estricto sobre quién tiene acceso a qué sistemas y datos. Actualmente, muchos usuarios utilizan contraseñas débiles y reutilizadas, sin mecanismos de verificación adicional. No se ha implementado autenticación multifactor (MFA) en ningún sistema crítico; el acceso remoto a correos o sistemas internos se realiza solo con usuario y contraseña, lo que facilita compromisos ante robo de credenciales. Tampoco existen roles y perfiles de acceso bien definidos: algunos usuarios cuentan con privilegios administrativos o de amplia accesibilidad sin justificación, rompiendo el principio de mínimo privilegio. Esta situación de controles de acceso laxos aumenta enormemente el riesgo de brechas: muchas intrusiones se originan precisamente por credenciales expuestas o controles de acceso inadecuados.

Se recomienda fortalecer la gestion de accesos y privilegios. En primer lugar, definir roles de usuario con privilegios delimitados según funciones (por ejemplo: funcionarios que den servicio de cara al público, equipo administrativo interno, equipo de IT/Informática, etc.).

Asimismo, se recomienda implementar autenticación multifactor en todos los sistemas posibles, especialmente para accesos remotos o a información sensible, de forma que además de la contraseña se requiera un segundo factor (token, app móvil, etc.). Esto dificulta enormemente que un atacante use credenciales robadas.

Se deben establecer políticas de contraseñas robustas (longitud mínima, complejidad, caducidad periódica) y educar al personal para no reutilizar contraseñas corporativas en otros servicios. Adicionalmente, se debe aplicar el principio de privilegio mínimo, es decir, revocar accesos o privilegios que no sean indispensables; por ejemplo, los usuarios finales no deberían tener derechos de administrador local en sus equipos a menos que sea necesario.

Se debería de implantar una herramienta de gestión de accesos privilegiados (PAM) que permitiera controlar cuentas de alto nivel (como las de administradores de sistemas) con bóveda de contraseñas y registro de uso.

Finalmente, se debe llevar a cabo revisiones de permisos regularmente, para detectar y corregir acumulación indebida de privilegios. Estas acciones reducirán drásticamente las posibilidades de escalada de privilegios o uso de cuentas comprometidas en ataques, cerrando una vía común de brechas de seguridad.

### *Control 7: Gestión continua de vulnerabilidades*

Actualmente INSESO no realiza análisis de vulnerabilidades ni tiene un programa de gestión de parches eficaz. Múltiples sistemas operativos y aplicaciones se encuentran sin actualizar, con parches de seguridad pendientes desde hace meses o años. Debido a la antigüedad del parque tecnológico, en los equipos a los que ha tenido acceso el equipo auditor se han observado versiones fuera de soporte que ya no reciben actualizaciones, lo que deja vulnerabilidades abiertas permanentemente. No se monitorizan de forma proactiva los avisos de nuevas vulnerabilidades ni se evalúa el nivel de riesgo en la infraestructura. Esta situación es extremadamente peligrosa pues los atacantes suelen escanear internet en busca de sistemas con vulnerabilidades conocidas para explotarlos rápidamente.

### *Control 8: Gestión de registros de auditoría (logs)*

La institución no cuenta con una estrategia de manejo de logs de seguridad. Muchos sistemas tienen la auditoría de eventos deshabilitada o funcionando con configuraciones por defecto de bajo detalle. En los casos donde se generan registros, no existe una centralización: los logs quedan almacenados localmente en cada equipo o dispositivo de red, y rara vez son revisados. Tampoco se han definido alertas para detectar eventos anómalos. En la práctica, si ocurriera una intrusión o actividad maliciosa, es muy probable que pase inadvertida, ya que nadie está monitoreando los eventos de seguridad. Además, la ausencia de logs centralizados dificultaría enormemente investigar un incidente después de ocurrido, al no tener evidencias recopiladas. Por ejemplo, intentos de acceso no autorizados, movimientos laterales en la red o exfiltración de datos podrían no dejar rastro detectable en la situación actual.

Como se ha comprobado durante los trabajos realizados, hubo varios intentos, algunos, exitosos, de borrar logs del sistema, al carecerse de copia de los mismos en un sistema redundado (espejo).

Se recomienda desplegar una solución de gestión centralizada de logs (como un SIEM – Security Information and Event Management – o al menos un servidor central de syslog) para recopilar y correlacionar los registros de todos los sistemas críticos: servidores, estaciones, dispositivos de red, aplicaciones clave, etc. Configurar cada activo para que envíe sus eventos relevantes de seguridad a esta plataforma central. Asimismo, definir qué eventos son importantes de auditar (ej. inicios de sesión exitosos y fallidos, cambios de configuraciones, acceso a datos sensibles, arranque/parada de servicios importantes, etc.) y habilitar la generación de dichos logs en los sistemas (ajustar las políticas de

auditoría del sistema operativo y aplicaciones). Una vez centralizados los datos, establecer alertas automáticas ante eventos sospechosos (por ejemplo, múltiples intentos fallidos de login, escalamiento de privilegios, transferencias masivas de datos fuera de horario, etc.) de forma que el personal de TI sea notificado inmediatamente y pueda investigar.

También es necesario asignar responsabilidad para revisar periódicamente los logs consolidados y así detectar patrones o incidentes que las alertas automáticas no capturen. Finalmente, almacenar los logs por un período adecuado (varios meses al menos) para poder hacer análisis forense si se descubre tardíamente una brecha. Con estas acciones, INSESO podrá detectar e incluso anticipar incidentes de seguridad que antes pasarían desapercibidos, mejorando significativamente su capacidad de respuesta.

### *Control 9: Protecciones de correo electrónico y navegadores web*

El vector email y la navegación web suponen una de las mayores superficies de ataque en las organizaciones en general. Si bien este control no ha podido revisarse por encontrarse fuera del alcance de los trabajos, por las informaciones transmitidas a los auditores en las diferentes entrevistas, el estado de ellas sería de tipo inicial, es decir, disponen de margen de mejora.

Se recomienda realizar una evalución técnica de seguridad de ambos entornos con el fin de poder disponer de una fotografía realista de su situación.

