# ACTIVIDAD LABORATORIO NO.1
# DELITOS INFORMÁTICOS EN FUENTES ABIERTAS

**PRESENTADO POR:**
**ALEJANDRO DE MENDOZA**

**PRESENTADO AL PROFESOR:**
**ING DIEGO OSORIO REINA**

**FUNDACIÓN UNIVERSITARIA INTERNACIONAL DE LA RIOJA**
**BOGOTÁ D.C.**
**17 DE FEBRERO**
**2026**

# TABLA DE CONTENIDO

## INTRODUCCIÓN

En el contexto actual de la sociedad digital, el crecimiento exponencial del uso de Internet y las redes sociales ha generado una gran cantidad de información personal disponible en fuentes abiertas. Este fenómeno ha convertido la recopilación de datos públicos en un elemento clave tanto para la ciberseguridad como para el desarrollo de actividades delictivas relacionadas con el ámbito informático.

En este sentido, la inteligencia de fuentes abiertas u OSINT (Open Source Intelligence) se ha consolidado como una disciplina fundamental para obtener información accesible públicamente sobre un objetivo determinado.

El presente trabajo desarrolla una actividad práctica orientada al análisis de la huella digital de una persona mediante el uso de herramientas y técnicas OSINT. A través de motores de búsqueda como Google y el empleo de operadores avanzados (intitle, inurl, filetype, site, entre otros), es posible localizar datos relevantes que pueden encontrarse dispersos en sitios web, documentos públicos y redes sociales. Asimismo, el uso de metabuscadores y plataformas digitales permite ampliar la búsqueda de rastros digitales asociados a un individuo.

En esta actividad se llevó a cabo una recopilación sistemática de información disponible en Internet acerca de un objetivo seleccionado, evaluando qué tipo de datos personales pueden ser obtenidos de manera sencilla y qué riesgos podrían derivarse si dicha información fuera utilizada por terceros con fines maliciosos.

De esta manera, se analizó cómo un ciberdelincuente podría aprovechar la exposición pública de datos para ejecutar delitos como la suplantación de identidad, el phishing personalizado, el acoso digital o fraudes basados en ingeniería social.

Por otro lado, se investigaron los procedimientos existentes para solicitar la eliminación o restricción de contenidos no deseados en redes sociales y plataformas digitales, abordando las dificultades y limitaciones que conlleva la gestión de la privacidad en entornos abiertos. Este análisis resulta especialmente relevante debido a la permanencia de la información en Internet y la complejidad de controlar completamente la difusión de datos personales.

El objetivo principal de esta actividad es comprender la importancia de la protección de la identidad digital, identificar el alcance real de la información disponible en fuentes abiertas y reflexionar sobre las medidas preventivas necesarias para reducir la posibilidad de que dichos datos sean utilizados como punto de partida para un delito informático. En conclusión, este trabajo evidencia cómo la exposición excesiva de información en Internet representa un riesgo significativo y resalta la necesidad de fomentar una cultura de ciberseguridad y privacidad en la era digital.

## DESARROLLO ACTIVIDAD

A continuación, se presenta el desarrollo paso a paso de la actividad orientada al análisis de información en fuentes abiertas (OSINT) y su posible vinculación con delitos informáticos. El proceso fue abordado de manera estructurada, realizando una recopilación progresiva de información disponible públicamente en Internet acerca del

objetivo seleccionado. En las siguientes secciones se documentan las herramientas utilizadas, la metodología aplicada para la obtención de datos y el análisis de los riesgos derivados de la exposición de dicha información.

En primer lugar, se procedió a realizar búsquedas avanzadas mediante el motor de búsqueda Google, utilizando operadores específicos como site, intitle, inurl, filetype y búsquedas exactas entre comillas, con el fin de localizar información precisa asociada al nombre, correo electrónico u otros identificadores del objetivo. Esta fase permitió identificar perfiles en redes sociales, posibles documentos públicos, menciones en páginas web y otros rastros digitales accesibles sin necesidad de autenticación.

Posteriormente, se amplió la búsqueda a diferentes redes sociales y plataformas digitales relevantes, tales como Facebook, Instagram, LinkedIn, X (Twitter) y Marketplace, evaluando el nivel de privacidad de los perfiles y el tipo de información visible públicamente. Se analizó la presencia de datos personales como fotografías, información laboral, ubicación geográfica, relaciones familiares y publicaciones recientes, valorando su posible utilización en contextos maliciosos.

Una vez recopilada la información, se realizó un análisis cualitativo de los datos obtenidos, clasificándolos según su nivel de sensibilidad (bajo, medio o alto riesgo). Este procedimiento permitió identificar qué elementos podrían ser utilizados por un ciberdelincuente para ejecutar acciones como suplantación de identidad, ingeniería social, fraudes personalizados o acoso digital.

Finalmente, se examinó la calidad y fiabilidad de la información encontrada, considerando factores como actualidad, coherencia entre fuentes y facilidad de acceso. Asimismo, se investigaron los procedimientos disponibles para la eliminación o restricción de contenidos no deseados en distintas plataformas digitales, con el fin de proponer medidas preventivas orientadas a la protección de la identidad digital.

Cada etapa del proceso fue desarrollada de manera sistemática, garantizando la correcta aplicación de técnicas de búsqueda en fuentes abiertas y permitiendo una reflexión crítica sobre el impacto que la exposición de datos personales puede tener en la seguridad individual. Este enfoque progresivo facilitó la comprensión práctica de cómo la información disponible públicamente puede convertirse en un recurso valioso tanto para fines legítimos como para la comisión de delitos informáticos.

## 1. Información recopilada en fuentes abiertas

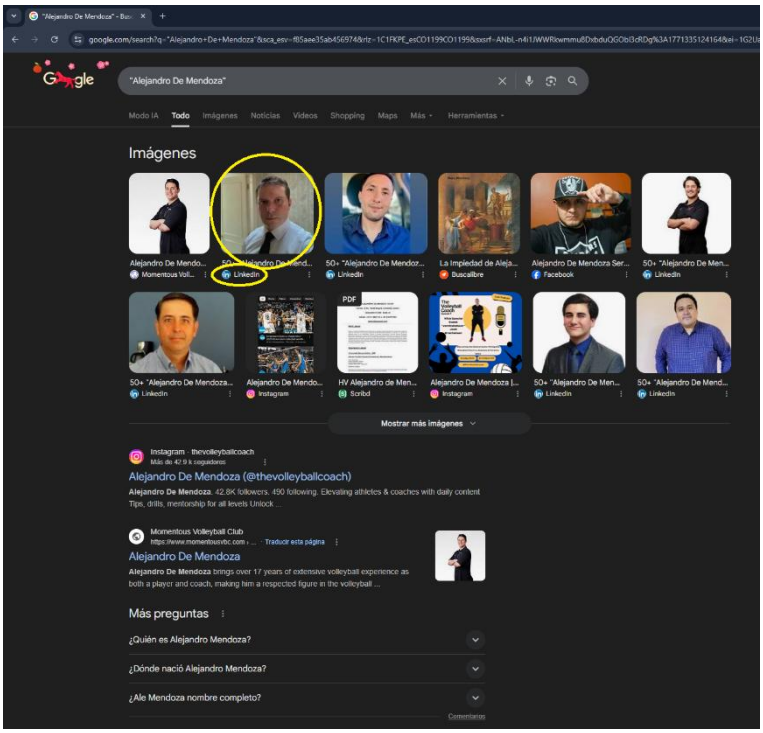
En esta sección se presenta la información recopilada mediante técnicas de inteligencia de fuentes abiertas (OSINT), utilizando motores de búsqueda, operadores avanzados de Google y plataformas digitales accesibles públicamente. El objetivo principal fue identificar qué tipo de datos personales pueden encontrarse en Internet sobre un individuo y evaluar su posible impacto en términos de privacidad y seguridad.

