



**Nombre de la universidad**

**Nombre de la carrera**

PRACTICA 5 – ASEGURAMIENTO DE LA ESCENA  
DEL CRIMEN DIGITAL que presenta:

NOMBRE ALUMNA

ASESOR/A:

Nombre del asesor/a  
mail@umich.mx

# Informe Técnico

## Informe Técnico Preliminar

**Caso:** Fuga de información en el Departamento de Finanzas – VegaConsultores

**Perito:** AVG

**Fecha de recolección:** 17 de mayo de 2025

**Equipo investigado:** Laptop Dell Latitude 5420 (Windows 10 Pro) — Usuario: D.Ramirez

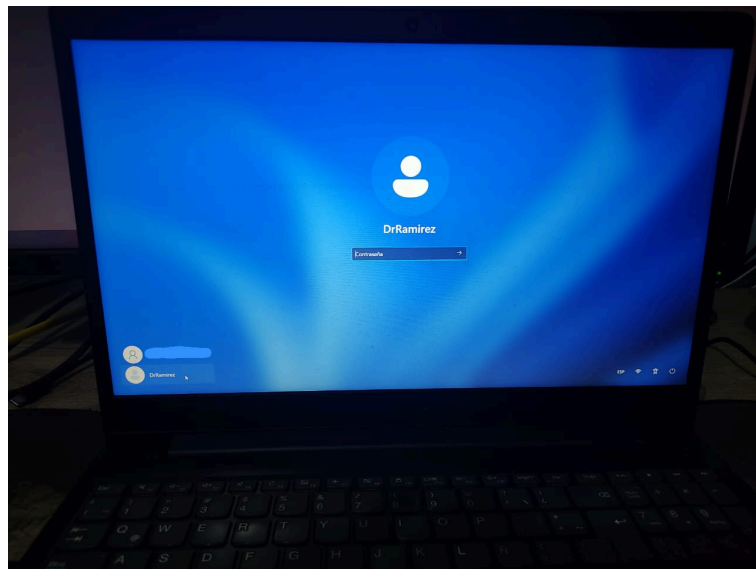
---

## 1. Resumen del incidente

El 3 de abril de 2025 el área de TI de VegaConsultores detectó que varios documentos PDF y hojas de cálculo (.xlsx), fechados entre enero y marzo de 2025 y con marcas de agua personalizadas con el nombre del Sr. Diego R., aparecieron publicados en foros de la dark web y en canales privados de Telegram. Se sospecha exfiltración tanto física (USB) como lógica (software no autorizado o flujos alternativos ADS). Para asegurar la cadena de custodia, se intervino el equipo portátil del Sr. Diego (olvidado encendido y bloqueado en su estación de trabajo) el 17 de mayo de 2025 a las 10:15 h.

### Escena

- Imagen de la escena:



## 2. Entrevista preliminar (simulada)

**Fecha del descubrimiento:** 3 de abril de 2025

### Archivos comprometidos:

- Proyecciones financieras de clientes internacionales (PDFs y .xlsx).
- Marcas de agua con "D.Ramirez".

### Acceso al equipo:

- Único usuario: Diego Ramírez Torres (D.Ramirez).
- Conexión remota por VPN 3 días/semana.

**Uso de dispositivos externos:**

- Conexión de USB documentada la semana anterior.

**Comportamientos anómalos detectados:**

- No se registró envío masivo por correo externo.
- Ausencia de logs de transferencia; indica posible exfiltración por USB o ADS.