A nivel general, en el correo electrónico se debería de implementar un gateway de seguridad de correo o servicios en la nube equivalentes, que incluyan filtrado de spam, detección de intentos de phishing y análisis de adjuntos para bloquear malware conocido (e incluso análisis en sandbox de adjuntos sospechosos). Configurar políticas de correo como DMARC, DKIM y SPF para reducir la suplantación de dominios en emails. Capacitar a los usuarios (ver Control 14) para que sepan identificar correos maliciosos, pero apoyados por herramientas automáticas que eliminen la mayoría de esas amenazas antes de llegar a la bandeja de entrada. Para la navegación web, considerar la instalación de un proxy filtrante o firewall con filtrado web que bloquee el acceso a sitios maliciosos o no relacionados con el trabajo. A nivel de cada equipo, mantener los navegadores actualizados a sus últimas versiones y con las configuraciones de seguridad adecuadas: habilitar listas de bloqueo de sitios reportados como peligrosos (muchos navegadores ya lo incorporan), deshabilitar complementos obsoletos (ej: Flash, Java, si aún estuvieran presentes), y quizás instalar extensiones de seguridad (como bloqueadores de anuncios maliciosos). También sería recomendable activar políticas de restricción de descarga de ciertos tipos

de archivos desde Internet, o al menos inspeccionarlos con el antivirus corporativo. Estas medidas combinadas reducirán la probabilidad de que un empleado sea víctima de phishing o que sin querer descargue código malicioso al navegar.

### *Control 10: Defensas contra malware*

En la actualidad, la protección antimalware en INSESO es insuficiente. Se requiere de una tecnología moderna y actualizada, con gestión centralizada. Tampoco existe un sistema de monitorización de posibles infecciones. Por norma general, la institución depende de que los usuarios noten comportamientos anómalos o mensajes de alerta por defecto. Dado el panorama descrito (sistemas sin parches, usuarios sin capacitación, filtrado de correos deficiente), la probabilidad de infección por virus, ransomware u otro malware es alta. Sin defensas adecuadas, un código malicioso podría propagarse por la red sin ser detenido, infectando múltiples equipos y causando un incidente mayor. Por ejemplo, la ausencia de control de dispositivos USB también puede permitir que malware ingrese vía memorias extraíbles infectadas sin ningún obstáculo.

Se recomienda establecer una estrategia integral de defensa antimalware. Esto implica adquirir e instalar software de seguridad endpoint en todos los equipos (estaciones de trabajo y servidores) que ofrezca protección en tiempo real contra virus, spyware, ransomware y otras amenazas. Idealmente, optar por una solución de clase empresarial administrada centralmente, como pueda ser Coro Security o tecnologías similares, de modo que el área de TI pueda asegurarse de que todos los sistemas estén protegidos, recibir alertas inmediatas de detecciones y generar reportes de estado.

Se debe configurar ese software para que realice análisis completos periódicos y, muy importante, que mantenga actualizadas sus firmas o bases de datos de amenazas diariamente. Adicionalmente, complementar con herramientas de detección más avanzadas (EDR - Endpoint Detection & Response) si el presupuesto lo permite, para detectar comportamientos anómalos que pudieran indicar malware desconocido.

Otra medida a aplicar es el control de los dispositivos extraíbles: se puede habilitar la verificación automática de USBs y otras unidades al conectarse, o incluso restringir su uso si no es necesario. Junto con las soluciones tecnológicas, se deben reforzar las políticas. En general, prohibir la descarga y ejecución de software no autorizado (relacionado con el Control 2) y asegurarse de que los usuarios sepan notificar inmediatamente al equipo de TI si observan algún indicio de infección (mensajes sospechosos, lentitud extrema, comportamientos

inusuales en sus equipos). Con una combinación de antivirus actualizado, monitorización central y buenas prácticas de usuario, el riesgo de infecciones masivas de malware se reducirá considerablemente y se podrá contener rápidamente cualquier foco que aparezca.

### *Control 11: Recuperación de datos*

Uno de los hallazgos más críticos es la ausencia de un sistema confiable de copias de seguridad (backups) para la información y sistemas clave. Actualmente, las copias de datos se realizan de manera ad-hoc (por ejemplo, algunos técnicos hacen respaldos manuales esporádicos en discos externos), pero no existe una política institucional de backup ni procedimientos documentados de recuperación. No hay certeza de que todos los datos críticos (historias, bases de datos administrativas, expedientes de personal, etc.) estén siendo respaldados regularmente. Esta situación significa que ante una falla grave de hardware, un error humano o un ataque como ransomware que cifre los datos, INSESO podría perder información esencial o interrumpir sus servicios por tiempo prolongado.

En los trabajos realizados si que se ha localizado una tecnología de backup del fabricante Symantec, pero que parece no presentar actividad desde el año 2016.

Adicionalmente, no se han observado evidencias de que estén siendo realizadas pruebas de restauración pues el personal local no fue capaz de recuperar los sistemas tras sufrir un incidente de seguridad hasta pasados varios días; por tanto, aunque existan algunos respaldos aislados, no se sabe si serían restaurables con éxito en caso de emergencia.

Por tanto, la falta de planes de continuidad y recuperación pone en riesgo la capacidad del sistema sanitario-social de Guinea para retomar operaciones tras un incidente.

Se recomienda diseñar e implementar de inmediato un plan de copias de seguridad y recuperación robusto. Identificar primero qué datos y sistemas son críticos (priorizando bases de datos de pacientes, sistemas de gestión hospitalaria, etc.) y establecer para ellos políticas de respaldo frecuentes (diarias o semanales según la criticidad y tasa de cambio de los datos). Seleccionar e implementar una solución de backup centralizada que automatice la copia de seguridad de servidores y datos esenciales, almacenando los respaldos en ubicaciones seguras. Es fundamental mantener copias de seguridad offline o fuera de la red principal (por ejemplo, en cintas magnéticas, almacenamientos externos desconectados o servicios cloud seguros) para que, si ocurre un ataque tipo ransomware, las copias no se vean afectadas.

Se deben documentar procedimientos de restauración y realizar pruebas periódicas de recuperación para validar que los backups pueden restaurarse correctamente dentro de los tiempos requeridos. Este plan de recuperación de datos debe enmarcarse dentro de un Plan de Continuidad del Negocio más amplio, asegurando que la organización pueda volver a funcionar tras un incidente grave. En la priorización de acciones, la recuperación de datos es fundamental: ningún entorno está libre de riesgo al 100%, por lo que disponer de backups efectivos es el último recurso que garantiza la continuidad operativa tras un ataque.

### *Control 12: Gestión de la infraestructura de red*

Por lo que se ha podido chequear, la red de INSESO presenta debilidades estructurales en su diseño y mantenimiento. Los dispositivos de infraestructura (enrutadores, switches, etc.) son en su mayoría antiguos y no han recibido actualizaciones de firmware en mucho tiempo. La segmentación de la red es prácticamente inexistente: la red interna es relativamente plana, con sistemas comunicándose sin restricción, lo que facilita que un atacante o malware que comprometa un equipo se desplace lateralmente por toda la red. Tampoco hay un inventario claro de los componentes de red ni se gestionan activamente las configuraciones (no hay copias de seguridad de configuraciones de routers, por ejemplo). Esta falta de gestión deja la infraestructura vulnerable a caídas o ataques: una mala configuración o un ataque a un punto de la red podría derribar comunicaciones críticas.