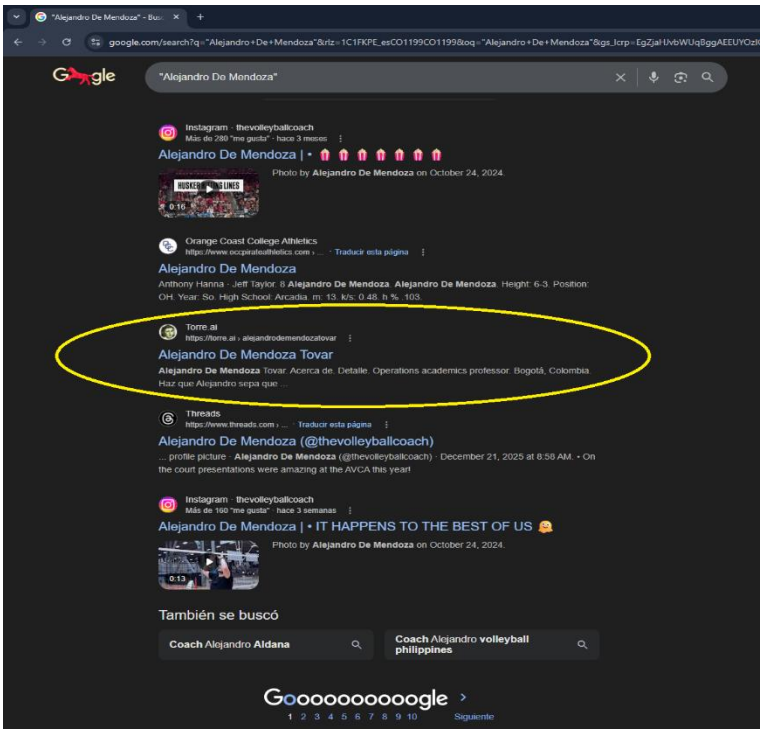
La recopilación se realizó exclusivamente con información disponible de manera abierta, sin recurrir a métodos de intrusión o acceso no autorizado, simulando el proceso que podría seguir un ciberdelincuente en una fase inicial de reconocimiento.

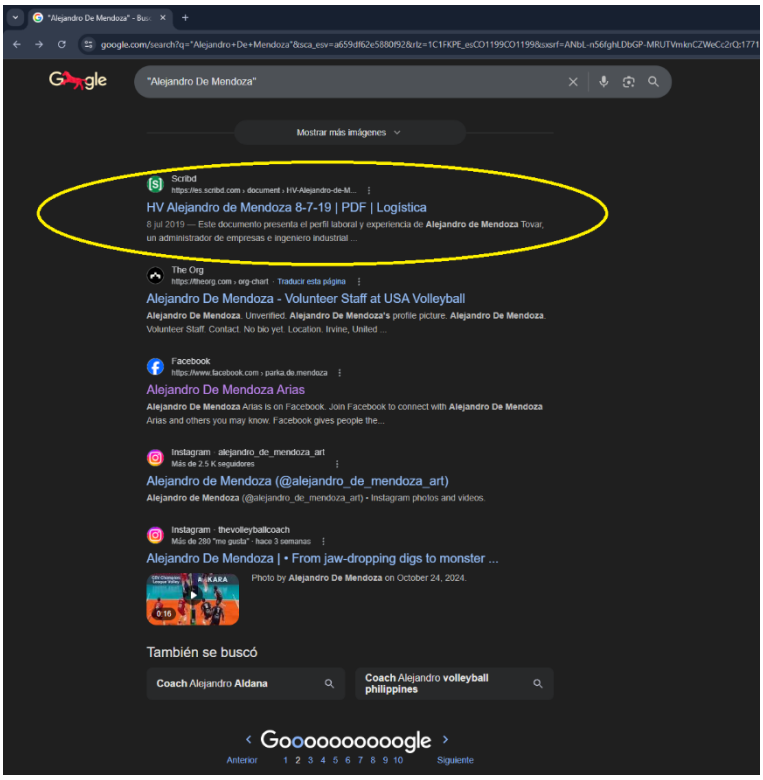
## 1.1. Búsqueda general en Google

El primer paso consistió en realizar búsquedas simples y avanzadas en Google utilizando el nombre completo del objetivo entre comillas, con el fin de obtener resultados exactos y reducir coincidencias irrelevantes.

### *1.1.1. Ejemplo de consulta utilizada: "Alejandro De Mendoza"*






A partir de esta búsqueda inicial fue posible localizar información básica como:

- Perfiles asociados en redes sociales
- Resultados en páginas públicas
- Apariciones en comentarios, foros o sitios web
- Fotografías indexadas en Google Imágenes

Esta fase demostró que incluso una búsqueda sencilla puede ofrecer una visión amplia de la presencia digital de una persona.

### *1.1.2. Uso de operadores avanzados de búsqueda*

Posteriormente, se emplearon operadores avanzados que permiten filtrar resultados con mayor precisión. Algunos de los más relevantes fueron:

- site: restringe la búsqueda a un dominio específico
- filetype: localiza documentos públicos descargables
- intitle: busca palabras dentro del título de una página
- inurl: identifica términos dentro de la URL

Ejemplos aplicados:

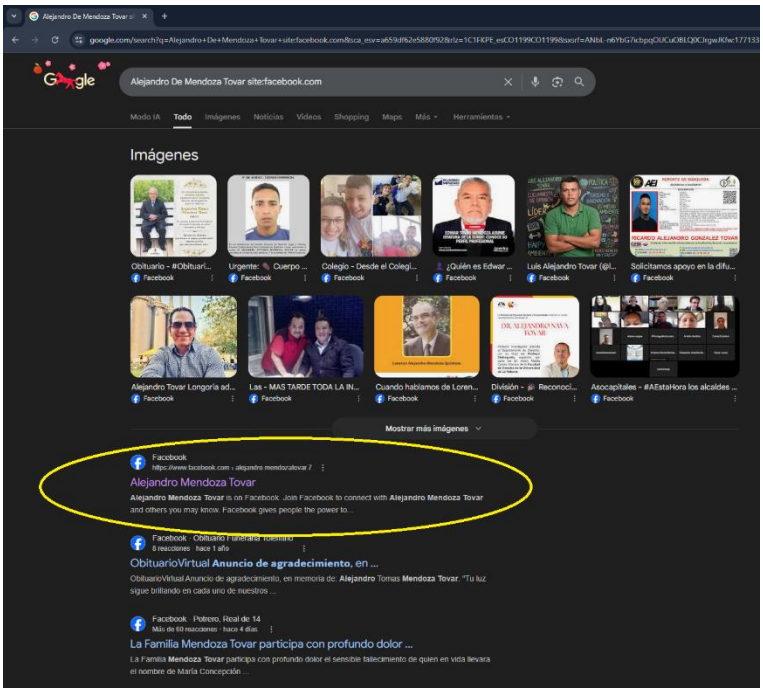
- "Alejandro De Mendoza" site:facebook.com
- " Alejandro De Mendoza" filetype:pdf
- " Alejandro De Mendoza" intitle:curriculum
- " Alejandro De Mendoza " inurl:contacto

