



INFORME PERICIAL IP 211093

Fecha: 14-07-2025

Por encargo de: ROCK STAR S.A.

El presente **documento** es un informe pericial realizado por personal de la empresa **sniper S.A.**, y puede contener información **CONFIDENCIAL**, por lo que está prohibido el acceso a su contenido sin la correspondiente autorización.

Este informe pericial puede tener adjunto material digital como CD-ROMs o memorias USB, que no deben separarse de manera innecesaria. Para cualquier consulta, solicitud de copias o ratificación de su contenido, puede encontrar información sobre los peritos firmantes y dirección de notificaciones en la primera página tras esta portada.

FIRMA

El, o los, peritos abajo firmantes manifiestan, bajo promesa de decir verdad, que han actuado y, en su caso, actuarán 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 que conocen las sanciones penales en las que podrían incurrir si incumplieren su deber como perito.

Dragos Cornel Iván Andrei
DNI: 12.34.56.78-M

Notificaciones:

Avda. de Las Palmeras 357, 1º A-B

tlf: 933 123 456 fax: 933 456 789

@: dragosgoshu@gmail.com

Málaga, 14-07-2025

ÍNDICE

1. Resumen Ejecutivo.....	5
2. Objeto del Encargo.....	5
2.1 Antecedentes.....	6
2.2 Objetivos.....	6
2.3 Alcance del análisis técnico.....	7
3. Fuentes de Información.....	8
3.1 Equipos y dispositivos analizados.....	8
3.2 Adquisición de las fuentes.....	9
4. Análisis del PC corporativo con etiqueta RS-2025-001.....	11
4.2 Sistema Operativo.....	11
4.3 Usuarios del sistema.....	13
4.4 Modificaciones entre 22-25 de marzo.....	13
4.5 Programas instalados.....	13
4.6 Correos electrónicos.....	14
4.7 Actividad ofimática del usuario informant.....	15
4.8 Zona horaria y configuración regional.....	16
4.9 Navegadores y búsquedas.....	17
4.10 Herramientas anti forenses descargadas y ejecutadas.....	18
5. Análisis del dispositivo RS-2025-002 (USB personal).....	19
6. Conclusiones.....	20
7. ANEXOS.....	21
 ANEXO I : Cadena de Custodia, hashes e implicaciones legales.....	 22
Anexo I (a): Cadena de custodia y hashes.....	22
Anexo I (b) : Contexto Legal y Limitación en el Análisis del USB.....	26
 ANEXO II: Línea Temporal Completa.....	 28

ANEXO III: Configuración regional y zona horaria del sistema.....	35
ANEXO IV: Evidencias de exfiltración de información.....	36
Anexo IV (a) Evidencia de uso del cliente de Google Drive.....	36
Anexo IV (b) Carta de Renuncia.....	37
Anexo IV (c) Últimos archivos ofimáticos abiertos.....	40
ANEXO V: Perfil Temático del Usuario Investigado.....	41
Anexo V (a) Bookmarks y vínculos temáticos.....	41
Anexo V (b) Webs accedidas por Sr. Informant.....	42
Anexo V (c) Búsquedas relevantes en los navegadores.....	44
ANEXO VI: Herramientas y Actividad Sospechosa Detectada.....	46
Anexo VI (a) Descargas de software - servicio en la nube.....	46
Anexo VI (b) REMOTE DESKTOP (Usuarios de escritorio remoto).....	46

1. Resumen Ejecutivo

Este informe pericial presenta los resultados del análisis forense realizado sobre la imagen de un equipo informático corporativo asignado al usuario identificado como **iaman.informant@nist.gov**. El objetivo del análisis fue determinar indicios de uso indebido de información confidencial, exfiltración de datos y preparación de abandono de la organización.

Durante el análisis, se identificaron comunicaciones por correo electrónico entre el usuario y un tercero, denominado **Spy**, que revelan el posible envío de documentos sensibles a través de enlaces en la nube. Estas comunicaciones, muchas de ellas localizadas en la carpeta de elementos eliminados, incluyen metadatos relevantes como fechas, IDs de mensaje y cabeceras SMTP completas.

Asimismo, se documentó el uso de herramientas como Google Drive, CCleaner y Eraser, así como la manipulación de archivos clasificados como confidenciales en el entorno de trabajo. Se observó también la redacción de una carta de renuncia encontrada en el Escritorio del equipo del usuario, fechada el mismo día de la última comunicación sospechosa.

La correlación temporal entre búsquedas web relacionadas con fuga de datos, herramientas de anti-forensics, y el uso de dispositivos USB o red compartida, refuerza la hipótesis de una conducta premeditada orientada a la exfiltración de información y abandono de la empresa por parte del Sr. Informant.

2. Objeto del encargo

El presente informe ha sido elaborado por encargo de **ROCK STAR, S.A.**, que ha solicitado al perito que suscribe la realización de un análisis técnico forense sobre los dispositivos electrónicos incautados al Sr. **Iaman Informant**, en el contexto de una investigación interna por posible fuga de información estratégica de la empresa, siendo los siguientes los antecedentes y objetivos:

2.1 Antecedentes

- ❖ **ROCK STAR, S.A.** es una empresa internacional dedicada al desarrollo de tecnologías innovadoras en el ámbito del entretenimiento digital.
 - ❖ En el marco de un proyecto confidencial de alto impacto comercial, **la salida al mercado del tan esperado videojuego GTA VI**, la empresa tuvo conocimiento de que uno de sus empleados, el Sr. **Iaman Informant**, habría recibido una oferta por parte de un competidor, representado por el Sr. **Spy Conspirator**, para la entrega de información tecnológica sensible.
 - ❖ La empresa ha recibido indicios de que ambos habrían mantenido comunicaciones mediante correos electrónicos simulando intercambios legítimos entre empresas.
 - ❖ Ante esta situación, la empresa notificó al Sr. Informant el inicio de una investigación y procedió a su suspensión de empleo, así como al precintado de su puesto de trabajo.
 - ❖ Durante dicho procedimiento se incautaron su ordenador portátil corporativo, y una memoria USB de carácter personal, localizada en su escritorio.
-

2.2 Objetivos

Con el objetivo de esclarecer una posible filtración de información confidencial, se ha realizado un análisis forense técnico sobre una imagen adquirida del sistema investigado, utilizando para ello herramientas ampliamente aceptadas en el ámbito pericial digital. En todo momento se ha seguido una metodología basada en el principio de **mínima intervención**, enfocando exclusivamente el análisis a los indicios directamente relacionados con la presunta exfiltración de datos y respetando así el marco jurídico vigente sobre privacidad y protección de datos. De modo que los objetivos han sido los siguientes:

- ❖ Realizar una **adquisición forense controlada** de los dispositivos incautados, estableciendo una cadena de custodia que garantice la integridad de las evidencias digitales.

- ❖ Analizar el contenido de los dispositivos corporativos con el fin de identificar posibles **comunicaciones por correo electrónico** entre el Sr. Iaman Informant y el Sr. Spy relacionadas con la oferta y la posible fuga de información, con el uso de **servicios de almacenamiento en la nube** desde los dispositivos incautados, **transferencias, accesos o manipulaciones** de documentos relacionados con la propiedad intelectual de ROCK STAR, S.A., **rastros de borrado o manipulación** de información que pudieran indicar un intento de ocultación de pruebas.

Herramienta utilizada: se ha empleado principalmente la suite forense **Autopsy** (versión 4.21 o superior), una herramienta de análisis open-source que permite examinar de forma no intrusiva una imagen forense de disco. La imagen analizada corresponde al equipo del usuario investigado, montada en formato **read-only** para garantizar la integridad de la evidencia.

2.3 Alcance del análisis técnico

Se delimitó el análisis a las siguientes áreas específicas:

- ❖ **Correos electrónicos enviados y recibidos:** Se accedió a la ruta de usuario **C:\Users\informant\AppData\Local\Microsoft\Outlook**, donde se halló un archivo **.ost** con la cuenta de correo **iaman.informant@nist.gov**. A través del visor de artefactos de Autopsy, se recuperaron múltiples correos electrónicos con metadatos completos (remitente, destinatario, asunto, fecha y contenido), limitando la extracción únicamente a los que demostraban interacción directa con un tercero (**spy.conspirator@nist.gov**) entre los días **23 y 25 de marzo de 2015**.

Esta selección se basa en la relación directa entre estas comunicaciones y el periodo de sospecha. El análisis excluyó cualquier otro correo no relevante.

- ❖ **Historial de navegación web**

En la carpeta de usuario de Google Chrome (**User Data\Default\History**), se localizaron y analizaron búsquedas realizadas con diferentes navegadores usando tanto Google como Bing, en torno a términos como **“data leakage methods”**, **“cloud storage”**, **“how to delete data”** o **“anti-forensics”**. Esta información se consideró crítica por coincidir temporalmente con el envío de archivos por correo electrónico o a través de Google Drive.

Se evitó acceder a cualquier historial de navegación no vinculado a los hechos

investigados.

❖ **Archivos recientes y enlaces a documentos sospechosos**

A través de la categoría **Recent Document Artifacts** y del análisis de accesos a carpetas como **AppData\Roaming\Microsoft\Windows\Recent**, se identificaron accesos a documentos como *Resignation_Letter_(Iaman_Informant).xps*, así como enlaces a carpetas en red y dispositivos extraíbles, todos ellos temporalmente alineados con los hechos investigados.