Se recomienda aplicar buenas prácticas de administración de la red. En primer lugar, actualizar o reemplazar los equipos de red obsoletos que no puedan ser asegurados. Para todos los dispositivos (routers, switches, APs), cambiar cualquier contraseña por defecto y usar credenciales únicas y robustas; además, restringir el acceso de administración de estos equipos solo a direcciones IP de la red de gestión de TI. Implementar una segmentación de la red por zonas o VLANs: por ejemplo, separar la red de administración, la red de equipos que den soporte a la red de INSESO distribuida por el país, la red de usuarios generales y la red de invitados/público. Cada segmento debe comunicarse con otros solo cuando sea necesario y a través de reglas controladas (posiblemente mediante un firewall interno). De esta forma, si ocurre una intrusión en un segmento (p.ej., un PC de usuario se infecta), el atacante no podrá llegar fácilmente a los servidores que tengan información laboral o sanitaria, por ejemplo. Adicionalmente, activar las funciones de seguridad disponibles en los equipos de red: por ejemplo, en los switches habilitar listas de control de acceso (ACLs)

básicas, protección contra spoofing o contra tormentas de broadcast si es aplicable.

Se deben gestionar de forma centralizada las configuraciones de red, guardando copia de la configuración actual de cada dispositivo para recuperarla en caso de fallo. También se debe monitorizar la capacidad y rendimiento de la red para detectar comportamientos anómalos que puedan indicar un ataque (esto se relaciona con el siguiente Control 13). En resumen, asegurar la infraestructura de red implica tanto usar configuraciones seguras en cada dispositivo como estructurar la red en defensas en profundidad para contener amenazas.

### *Control 13: Monitorización y defensa de la red*

Actualmente no existe un sistema para monitorizar activamente eel tráfico o de las actividades en la red de INSESO, ni sistemas de bloqueo de tipo NAC. No se cuenta con sistemas de detección de intrusos (IDS/IPS) ni con herramientas de análisis de flujo de red. El personal de TI no dispone de un panel de control o alertas en tiempo real sobre eventos de seguridad en la red. Esto significa que un atacante podría estar moviéndose dentro de la red o extrayendo datos sin ser detectado. Dada la falta de segmentación mencionada, un atacante con presencia en la red podría escanear y atacar otros sistemas libremente. La ausencia de defensas activas a nivel de red deja al organismo ciego ante ataques sofisticados: por ejemplo, no se detectaría si un equipo interno empieza a conectarse a servidores externos inusuales (posible C2 - comando y control) ni si hay picos de tráfico anómalos que puedan indicar exfiltración de datos o movimiento de malware.

Se recomienda implementar mecanismos de monitorización de red y defensa activa. Una opción es desplegar un sistema IDS/IPS que analice el tráfico de red en puntos clave (por ejemplo, en la frontera de la red con Internet y entre segmentos internos críticos) para identificar patrones maliciosos o conocidos (firmas de ataques, tráfico hacia dominios maliciosos, exploración de puertos, etc.). Herramientas IDS basadas en firma (como Snort, Suricata, o soluciones comerciales) podrían ser integradas con el SIEM para correlacionar eventos. Además del IDS, considerar soluciones de monitorización de flujo de red (NetFlow o similares) que permitan ver tendencias de tráfico y detectar comportamientos fuera de lo normal. Se deben configurar alertas para el personal de seguridad cuando ocurran eventos importantes, de modo que haya capacidad de respuesta temprana. Otra recomendación es habilitar la funcionalidad de registro en los firewalls o routers perimetrales para captar

intentos de intrusión o tráfico bloqueado, integrándolos también en la plataforma central de logs (Control 8).

En cuanto a defensa activa, se puede configurar el IPS para que, una vez afinado y comprobado que no produce falsos positivos críticos, bloquee automáticamente ciertos ataques comunes (por ejemplo, intentos de explotar vulnerabilidades conocidas o tráfico desde/hacia direcciones maliciosas conocidas).

Por último, se debe entrenar al personal de TI en la interpretación de alertas y manejo de eventos de red, para que puedan responder (aislar un host, bloquear una IP, etc.) cuando salte una alarma. Con estas medidas, INSESO podrá detectar amenazas en tiempo real en su red y reaccionar antes de que causen daño mayor, elevando sustancialmente su capacidad defensiva.

### *Control 14: Concienciación y capacitación en seguridad*

La cultura de seguridad en la organización es prácticamente inexistente. El personal, tanto técnico como administrativo, no ha recibido formación en ciberseguridad. No se realizan sesiones de concienciación sobre buenas prácticas (por ejemplo, cómo reconocer un correo de phishing, la importancia de usar contraseñas seguras, políticas de uso aceptable de los sistemas, etc.). Esta falta de capacitación se traduce en comportamientos de riesgo: uso de contraseñas débiles o anotadas en papel, desconocimiento ante posibles fraudes electrónicos, y en general poca percepción del peligro digital. Como consecuencia, los empleados pueden convertirse inadvertidamente y de forma inocente, en vectores de ataque (haciendo clic en enlaces maliciosos, proporcionando información sensible a atacantes que se hacen pasar por soporte, conectando dispositivos no seguros a la red, etc.). De hecho, en el sector se observa que casi la mitad de los incidentes de seguridad tienen origen interno involuntario (errores o descuidos del personal) y este riesgo aumenta notablemente cuando la formación en ciberamenazas es limitada

Se debe desarrollar un programa continuo de concienciación y entrenamiento en seguridad para todos los niveles de personal de INSESO. En primer lugar, establecer políticas de seguridad de la información claras y difundirlas (por ejemplo, una política de uso aceptable de equipos, política de contraseñas, procedimiento para reportar incidentes sospechosos, etc.). Luego, impartir formaciones periódicas: talleres, cursos o al menos charlas semestrales, adaptadas a distintos perfiles (personal médico, administrativos, técnicos). Temas clave deben incluir: cómo identificar intentos de phishing y estafas comunes, manejo seguro de información sensible (especialmente datos de

pacientes), importancia de las actualizaciones y parches, uso correcto de contraseñas y MFA, y qué hacer ante un incidente (no ocultarlo sino reportarlo de inmediato). Complementariamente, se pueden realizar simulacros para reforzar el aprendizaje, por ejemplo, simulaciones de phishing enviando correos de prueba al personal para evaluar cuántos los identifican y luego retroalimentar con los resultados. Este tipo de ejercicios, junto con la formación teórica, ayudará a crear reflejos de seguridad en la plantilla. Es fundamental también capacitar al equipo de TI en áreas más especializadas (gestión de incidentes, configuración segura, respuesta ante malware, etc.) dado que actualmente su conocimiento es limitado. Una fuerza laboral informada y consciente de las amenazas es una de las mejores defensas para la organización; disminuirá la probabilidad de errores humanos que comprometan la seguridad y fomentará que todos colaboren activamente en proteger los activos informáticos y la información de pacientes.