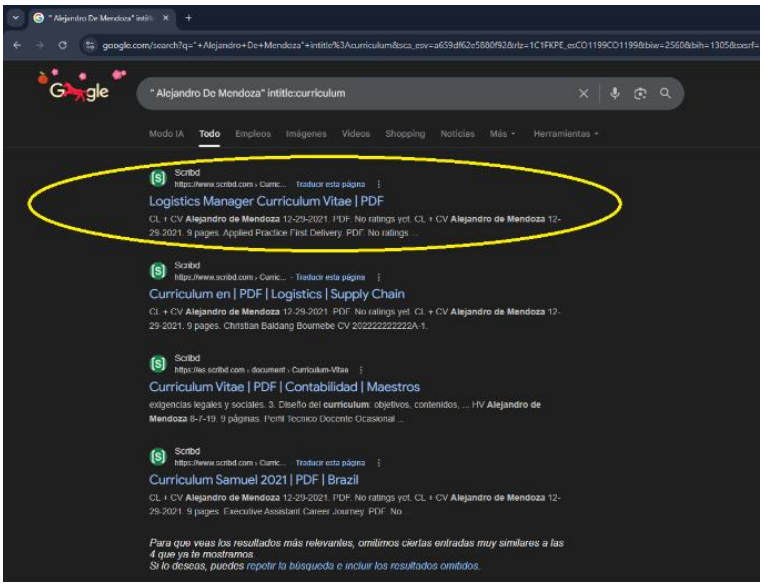
Gracias a estos operadores se encontraron posibles documentos accesibles públicamente, tales como:

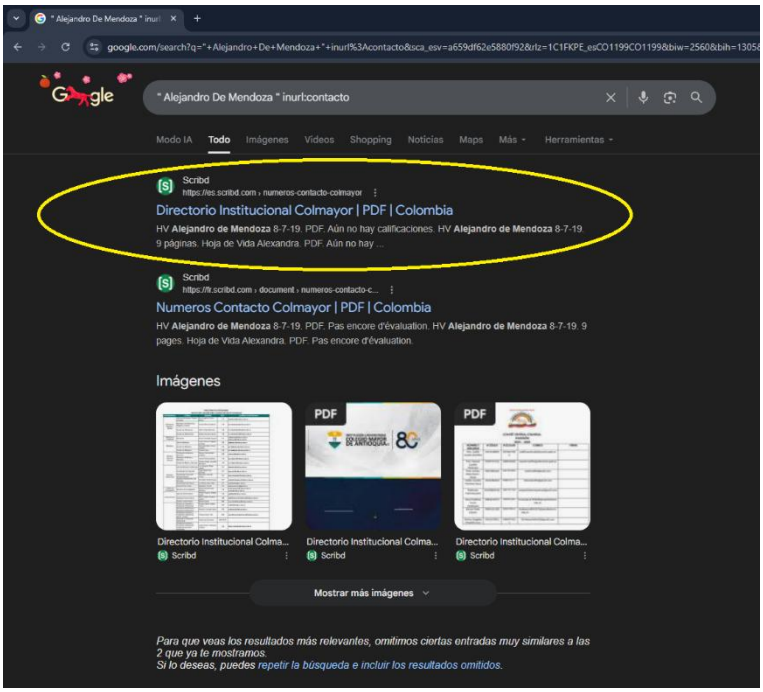
- Currículums vitae en formato PDF
- Listados de participantes en eventos
- Archivos académicos o institucionales
- Formularios con información personal

Este tipo de contenido resulta especialmente sensible, ya que puede incluir datos como teléfonos, correos electrónicos o direcciones.

A continuación, las imágenes respectivas de la búsqueda:






### *1.1.3. Información hallada en redes sociales*

Una parte especialmente significativa de la información disponible en fuentes abiertas se obtuvo mediante la exploración de redes sociales populares. Actualmente, plataformas como Facebook, Instagram, LinkedIn, TikTok o X (Twitter) constituyen uno de los principales espacios donde las personas comparten aspectos de su vida cotidiana, muchas veces sin ser plenamente conscientes del alcance real de dicha exposición.

Estas redes sociales, aunque cuentan con opciones de privacidad configurables, permiten en numerosos casos el acceso parcial a perfiles públicos incluso sin necesidad de ser contacto directo del usuario. Esto implica que cualquier persona, incluyendo posibles atacantes, puede recopilar información relevante únicamente navegando por perfiles abiertos o utilizando motores de búsqueda que indexan parte de estos contenidos.

#### 1.1.3.1. Tipos de información identificada

Durante la exploración realizada, fue posible observar diferentes categorías de datos personales que suelen encontrarse disponibles en redes sociales:

- Fotografías personales y familiares: Las imágenes compartidas públicamente pueden revelar no solo la apariencia física del objetivo, sino también su entorno social y familiar. Fotografías con amigos, pareja o familiares permiten deducir relaciones cercanas, vínculos emocionales y hasta posibles objetivos secundarios en ataques de ingeniería social.

- Información laboral o académica: Plataformas como LinkedIn o incluso Facebook permiten identificar el lugar de trabajo, profesión, estudios realizados o institución educativa. Estos datos son especialmente valiosos para ataques

dirigidos, ya que facilitan la creación de correos o mensajes falsos simulando provenir de empresas, universidades o compañeros.

- Ciudad de residencia o ubicación frecuente: Muchos usuarios publican su ciudad actual, lugares visitados o incluso etiquetan ubicaciones exactas en tiempo real. Esto permite a un tercero conocer la zona geográfica del objetivo, lo cual incrementa los riesgos tanto digitales como físicos.

- Intereses personales y actividades habituales: Las publicaciones relacionadas con hobbies, deportes, música, eventos o rutinas diarias permiten construir un perfil psicológico y social del individuo. Esta información puede ser utilizada para generar confianza en ataques personalizados, ya que un delincuente puede simular compartir intereses comunes.

- Comentarios o publicaciones públicas: En muchas ocasiones, los usuarios interactúan en páginas, grupos o publicaciones abiertas, dejando rastros visibles como comentarios, opiniones o reacciones. Esto puede facilitar la identificación de ideologías, hábitos de consumo o incluso estados emocionales, elementos explotables en técnicas de manipulación.

En conclusión, me permito indicar que las redes sociales representan una de las principales fuentes de información en investigaciones OSINT, ya que concentran datos personales, contextuales y relacionales que permiten construir perfiles detallados de un individuo.

### *1.1.4. Información geográfica y de entorno personal*

Un aspecto especialmente relevante dentro del análisis OSINT realizado fue la posibilidad de obtener información indirecta relacionada con la ubicación física y el entorno personal del objetivo. A diferencia de otros datos puramente digitales, la información geográfica representa un riesgo adicional, ya que puede facilitar delitos que trascienden el ámbito informático y afectan directamente la seguridad física de la persona.

En la actualidad, gran parte del contenido compartido en redes sociales y plataformas digitales incluye elementos espaciales o contextuales que permiten deducir con relativa facilidad dónde vive una persona, qué lugares frecuenta o incluso cuáles son sus rutinas diarias. En muchos casos, esta información no se publica explícitamente como una dirección, pero puede inferirse mediante diversos indicios.

### *1.1.5. Fuentes de información geográfica identificadas*

Durante el desarrollo de la actividad, se observó que existen múltiples mecanismos mediante los cuales es posible obtener datos de localización del objetivo:

Fotografías con fondos reconocibles:
Las imágenes compartidas públicamente pueden revelar información sobre el entorno del individuo. Elementos como edificios, calles, establecimientos comerciales o paisajes característicos permiten identificar ubicaciones aproximadas mediante simples búsquedas inversas o reconocimiento visual. Incluso detalles como matrículas

de vehículos, señalización urbana o interiores de viviendas pueden aportar pistas relevantes.