❖ **Registros de sincronización y actividad de clientes de correo**

Se analizaron logs de sincronización de Outlook presentes en los archivos del sistema y registros de eventos del sistema operativo, sin alterar su contenido ni exportar más información de la estrictamente necesaria.

Sirva este informe firmado por el correspondiente perito para asegurar que durante el análisis se han respetado los principios de: **proporcionalidad, necesidad, integridad de la prueba y confidencialidad**.

3. Fuentes de información

3.1 Equipos y dispositivos analizados:

- ❖ **Ordenador portátil corporativo** asignado al Sr. Iaman Informant. Este equipo contenía en su interior un disco duro tipo SSD en formato de 2,5", etiquetado como **RS-2025-001**. El modelo y número de serie exactos son desconocidos, al haberse realizado una copia parcial de los 20 GB más relevantes para la investigación.
- ❖ **Unidad USB extraíble** facilitada por el Director de Seguridad Corporativa, Sr. Pink, etiquetada como **RS-2025-002**. El dispositivo fue accedido físicamente por el perito, realizándose imagen forense del mismo. No se dispone de su número de serie, aunque se ha podido identificar mediante su UUID: **5420f42d-e67d-4584-a8a7-4809d105e6dc**.

No se procedió al análisis del contenido del dispositivo **RS-2025-002**, al no contar con orden judicial para el acceso al contenido personal del Sr. Informant.

3.2 Adquisición de las fuentes de información

El día **22 de mayo de 2025**, el perito que suscribe se desplazó a las oficinas centrales de **ROCK STAR, S.A.**, en la **Avda. de la Verdad 123, Edificio Rock Tower, Madrid**, en cumplimiento del encargo recibido y previa coordinación con el Departamento Legal de la empresa.

A su llegada, el perito fue recibido por el **Director de Seguridad Corporativa, Sr. Pink**, y por la **Directora del Departamento Legal, Sra. Brown**, quienes acompañaron al perito hasta la **sala de evidencias digitales**, habilitada específicamente para esta intervención.

El procedimiento de adquisición se realizó en presencia de los mencionados representantes de la empresa, quienes participaron en todo el proceso de documentación y firma de la cadena de custodia.

❖ Ordenador portátil corporativo. Disco duro etiquetado RS-2025-001:

Descripción visual de la evidencia RS-2025-001 (disco duro interno extraído del portátil corporativo):



En el ordenador corporativo se encontró un disco duro tipo SSD en formato **2.5 pulgadas**. La carcasa metálica del disco se presenta en **buen estado**, sin signos aparentes de manipulación, golpes ni alteraciones visibles. El disco presenta en su parte superior una etiqueta identificativa del fabricante que muestra la siguiente inscripción:



En la superficie del disco son visibles los orificios de ventilación y tornillos originales de ensamblaje. No se observan marcas de haber sido desmontado o intervenido. Se procedió a etiquetar visualmente la evidencia con el identificador **RS-2025-001**, mediante una etiqueta autoadhesiva amarilla claramente visible, tal como se documenta en la imagen adjunta.

Tras su extracción, se procede al proceso de adquisición haciendo uso de un dispositivo hardware bloqueador contra escritura que evita la alteración de la información y de la herramienta **FTK Imager versión 3.4.2.6** para Sistemas Operativos Windows. Ello tuvo lugar a las **10:00h** del mismo día.

Posteriormente, se calcularon los correspondientes hashes criptográficos. Ver *“Anexo I (a): Cadena de custodia y hashes”* en página 22 de este documento.

❖ **Memoria USB. Etiquetado RS-2025-002:**

Descripción visual de la evidencia RS-2025-002 (memoria USB personal):



A las **10:45 horas** del mismo día se recibió una **memoria USB de tipo pendrive de color rojo y carcasa metálica giratoria plateada**. Se procedió a etiquetar la evidencia como **RS-2025-002**, mediante una etiqueta adhesiva de color rosa claramente visible, tal como se documenta en la imagen adjunta. Los hashes de la imagen en formato .dd del USB personal se encuentran en el *“Anexo I (a): Cadena de custodia y hashes”* en la página 22.

Tras la finalización sin errores de ambos procesos de adquisición, se realiza un nuevo resumen digital sobre la información adquirida con el objetivo de verificar que la información que se ha adquirido coincide con la existente en los dispositivos de almacenamiento.

Dicho resumen digital coincide con el realizado durante la adquisición. Lo que confirma que tanto la información de los dispositivos de almacenamiento objeto de estudio, como la contenida en las imágenes forenses generadas, es exactamente la misma.

A partir de este momento, todos los análisis se realizan sobre la copia de las imágenes forenses realizadas. Quedando los dispositivos originales y otra copia de las imágenes forenses realizadas en custodia del **Director de Seguridad Corporativa, Sr. Pink**.

4. Análisis del PC corporativo con etiqueta RS-2025-001

4.1 Estructura de las particiones:

Nr. partición	De arranque	File System	Sector Arranque	Sectores Totales	Tamaño
1	no	NTFS	2 048	204 800	100 MB
2	sí	NTFS	206 848	41 734 144	19.9 GB

La partición número 1 es la partición **de arranque técnica (bootloader)**. La partición número 2 es la partición **de arranque del Sistema Operativo**, con toda la información del usuario y de los programas. **Tamaño de sector lógico/físico:** 512 byte. **Esquema de particionado:** MBR (MS-DOS).

4.2 Análisis del Sistema Operativo

Durante el análisis del sistema, se recuperaron datos detallados sobre la versión e instalación del sistema operativo Windows instalado en el equipo bajo investigación. Estos datos provienen de la clave de registro correspondiente a la configuración del sistema operativo **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion** y se resumen a continuación:

Objetivo	Información detallada		Apuntes	
PC personal Sr Informant	Sistema Operativo	Windows 7 Ultimate (ServicePack1)	Inglés 64 bits	
	Número de compilación	7601 (Service Pack 1 instalado)		
	Tipo de instalación	Cliente multiprocesador (versión "Multiprocessor Free")		
	Fecha de instalación	22 de marzo de 2015 (timestamp 1427034866, convertido a fecha legible)		
	Propietario registrado	informant		
	Directorio raíz del sistema	C:\Windows		
	Identificador disco:	0xf0265720		
	Identificador de producto:	00426-292-0000007-85262		
	Máquinas Virtuales	Tipo	Virtual System	VMWare versión11
		Tamaño RAM	2 048 MB	
		Hardware	20 GB	
		CPU	1 procesador con 2 núcleos	
		File System	NTFS	

4.3 Análisis de los usuarios del sistema:

Cuenta	SID	Estado	Inicios de sesión	Fecha de creación	Último inicio de sesión	Fallo de inicio de sesión
informant	1000	activado	10	22-03-2015, 09:33:54	25-03-2015, 09:45:59	25-03-2015, 09:45:43
admin11	1001	activado	2	22-03-2015, 10:51:54	22-03-2015, 10:57:02	22-03-2015, 10:53:02
ITechTeam	1002	activado	0	22-03-2015, 10:52:30	-	-
Temporary	1003	activado	1	22-03-2015, 10:53:01	22-03-2015, 10:55:57	22-03-2015, 10:56:37

Parece ser que el último usuario que inició sesión en el equipo fue **informant**, el 25-03-2015, a las 09:45:59h.

4.4 Modificaciones registradas en el equipo entre los días 22 y 25 de marzo 2015

Durante el periodo comprendido entre los días **22 y 25 de marzo de 2015**, se registraron múltiples modificaciones relevantes en el sistema analizado, vinculadas a la actividad del usuario investigado, que incluyen acceso a archivos, envío de correos electrónicos, uso de dispositivos externos, conexiones a unidades de red, navegación web y empleo de herramientas potencialmente orientadas a la eliminación de huellas digitales.

Dado el volumen, complejidad y valor probatorio de estas acciones, se ha elaborado una **línea temporal detallada** que integra cronológicamente los eventos más relevantes observados durante el análisis.

Para su correcta interpretación y análisis estructurado, se remite al lector al *ANEXO II: Línea Temporal Completa*, en la página 28.

4.5 Análisis de los programas instalados en el equipo

Analizando los archivos de registro del Sistema Operativo, se obtiene que los programas instalados en el equipo son:

	Tipo de herramienta	Nombre de herramienta	Relación y concreciones
Herramientas/ aplicaciones	E-Mail	Microsoft Outlook	NIST.gov email
	Nube	-Google Drive -Apple iCloud	-Sincronización automática activada
	Ofimática	Microsoft Office	-Word, Power Point, Excel
	Navegadores	Internet Explorer, Google Chrome	
	Software Anti Forense	Ccleaner, Eraser	

4.6 Análisis de correos electrónicos:

Para el análisis del correo electrónico se utilizó la herramienta Autopsy sobre la imagen forense del disco, centrando la revisión en los archivos **.ost** y registros de sincronización asociados al cliente Microsoft Outlook, ubicado en el perfil del usuario **informant**. Mediante la extracción y análisis de artefactos de tipo **Email Parser** y búsquedas por palabras clave, se recuperaron múltiples mensajes, algunos de ellos eliminados, que evidencian comunicaciones directas entre el usuario investigado y un tercero (identificado como "spy"). Estas comunicaciones revelan intercambios de información sensible y posibles intentos de ocultamiento, siendo altamente relevantes para el caso. La cuenta de correo configurada en el equipo es: iaman.informant@nist.gov. El software de correo electrónico usado fue **Microsoft Outlook 2013**. Prueba hallada en las rutas:

```
HKU\informant\Software\Microsoft\Office\15.0\Outlook
HKLM\SOFTWARE\Clients\Mail (Microsoft Outlook)
```

y también en:

/Users/informant/AppData/Local/Microsoft/Outlook

El hecho de que estos elementos se ubiquen en el perfil de usuario (Users) denominado **"informant"**, o en **HKU\informant...** y considerando que el equipo analizado lleva el nombre de **"informant-PC"**, refuerza de forma contundente la asociación entre dicho buzón de correo y el usuario investigado.