### *Control 15: Gestión de proveedores de servicios*

INSESO trabaja con diversos proveedores externos para sus sistemas, pero, por lo que se ha visto durante los trabajos, no cuenta con un proceso formal para asegurar la seguridad en la cadena de suministro de TI. No se realizan evaluaciones de seguridad a los proveedores ni se les exige contractualmente cumplir requisitos mínimos de ciberseguridad. Esto implica que, si un proveedor con acceso a datos de INSESO o a sus sistemas es comprometido, podría traducirse en una brecha para la institución. También puede haber riesgos por el uso de software de terceros desactualizado o vulnerado (supply chain attacks). Actualmente, INSESO no lleva un registro detallado de qué acceso o datos tiene cada proveedor, ni ha designado responsables para supervisar esos contratos desde la óptica de seguridad.

Por todo ello, se recomienda implementar un proceso de gestión de riesgos de terceros. En primer lugar, se debe elaborar un inventario de todos los proveedores de servicios de TI (y otros que tengan acceso a sistemas o datos sensibles), identificando qué sistemas tocan o qué datos manejan. Para los proveedores críticos, establecer requisitos de seguridad en los contratos (por ejemplo, que cumplan con normas tipo ISO 27001 o similares, que notifiquen incidentes de seguridad que les afecten, que apliquen cifrado a los datos de INSESO que tratan, etc.). Desarrollar un procedimiento de evaluación de proveedores donde previo a contratar (o renovar contrato) se revise su postura de seguridad mediante cuestionarios, evidencias o incluso auditorías si fuera posible.

Por otro lado, se debe limitar técnicamente el acceso de los proveedores. Si un proveedor de software tiene que dar soporte remoto, que sea a través de conexiones seguras y controladas (VPN con MFA y cuentas temporales, por ejemplo).

Se deben establecer acuerdos de confidencialidad y de nivel de servicio que cubran aspectos de seguridad (tiempos de respuesta ante incidentes, resguardo de datos personales según leyes de protección de datos, etc.). Por otro lado, internamente asignar a un dueño por cada relación con terceros que supervise que el proveedor cumple con los controles acordados.

Finalmente, se debe incluir a los proveedores en el plan de respuesta a incidentes (Control 17), definiendo cómo se les contactará y qué apoyo brindarán si un incidente involucra sus sistemas o servicios. Con este control, INSESO reducirá la probabilidad de ser víctima por debilidades de sus socios externos, asegurando que los proveedores que manejan datos o plataformas críticas también los protejan adecuadamente

### *Control 16: Seguridad de las aplicaciones (software)*

En INSESO no se realizan, en la práctica, análisis de vulnerabilidades de aplicaciones (por ejemplo, pruebas de penetración en aplicaciones web, revisiones de código fuente, análisis de vulnerabilidades OWASP en aplicaciones web públicas). Las actualizaciones de estas aplicaciones son esporádicas y no está claro si se corrigen fallos de seguridad cuando se actualizan. Esto deja a las aplicaciones expuestas a vulnerabilidades que podrían ser explotadas para extraer datos sensibles o alterar información médica. Por ejemplo, una aplicación web desactualizada podría ser vulnerable a inyecciones SQL o a ataques de cross-site scripting, permitiendo a un atacante externo robar datos de pacientes. Además, es posible que no se tengan entornos separados de pruebas: cualquier cambio de software se haría directamente en producción, aumentando el riesgo de introducir errores o fallos de seguridad inadvertidamente.

Se recomienda adoptar prácticas de seguridad en el ciclo de vida de las aplicaciones. Si hubiese desarrollos internos, algo no evaluado durante el presente trabajo de auditoría, se deben establecer estándares de codificación segura y capacitaciones en seguridad para los desarrolladores. En todos los casos, someter las aplicaciones críticas (sean desarrolladas en casa o por terceros) a pruebas de seguridad periódicas: esto incluye realizar análisis estáticos de código (SAST) y análisis dinámicos (DAST) para identificar vulnerabilidades conocidas.

Se recomienda encarecidamente contratar pruebas de penetración anuales o semestrales enfocadas en las aplicaciones que manejen información sensible de INSESO. Cualquier hallazgo de seguridad debe priorizarse para su remediación con los fabricantes o equipos de desarrollo. Asimismo, se debe de implementar un proceso de gestión de parches específico de aplicaciones: cuando el proveedor lance una actualización que corrija fallos (especialmente de seguridad), instalarla pronto previo testeo básico.

Se recomienda también separar los entornos: tener un ambiente de desarrollo/pruebas por separado donde se puedan probar cambios o nuevas versiones de forma segura antes de pasarlas a producción. Para las aplicaciones ya en uso, configurar al menos medidas de mitigación si no se pueden arreglar inmediatamente vulnerabilidades (por ejemplo, reglas en el firewall o WAF – Web Application Firewall – frente a un patrón de ataque conocido hasta que se corrija la aplicación).

Se debe documentar además un inventario de todas las aplicaciones en la organización (relacionado con Control 2) con información de sus versiones y últimas actualizaciones aplicadas. En resumen, asegurar las aplicaciones implica integrarlo en la rutina: pruebas de seguridad, actualizaciones diligentes y desarrollo con buenas prácticas, para prevenir, detectar y corregir debilidades de seguridad en el software antes de que impacten a la organización

### *Control 17: Gestión de respuesta a incidentes*

Como se ha podido comprobar, INSESO no dispone de un plan formal de respuesta a incidentes de seguridad, ni playbooks informales. Si ocurriera hoy un ataque o brecha, la reacción sería improvisada, sin roles ni procedimientos definidos. El personal de TI no ha sido entrenado en manejo de incidentes y probablemente habría demoras significativas en contener el problema y notificar a la dirección o a las autoridades competentes (por ejemplo, en caso de filtración de datos personales, notificar a agencia de protección de datos si aplica). Esta carencia es muy peligrosa, dado que actualmente los ataques al sector son muy frecuentes. Sin un plan, es probable que valiosos minutos u horas se pierdan decidiendo qué hacer y quién lo hace, lo que puede agravar el impacto. Adicionalmente, no tener definido un plan puede implicar que tras el incidente no se realice una adecuada recuperación o lecciones aprendidas, repitiéndose los mismos errores en el futuro.