### *1.1.6. Etiquetas de localización en publicaciones:*

Muchas redes sociales permiten añadir ubicaciones exactas en fotos o estados. Etiquetas como “en casa”, “en el trabajo” o en un restaurante específico facilitan que terceros conozcan los movimientos del usuario en tiempo real o reconstruyan patrones de desplazamiento.

### *1.1.7. Información compartida en Marketplace o anuncios online:*

Una fuente de información especialmente relevante dentro del análisis OSINT realizado fue Facebook Marketplace, plataforma de compraventa integrada dentro de Facebook que permite a los usuarios publicar anuncios de productos y servicios de manera pública. A diferencia de otras secciones de la red social, Marketplace no requiere que el visitante sea contacto del vendedor para acceder a la información publicada, lo que la convierte en una fuente abierta de datos personales de alto valor.

Durante la exploración realizada, se identificó que este tipo de plataforma puede exponer de manera involuntaria información sensible del objetivo, entre la que destacan los siguientes elementos:

- Zona aproximada de residencia: Los anuncios publicados en Marketplace muestran automáticamente el área geográfica desde la cual se realiza la publicación, permitiendo inferir el sector o barrio donde reside el usuario sin necesidad de que este lo indique explícitamente.
- Número de contacto directo o enlace a WhatsApp: Es común que los vendedores incluyan su número telefónico personal o un botón de contacto directo mediante WhatsApp, facilitando que cualquier persona, incluido un potencial atacante, establezca comunicación directa con el objetivo.
- Fotografías del entorno interior del domicilio: En anuncios de venta de muebles, electrodomésticos u objetos del hogar, los usuarios frecuentemente publican fotografías tomadas dentro de su vivienda. Estas imágenes pueden revelar características físicas del domicilio, nivel socioeconómico aproximado y detalles del entorno personal.
- Disponibilidad horaria y rutinas: Algunos vendedores indican en sus publicaciones los horarios en los que pueden atender visitas o realizar entregas, lo que expone indirectamente sus rutinas y momentos de presencia o ausencia en el hogar.
- Historial de publicaciones: A través del perfil público del vendedor es posible acceder al historial de anuncios publicados, lo que permite reconstruir un patrón de comportamiento, identificar objetos de valor en su poder y estimar su nivel económico.

#### 1.1.7.1. Riesgos específicos derivados de Marketplace

La combinación de los datos obtenidos a través de Marketplace con información recopilada en otras redes sociales permite construir un perfil detallado del objetivo.

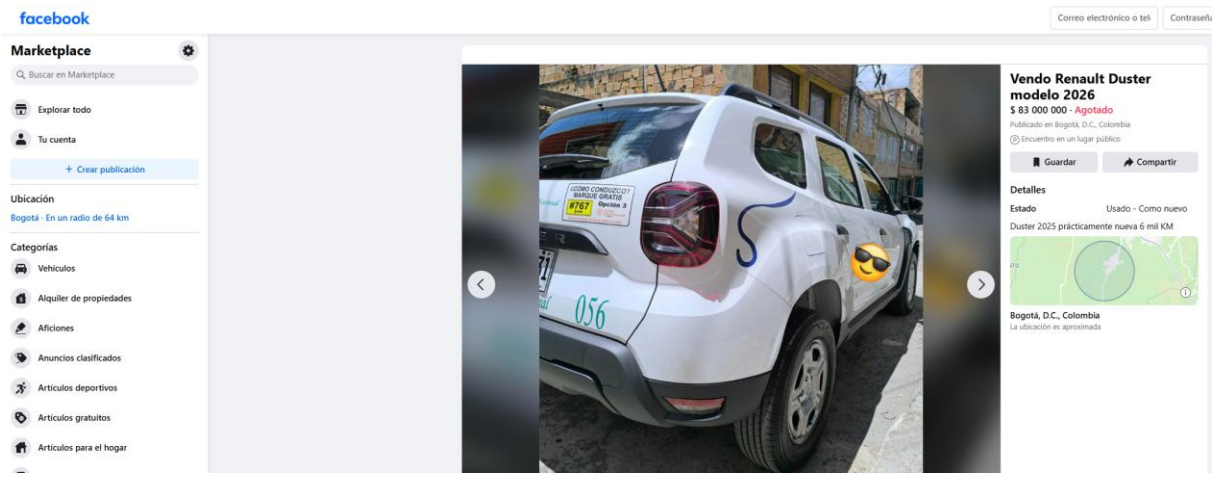
Entre los principales riesgos identificados asociados a esta plataforma se encuentran los siguientes:

- Estafas dirigidas: Un atacante puede contactar al objetivo simulando ser un comprador interesado, con el fin de obtener datos adicionales, enviar comprobantes de pago falsos o ejecutar fraudes mediante transferencias reversibles.
- Reconocimiento del domicilio: Las fotografías del interior de la vivienda y la información geográfica permiten a un delincuente identificar la ubicación aproximada del objetivo y evaluar las características físicas de su hogar como paso previo a un posible robo.
- Ingeniería social personalizada: Conocer los objetos que el objetivo posee, sus necesidades económicas o sus horarios disponibles proporciona al atacante elementos concretos para diseñar engaños altamente personalizados y creíbles.

En conclusión, Facebook Marketplace representa una fuente de información abierta frecuentemente subestimada por los usuarios, que puede exponer datos de alto valor para un ciberdelincuente. La publicación de anuncios sin considerar el impacto en términos de privacidad incrementa significativamente el nivel de vulnerabilidad del objetivo, especialmente cuando esta información se combina con datos obtenidos en otras plataformas digitales.

### 1.1.7.2. Imagen de Marketplace

A continuación, doy una imagen como referencia de Marketplace donde se generan evidencias:




### 1.1.7.3. Participación en eventos con ubicación pública:

La asistencia a eventos, reuniones o actividades públicas también puede ser visible en redes sociales. Cuando un usuario confirma su participación en un evento, se expone indirectamente su presencia en un lugar específico, lo cual puede ser utilizado por atacantes para anticipar movimientos o identificar hábitos.

### *1.1.8. Riesgos asociados a la información geográfica*

La información geográfica representa un riesgo crítico debido a que puede ser utilizada para fines delictivos más allá del entorno digital. Entre los principales escenarios posibles se encuentran:

- Robos domiciliarios, aprovechando publicaciones que revelen ausencia del hogar.
- Vigilancia o seguimiento, mediante el análisis de ubicaciones frecuentes.
- Acoso físico o digital, cuando un atacante conoce zonas de residencia o lugares visitados.
- Estafas presenciales, especialmente en contextos de compraventa o alquiler.

A diferencia de otros delitos informáticos, estos riesgos implican consecuencias directas sobre la integridad y seguridad personal del individuo. Además, el análisis realizado evidencia que la información geográfica y contextual compartida en plataformas digitales constituye uno de los elementos más sensibles dentro de la huella digital. Aunque muchas veces se publica de forma cotidiana e inconsciente, su combinación con otras fuentes abiertas puede facilitar delitos graves que afectan tanto la privacidad como la seguridad física. Por ello, resulta fundamental limitar la publicación de ubicaciones, revisar configuraciones de privacidad y evitar compartir detalles del entorno personal en espacios públicos de Internet.

### *1.1.9. Evaluación de la sensibilidad de la información recopilada*

La información obtenida fue clasificada según el nivel de riesgo que representa en caso de ser utilizada por un atacante:

| Tipo de información | Ejemplo | Nivel de riesgo |
|---|---|---|
| Datos generales | Nombre, fotos públicas | Bajo |
| Datos de contacto | Teléfono, correo | Medio |
| Ubicación o rutina | Ciudad, lugares frecuentes | Alto |
| Documentos personales | CV, archivos PDF | Alto |
| Información familiar | Fotos con menores o familiares | Muy alto |

Se concluye que gran parte de estos datos, aunque aparentemente inofensivos, pueden convertirse en elementos peligrosos cuando se combinan.