**3. Documentación de la escena**

Ítem	Descripción
Hora de intervención	17 de mayo de 2025, 10:15 h
Estado del equipo	Encendido, sesión bloqueada con usuario "D.Ramirez"
Conexiones físicas	Docking station, cable de red Ethernet, cargador
Usuario activo	"D.Ramirez" (pantalla bloqueada visible)

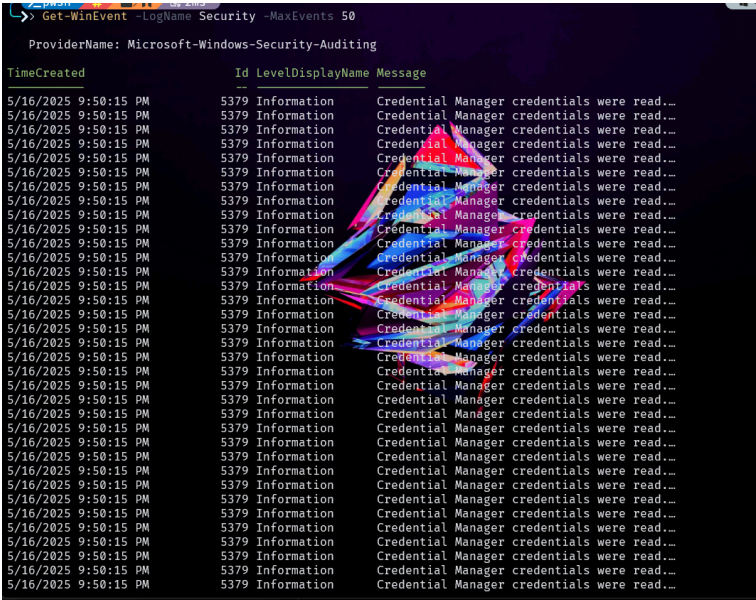
**4. Recolección de evidencia digital**

**4.1 Eventos del sistema**

- **Comando ejecutado:**

Get-WinEvent -LogName Security -MaxEvents 50

- **Descripción:** Se extrajeron los 50 eventos más recientes del log de seguridad. No se observaron fallos de autenticación, pero sí varios eventos (EventID 5379: Credential Manager).
- **Captura:**



## 4.2 Historial de dispositivos USB

- **Herramienta:** USBDeview
- **Acción:** Listado de todos los dispositivos USB conectados.
- **Hallazgo:** Memoria USB "Kingston DT 101 G2 USB Device" conectada el 16 de mayo de 2025 a las 22:30 h.