Se recomienda desarrollar un Plan de Respuesta a Incidentes (PRI) adaptado a INSESO. Este plan debe incluir una definición clara de qué constituye un incidente de seguridad y una guía paso a paso de cómo gestionarlo. Es

importante asignar un equipo de respuesta a incidentes, con roles y responsabilidades específicos: por ejemplo, quién lidera la gestión (un CISO o responsable de TI), quién se encarga de comunicaciones (tanto internas a la organización como externas a autoridades o prensa si fuera necesario), quién realiza el análisis técnico, etc. El plan debe contemplar distintos tipos de incidentes posibles (malware/ransomware, robo de un dispositivo con datos, acceso no autorizado a una base de datos, indisponibilidad de sistemas críticos, etc.) y detallar acciones iniciales de contención para cada caso (e.g., en caso de malware, aislar la máquina afectada de la red; en caso de detección de intruso, cambiar contraseñas comprometidas y cerrar accesos; etc.).

También debe incluir procedimientos de backup y recuperación de sistemas en caso de daños (ligado al Control 11), y criterios de notificación obligatoria si aplica (por ejemplo, notificar a los pacientes cuyos datos fueron expuestos dentro de cierto plazo, siguiendo las leyes locales de protección de datos). Una vez redactado el plan, es fundamental entrenar al personal involucrado en su uso y realizar simulacros o ejercicios (table-top exercises) para probar la eficacia del plan y ajustarlo según se identifiquen brechas. Cabe destacar que tener un plan no solo reduce el impacto en tiempo real (permite responder más rápido y eficientemente), sino que también minimiza consecuencias legales y financieras – la falta de preparación puede derivar en pérdidas mayores e incluso sanciones. Con un buen programa de respuesta a incidentes, INSESO estará preparado para reaccionar ante un ataque inevitable de manera organizada, limitando el daño y recuperando operaciones lo antes posible.

En la auditoría pudo observarse como el CPD donde se encontraban ubicados los sistemas revisados tampoco reunía las características básicas a nivel de refrigeración y aislamiento. Además, presentaba humedades preocupantes, tal y como puede verse en la siguiente evidencia.

### *Control 18: Pruebas de penetración*

Hasta la fecha, y por lo transmitido por el contratante, no hay evidencias de que INSESO haya llevado a cabo pruebas de penetración (pentests) ni ejercicios similares para evaluar sus defensas. No se han simulado ciberataques controlados contra la infraestructura o aplicaciones para descubrir sus debilidades, ni tan siquiera se han realizado ejercicios proactivos de Red Teaming. Esto significa que muchas vulnerabilidades pueden existir latentes sin ser descubiertas por el equipo interno – quedando a la espera de que un

atacante real las encuentre primero. También implica que los procesos de respuesta (Control 17) no han sido puestos a prueba en un entorno realista.

Dada la inmadurez en seguridad actual, es muy probable que un pentester externo encuentre rápidamente numerosos problemas graves (como credenciales débiles, sistemas expuestos desde Internet sin parches, inyecciones SQL en aplicaciones web, etc.). La ausencia de estas evaluaciones proactivas deja a la organización sin una línea de base de qué tan vulnerable es y cuáles son sus mayores fallos.

Se recomienda programar pruebas de penetración periódicas realizadas por expertos independientes. Inicialmente, se sugiere realizar un pentest exhaustivo una vez que se hayan abordado los controles más básicos (por ejemplo, después de mejorar inventarios, parches y configuraciones, para no gastar recursos en señalar problemas ya sabidos). Las pruebas deben cubrir tanto la red interna como los sistemas expuestos a Internet, y las aplicaciones críticas. Un equipo de profesionales podrá simular técnicas de ataque utilizadas por ciberdelincuentes para identificar puntos de entrada y debilidades explotables. Es importante que se realicen bajo contrato formal, con el alcance bien definido y las debidas precauciones para no interrumpir servicios vitales durante la ejecución. Los resultados del pentest proporcionarán a INSESO una lista priorizada de vulnerabilidades y debilidades a corregir, complementando los procesos de gestión de vulnerabilidades (Control 7).

Adicionalmente, en el futuro, cuando el nivel de madurez sea mayor, INSESO podría considerar ejercicios de Red Team completos, que simulen ataques dirigidos de manera más sorpresiva, para evaluar no solo la tecnología sino también la capacidad de detección y respuesta del personal. Por ahora, iniciar con pentests anuales ayudará a medir el progreso de las mejoras de seguridad y asegurarse de que los controles implementados están siendo efectivos en prevenir intrusiones. Identificar y remediar debilidades mediante pruebas controladas fortalecerá la resiliencia global del sistema antes de que atacantes reales intenten lo mismo.

# 7. Conclusiones

El presente análisis forense pericial ha sido solicitado por D. Roberto Nsue, en calidad de CEO y Apoderado de Inverfin Holding S.A., a petición del Instituto de Seguridad Social (INSESO) de Guinea Ecuatorial, con el objetivo de clonar, poner en custodia y analizar la existencia y autenticidad de una serie de logs o trazas de auditoría que pudiesen contener indicadores de mal funcionamiento o anomalías sobre el comportamiento habitual de las aplicaciones de gestión de INSESO. Concretamente, el contratante solicitó la revisión de logs del sistema Agresso, ubicación donde se encontrarían las trazas del core del sistema que se gestiona. De forma añadida al trabajo pericial, el contratante solicitó al equipo auditor un Análisis GAP inicial, con el objetivo de tener una referencia que le permita conocer de primera mano si los sistemas informáticos de INSESO presentan un estado de salud adecuado.

Para la realización del estudio forense, INSESO suministró a los peritos las credenciales de acceso a insesobck02. Posteriormente, los peritos levantaron la debida cadena de custodia y realizaron el clonado de varias particiones del servidor corporativo. Una vez finalizado el proceso, las copias fueron firmadas digitalmente con el fin de garantizar la inalterabilidad de la información contenida, cumplimentando dicha información en la cadena de custodia.

Debido a una incidencia ocurrida, que paró el servicio de INSESO, se solicitó a los peritos forenses que centrasen sus esfuerzos en analizar la muestra de trazas de log recuperadas por los técnicos de INSESO, con el objetivo de identificar su origen. Dentro del estudio, fue verificado por los peritos que se produjo un apagado de la máquina virtual objeto de estudio, motivo por el cual se les requirió dar soporte al personal local para revocar privilegios de acceso al personal que no fuese imprescindible.