### *1.1.10. Reflexión sobre la calidad de la información obtenida*

En términos generales, las herramientas OSINT ofrecen información rápida, accesible y en muchos casos precisa. Sin embargo, también presentan limitaciones:

- No toda la información encontrada es actual
- Puede haber homónimos o perfiles falsos
- Los datos pueden estar incompletos o descontextualizados

A pesar de ello, el nivel de exposición observado demuestra que Internet constituye una fuente poderosa de recopilación para fases iniciales de un delito informático.

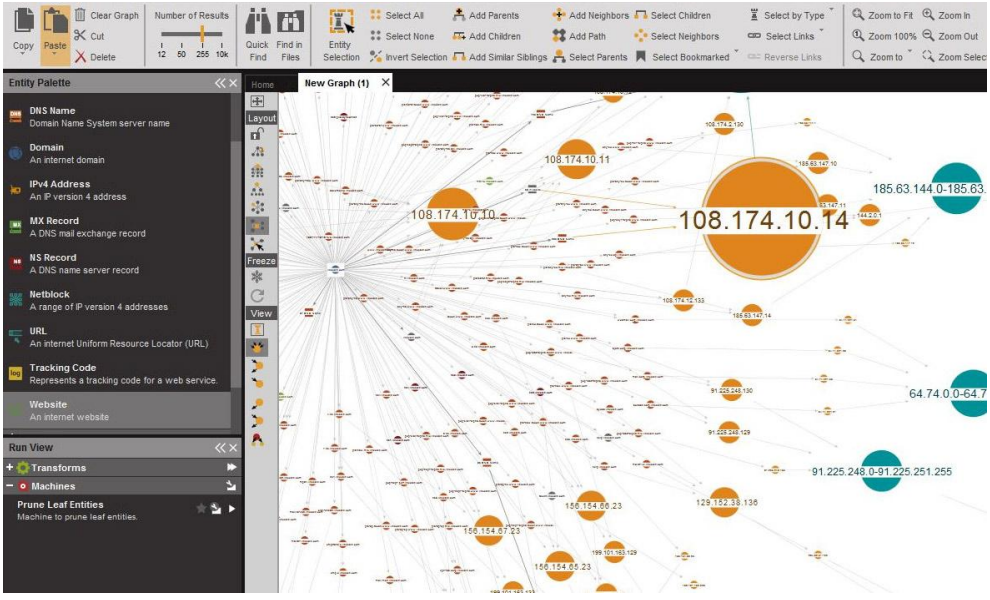
## 1.2. Herramientas OSINT especializadas utilizadas (Las imágenes tienen enlaces a las páginas web)

Además de los operadores avanzados de Google, existen herramientas especializadas en inteligencia de fuentes abiertas que permiten ampliar y profundizar la recopilación de información sobre un objetivo. A continuación, se describen las principales herramientas consultadas durante el desarrollo de esta actividad.

### *1.2.1. Maltego*

Maltego es una de las plataformas más reconocidas en el ámbito del análisis OSINT profesional. Permite visualizar de manera gráfica las relaciones entre diferentes elementos de información, tales como nombres, correos electrónicos, dominios, perfiles en redes sociales y números de teléfono. Su capacidad para mapear conexiones entre datos dispersos la convierte en una herramienta especialmente útil para identificar el entorno digital de un objetivo y descubrir vínculos que no serían evidentes mediante búsquedas convencionales. En el contexto de esta actividad, Maltego permitiría construir un grafo de relaciones a partir del nombre del objetivo, conectando perfiles sociales, correos y posibles asociaciones laborales o familiares.

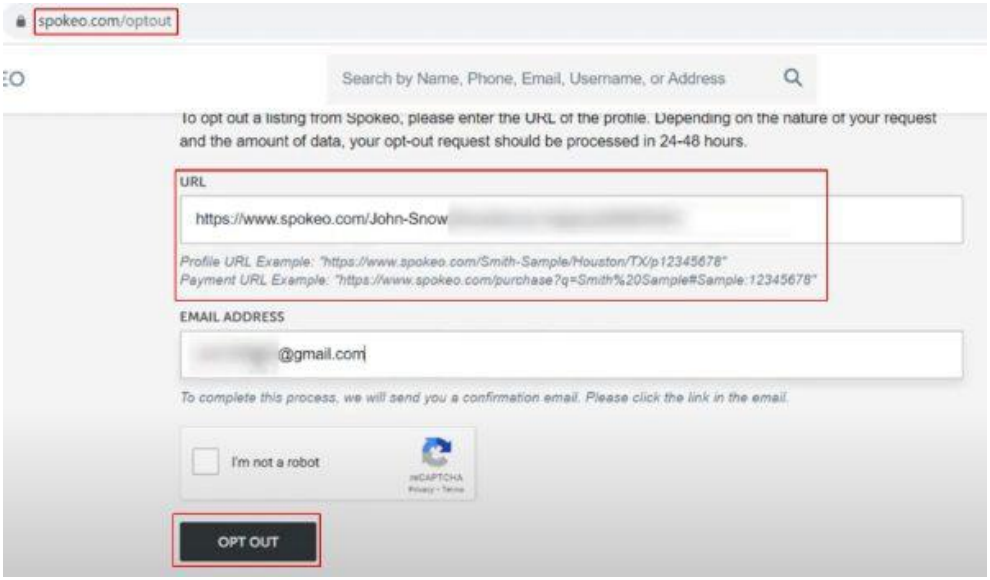
A continuación, una imagen de referencia de una búsqueda en Maltego:




### *1.2.2. Spokeo y Pipl*

Spokeo y Pipl son metabuscadores de personas especializados en la agregación de datos públicos disponibles en Internet. Estas plataformas consolidan información proveniente de registros públicos, redes sociales, directorios telefónicos y bases de datos abiertas, ofreciendo en un solo resultado datos como nombre completo, direcciones, números de teléfono, correos electrónicos, perfiles en redes sociales y posibles familiares o asociados. Su uso en investigaciones OSINT resulta especialmente relevante porque automatiza la búsqueda manual y reduce el tiempo necesario para construir un perfil básico del objetivo.