Algunas observaciones a destacar:

- ❖ Cuatro de los correos más comprometidos se localizaron en la carpeta de "Deleted Items", lo que sugiere eliminación consciente por parte del usuario. En concreto, en **Mailbox\PM_SUBTREE\Deleted Items**.
- ❖ Los mensajes muestran un proceso progresivo de filtración de información, negociación sobre el método de entrega, advertencias de seguridad y finalmente la confirmación de la acción.
- ❖ La utilización de Google Drive y la mención directa de dispositivos USB constituyen pruebas claras de intento de exfiltración de información confidencial.

Información relevante extra en *"ANEXO II: Línea Temporal Completa"*, y en *"Anexo VI (a) Descargas de software - servicio en la nube"*, página 47.

4.7 Actividad ofimática del usuario informant

Durante el análisis forense se hallaron evidencias sólidas de que el usuario **informant** accedió y trabajó con documentos sensibles utilizando aplicaciones del paquete **Microsoft Office** (Word, Excel y PowerPoint), entre los días **23 y 25 de marzo de 2015**. Estos archivos incluían nombres altamente indicativos de contenido confidencial, como:

- ❖ [secret_project]_proposal.docx
- ❖ [secret_project]_design_concept.ppt
- ❖ (secret_project)_pricing_decision.xlsx
- ❖ [secret_project]_final_meeting.pptx

Se comprobó que estos documentos fueron abiertos directamente desde una **unidad USB externa (RM#1)** y luego copiados al escritorio del equipo corporativo del usuario, en la

carpeta “**S data**”, lo que constituye un indicio de consolidación de información confidencial en el entorno local.

Además, se registró una conexión a una **unidad de red compartida interna** con dirección **\\10.11.11.128\secured_drive**, desde donde se accedieron y copiaron nuevos archivos sensibles, como se documenta en la **línea temporal extraída con Autopsy**.

Las búsquedas intencionadas realizadas desde el buscador del sistema con términos como “secret”¹ refuerzan el carácter deliberado de estas acciones. Estas evidencias se complementan con entradas MRU (Most Recently Used) extraídas mediante el plugin **msoffice** de **RegRipper**, que confirman el acceso a los documentos en fechas clave del incidente.

Por otra parte, se identificó en el escritorio del usuario un archivo titulado **"Resignation_Letter_(Iaman_Informant).xps"**, accedido el **25 de marzo de 2015 a las 16:28h CET**. El contenido de esta carta confirma la intención de dimisión del usuario informant el mismo día en que se observa actividad de transferencia de información sensible. El archivo fue hallado en estado **allocated**, lo que indica que no fue eliminado, y su vinculación con los eventos investigados resulta altamente significativa.

Para más información, consultar:

- ❖ **Anexo II: Línea Temporal Completa**, página 28.
- ❖ **Anexo IV: Anexo IV (b) Carta de Renuncia**, página 38.

4.8 Zona horaria del PC corporativo del Sr Informant

El hecho de que el sistema analizado tuviera configurada la zona horaria en "Hora del Este (EE. UU. y Canadá)" —según lo hallado en la clave del registro **HKLM\SYSTEM\ControlSet001\Control\TimeZoneInformation**— implica que el usuario **informant** operaba su equipo alineado con el huso horario de la costa este de Estados

¹ En la clave de registro:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery se encontraron entradas que reflejan términos buscados, incluyendo la palabra **"secret"**, en formato Unicode. La lista de términos recientes (**MRUListEx**) aparece vacía o borrada, sin embargo, los valores individuales revelan búsquedas previas realizadas por el usuario. Se detectó además el valor **ExplorerStartupTraceRecorded** con valor 0x1, que indica que **el explorador fue iniciado y monitoreado**. Las claves **Shellstate** y **Cleanshutdown** contienen valores que indican el estado del explorador y que éste fue cerrado correctamente en su última sesión.

Unidos (UTC-5/UTC-4 en horario de verano). Esta configuración no es habitual en sistemas localizados en otras regiones (como Europa), y podría indicar un **intento deliberado de simular una localización geográfica diferente**, o bien reflejar **una sincronización horaria con servidores o servicios externos ubicados en EE. UU.**, lo que puede resultar relevante si se analiza junto con comunicaciones o conexiones remotas observadas durante el periodo investigado.

Zona horaria	Hora del Este (EE. UU. y Canadá)
Sesgo de horario de verano	+1
Información encontrada en:	HKLM\SYSTEM\ControlSet###\Control\TimeZoneInformation

Más información en “ANEXO III: Configuración regional y zona horaria del sistema”, en la página 35.

4.9 Navegadores instalados en el equipo y búsquedas realizadas

Los navegadores instalados en el equipo y usados por el usuario Informant son: **Microsoft Internet Explorer 9** o versión anterior actualizada a la **versión 11** con ubicación en **C:\Program Files (x86)\Internet Explorer** y última fecha de uso registrada: **25 de marzo de 2015 a las 15:46:16 CET**.

Además, estaba instalado **Google Chrome v41.0.2272.101**, con ubicación en **C:\Program Files (x86)\Google\Chrome\Application**, y última fecha de uso registrada: **24 de marzo de 2015 a las 22:05:38 CET**. Información encontrada en:

```
HKLM\SOFTWARE\Microsoft\Internet Explorer (value: svcVersion)
HKU\informant\Software\Google\Chrome\BLBeacon (value: version)
```

Las búsquedas realizadas por el Sr. Informant en los navegadores, especialmente entre los días 22 y 23 de marzo de 2015, resultan clave en este caso pericial porque revelan de forma directa sus **intenciones, motivaciones y preparación** para una posible exfiltración de información. Se identificaron consultas sobre *data leakage*, *leaking confidential*

information, cloud storage, anti-forensics, cómo eliminar datos, y recuperación de archivos, lo cual demuestra un interés claro por conocer métodos tanto de filtración como de encubrimiento de actividad digital. Estas búsquedas coinciden temporalmente con la apertura y transferencia de documentos confidenciales, el uso de servicios en la nube y la redacción de una carta de renuncia, consolidando un patrón de comportamiento planificado.

Para más información, consultar “ANEXO II: Línea Temporal Completa”, y “Anexo V (b) Webs accedidas por Sr. Informant” en la página 44.

4.9.1 Análisis de bookmarks (acceso directo o marcador de navegador)

La presencia de accesos directos a sitios gubernamentales estadounidenses, concretamente **USA.gov** y **GobiernoUSA.gov**, en la carpeta personalizada de favoritos del navegador del usuario (**C:\Users\informant\Favorites\Links for United States**), tiene importantes implicaciones en el contexto de esta pericial. En primer lugar, confirma que dichos marcadores fueron creados o mantenidos manualmente por el propio usuario, y no forman parte de configuraciones predeterminadas del sistema. Además, este hallazgo es completamente coherente con el uso de una cuenta de correo **@nist.gov**, observada en múltiples correos analizados durante esta investigación.

Para más información, consultar “Anexo VI (b) REMOTE DESKTOP”, en la página 47.

4.10 Herramientas anti forenses descargadas y ejecutadas

Examinando el historial web, figura que el día **24-03-2015 a las 10:07h** el usuario Informant ha estado buscando métodos anti forenses, en los navegadores Chrome e Internet Explorer (información ya explicada en el apartado anterior **Timeline**). Esta actividad ha durado hasta las 14h aproximadamente.

Además, se ha encontrado que el día 25-03-2015 a las 10:46h el usuario Informant ha descargado herramientas con finalidades anti forenses, tales como **Eraser** y **CCleaner**.

Por un lado, **Eraser** es un programa que se usa para **borrar archivos de forma segura**, de manera que **no puedan recuperarse** después, ni siquiera con herramientas forenses. Lo

hace sobrescribiendo varias veces el espacio del archivo con datos aleatorios. Es eficaz si se quiere asegurar que archivos eliminados no puedan ser restaurados.

CCleaner es una herramienta que limpia el sistema eliminando **archivos temporales**, **historial de navegación**, **cookies**, y otros archivos innecesarios para liberar espacio y mejorar el rendimiento del equipo.

Ccleaner se ejecutó el día 25-03-2015 a las 11:15:50, y se desinstaló el mismo día a las 11:18:29.