El análisis de los logs procedentes del nodo reportó un intento de inicio de sesión con la cuenta de dominio “Administrador@inseso01.local”, una hora después de la revocación de privilegios (y de deshabilitar la cuenta), lo que parece dar indicios de que el apagado de la máquina no fue casual y de que podría tratarse de un ataque premeditado de un usuario que conocía y disponía de las credenciales del sistema.

Con el análisis de las particiones se puede concluir que:

- Ocurre un evento en el servidor en el que se aloja la máquina virtual en el rango temporal en el que se indica a los peritos que se produce la caída.

- Ocurre un evento de inicio de sesión denegado por cuenta deshabilitada, para la cuenta de administración por defecto del dominio.
- Ocurren eventos relacionados con el usuario objeto de estudio en febrero y mayo de 2025.
- Se identifican vacíos temporales y eventos ausentes en los registros del sistema.

Estos hallazgos son compatibles con posibles borrados premeditados y que podrían tener su origen en el usuario de "Antonio Sánchez".

Asimismo, se debe remarcar que los resultados obtenidos a partir del análisis de los registros disponibles en "*nodo03sistema*" ofrecen una **visión parcial de la actividad registrada en el sistema**. Durante el proceso se ha detectado la **ausencia de determinados eventos** que, según la información contenida en otros registros presentes - por ejemplo, eventos que hacen referencia a acciones que presupone la existencia de eventos previos concretos -, deberían figurar en los logs. **Esta inconsistencia sugiere que los datos analizados no reflejan de forma íntegra todo lo ocurrido, faltando información que podría aportar valor**.

Finalmente, del análisis GAP realizado por los auditores en paralelo, se ha revelado que INSESO se encuentra en un estado de seguridad muy por debajo de lo aceptable en una institución gubernamental en pleno año 2025, incumpliendo prácticamente la totalidad de los Controles CIS. Esta situación representa un riesgo inminente para la confidencialidad de los datos de la ciudadanía, la disponibilidad de los servicios de salud y la integridad de sus operaciones. Dada la criticidad del sector, es imperativo tomar acciones urgentes y coordinadas para subsanar estas deficiencias.

Como plan de acción priorizado, iniciando el trabajo por lo más básico, se recomienda comenzar a abordar de manera prioritaria los controles fundamentales (IG1), que sientan las bases de la ciberseguridad. Entre ellos destacan:

- **Inventario de activos (Controles 1 y 2):** Sin un conocimiento completo de los dispositivos y software en uso, no se puede proteger el entorno. Este es el punto de partida para todas las demás mejoras; debe emprenderse inmediatamente la identificación y regularización de los activos de TI.
- **Control de accesos (Controles 5 y 6):** Gestionar adecuadamente las cuentas y privilegios para asegurarse de que solo el personal autorizado acceda a sistemas según su rol. Esto incluye introducir autenticación multifactor cuanto antes para reducir el riesgo de intrusiones por credenciales robadas.

- **Protección contra malware y vulnerabilidades (Controles 7 y 10):** Acelerar la aplicación de parches en todos los sistemas (especialmente en aquellos expuestos a Internet o críticos) y desplegar soluciones antimalware actualizadas. Muchos ataques se aprovechan de vulnerabilidades conocidas o de la falta de defensas básicas; al cerrar estas brechas se mitiga un gran porcentaje de amenazas comunes
- **Respaldo de datos (Control 11):** Establecer inmediatamente backups regulares de los sistemas críticos. La recuperación de datos debe ser prioridad absoluta, ya que ningún entorno es inmune a todos los riesgos cibernéticos, y contar con copias de seguridad efectivas garantiza que la organización pueda recuperarse y continuar operando ante incidentes.

**Una vez afianzados estos controles esenciales, INSESO debe avanzar con los siguientes niveles (IG2 e IG3)** para lograr una postura de seguridad acorde a su perfil de riesgo alto. Esto incluye inversiones en monitorización (logs centralizados, detección de intrusos), mejoras de infraestructura (segmentación de red, reemplazo de sistemas obsoletos) y establecimiento de procesos formales (respuesta a incidentes, evaluaciones de proveedores, desarrollo seguro). Será crucial contar con apoyo de la alta dirección para obtener los recursos necesarios (presupuesto, personal capacitado y posiblemente asesoría externa) que posibiliten esta transformación.

# 8. Juramento de actuación pericial

Daniel Puente Ramírez, José Luis González y Juan A. Calles, como peritos intervinientes en la actuación, son conocedores y garantizan la objetividad de la intervención, siguiendo los principios establecidos en la Sección 5ª del Dictamen de Peritos regulado en la Ley de Enjuiciamiento Civil del ordenamiento jurídico del Reino de España.

Por lo tanto:

"juran haber actuado con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes, y conociendo las sanciones penales en las que podría incurrir si incumpliese su deber como peritos."

D. Daniel Puente Ramírez
9 de julio de 2025

D. José Luis González Rueda
9 de julio de 2025

D. Juan A. Calles
9 de julio de 2025

# Anexo A: Perfil detallado de los peritos

El análisis forense digital documentado en el presente informe pericial ha sido realizado por los peritos:

*D. Juan A. Calles*, Doctor "Cum Laude" en Informática, Ingeniero en Informática de Sistemas, Postgrado en Tecnologías de la Información y Sistemas Informáticos y Postgrado en Ingeniería de Sistemas de Decisión por la Universidad Rey Juan Carlos de Madrid. Director de Seguridad Privada por el Ministerio del Interior de España, con TIP 23.361. Certified Hacking Forensic Investigator por Ec-Council, con número de licencia ECC971566. Autopsy Certified, con número de licencia 16344018. Microsoft Most Valuable Professional con número de licencia 5003773. Autor del libro “Análisis Forense de Correos Electrónicos en Office 365”.

*D. Daniel Puente Ramírez*, Ingeniero Informático por la Universidad de Burgos con menciones honoríficas en Sistemas y Computación. Certificado en ciberseguridad ofensiva, con certificaciones como OSCP, RTO I, CARTP, PNPT, todas ellas de relevantes empresas de ciberseguridad del sector. Instructor en bootcamps de ciberseguridad ofensiva y defensiva, además de personal técnico e instructor en másters de ciberseguridad por las universidades – Kschool (ESPAÑA), MIU (EE. UU.).