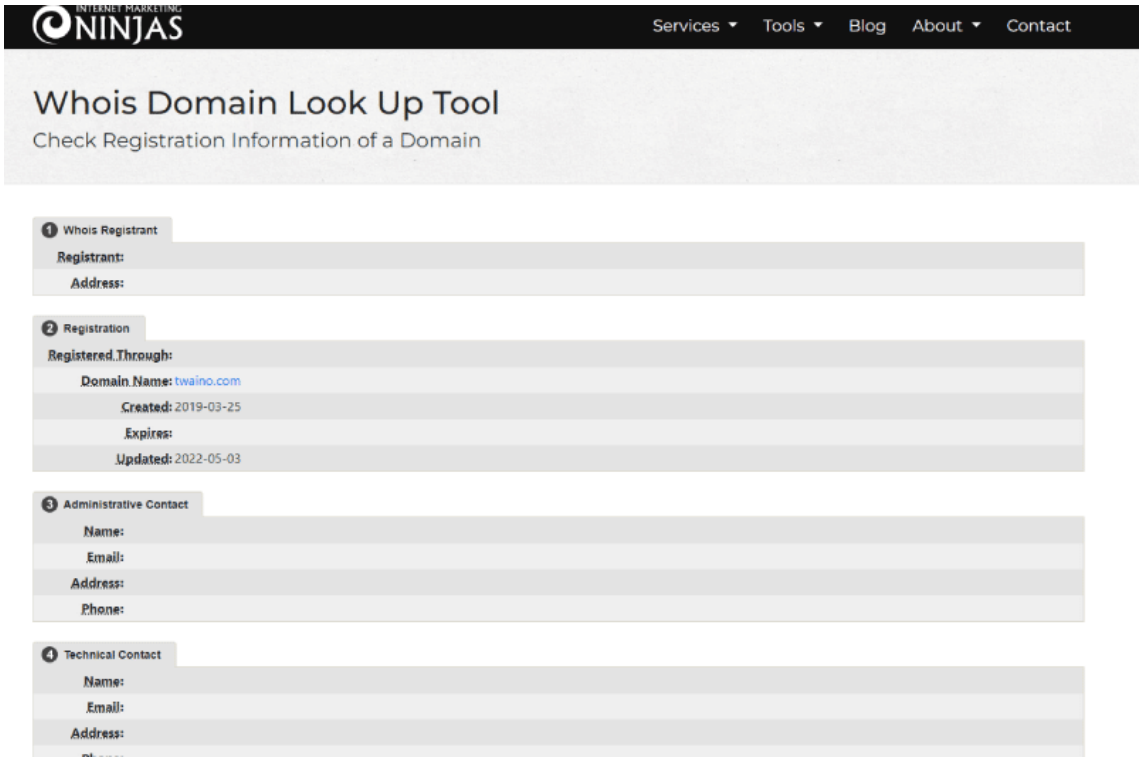
A continuación, una imagen de referencia de una búsqueda en Spokeo:




### *1.2.3. Whois*

La herramienta Whois permite consultar información pública sobre el registro de dominios en Internet. A través de esta plataforma es posible identificar datos como el propietario de un sitio web, la fecha de registro, los servidores de nombres utilizados y en algunos casos información de contacto del registrante. En el contexto de esta actividad, Whois resulta útil para verificar si el objetivo posee algún dominio web registrado a su nombre o asociado a su actividad profesional, lo que podría revelar información adicional sobre su identidad digital.

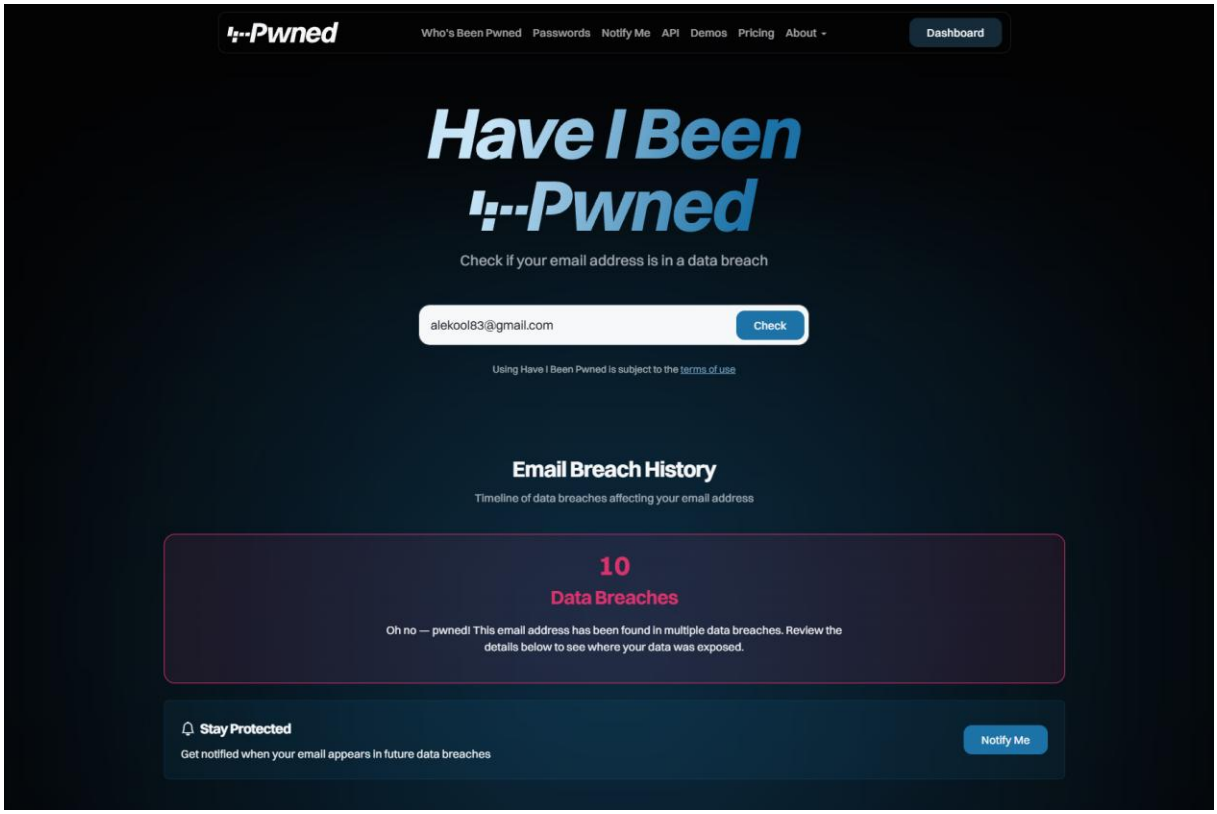
A continuación, una imagen de referencia de una búsqueda en Whois:




### *1.2.4. Have I Been Pwned*

Have I Been Pwned es una plataforma gratuita que permite verificar si una dirección de correo electrónico ha sido comprometida en alguna filtración de datos conocida. Introduciendo el correo electrónico del objetivo, la herramienta indica si dicha dirección aparece en bases de datos filtradas públicamente, lo que permite evaluar el nivel de exposición de sus credenciales digitales. Este tipo de información es especialmente relevante para un atacante, ya que una cuenta comprometida puede facilitar el acceso a otros servicios vinculados mediante la misma contraseña.

A continuación, una imagen de referencia de una búsqueda un correo en Have I Been Pwned:




### *1.2.5. Evaluación general de las herramientas*

El uso combinado de estas herramientas especializadas con los operadores avanzados de Google amplía significativamente la capacidad de recopilación en fuentes abiertas. Mientras que los buscadores convencionales ofrecen una visión general de la presencia digital del objetivo, las herramientas OSINT especializadas permiten profundizar en conexiones, historial de exposición y relaciones entre datos, incrementando el nivel de detalle del perfil construido.

Es importante destacar que todas estas herramientas operan únicamente sobre información públicamente disponible, sin vulnerar sistemas ni acceder a datos privados. Sin embargo, la cantidad y calidad de información que pueden agregar evidencia que la frontera entre lo público y lo privado en el entorno digital es cada vez más difusa, lo que refuerza la necesidad de adoptar medidas preventivas en la gestión de la identidad digital.

## 2. Posibles delitos a ejecutar con la información recopilada

A partir de la información obtenida mediante técnicas de inteligencia de fuentes abiertas (OSINT), es posible identificar diversos escenarios delictivos que podrían materializarse si dichos datos fueran utilizados por personas con intenciones maliciosas. Aunque la recopilación se realizó únicamente con fines académicos, los resultados evidencian que la información pública puede convertirse en una herramienta poderosa para la comisión de delitos informáticos.