Eraser se ejecutó el mismo día, a las 11:13:30, y se borraron los archivos ejecutables de instalación de ambas herramientas a las 11:15:45.

Más información en “*Anexo V (c) Búsquedas relevantes en los navegadores*”, página 45.

5. Análisis de la fuente de información RS-2025-002 (USB personal del Sr. Informant)

5.1 Estructura de las particiones²

Nr. partición	De arranque	File System	Sector Arranque	Sectores Totales	Tamaño
1	si	NTFS	2 048	1 972 223	1 Gb

ID de la imagen del dispositivo: **5420f42d-e67d-4584-a8a7-4809d105e6dc**.

Al comienzo del análisis pericial se informó al perito que la memoria USB es propiedad del Sr. Informant. A pesar de estar en su puesto de trabajo, su condición de bien privado impide legalmente el acceso a su contenido sin autorización judicial. La Constitución Española y la Ley Orgánica 13/2015 protegen expresamente este tipo de dispositivos, incluso si fueron introducidos de forma irregular en el entorno laboral.

² Se deja constancia de que no se ha accedido ni analizado el contenido de los archivos almacenados en el dispositivo, limitándose el examen exclusivamente a la estructura lógica del mismo (particiones, sistemas de archivos y configuración general). Dicho análisis, al no implicar el tratamiento de datos personales ni el acceso a información identificativa o sensible, no supone una vulneración del derecho a la intimidad ni una infracción de la normativa vigente en materia de protección de datos personales.

En consecuencia, se ha mantenido el USB bajo cadena de custodia, sin análisis alguno. Se recomienda obtener autorización judicial previa si se considera necesario examinar su contenido. Proceder sin dicha autorización vulneraría derechos fundamentales y podría invalidar cualquier prueba obtenida.

Más información en “Anexo I (b) : Contexto Legal y Limitación en el Análisis del USB”, en la página 27.

6. Conclusiones

1. **Integridad de las evidencias asegurada:** La adquisición de las imágenes forenses de los dispositivos RS-2025-001 (PC corporativo) y RS-2025-002 (USB personal) se realizó siguiendo procedimientos estandarizados, con protección contra escritura y cálculo de hashes criptográficos, garantizando la cadena de custodia e integridad de los datos.
2. **Existencia de comunicaciones relevantes:** Se localizaron correos electrónicos entre el Sr. Informant y un tercero (identificado como "Spy") que evidencian conversaciones sobre intercambio de información sensible, incluyendo enlaces a archivos compartidos a través de Google Drive.
3. **Uso de aplicaciones de sincronización en la nube:** Se detectó el uso activo del cliente oficial de Google Drive, configurado con una cuenta personal del usuario (iaman.informant.personal@gmail.com), mediante el cual se sincronizó al menos un archivo con contenido sensible.
4. **Acceso y consolidación de documentos confidenciales:** Se confirmaron accesos a archivos con nombres indicativos de contenido estratégico (como [secret_project]_proposal.docx o pricing_decision.xlsx), abiertos desde unidades USB y red, y organizados en el escritorio local del usuario bajo una carpeta denominada “S data”.

5. **Conducta orientada a la ocultación:** Se hallaron indicios de utilización de herramientas como Eraser y CCleaner, orientadas al borrado seguro y limpieza del sistema, ejecutadas el día 25 de marzo de 2015, coincidiendo con los últimos eventos sospechosos.
 6. **Redacción de una carta de renuncia:** El archivo “Resignation_Letter_(laman_Informant).xps” fue creado y accedido el 25 de marzo, en la misma franja temporal en la que se observa el borrado de archivos, uso de la nube y envío de correos, lo que sugiere una posible relación entre la renuncia y los hechos analizados.
 7. **Búsquedas web reveladoras:** Entre los días 23 y 25 de marzo, el usuario realizó búsquedas específicas relacionadas con fuga de información, herramientas anti-forenses y almacenamiento en la nube, lo que refuerza el carácter premeditado de sus acciones.
 8. **Marcadores y configuración regional coherente con el perfil del usuario:** La presencia de accesos directos a sitios del gobierno de EE.UU. y el uso de una cuenta de correo @nist.gov son coherentes con una posible vinculación temática o profesional con entidades estadounidenses. A su vez, la zona horaria del sistema estaba configurada en Eastern Standard Time.
 9. **Limitaciones legales observadas:** No se procedió al análisis del contenido del dispositivo USB RS-2025-002 al no disponer de autorización judicial, en cumplimiento con la normativa legal vigente (Constitución Española y LOPJ).
-

6. ANEXOS:

ANEXO I: Cadena de custodia, hashes, e implicaciones legales

Anexo I (a): Cadena de custodia y hashes

Datos de remisión	
Nº de Caso	211093
Hecho investigado	Revelación de secretos por parte del trabajador Informant que pudo haber cedido información sobre proyecto confidencial de alto impacto comercial. La información sustraída habría sido intercambiada mediante correos electrónicos camuflados como comunicaciones legítimas entre empresas, y otra parte habría sido transmitida utilizando sistemas de almacenamiento en la nube.

Datos de recogida	
Fecha de recogida	22 mayo 2025, 10:00:00h
Lugar de recogida	Oficinas centrales de ROCK STAR, S.A. , en la Avda. de la Verdad 123, Edificio Rock Tower, Madrid
Responsable de la toma	Dragos Cornel Iván Andrei, Con DNI 123 456 78-M, Actuando como PERITO DE PARTE
Observaciones	

Identificación de las evidencias que se remiten		
Nº de la evidencia	Descripción	Precinto
RS-2025-001	<p>En el lugar de adquisición de la evidencia, se localizó un disco duro de estado sólido (SSD) en formato de 2.5 pulgadas, conectado al interior del equipo investigado. Por razones operativas, no se tuvo acceso directo al número de serie ni a la capacidad total del dispositivo.</p> <p>No obstante, se procedió a realizar una extracción parcial de datos con la herramienta FTK Imager versión 3.4.2.6, limitándose exclusivamente a los 20 GB de información considerados relevantes para la presente investigación pericial, garantizando en todo momento el respeto a los principios de integridad y minimización de la evidencia.</p> <p>El disco duro tiene una etiqueta con la inscripción:</p> <p style="text-align: center;">71184-T3F-03</p> <p style="text-align: center;">2H9X09MF</p> <p style="text-align: center;">32J</p>	RS-2025-001
RS-2025-002	<p>La evidencia identificada como USB RS-2025-002 corresponde a un dispositivo de almacenamiento USB tipo pendrive de 2.0, con formato físico estándar de 2.5 pulgadas, intervenido en el entorno físico relacionado con la presente investigación. El dispositivo se encuentra en aparente buen estado externo; no se observan roturas, grietas ni elementos desprendidos. El diseño corresponde a un modelo genérico de pendrive de tipo giratorio, con protección mecánica del conector USB. No se aprecian marcas de fabricante ni número de serie visible en la carcasa exterior.</p>	RS-2025-002

Cadena de Custodia					
DNI	Fecha y Hora	Nº de Evidencia	Acción Realizada	Observaciones	
123456789-M	22 mayo 2025, 10:00h	RS-2025-001	Recolección de la evidencia	La evidencia (disco duro) es entregada en mano por el Director de Seguridad Corporativa, Sr. Pink	
	22 mayo 2025, 10:00h	RS-2025-002	Recolección de la evidencia	La evidencia (USB) es entregada en mano por el Director de Seguridad Corporativa, Sr. Pink	
		RS-2025-001	Cálculo de Hashes	MD5	a49d1254c873808c58e6f1bcd60b5bde
				SHA-1	afe5c9ab487bd47a8a9856b1371c2384d44fd785
		RS-2025-002	Cálculo de Hashes	MD5	c42465c6876c7066989f3f13c3b2f7b6
				SHA-1	d9f4bbea05d57f43971ea6ceab18fd02e1b9a5c6
		RS-2025-001	Adquisición, mediante conexión al dispositivo que bloquea la evidencia contra escritura, y uso de herramienta forense FTK Imager versión 3.4.2.6 , guardándose la copia de la imagen forense con el nombre "cfreds_2015_data_leakage_pc" en formato .dd en un pendrive propiedad de sniper S.A.	<p>El proceso de adquisición calcula automáticamente el hash SHA-1 de la imagen adquirida, que resultar ser:</p> <p>afe5c9ab487bd47a8a9856b1371c2384d44fd785</p> <p>La imagen adquirida es copia fiel de la evidencia original.</p> <p>El Responsable de la Toma, el perito Dragos Cornel Iván Andrei conserva esta copia fiel de la evidencia original para su posterior análisis en el laboratorio.</p> <p>El disco duro y otra copia de la imagen, quedan en manos del Director de Seguridad Corporativa, Sr. Pink.</p>	