*D. José Luis González Rueda*, Director de Seguridad Privada habilitado por el Ministerio del Interior con TIP 4.826 y Detective Privado con TIP 2.121. Cuenta con una sólida formación en ciberseguridad, análisis de evidencias digitales e inteligencia, destacando el Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen y el título de Experto en Inteligencia, ambos por la Universidad Autónoma de Madrid. Además, es Graduado en Ciencias Criminológicas y de la Seguridad, Especialista en Criminalística y Licenciado en Gestión Comercial y Marketing por ESIC. Posee las certificaciones de Auditor Líder y Auditor Interno en la norma ISO/IEC 27001:2022, y acumula experiencia en la implantación y adecuación de sistemas de gestión conforme a ISO 27001 y el Esquema Nacional de Seguridad, apoyo en auditorías internas y externas, revisión de declaraciones de aplicabilidad (SoA), desarrollo de auditorías internas, análisis de riesgos y elaboración de informes técnicos y de auditoría.

Todos los peritos forman parte del equipo de Zerolynx S.L., compañía galardonada en 2020 y 2023 en el Top 5 de empresas de servicios forenses de

España y Top 10 de Europa respectivamente, por la revista Enterprise Security Magazine.

El presente informe consta de 74 hojas, numeradas del 1 a la 74.

Madrid, a 9 de julio de 2025

D. Daniel Puente Ramírez
9 de julio de 2025

D. José Luis González Rueda
9 de julio de 2025

D. Juan A. Calles
9 de julio de 2025

# Anexo B: Cadena de custodia

| Case Nº: | 202505/05 | Page | 1 | Of: | 2 |
|---|---|---|---|---|---|

**ELECTRONIC MEDIA DETAILS**

| Item | Model | Description |
|---|---|---|
| Clonación particiones máquina virtual "INSESODB" | Clonación Bit -Bit | Clonación de cada una de las particiones existentes en la máquina virtual "INSESODB" alojada en el servidor "INSESOBCK02"- se clonan 5 particiones. |

**IMAGE DETAILS**

| Date/Time | Created by | Method Used |
|---|---|---|
| 20 de mayo de 2025 a las 17: | Daniel Puente Ramírez<br>Jose Luis González Rueda | Exportación forense de Servidor |
| **Image Name** | **Hash SHA256** | |
| C | 12c1eb545126a540e35987b2a5acbb10e5c5c6984ad2ccd375d15383b47cfca7 | |
| INDEX - I | d03bccb17039478b441b3b2b81b8301431d4232ff7caffbc9eb82c52ad0e93cf | |
| LOG - G | f3a588eb37f2fdf9bf60b422a24f9cb7235b0a3772aac67850dc4823cb956b7a | |
| RDBMS - F | 2e7695860b6e6813252682f27f367f461b8b14b9c91daea165b8abf75d323d7f | |
| TEMP - H | 3acd6eda2094f91e98801f2f3022435794745393c60b1d3e342f78b7518534bc | |
| | | |

**CHAIN OF CUSTODY**

| Tracking Nº | Date/Time | From | To | Reason |
|---|---|---|---|---|
| 001 | 20/05/2025 13:15h | Rosendo clemente Engonga (000131942) | Daniel Puente Ramírez (71303486-J)<br><br>Jose Luis González Rueda | Se entregan credenciales para poder realizar el forense desde el servidor que contiene la maquina "INSESODB".<br>Se procede a la extracción y se procede para su posterior análisis |

| | | | | |
|---|---|---|---|---|
| | | | (07518442-H) | |
| 002 | 20/05/2025 17:36:20 | Daniel Puente Ramirez (71303486-J)<br>José Luis Gonzalez Rueda (07518442-H) | Rosendo clemente Engonga (000131942) | Se entrega portable Solid State Drive USB-3.2 Z Slim<br>Dicho dispositivo contiene la clonación realizada en su totalidad para su custodia en las dependencias de INSESO Avd. de la Independencia, s/n . Malabo |

Se procede a la apertura de un USB en presencia de D. Rosendo Clemente y D. Manuel MBA En representación de INSESO y D.Otto Okenve como representante de INVERFIN

(000131942) (000154293) (00099974) (71303486J) (07518442H)

| Case Nº: | 202505/05 | Page | 1 | Of: | 2 |
|---|---|---|---|---|---|

## ELECTRONIC MEDIA DETAILS

| Item | Model | Description |
|---|---|---|
| Clonación particiones máquina virtual INSESODB<br>Exportacion directorio activo | Clonación Bit - Bit<br><br>Ficheros.dat | Clonación de cada una de las particiones existentes en la máquina virtual "INSESODB" alojada en el servidor "INSESOBCK02"- se clonan 5 particiones.<br>Exportación de los objetos del dominio |

## IMAGE DETAILS

| Date/Time | Created by | Method Used |
|---|---|---|
| 21 de mayo de 2025 a las 18:20 | Daniel Puente Ramírez<br>Jose Luis González Rueda | Exportación forense de Servidor<br>Exportación de los objetos del dominio |

| Image Name | Hash SHA256 |
|---|---|
| C | 12c1eb545126a540e35987b2a5acbb10e5c5c6984ad2ccd375d15383b47cfca7 |
| INDEX - I | d03bccb17039478b441b3b2b81b8301431d4232ff7caffbc9eb82c52ad0e93cf |
| LOG - G | f3a588eb37f2fdf9bf60b422a24f9cb7235b0a3772aac67850dc4823cb956b7a |
| RDBMS - F | 2e7695860b6e6813252682f27f367f461b8b14b9c91daea165b8abf75d323d7f |
| TEMP - H | 3acd6eda2094f91e98801f2f3022435794745393c60b1d3e342f78b7518534bc |
| ESTRACCION DA.dat | 8b 7f 0f d2 d2 78 b8 aa 7a d2 05 f3 ba 86 52 ed 00 f3 b6 e8 fd 18 f1 73 b2 62 70 b9 e7 1a 86 03 |
| ESTRACCION DA1.dat | 06 fc 7b 73 37 11 4b 02 13 49 22 f5 36 e5 5c 67 1a 0c 38 ef c7 a6 3a 71 73 a6 b7 03 0e d7 cf 6d |

## CHAIN OF CUSTODY

| Tracking Nº | Date/Time | From | To | Reason |
|---|---|---|---|---|
| 001 | 21/05/2025 18:00h | Rosendo clemente Engonga (000131942) | Daniel Puente Ramírez (71303486-J)<br><br>Jose Luis González Rueda (07518442-H) | Se entregan credenciales para poder realizar el forense desde el servidor que contiene la maquina INSESODB .<br>Se procede a la extracción y se procede para su posterior análisis Exportación de los objetos del dominio<br><br>Exortacion de la totalidad del dominio |
| 002 | 21/05/2025 18:40h | Daniel Puente Ramírez (71303486-J)<br><br>Jose Luis González Rueda (07518442-H) | Rosendo clemente Engonga (000131942) | Se entrega portable Solid State Drive USB-3.2<br>Z Slim<br>Dicho dispositivo contiene la clonación realizada en su totalidad para su custodia en las dependencias de INSESO<br>Avd. de la Independencia, s/n . Malabo |