### 2.1. Suplantación de identidad

La suplantación de identidad constituye uno de los delitos informáticos más frecuentes derivados de la información disponible en fuentes abiertas. Este delito consiste en hacerse pasar por otra persona utilizando sus datos personales con el fin de obtener beneficios económicos, acceder a información privada o manipular a terceros mediante engaño.

En el contexto actual, la disponibilidad de datos como nombre completo, fotografías públicas, información laboral, ciudad de residencia y vínculos sociales facilita enormemente la creación de perfiles falsos en redes sociales. A través de técnicas OSINT, un atacante puede recopilar información suficiente para construir una identidad digital creíble sin necesidad de vulnerar sistemas ni hackear cuentas.

#### *2.1.1. Facilidad de ejecución mediante redes sociales*

Las plataformas digitales permiten que un delincuente copie elementos visibles de un perfil real, tales como:

- Fotografías personales compartidas públicamente.
- Información biográfica (estudios, empleo, ciudad).
- Lista de contactos o familiares.
- Publicaciones, intereses o estilo de comunicación.

Con estos datos, el atacante puede crear un perfil fraudulento que resulte difícil de distinguir del original, especialmente para personas cercanas a la víctima.

#### *2.1.2. Posibles acciones del atacante*

Un ciberdelincuente podría utilizar esta información para múltiples fines maliciosos, entre ellos:

- Crear cuentas fraudulentas en redes sociales simulando ser la víctima, con el objetivo de engañar a otros usuarios o acceder a círculos privados de confianza.
- Contactar a familiares, amigos o compañeros de trabajo, solicitando dinero o ayuda urgente mediante excusas falsas, aprovechando la confianza emocional y la urgencia como herramientas de manipulación.
- Generar confianza en terceros simulando ser la víctima, lo que puede facilitar estafas, acceso a información privada o incluso la obtención de credenciales mediante técnicas de phishing.

- Daño reputacional, ya que el perfil falso puede publicar contenido ofensivo o realizar acciones que afecten la imagen pública de la persona suplantada.

### *2.1.3. Consecuencias de la suplantación de identidad*

Este tipo de delito puede derivar en impactos significativos tanto a nivel personal como profesional. Entre las principales consecuencias destacan:

- Fraudes económicos, cuando se solicita dinero a contactos cercanos o se realizan compras utilizando datos de la víctima.
- Pérdida de reputación digital, especialmente si el atacante publica información falsa o comprometedora.
- Riesgos legales o administrativos, en casos donde la identidad se utiliza para cometer otros delitos.
- Pérdida de confianza en entornos digitales, ya que la víctima puede ver afectadas sus relaciones personales y profesionales.

### *2.1.4. Importancia de la prevención*

La suplantación de identidad evidencia cómo la exposición excesiva de información en redes sociales puede convertirse en un recurso directo para el delito. Por ello, resulta fundamental aplicar medidas preventivas como:

- Configurar adecuadamente la privacidad del perfil.
- Limitar la visibilidad de fotos y datos personales.
- Verificar solicitudes sospechosas incluso si provienen de contactos conocidos.
- Reportar perfiles falsos de manera inmediata.

En conclusión, la suplantación de identidad es un delito que puede iniciarse fácilmente a partir de información pública obtenida en redes sociales. La actividad desarrollada demuestra que, en manos no adecuadas, los datos personales accesibles en fuentes abiertas pueden convertirse en la base para ataques fraudulentos, afectando gravemente la seguridad, privacidad y reputación de las personas en el entorno digital.

## 2.2. Ingeniería social y phishing personalizado

La ingeniería social representa una de las técnicas más utilizadas dentro de la ciberdelincuencia moderna, ya que no se basa principalmente en vulnerabilidades técnicas, sino en la manipulación psicológica de las personas. Este tipo de ataque aprovecha la confianza, la curiosidad, el desconocimiento o incluso el miedo de la víctima para inducirla a realizar acciones que comprometan su seguridad, como proporcionar información confidencial o acceder a enlaces maliciosos.

En este contexto, el conocimiento de detalles personales obtenidos mediante fuentes abiertas, tales como lugar de trabajo, estudios, intereses, relaciones sociales o rutinas diarias, permite diseñar ataques altamente personalizados. A diferencia del phishing tradicional, que suele ser masivo y genérico, el phishing personalizado (también conocido como spear phishing) se dirige a una persona concreta utilizando información real para aumentar la credibilidad del engaño.

### 2.2.1. *Importancia de la información personal en estos ataques*

La información recopilada a través de redes sociales y buscadores puede incluir:

- Nombre completo y fotografía.
- Empresa o institución donde trabaja o estudia.
- Eventos recientes a los que ha asistido.
- Publicaciones sobre hobbies o intereses.
- Datos sobre familiares, amigos o contactos cercanos.

Estos elementos permiten que el atacante construya mensajes que parecen auténticos y difíciles de detectar como fraudulentos.

### 2.2.2. *Ejemplos de ataques personalizados*

Un ciberdelincuente podría emplear esta información para ejecutar diferentes modalidades de ingeniería social, como las siguientes:

- Envío de correos electrónicos simulando provenir de la empresa donde trabaja la víctima: Por ejemplo, un atacante podría enviar un mensaje falso indicando que es necesario “actualizar credenciales” o “confirmar información de nómina”, logrando que la víctima entregue datos sensibles.
- Mensajes fraudulentos relacionados con actividades recientes publicadas en redes sociales: Si la víctima publica que asistió a un evento o realizó un viaje, el atacante puede aprovecharlo para enviar mensajes como “aquí están tus fotos del evento” o “confirmación de tu reserva”, incluyendo archivos o enlaces maliciosos.
- Enlaces adaptados a intereses específicos: Si se identifica que la víctima tiene interés en deportes, música o tecnología, el atacante puede enviar supuestas promociones, invitaciones o noticias relacionadas, aumentando la probabilidad de que la persona haga clic.

### 2.2.3. *Incremento en la probabilidad de éxito*

Este tipo de ataques incrementa considerablemente su efectividad debido a que se basa en información real y contextual. La víctima tiende a confiar más cuando el mensaje incluye detalles personales correctos, lo que reduce su capacidad de sospecha.

Además, la ingeniería social puede combinarse con técnicas como:

- Suplantación de identidad.
- Malware distribuido mediante enlaces.
- Robo de credenciales.
- Acceso a cuentas corporativas.

Esto demuestra que el phishing personalizado suele ser el primer paso para ataques más graves.

### *2.2.4. Consecuencias potenciales*

Los ataques de ingeniería social pueden derivar en consecuencias importantes, tales como:

- Robo de contraseñas y acceso a cuentas personales.
- Compromiso de información bancaria o financiera.
- Acceso a sistemas empresariales si la víctima trabaja en una organización.
- Instalación de software malicioso.
- Pérdida de privacidad y daños reputacionales.

En conclusión, la ingeniería social y el phishing personalizado representan una amenaza crítica en el ámbito de la ciberseguridad, ya que aprovechan la información disponible públicamente para manipular a las víctimas de manera directa. La actividad desarrollada evidencia que los datos expuestos en fuentes abiertas pueden convertirse en una herramienta clave para construir ataques altamente creíbles, lo que resalta la necesidad de fortalecer la concienciación y la protección de la identidad digital.

## 2.3. Fraudes y estafas digitales

Los fraudes y estafas digitales constituyen una de las consecuencias más frecuentes derivadas de la exposición de datos personales en fuentes abiertas. A diferencia de otros delitos más complejos, estos ataques no requieren conocimientos técnicos avanzados, sino que se apoyan principalmente en la obtención y utilización estratégica de información de contacto, como números telefónicos y direcciones de correo electrónico.