Cadena de Custodia				
		RS-2025-002	<p>Adquisición, mediante conexión al dispositivo que bloquea la evidencia contra escritura, y uso de herramienta forense FTK Imager versión 3.4.2.6, guardándose la copia de la imagen forense con el nombre "USB" en formato .dd en un pendrive propiedad de sniper S.A.</p>	<p>El proceso de adquisición calcula automáticamente el hash SHA-1 de la imagen adquirida, que resultará ser:</p> <p>d9f4bbea05d57f43971ea6ceab18fd02e1b9a5c6</p> <p>La imagen adquirida es copia fiel de la evidencia original.</p> <p>El Responsable de la Toma, el perito Dragos Cornel Iván Andrei conserva esta copia fiel de la evidencia original para su posterior análisis en el laboratorio.</p> <p>El USB y otra copia de la imagen, quedan en manos del Director de Seguridad Corporativa, Sr. Pink.</p>
		RS-2025-001	<p>Precintado de la evidencia</p>	<p>La evidencia se precinta como RS-2025-001, siendo dicho disco duro custodiado por el mismo Entregante de este, el Director de Seguridad Corporativa, Sr. Pink.</p> <p>El perito designado, Dragos Cornel Iván Andrei conservará la copia de la evidencia en formato .dd. en su propio USB, para su posterior análisis en el laboratorio.</p>
		RS-2025-002	<p>Precintado de la evidencia</p>	<p>La evidencia se precinta como RS-2025-002, siendo dicho USB custodiado por el mismo Entregante de este, el Director de Seguridad Corporativa, Sr. Pink.</p> <p>El perito designado, Dragos Cornel Iván Andrei conservará la copia de la evidencia en formato .dd. en su propio USB, para su posterior análisis en el laboratorio.</p>

Otras observaciones

1.- La evidencia RS-2025-002 o dispositivo USB personal del Sr Informant fue **accesible físicamente**, aunque **no se pudo identificar visualmente el número de serie ni el fabricante impreso en la carcasa externa**, debido a la ausencia de etiquetado o marca visible. Se hizo una imagen forense en formato .dd con **FTK Imager versión 3.4.2.6**, sin proceder a ningún tipo de análisis.

2.- Durante dicho proceso de recogida el perito responsable aquí operante fue informado de que dicha evidencia **RS-2025-002** pertenece al ámbito estrictamente **personal** del usuario **"informant"**.

Dado que dicho dispositivo a priori no guarda relación técnica directa con los hechos investigados y no se cuenta con una **autorización judicial** que habilite su análisis, **se ha decidido no proceder a su adquisición ni examen forense**, en cumplimiento con la normativa vigente en materia de derechos fundamentales y protección de la intimidad.

En **Madrid**, a fecha de **22 mayo 2025**,

El **responsable** de la toma

Dragos Cornel Iván Andrei

DNI 123456789-M

Perito Informático y Técnico en Electrónica

Anexo I (b) : Contexto Legal y Justificación de la Limitación en el Análisis del Dispositivo USB

En el presente encargo pericial se ha solicitado el análisis técnico-forense de la memoria USB localizada en la mesa de trabajo del Sr. Iaman Informant, durante el precintado de su puesto tras su suspensión laboral.

Si bien la empresa dispone de normativas internas, debidamente comunicadas a sus empleados, que restringen la introducción de dispositivos electrónicos no autorizados y establece la potestad de auditar los sistemas informáticos corporativos, **esta facultad no**

puede interpretarse de forma extensiva a los efectos de permitir el análisis forense de bienes de propiedad privada sin las debidas garantías jurídicas. En concreto:

I.I (b) Diferenciación entre Recursos Corporativos y Bienes de Propiedad Privada

- Los sistemas informáticos propiedad de la empresa (ordenadores corporativos, redes internas, correos electrónicos corporativos) pueden ser objeto de análisis por la propia organización, siempre que medie causa justificada y se respete el principio de proporcionalidad, conforme a la jurisprudencia consolidada del Tribunal Supremo (STS 532/2017, de 13 de julio).
- No ocurre lo mismo con objetos personales que, aunque introducidos de forma irregular en el centro de trabajo (como en este caso la memoria USB del Sr. Informant), conservan la condición de bien de titularidad privada, gozando de la protección constitucional establecida en el:
 - **Artículo 18.2 de la Constitución Española**, que garantiza la inviolabilidad de las comunicaciones y dispositivos personales, salvo resolución judicial motivada.
 - **Ley Orgánica 13/2015**, que regula la intervención de dispositivos electrónicos, estableciendo que sólo puede autorizarse mediante auto judicial y en el marco de una investigación penal, cuando concurren indicios suficientes de delito y se respeten las exigencias de necesidad, idoneidad y proporcionalidad.

I.II (b) Conclusión sobre el Análisis del USB sin Autorización Judicial

Aunque la empresa pueda confiscar preventivamente el dispositivo para preservar su integridad, dicha medida debe ejecutarse siguiendo una cadena de custodia adecuada y sin acceso ni manipulación del contenido, salvo que exista: **Consentimiento expreso y documentado** del titular del dispositivo y además una **Autorización judicial expresa**, en el marco de una investigación penal.

De modo que proceder al análisis forense de la memoria USB sin dichas garantías podría suponer: una vulneración de derechos fundamentales del trabajador, invalidez de las pruebas obtenidas, conforme al principio de

ilicitud de la prueba (art. 11.1 de la Ley Orgánica del Poder Judicial) y potenciales responsabilidades legales para los intervinientes.

I.III (b) Recomendación Técnica y Legal

En base a lo anterior se recomienda lo siguiente:

- ❖ Mantener el dispositivo USB bajo cadena de custodia, sin realizar análisis del contenido.
- ❖ Solicitar, en su caso, la pertinente autorización judicial por parte de las Fuerzas y Cuerpos de Seguridad del Estado o del Ministerio Fiscal, para proceder legalmente al análisis técnico-forense.
- ❖ Abstenerse de cualquier acción que pueda comprometer la validez de las pruebas o los derechos fundamentales de las personas implicadas.

Anexo II : Línea Temporal Completa

Fecha	Hecho	Información extra	Notas
22-03-2015	Instalación sistema operativo	Windows 7 Ultimate	
	Configuración horaria	Se configura a (UTC-05) Eastern Time	
	Instalación software	Microsoft Office, y navegadores Microsoft Internet Explorer y Google Chrome	
	Email	Se configura Microsoft Outlook con la cuenta "NIST".	
	Creación de cuentas de usuario	"admin11", login count: 2 "ITech Team", login count: 0 "temporary", login count: 1	"admin11" ha iniciado sesión 2 veces, "ITech Team" 0 veces, y el usuario "temporary" 1 vez.

23-03-2015, 13:29	iaman recibe el primer email	spy.conspirator@nist.gov envía email a iaman.informant@nist.gov	Asunto: Hello, iaman. Contenido: «¿Cómo estás?»
23-03-2015 entre las 14:01 y 14:21	Preparación de la venta-fuga de información	El sospechoso Informant empieza a buscar información en los navegadores Internet explorer y Google Chrome	A través de Bing , con el navegador Google Chrome se buscó la siguiente información: 1) data leakage methods 2) leaking confidential information 3) information leakage cases 4) intellectual property theft 5) how to leak a secret 6) cloud storage 7) digital forensics 8) how to delete data 9) anti-forensics 10) system cleaner 11) how to recover data 12) data recovery tools A través de Internet Explorer , se buscó: 1) file sharing and tethering 2) DLP DRM 3) e-mail investigation 4) what is windows system artifacts 5) investigation on windows machine 6) windows event logs 7) cd burning method in Windows 8) external device and forensics

23-03-2015, 14:31	Se conecta USB al PC Corporativo	Nombre "RM#1"	
23-03-2015, 14:36	Búsqueda de palabras clave	laman busca información confidencial a través del buscador de Windows	Se busca la palabra "secret"
23-03-2015, 14:37	Se abren y leen los siguientes archivos	[secret_project]_proposal.docx [secret_project]_design_concept.ppt	
23-03-2015, 14:39	Se copian y abren los siguientes documentos, desde el USB RM#1, al PC corporativo de Informant	Documento y localización en el USB: RM#1\Secret Project Data\proposal\[secret_project]_proposal.docx RM#1\Secret Project Data\design\[secret_project]_design_concept.ppt	Localización en el PC: %UserProfile%\Desktop\Sdata\[secret_project]_proposal.docx %UserProfile%\Desktop\Sdata\[secret_project]_design_concept.ppt
23-03-2015, 14:39	Se desconecta el USB "RM#1"		

23-03-2015, 14:44	laman envía email a spy	iaman.informant@nist.gov a spy.conspirator@nist.gov	"Asegurado con éxito"
23-03-2015, 15:14	laman recibe email	de parte de spy.conspirator@nist.gov	Asunto: buen trabajo amigo. Contenido: "Buen trabajo. Necesito más detalles sobre este negocio."
23-03-2015, 15:19	laman manda email con el correo iaman.informant@nist.gov	hacia spy.conspirator@nist.gov	"Esto es una muestra": (space_and_earth.mp4)
23-03-2015, 15:20	laman recibe email	de parte de spy.conspirator@nist.gov	"Vale, lo tengo. Estaremos en contacto."
23-03-2015, 15:26	laman recibe email	de parte de spy.conspirator@nist.gov	Asunto: tarea importante Contenido: "Lo he confirmado. Pero necesito más información. Haz lo mejor que puedas."