Se procede a la apertura de un USB en presencia de D. Rosendo Clemente y D.Manuel MBA En representación de INSESO y D.Otto Okenve como representante de INVERFIN

(000131942)
(07518442H)

(000154293)

(00099974)

(71303486J)

| Case Nº: | 202505/05 | Page | 1 | Of: | 2 |
|---|---|---|---|---|---|

## ELECTRONIC MEDIA DETAILS

| Item | Model | Description |
|---|---|---|
| Clonación particiones máquina virtual "INSESODB" | Clonación Bit - Bit | Clonación de cada una de las particiones existentes en la máquina virtual "INSESODB" alojada en el servidor "INSESOBCK02"- se clonan 5 particiones.<br>Y evidencias, se añaden logs de windows.zip |

## IMAGE DETAILS

| Date/Time | Created by | Method Used |
|---|---|---|
| 22 de mayo de 2025 a las 17: | Daniel Puente Ramírez<br>Jose Luis González Rueda | Exportación forense de Servidor |
| **Image Name** | **Hash SHA256** | |
| C | 12c1eb545126a540e35987b2a5acbb10e5c5c6984ad2ccd375d15383b47cfca7 | |
| INDEX - I | d03bccb17039478b441b3b2b81b8301431d4232ff7caffbc9eb82c52ad0e93cf | |
| LOG - G | f3a588eb37f2fdf9bf60b422a24f9cb7235b0a3772aac67850dc4823cb956b7a | |
| RDBMS - F | 2e7695860b6e6813252682f27f367f461b8b14b9c91daea165b8abf75d323d7f | |
| TEMP - H | 3acd6eda2094f91e98801f2f3022435794745393c60b1d3e342f78b7518534bc | |
| logs de windows.zip | 32773acbf94f76ca95bd81bea76dcb16dcd2efe31d346672610be1f63a60d32b | |

## CHAIN OF CUSTODY

| Tracking Nº | Date/Time | From | To | Reason |
|---|---|---|---|---|
| 001 | 22/05/2025 11:19h | Rosendo clemente Engonga (000131942) | Daniel Puente Ramírez (71303486-J)<br>Jose Luis González Rueda | Se entregan credenciales para poder realizar el forense desde el servidor que contiene la maquina "INSESODB".<br>Se procede a la extracción y se procede |

| | | | | |
|---|---|---|---|---|
| | | | (07518442-H) | para su posterior análisis |
| 002 | 22/05/2025 | Daniel Puente Ramírez (71303486-J)<br><br>Jose Luis González Rueda (07518442-H) | Rosendo clemente Engonga (000131942) | Se entrega portable Solid State Drive USB-3.2 Z Slim Dicho dispositivo contiene la clonación realizada en su totalidad para su custodia en las dependencias de INSESO Avd. de la Independencia, s/n . Malabo |

Se procede a la apertura de un USB en presencia de D. Rosendo Clemente y D. Manuel MBA En representación de INSESO y D.Otto Okenve como representante de INVERFIN

(000131942) (07518442H) (000154293) (00099974) (71303486J)

| Case Nº: | 202505/05 | Page | 1 | Of: | 2 |
|---|---|---|---|---|---|

## ELECTRONIC MEDIA DETAILS

| Item | Model | Description |
|---|---|---|
| Clonación particiones máquina virtual "INSESODB" | Clonación Bit - Bit<br>Extracción directorio activo<br>Revocación de permisos<br>"logs de windows.zip" y análisis | Clonación de cada una de las particiones existentes en la máquina virtual "INSESODB" alojada en el servidor "INSESOBCK02"- se clonan 5 particiones.<br>Y evidencias, se añaden "logs de windows.zip" , se realiza la extracción del directorio activo de los objetos procede a la revocación de permisos, |

## IMAGE DETAILS

| Date/Time | Created by | Method Used |
|---|---|---|
| 23 de mayo de 2025 a las 10:17 | Daniel Puente Ramírez<br>Jose Luis González Rueda | Exportación forense de Servidor |

| Image Name | Hash SHA256 |
|---|---|
| C | 12c1eb545126a540e35987b2a5acbb10e5c5c6984ad2ccd375d15383b47cfca7 |
| INDEX - I | d03bccb17039478b441b3b2b81b8301431d4232ff7caffbc9eb82c52ad0e93cf |
| LOG - G | f3a588eb37f2fdf9bf60b422a24f9cb7235b0a3772aac67850dc4823cb956b7a |
| RDBMS - F | 2e7695860b6e6813252682f27f367f461b8b14b9c91daea165b8abf75d323d7f |
| TEMP - H | 3acd6eda2094f91e98801f2f3022435794745393c60b1d3e342f78b7518534bc |
| ESTRACCION DA.dat | 8b 7f 0f d2 d2 78 b8 aa 7a d2 05 f3 ba 86 52 ed 00 f3 b6 e8 fd 18 f1 73 b2 62 70 b9 e7 1a 86 03 |
| ESTRACCION DA1.dat | 06 fc 7b 73 37 11 4b 02 13 49 22 f5 36 e5 5c 67 1a 0c 38 ef c7 a6 3a 71 73 a6 b7 03 0e d7 cf 6d |
| logs de windows.zip | 32773acbf94f76ca95bd81bea76dcb16dcd2efe31d346672610be1f63a60d32b |

| Tracking Nº | Date/Time | From | To | Reason |
|---|---|---|---|---|
| 001 | 22/05/2025 11:19h | Rosendo clemente Engonga (000131942) | Daniel Puente Ramírez (71303486-J)<br><br>Jose Luis González Rueda (07518442-H) | Se entregan credenciales para poder realizar el forense desde el servidor que contiene la maquina "INSESODB".<br>Se procede a la extracción y se procede para su posterior análisis |
| 002 | 22/05/2025 11:38 | Daniel Puente Ramírez (71303486-J)<br><br>Jose Luis González Rueda (07518442-H) | D.Otto Okenve (00099974) como representante (CTO) de INVERFIN | Se entrega portable Solid State Drive USB-3.2 Z Slim<br>Dicho dispositivo contiene la clonación realizada en su totalidad para su custodia en las dependencias de INSESO<br>Avd. de la Independencia, s/n . Malabo |

Se procede a la apertura de un USB en presencia de D. Rosendo Clemente y D. Manuel MBA En representación de INSESO y D.Otto Okenve como representante de INVERFIN

(000131942) (00099974) (71303486J) (07518442H)