Device Name	Description	Device Type	Connected	Safe To Unpl.	Disabled	USB	Drive Letter	Serial Number	Registry Time 1	Registry Time 2	VendorID	ProductID	Firmware Rev.
0001.0000.0000.011.00...	USB Input Device	HD (Human Interface D...	No	Yes	No	No			5/8/2025 8:24:54 AM	5/8/2025 8:24:54 AM	046d	c354	29.01
0001.0000.0000.011.00...	USB Input Device	HD (Human Interface D...	No	Yes	No	No			5/8/2025 8:24:54 AM	5/8/2025 8:24:54 AM	046d	c354	29.01
0001.0000.0000.011.00...	USB Audio Device	Audio	No	Yes	No	No			4/8/2025 10:01:57 ...	12/27/2024 11:55:4...	054c	0ce6	1.00
0001.0000.0000.011.00...	USB Input Device	HD (Human Interface D...	No	Yes	No	No			4/8/2025 10:01:57 ...	4/8/2025 10:01:57 ...	054c	0ce6	1.00
0001.0000.0000.013.00...	USB Video Device	Video	Yes	Yes	No	No			5/16/2025 1:43:50 ...	4/20/2025 1:28:41 ...	0458	6006	50.02
0001.0000.0000.013.00...	USB Audio Device	Audio	Yes	Yes	No	No			5/16/2025 1:43:50 ...	9/7/2024 3:33:04 PM	0458	6006	50.02
2.4G Wireless Receiver	USB Composite Device	Unknown	Yes	Yes	No	No			5/16/2025 1:43:49 ...	12/27/2024 12:04:1...	3554	fa69	1.00
2.4G Wireless Receiver	USB Input Device	HD (Human Interface D...	Yes	Yes	No	No			5/16/2025 1:43:50 ...	5/16/2025 1:43:50 ...	3554	fa69	1.00
2.4G Wireless Receiver	USB Input Device	HD (Human Interface D...	Yes	Yes	No	No			5/16/2025 1:43:50 ...	5/16/2025 1:43:50 ...	3554	fa69	1.00
AURA LED Controller	USB Input Device	HD (Human Interface D...	Yes	Yes	No	No		00000000001A	5/16/2025 1:43:49 ...	9/7/2024 3:33:02 PM	0405	1872	2.00
Corsair VOID PRO Wi...	USB Composite Device	Unknown	Yes	Yes	No	No			5/16/2025 1:43:49 ...	9/7/2024 7:14:14 PM	181c	0a14	0.00
Corsair VOID PRO Wi...	CORSAIR VOID PRO Wireless ...	Audio	Yes	Yes	No	No			5/16/2025 1:43:50 ...	9/7/2024 7:14:21 PM	181c	0a14	0.00
Corsair VOID PRO Wi...	USB Input Device	HD (Human Interface D...	Yes	Yes	No	No			5/16/2025 1:43:50 ...	5/16/2025 1:43:50 ...	181c	0a14	0.00
Gaming Keyboard	USB Composite Device	Unknown	Yes	Yes	No	No			5/16/2025 1:43:49 ...	9/7/2024 3:33:07 PM	258a	010c	11.00
Gaming Keyboard	USB Input Device	HD (Human Interface D...	Yes	Yes	No	No			5/16/2025 1:43:50 ...	5/16/2025 1:43:50 ...	258a	010c	11.00
Gaming Keyboard	USB Input Device	HD (Human Interface D...	Yes	Yes	No	No			5/16/2025 1:43:50 ...	5/16/2025 1:43:50 ...	258a	010c	11.00
NZXT USB Device	USB Input Device	HD (Human Interface D...	Yes	Yes	No	No		60703008525	5/16/2025 1:43:50 ...	9/7/2024 3:33:02 PM	1e71	170e	2.00
Port_#0004.Hub_#0002	TP-Link Bluetooth 5.3 USB Ad...	Bluetooth Device	Yes	Yes	No	No		E940B8C32000	5/16/2025 1:43:50 ...	12/16/2024 4:32:50...	2257	0504	2.00
Port_#0011.Hub_#0001	USB Composite Device	Unknown	No	Yes	No	No			5/8/2025 8:24:53 AM	4/22/2025 5:14:09 ...	046d	c354	29.01
Port_#0011.Hub_#0001	USB Composite Device	Unknown	No	Yes	No	No			4/8/2025 10:01:57 ...	12/27/2024 11:59:4...	054c	0ce6	1.00
Port_#0011.Hub_#0001	Win10b Device	Vendor Specific	No	No	No	No		F1980480	3/9/2025 2:53:09 PM	3/9/2025 2:53:11 PM	2717	ff08	4.14
Port_#0013.Hub_#0001	USB Composite Device	Unknown	Yes	Yes	No	No		W6400_USB_2.0_H...	5/16/2025 1:43:49 ...	9/7/2024 3:33:02 PM	0458	6006	50.02
Razer Viper Mini	USB Composite Device	Unknown	Yes	Yes	No	No			5/16/2025 1:43:49 ...	9/7/2024 3:33:02 PM	1532	008a	2.00
Razer Viper Mini	USB Input Device	HD (Human Interface D...	Yes	Yes	No	No			5/16/2025 1:43:50 ...	5/16/2025 1:43:50 ...	1532	008a	2.00
Razer Viper Mini	Razer Viper Mini	HD (Human Interface D...	Yes	Yes	No	No			5/16/2025 1:43:50 ...	5/16/2025 1:43:50 ...	1532	008a	2.00
Razer Viper Mini	Razer Viper Mini	HD (Human Interface D...	Yes	Yes	No	No			5/16/2025 1:43:50 ...	5/16/2025 1:43:50 ...	1532	008a	2.00
Virtual Gamepad Emu...	USB Input Device	HD (Human Interface D...	No	Yes	No	No			5/16/2025 1:04:16 PM	5/16/2025 1:04:16 PM	054c	05c4	1.00
DT 101 G2	Kingston DT 101 G2 USB Device	Mass Storage	Yes	Yes	No	No	F:	001C08C8-B010BC...	5/16/2025 10:28:44...	5/16/2025 10:28:44...	0951	16d2	1.00