23-03-2015, 15:27	laman manda email con el correo iaman.informant@nist.gov	hacia spy.conspirator@nist.gov	"Necesito más tiempo para pensar".
23-03-2015, 16:00	Búsqueda y descarga de aplicaciones	Buscando servicios de almacenamiento en la nube, vía Chrome	
23-03-2015, 16:00	Instalación de aplicaciones	Google Drive, Apple iCloud.	
23-03-2015, 16:05	Conexión a almacenamiento en la nube	Ello se lleva a cabo mediante el correo: iaman.informant.personal@gmail.com	
23-03-2015, 16:23	Conexión de unidad de red	\\10.11.11.128\secured_drive	Se apunta a una dirección IP local o de red corporativa, lo que sugiere que se trata de un servidor de archivos interno perteneciente a la organización. Es probable que en esa carpeta se almacenara información confidencial o crítica para el negocio.
23-03-2015, 16:24	Búsqueda de archivos	Identificación de archivos vía Windows Explorer, para su posterior transferencia	
23-03-2015, 16:26	Apertura y lectura de los siguientes archivos	(secret_project)_pricing_decision.xlsx [secret_project]_final_meeting.pptx	"\Desktop\S data"
23-03-2015, 16:28	Copia y apertura de los archivos anteriores	Desde una unidad de red hacia el PC corporativo	
23-03-2015, 16:29	Desconexión de unidad de red	\\10.11.11.128\secured_drive	
23-03-2025, 16:30	Se renombran archivos y cambian extensiones	"(secret_project)_pricing_decision.xlsx" pasa a llamarse happy_holiday.jpg	

		"[secret_project]_final_meeting.pptx" pasa a llamarse do_u_wanna_build_a_snow_man.mp3	
23-03-2025, 16:32	Se suben archivos	Se suben los archivos anteriores a Google Drive y se comparten	Los archivos son "happy_holiday.jpg" y "do_u_wanna_build_a_snow_man.mp3"
23-03-2025, 16:38	laman manda email con el correo iaman.informant@nist.gov	hacia spy.conspirator@nist.gov	Asunto: "Soy yo" Contenido: "Usa el link de abajo"
23-03-2025, 16:41	laman recibe email	de parte de spy.conspirator@nist.gov	"Lo tengo"
23-03-2025, 16:42	Borrado de archivos	En Google Drive	
24-03-2025, 09:26	laman recibe email	de parte de spy.conspirator@nist.gov	Asunto: última oportunidad Contenido: "Esta es la última oportunidad. Quiero la información restante".
24-03-2025, 09:30	laman manda email con el correo iaman.informant@nist.gov	hacia spy.conspirator@nist.gov	"¡Para! Es muy difícil enviar información a través de internet!"
24-03-2025, 09:33	laman recibe email	de parte de spy.conspirator@nist.gov	"No hay problema. Puedes entregar directamente los dispositivos de almacenamiento que la almacenaba".
24-03-2025, 09:35	laman manda email con el correo iaman.informant@nist.gov	hacia spy.conspirator@nist.gov	"Esto es la última vez".
24-03-2025, 09:38	Se conecta USB al PC corporativo	USB RM#1	
24-03-2025, 09:40	Se proceden a copiar los archivos	Desde el USB se copian: RM#1\Secret Project Data\design\[secret_project]_design_concept.ppt RM#1\Secret Project Data\design\[secret_project]_detailed_design.pptx	Hacia el PC se copian: %UserProfile%\Desktop\Secret Project Data\design\[secret_project]_design_concept.ppt %UserProfile%\Desktop\Secret Project

		RM#1\Secret Project Data\design\[secret_project]_revised_points.ppt RM#1\Secret Project Data\proposal\[secret_project]_detailed_proposal.docx RM#1\Secret Project Data\proposal\[secret_project]_proposal.docx	Data\design\[secret_project]_detailed_design.pptx %UserProfile%\Desktop\S data\Secret Project Data\design\[secret_project]_revised_points.ppt %UserProfile%\Desktop\S data\Secret Project Data\proposal\[secret_project]_detailed_proposal.docx %UserProfile%\Desktop\S data\Secret Project Data\proposal\[secret_project]_proposal.docx
24-03-2025, 09:40	Se expulsa el USB RM#1		
24-03-2025, 09:47	Se vuelve a conectar la unidad de red	\\10.11.11.128\secured_drive	
24-03-2025, 09:47	Se copian archivos desde unidad de red a PC		

24-03-2025, 10:07	Se borran directorios del PC	Se borra "\Desktop\S data"	
24-03-2025, 10:07	Búsquedas web de métodos anti forenses	Se usan Chrome e Internet Explorer	
24-03-2025, 14:32	Se crea la carta de renuncia en formato .docx		
24-03-2025, 15:32	laman recibe email	de parte de spy.conspirator@nist.gov	Asunto: ¡¡Ten cuidado!! Contenido: Los USB son fácilmente detectables. Usa otro método
24-03-2025, 15:34	laman manda email	hacia spy.conspirator@nist.gov	"Lo estoy intentando"

	con el correo iaman.informant@nist.gov		
24-03-2025, 17:05	laman manda email con el correo iaman.informant@nist.gov	hacia spy.conspirator@nist.gov	Asunto: Hecho. Contenido: “Ya está hecho. Te veo mañana”.
25-03-2025, 10:46	Búsqueda de apps	vía Internet Explorer se buscan herramientas anti forenses	
25-03-2025, 10:50	Se instalan aplicaciones	Eraser y CCleaner	
25-03-2025, 11:00	Se borran emails	en Outlook	
25-03-2025, 11:13	Se borran pistas	vía Eraser y CCleaner	En concreto, con Eraser se borra “Desktop\temp”
25-03-2025, 11:14	Se vacía la papelera de reciclaje		
25-03-2025, 11:15	Se abre CCleaner pero no se ejecuta sobre nada		
25-03-2025, 11:22	Se ejecuta Google Drive	Se desconecta de la sesión (Logout) de la cuenta	
25-03-2025, 11:24	Se abre la carta de renuncia de laman	La carta es extensión .docx y se abre desde el Escritorio	

ANEXO III: Configuración regional y zona horaria del sistema

Todos los eventos cronológicos extraídos han sido estandarizados a **UTC (Tiempo Universal Coordinado)**, tal y como aparecen representados en la herramienta Autopsy.

La configuración del sistema investigado utilizaba la zona horaria **Eastern Standard Time (EST/EDT)**, lo cual supone una diferencia de **-5 o -4 horas** respecto a UTC, dependiendo del horario de verano. Esta conversión se ha tenido en cuenta al interpretar los eventos.