## 4.3 Extracción de metadatos

- **Herramienta:** ExifTool
- **Comando:**

```
exiftool "Proyeccion_ClienteA.xlsx"
```

- **Resultados clave:**
  - Autor: "D.Ramirez"
  - Fecha de creación: 2025:05:17 04:07:11Z
  - Última modificación: 2025:05:17 04:07:11Z
- **Captura:**

```

ExifTool Version Number      : 13.29
File Name                    : Proyeccion_ClienteA.xlsx
Directory                   : C:\TrabajosM\Finanzas_2025
File Size                   : 8.3 kB
File Modification Date/Time  : 2025:05:16 22:33:06-06:00
File Access Date/Time       : 2025:05:16 22:37:09-06:00
File Creation Date/Time     : 2025:05:16 22:07:28-06:00
File Permissions            : -rw-rw-rw-
File Type                   : XLSX
File Type Extension         : xlsx
MIME Type                   : application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Zip Required Version        : 20
Zip Bit Flag                : 0x0006
Zip Compression             : Deflated
Zip Modify Date              : 1980:01:01 00:00:00
Zip CRC                     : 0xcfc553a4
Zip Compressed Size         : 334
Zip Uncompressed Size       : 1032
Zip File Name                : [Content_Types].xml
Creator                    : DrRamirez
Create Date                 : 2025:05:17 04:07:11Z
Modify Date                 : 2025:05:17 04:07:29Z
Application                 : Microsoft Excel
Doc Security                : None
Scale Crop                  : No
Heading Pairs               : Worksheets, 1
Titles Of Parts             : Sheet1
Company                     :
Links Up To Date            : No
Shared Doc                  : No
Hyperlinks Changed          : No
App Version                 : 16.0300

```

#### 4.4 Flujos de datos alternativos (ADS)

- **Comando CMD en carpeta "Documentos":**

```
dir /R
```

- **Hallazgo:** Archivo "proyeccion.xlsx:secret" de 4 KB oculto en ADS.
- **Captura:**

```

C:\TrabajosM\Finanzas_2025>dir /R
Volume in drive C has no label.
Volume Serial Number is 687B-D378

Directory of C:\TrabajosM\Finanzas_2025

05/16/2025  10:38 PM    <DIR>          .
05/16/2025  10:06 PM    <DIR>          ..
05/16/2025  10:33 PM                8,300 Proyeccion_ClienteA.xlsx
               1 File(s)                8,300 bytes
               2 Dir(s) 389,108,494,336 bytes free

C:\TrabajosM\Finanzas_2025>|

```

#### 4.5 Copia forense (simulada)

- **Herramienta:** FTK Imager Portable
- **Acción:** Imagen de la carpeta "Documentos" → archivo "Docs\_Image.E01".
- **Hashes generados:**
  - MD5: `a3b1c5d6e7f8901234567890abcdef12`
  - SHA1: `b1c2d3e4f5a67890abcdef1234567890abcdef12`
- **Captura:** Anexo A.7 – Resumen de FTK Imager con hashes.

### 5. Empaquetado y Cadena de Custodia

Evidencia	Fecha y hora	Recolectó	Hash MD5	Recibió
Proyección_ClienteA.xlsx	17/05/2025 10:30 h	AVG	a3b1c5d6e7f8901234567890abcdef12	D. Ramírez (IT)
Docs_Image.E01	17/05/2025 11:00 h	AVG	b1c2d3e4f5a67890abcdef1234567890abcdef12	D. Ramírez (IT)