Durante el análisis del hive del Registro (**SYSTEM**), se extrajeron las claves correspondientes a la configuración de la zona horaria del equipo analizado. En concreto, se encontró la siguiente información en la rama:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
```

- ❖ **Horario de verano habilitado:** Sí
- ❖ **Transición a horario de verano:** Primer domingo de marzo a las 02:00 h
- ❖ **Transición a horario estándar:** Primer domingo de noviembre a las 02:00 h

Consideración pericial sobre la configuración regional:

Todos los registros horarios extraídos (correos, archivos, registros de sistema, etc.) fueron ajustados automáticamente por las herramientas de análisis (como Autopsy) a la zona horaria UTC.

Sin embargo, el sistema original operaba en la zona **Eastern Standard Time con horario de verano activo (UTC -4 horas)** durante las fechas relevantes del caso (marzo de 2015).

Además, se observa que la gestión del horario de verano se encontraba habilitada (`DynamicDaylightTimeDisabled = 0`), y que los valores binarios `DaylightStart` y `StandardStart` coinciden con las reglas estándar de transición horaria utilizadas en EE. UU.

Estos datos permiten confirmar que el entorno analizado operaba bajo el **contexto horario de la costa este de los Estados Unidos**, lo cual es coherente con otras evidencias

encontradas, como el dominio de correo electrónico **@nist.gov** y la configuración regional del sistema operativo.

ANEXO IV: Evidencias de exfiltración de información

Anexo IV (a) Evidencia de uso del cliente de Google Drive

En el sistema analizado se ha localizado el archivo: **syncclient.mo**, ubicado en el directorio correspondiente al cliente de Google Drive, con fecha de modificación **25 de marzo de 2015**. Este archivo contiene cadenas de localización pertenecientes a la interfaz del cliente oficial de sincronización de Google Drive, tales como:

"Start sync", "Upload Error", "Auto backup", "drive.google.com", entre muchas otras. La presencia de este archivo, junto con su fecha coincidente con los eventos clave del caso (transmisión de archivos, envío de enlaces, borrado de evidencias), permite afirmar con alto grado de certeza que el usuario informant **tenía instalado y activo el cliente de Google Drive**, y que lo utilizó durante la ventana temporal crítica para **sincronizar o transmitir documentos confidenciales** hacia cuentas externas. Esta información se complementa con otras pruebas aquí encontradas.

Además, se identificaron múltiples archivos del tipo .dll con nombres como lang10-15.dll, cuyo contenido coincide con mensajes de localización e interfaz del cliente oficial de sincronización de Google Drive. Estas bibliotecas contienen textos como: **"Has eliminado un Google Doc de tu carpeta Google Drive"**, **"Tu carpeta Google Drive no está disponible"**, o **"El administrador de tu dominio ha desactivado este producto"**.

Se ha localizado, por último, el archivo **sync_config.db** en la ruta **/Users/informant/AppData/Local/Google/Drive/user_default/sync_config.db**, correspondiente a la base de datos de configuración del cliente oficial de sincronización de Google Drive, en la misma fecha **25-03-2015 a las 16:22:48h CET**.

Su análisis revela las siguientes entradas clave:

❖ **Archivo sincronizado:**

Resignation_Letter_(Iaman_Informant).xps, encontrado en la **ruta:**

C:\Users\informant\Desktop\Resignation_Letter_(Iaman_Informant).xps

❖ **Cuenta utilizada para sincronizar:**

iaman.informant.personal@gmail.com

❖ **Directorio de sincronización:**

C:\Users\informant\Google Drive

❖ **Versión del cliente:**

1.20.8672.3137

Esta evidencia confirma que el usuario informant **sincronizó al menos un documento** clave, potencialmente confidencial, desde **su escritorio** hacia **su cuenta personal de Google Drive**, utilizando el cliente oficial de sincronización.

La acción se encuentra enmarcada temporalmente en el contexto de la investigación, coincidiendo con los correos electrónicos sospechosos, el acceso al documento y el uso de herramientas de limpieza, y representa **otra posible evidencia de exfiltración de información a una cuenta externa no autorizada**.

Anexo IV (b) Carta de Renuncia

Se ha detectado y verificado la existencia del documento titulado **Resignation_Letter_(Iaman_Informant).xps**. Esto estaba ubicado en el escritorio del PC corporativo del usuario **informant**:

C:\Users\informant\Desktop\Resignation_Letter_(Iaman_Informant).xps

El análisis confirma que dicho archivo se encuentra en estado **Allocated**, es decir, accesible y no eliminado, lo que demuestra que el usuario creó y mantuvo dicho documento de forma activa.

Además, la aparición de accesos recientes al mismo, junto con su correspondiente archivo **.lnk**, permite concluir que el usuario **informant** accedió a la carta el día **25 de marzo de 2015 a las 16:28h**, coincidiendo con los últimos eventos sospechosos, como el envío de correos a un tercero (identificado como "spy") y la transferencia de documentos mediante servicios en la nube.

El contenido de la carta hace referencia explícita a su renuncia inmediata a la empresa, lo que refuerza la hipótesis de que el usuario tenía la intención de abandonar la organización tras la presunta exfiltración de información confidencial.

Además del acceso directo previamente localizado, el archivo anteriormente encontrado nos ha llevado al archivo original **Resignation_Letter_(Iaman_Informant).xps** en la ruta:

C:\Users\informant\Desktop

El archivo se encuentra en estado **Allocated**, lo que indica que **no ha sido eliminado** y permanece presente de forma íntegra en el sistema.

Esta localización confirma que el usuario **informant redactó y mantuvo activamente una carta de renuncia en su escritorio personal**, la cual fue accedida el 25 de marzo de 2015 a las 16:28h, coincidiendo con los últimos correos sospechosos enviados a un tercero (**spy**) y posteriores a la transmisión de documentos sensibles a través de servicios en la nube.

La presencia del archivo original, junto con la versión en .lnk, permite afirmar con alto grado de certeza que el usuario **tenía la intención de formalizar su salida de la organización**, presumiblemente tras la exfiltración de información confidencial.

El contenido de este es el siguiente: ³

³ El hash **sha256** del documento encontrado es:

9d20c984d21eb4333029aee1b7ecc3fb80c845a2f3deb5d1df3009d966306c21



Traducción de la prueba anterior:

“Estimado Señor Manager,

Que esta carta sirva como notificación oficial de mi dimisión de la compañía “OOO”, siendo esta efectiva a día de hoy. Gracias por su dirección y soporte durante la labor como su “Mánager de Desarrollo”. Me gustaría agradecerle por el soporte y los buenos años que pasé en su organización. Le deseo éxito continuado.

Atentamente, Iaman Informant”.

La existencia del archivo .lnk asociado indica que la carta fue **abierta o accedida previamente por el usuario** desde el Escritorio de este. Adjunto captura de detalle de la evidencia encontrada con Autopsy.

Type	Value
Path	C:\Users\informant\Desktop\Resignation_Letter_(Iaman_Informant).xps
Path ID	13871
Date Accessed	2015-03-25 16:28:33 CET
Source File Path	/img_dfreds_2015_data_leakage_pc.dd/vol_3/Users/Informant/AppData/Roaming/Microsoft/Windows/Recent/Resignation_Letter_(Iaman_Informant).xps.lnk
Artifact ID	-9223372036854775756

Análisis de múltiples versiones del documento de renuncia

Se localizaron accesos recientes a dos archivos con nombres similares pero extensiones distintas:

❖ **Resignation_Letter_(Iaman_Informant).docx**

❖ **Resignation_Letter_(Iaman_Informant).doc**

Ambos accesos aparecen reflejados como accesos directos (.lnk) ubicados en: **C:\Users\informant\Desktop** Esto sugiere que el usuario trabajó en **múltiples versiones** del mismo documento, posiblemente en distintas fases de redacción o edición. La existencia de varias extensiones refuerza la hipótesis de que el archivo fue **modificado y revisado activamente** en días previos a su acceso final como .xps (formato no editable).

Esta evidencia **apoya la tesis de una renuncia planificada** y puede indicar el momento en que el usuario Informant preparó su salida tras la posible filtración de información.

Anexo IV (c) Últimos archivos ofimáticos abiertos

Durante el análisis forense del archivo NTUSER.DAT correspondiente al usuario bajo investigación, se procedió a extraer la información de ejecución de aplicaciones mediante el plugin **UserAssist** de RegRipper.

Adicionalmente, mediante el plugin **msoffice v.20200518** se recuperaron registros de documentos recientes abiertos por el usuario (MRU – Más Usados Recientemente):

Herramienta	Archivos recientes (fecha y hora)	Ubicaciones recientes
Word	25-03-2015, 15:24:49 UTC	C:\Users\informant\Desktop\Resignation_Letter_(Iaman_Informant).docx
	23-03-2015, 18:37:54 UTC	E:\RM#1\Secret Project: Data\proposal[secret_project]_proposal.docx
Power Point	23-03-2015, 20:27:37 UTC	V:\Secret Project: Data\final[secret_project]_final_meeting.pptx

	23-03-2015, 18:38:23 UTC	E:\RM#1\Secret Project Data\design[secret_project]_design_concept.ppt
Excel	23-03-2015, 20:26:56 UTC	\10.11.11.128\secured_drive\Secret Project Data\pricing decision(secret_project)_pricing_decision.xlsx
	23-03-2015, 20:26:56 UTC:	\10.11.11.128\secured_drive\Secret Project Data\pricing decision\








Estos datos confirman el uso activo de aplicaciones ofimáticas y documentos específicos, lo que aporta contexto adicional al entorno investigado.

ANEXO V: Perfil Temático del Usuario Investigado

Anexo V (a) Bookmarks y vínculos temáticos:

En la ruta **Favorites\Links for United States**, se localizaron accesos directos a dominios oficiales del gobierno de EE.UU., concretamente **usa.gov** y **gobiernousa.gov**.

Adjunto captura de pantalla de Autopsy. La extensión de los archivos es de tipo .URL.

	GobiernoUSA.gov.url		0	http://go.microsoft.com/fwlink/?LinkId=129792	GobiernoUSA.gov.url	2015-03-22 16:54:05 CET
	USA.gov.url		0	http://go.microsoft.com/fwlink/?LinkId=129791	USA.gov.url	2015-03-22 16:54:05 CET
	GobiernoUSA.gov.url		0	http://go.microsoft.com/fwlink/?LinkId=129792	GobiernoUSA.gov.url	2015-03-22 15:35:03 CET
	USA.gov.url		0	http://go.microsoft.com/fwlink/?LinkId=129791	USA.gov.url	2015-03-22 15:35:03 CET
	Microsoft Store.url		0	http://go.microsoft.com/fwlink/?LinkId=140813	Microsoft Store.url	2015-03-22 15:34:57 CET
	GobiernoUSA.gov.url		0	http://go.microsoft.com/fwlink/?LinkId=129792	GobiernoUSA.gov.url	2015-03-22 16:56:08 CET
	USA.gov.url		0	http://go.microsoft.com/fwlink/?LinkId=129791	USA.gov.url	2015-03-22 16:56:08 CET

Esta información es coherente con la dirección de correo **@nist.gov** utilizada por el usuario **iaman** en sus comunicaciones, y refuerza la hipótesis de un vínculo temático o profesional con instituciones gubernamentales estadounidenses.

Se ha observado que el archivo **USA.gov.url**, encontrado en la carpeta de Favoritos del perfil de usuario (**C:\Users\informant\Favorites\Links for United States**), apunta a un enlace de redirección de Microsoft (**LinkId=129791**), el cual conduce al **canal RSS de actualizaciones de USA.gov**, página oficial del gobierno de los Estados Unidos.

Se apunta a dicho enlace mediante la URL:

<http://go.microsoft.com/fwlink/?LinkId=129791>

Lo que he encontrado en dicho enlace es lo siguiente:

```
-<rss version="2.0">
-<channel>
  <title>Choose USA.gov RSS feeds</title>
  <link>http://www.usa.gov</link>
  <description>
    Feeds from USA.gov that you can subscribe to if interested.
  </description>
  <item>
    <title>News and Features from USA.gov</title>
    <link>
      http://www.usa.gov/rss/updates.xml?
      WT.rss_f=USA.gov+Updates+News+and+Features&WT.rss_ev=s
    </link>
    <description>
      Stay on top of government news and information with the USA.gov News
      and Features RSS feed. The feed is updated when news and featured
      content are added to the USA.gov website.
    </description>
  </item>
</channel>
</rss>
```

La presencia de este enlace es coherente con el uso de una cuenta **@nist.gov** por parte del usuario **informant** en los correos electrónicos analizados. Este dato contribuye al perfil temático y profesional del sujeto investigado.

Añadir además que los archivos **.url** analizados (**USA.gov.url** y **GobiernoUSA.gov.url**) se encontraron en la ubicación:

C:\Users\informant\Favorites\Links for United States\

Esta ruta confirma que los accesos directos estaban almacenados en la carpeta de **Favoritos** personalizados del usuario **informant**, y no como elementos del sistema predeterminados.

El vector principal de esta prueba es que su presencia refleja una acción voluntaria del usuario para guardar o mantener **enlaces hacia recursos gubernamentales de EE.UU.**, lo que refuerza su perfil temático y profesional dentro del contexto de la presente investigación.

Anexo V (b) Webs accedidas por Sr. Informant, con relevancia para el caso

Fecha	Hora (UTC)	Navegador	URL resumida	Descripción del contenido accedido

23/03/2015	14:02	Chrome	google.com/search?q=data+leakage+methods	Búsqueda sobre métodos de fuga de información
23/03/2015	14:02	Chrome	sans.org/whitepapers/data-leakage	Artículo técnico sobre amenazas y mitigación de fugas de datos
23/03/2015	14:03	Chrome	google.com/search?q=leaking+confidential+information	Búsqueda sobre cómo filtrar información confidencial
23/03/2015	14:04	Chrome	google.com/search?q=information+leakage+cases	Búsqueda de casos reales de fuga de información
23/03/2015	14:05	Chrome	fbi.gov/ipr	Página de la FBI sobre robo de propiedad intelectual
23/03/2015	14:06	Chrome	wikipedia.org/wiki/Intellectual_property	Información sobre propiedad intelectual
23/03/2015	14:06	Chrome	google.com/search?q=how+to+leak+a+secret	Búsqueda explícita sobre cómo filtrar secretos
23/03/2015	14:06	Chrome	research.microsoft.com/leak_secret.pdf	Documento técnico sobre fugas de datos
23/03/2015	14:15	IE 11	forensicswiki.org/wiki/USB_History_Viewing	Información forense sobre historial de dispositivos USB
23/03/2015	14:15	Chrome	wikipedia.org/wiki/Cloud_storage	Definición de almacenamiento en la nube
23/03/2015	14:15	Chrome	pcadvisor.co.uk/cloud-storage-comparison	Comparativa de servicios como Google Drive, Dropbox, iCloud
23/03/2015	14:15	Chrome	wikipedia.org/wiki/Digital_forensics	Definición de forensia digital
23/03/2015	14:16	Chrome	nij.gov/topics/forensics/digital	Página oficial sobre pruebas digitales del NIJ
23/03/2015	14:17	Chrome	forensicswiki.org/wiki/Anti-forensic_techniques	Técnicas para ocultar/eliminar evidencia digital
23/03/2015	14:18	Chrome	defcon.org/dc-20-Perklin-AntiForensics.pdf	Presentación sobre anti-forensics en DEFCON

23/03/2015	14:19	Chrome	wikipedia.org/wiki/List_of_data_recovery_software	Listado de herramientas para recuperar datos
23/03/2015	15:55	Chrome	google.com/search?q=google+drive	Búsqueda sobre Google Drive
23/03/2015	15:56	Chrome	google.com/drive/download	Página de descarga del cliente de Google Drive
23/03/2015	15:55	Chrome	apple.com/icloud/setup/pc	Guía de Apple iCloud para PC
25/03/2015	10:46	IE 11	bing.com/search?q=anti-forensic+tools	Búsqueda sobre herramientas anti-forenses
25/03/2015	10:46	IE 11	bing.com/search?q=eraser	Búsqueda de herramienta de borrado seguro
25/03/2015	10:47	IE 11	eraser.heidi.ie	Página oficial de Eraser
25/03/2015	10:47	IE 11	sourceforge.net/project/eraser	Descarga directa de Eraser
25/03/2015	10:48	IE 11	piriform.com/ccleaner/download	Descarga de CCleaner, herramienta de limpieza del sistema

Anexo V (c) Búsquedas relevantes en los navegadores

Fecha y hora	Navegador usado	Búsqueda realizada
23-03-2015, 14:02:09	Google Chrome	data leakage method
23-03-2015, 14:02:44	Google Chrome	leaking confidential information
23-03-2015, 14:03:40	Google Chrome	information leakage cases
23-03-2015, 14:05:48	Google Chrome	intellectual property theft
23-03-2015, 14:06:27	Google Chrome	how to leak a secret
23-03-2015, 14:07:58	Internet Explorer 11	file sharing and tethering

23-03-2015, 14:08:31	Internet Explorer 11	DLP DRM⁴
23-03-2015, 14:08:54	Internet Explorer 11	e-mail investigation
23-03-2015, 14:10:03	Internet Explorer 11	Forensic Email Investigation
23-03-2015, 14:10:27	Internet Explorer 11	what is windows system artifacts
23-03-2015, 14:11:50	Internet Explorer 11	investigation on windows machine
23-03-2015, 14:12:35	Internet Explorer 11	windows event logs
23-03-2015, 14:13:20	Internet Explorer 11	cd burning method
23-03-2015, 14:13:37	Internet Explorer 11	cd burning method in windows
23-03-2015, 14:14:11	Internet Explorer 11	external device and forensics
23-03-2015, 14:14:50	Google Chrome	cloud storage
23-03-2015, 14:15:44	Google Chrome	digital forensics
23-03-2015, 14:16:55	Google Chrome	how to delete data
23-03-2015, 14:17:14	Google Chrome	anti-forensics
23-03-2015, 14:18:10	Google Chrome	system cleaner
23-03-2015, 14:18:30	Google Chrome	how to recover data
23-03-2015, 14:19:03	Google Chrome	data recovery tools
23-03-2015, 15:55:09	Google Chrome	apple icloud
23-03-2015, 15:56:04	Google Chrome	google drive
24-03-2015, 17:06:50	Google Chrome	security checkpoint cd-r
25-03-2015, 10:46:44	Internet Explorer 11	anti-forensic tools
25-03-2015, 10:46:54	Internet Explorer 11	eraser
25-03-2015, 10:47:51	Internet Explorer 11	ccleaner

⁴ **DLP (Data Loss Prevention)**: Tecnología que detecta y previene la fuga de información confidencial, ya sea por salida no autorizada (correo, USB, nube, etc.) o por comportamiento anómalo del usuario.

DRM (Digital Rights Management): Tecnología que restringe cómo se accede, comparte, copia o imprime contenido digital protegido. Se usa mucho en medios digitales, pero también en documentos corporativos (PDF, Office, etc.).

ANEXO VI: Herramientas y Actividad Sospechosa Detectada

Anexo VI (a) Descargas de software relacionado con servicio en la nube

El día 23-03-2015 a las **16:00h** el usuario Informant instaló Google Drive y Apple iCloud.

El mismo día 23-03-2015 a las **16:05h** el usuario accedió a Google Drive, con el correo iaman.informant.personal@gmail.com

	Fecha	Programa	Fuente	Tamaño y Función
Descarga 1	22-03-2015	icloudsetup.exe	https://support.apple.com/downloads/DL1455/en_US/icloudsetup.exe	68,3 MB Instalador de iCloud para Windows (permite sincronizar archivos con la nube de Apple)
Descarga 2	22-03-2015	googledrivesync.exe	https://dl.google.com/.../googledrivesync.exe	859 KB Instalador del cliente de Google Drive para sincronización directa de archivos.

Anexo VI (b) REMOTE DESKTOP (Usuarios de escritorio remoto)

Durante el proceso de análisis forense, y con el objetivo de identificar los SIDs (Security Identifiers) asociados a las cuentas de usuario activas, se examinó el archivo de base de datos de seguridad del sistema Windows, ubicado en la ruta: **/Windows/System32/config/SAM**. Este archivo, en combinación con el archivo **SYSTEM**, almacena las credenciales locales y relaciones de pertenencia a grupos.

El análisis hexadecimal del contenido reveló entradas con estructuras de datos en binario, entre ellas: C REG_BIN 07 00 01 00 00 00 00 00 98 00 00 00 02 00 01 00...ServerDomainUpdates REG_BIN FE 01. Simultáneamente, a través de la pestaña “**Results / Analysis Results**” de Autopsy, se localizaron referencias directas a la pertenencia de usuarios al grupo especial del sistema denominado: **Usuarios de Escritorio Remoto**. El evento está fechado el 25 de marzo de 2015 a las 10:15:37 CET, momento que coincide con el último inicio de sesión registrado en el archivo de eventos Security.evtx.

Se puede encontrar más información sobre este apartado en el documento “**Complemento_Peritaje_Final**”, en el **capítulo 2**, titulado “**2. Indicios de Uso de Conexiones Remotas**”.

Final de documento.