La disponibilidad pública de estos datos, ya sea en redes sociales, perfiles profesionales, anuncios clasificados o plataformas de compraventa, facilita que los ciberdelincuentes establezcan comunicación directa con la víctima. Una vez iniciado el contacto, el atacante puede emplear técnicas de manipulación y engaño para obtener dinero, datos bancarios o credenciales de acceso.

### *2.3.1. Modalidades de fraude más comunes*

A partir de la información recopilada en el análisis OSINT, se identifican diversas formas en que estos datos pueden ser explotados:

- Estafas mediante mensajería instantánea: Los delincuentes pueden enviar mensajes a través de WhatsApp, Telegram u otras plataformas simulando ser entidades confiables (bancos, empresas de mensajería, familiares o amigos). Al incluir información personal real en el mensaje, aumentan la credibilidad del engaño y reducen el nivel de sospecha de la víctima.

- Ofertas falsas relacionadas con productos publicados en Marketplace: Cuando una persona publica un anuncio de venta o alquiler, expone indirectamente su número de contacto y ubicación aproximada. Esto permite que un atacante envíe comprobantes de pago falsos, enlaces fraudulentos o solicitudes de adelanto de dinero bajo pretextos engañosos. También pueden realizarse

estafas inversas, donde el delincuente se hace pasar por comprador o vendedor legítimo.

- Intentos de fraude bancario mediante llamadas telefónicas (vishing): El término vishing hace referencia al phishing realizado por vía telefónica. En este tipo de ataque, el delincuente simula ser un representante bancario o de una entidad oficial, informando sobre supuestos movimientos sospechosos o bloqueos de cuenta. Aprovechando el miedo y la urgencia, solicita datos confidenciales como códigos de verificación o números de tarjeta.

### *2.3.2. Importancia del contexto en la construcción del engaño*

La combinación de información personal y datos contextuales permite que el delincuente construya escenarios altamente convincentes. Por ejemplo:

- Si la víctima ha publicado recientemente una compra o viaje, el atacante puede enviar un mensaje relacionado con la entrega del producto o la confirmación de reserva.
- Si se conoce el lugar de trabajo, puede simularse una llamada corporativa.
- Si se identifica la participación en una actividad específica, puede enviarse un mensaje relacionado con ese evento.

Este nivel de personalización incrementa significativamente la probabilidad de éxito del fraude, ya que el mensaje deja de ser genérico y se percibe como legítimo.

### *2.3.3. Impacto y consecuencias*

Las consecuencias de este tipo de delitos pueden ser graves, tanto en el ámbito económico como en el personal:

- Pérdidas financieras directas.
- Robo de credenciales bancarias.
- Uso indebido de datos personales para otros delitos.
- Estrés emocional y pérdida de confianza en plataformas digitales.

Además, una vez que una persona ha sido víctima de fraude, puede convertirse en objetivo recurrente, ya que sus datos circulan entre redes de estafadores.

En conclusión, los fraudes y estafas digitales representan una amenaza tangible y frecuente derivada de la exposición de datos personales en fuentes abiertas. La actividad desarrollada demuestra que la simple publicación de información de contacto puede ser suficiente para iniciar un proceso delictivo, especialmente cuando se combina con datos contextuales obtenidos mediante redes sociales y buscadores. Esto refuerza la importancia de limitar la visibilidad de datos sensibles y adoptar una actitud crítica frente a comunicaciones inesperadas.

## 2.4. Riesgos físicos derivados de la información digital

Más allá del ámbito estrictamente informático, uno de los aspectos más preocupantes asociados a la exposición de información en fuentes abiertas es la posibilidad de que

los datos digitales se conviertan en riesgos físicos para la víctima. En la actualidad, la frontera entre el mundo online y la vida cotidiana es cada vez más difusa, lo que implica que la información compartida en redes sociales puede tener consecuencias directas sobre la seguridad personal.

La publicación de datos geográficos, imágenes del entorno doméstico o detalles sobre rutinas diarias puede facilitar que un atacante no solo ejecute delitos virtuales, sino que también planifique acciones en el mundo real. Este fenómeno demuestra que la ciberseguridad no se limita únicamente a proteger sistemas informáticos, sino también a preservar la integridad física y la privacidad de las personas.

### *2.4.1. Exposición de información geográfica como factor de riesgo*

Muchas plataformas digitales permiten compartir ubicaciones mediante etiquetas, mapas o referencias indirectas. Incluso cuando no se publica una dirección explícita, un atacante puede inferirla a partir de:

- Fotografías tomadas cerca del domicilio.
- Lugares frecuentados con regularidad.
- Publicaciones en tiempo real durante viajes o salidas.
- Anuncios en plataformas de compraventa que muestran zonas residenciales.

La combinación de estos elementos permite construir un perfil espacial detallado del objetivo.

### *2.4.2. Delitos físicos facilitados por la huella digital*

Entre los principales riesgos identificados destacan los siguientes:

- Robo domiciliario: Cuando una persona publica que se encuentra de viaje o fuera de casa, expone indirectamente la vulnerabilidad de su vivienda. Los delincuentes pueden aprovechar esta información para seleccionar momentos oportunos para cometer robos, especialmente si además se ha compartido la ubicación aproximada del domicilio.
- Vigilancia no autorizada: La información sobre rutinas, horarios de trabajo o lugares visitados puede permitir que un atacante realice seguimiento sistemático del objetivo. Esto resulta especialmente peligroso en casos de violencia de género, conflictos personales o acoso prolongado.
- Acoso o seguimiento (stalking): La sobreexposición digital facilita que una persona malintencionada conozca la ubicación habitual de la víctima, sus relaciones sociales y sus movimientos diarios. Este tipo de situaciones puede derivar en amenazas, intimidación o persecución física, afectando gravemente la seguridad y bienestar psicológico del individuo.

### *2.4.3. Importancia de las rutinas como elemento explotable*

La exposición de rutinas constituye uno de los factores más sensibles dentro de la huella digital. Publicaciones como:

- Horarios habituales de gimnasio o trabajo.

- Lugares frecuentados semanalmente.
- Eventos confirmados con fecha y ubicación.
- Fotografías publicadas en tiempo real.

permiten que un atacante anticipe los movimientos del objetivo. Esto incrementa el riesgo de delitos físicos, ya que la información actúa como una guía indirecta sobre la vida cotidiana de la persona.

#### *2.4.4. Consecuencias e impacto*

Los riesgos físicos derivados de la información digital no solo implican pérdidas materiales, sino también consecuencias emocionales y psicológicas importantes:

- Sensación de inseguridad permanente.
- Vulneración grave de la privacidad.
- Afectación de la vida personal y social.
- Riesgo directo para la integridad física.

En muchos casos, la víctima no es consciente de que la información compartida aparentemente de forma inocente puede ser utilizada con fines criminales.

En conclusión, la información disponible públicamente en Internet puede trascender el ámbito digital y convertirse en un factor de riesgo físico real. La exposición de ubicaciones, rutinas e imágenes del entorno personal puede facilitar delitos como robos, vigilancia o acoso. Por ello, resulta fundamental adoptar medidas preventivas, limitar la publicación de información geográfica y reforzar la conciencia sobre el impacto que la huella digital puede tener en la seguridad integral de las personas.

### 2.5. Nivel de facilidad para la comisión del delito

El análisis realizado a lo largo de la actividad demuestra que no es necesario poseer conocimientos técnicos avanzados ni herramientas sofisticadas para recopilar información sensible sobre una persona. A diferencia de otros tipos de ataques que requieren vulnerar sistemas, explotar fallos de seguridad o desarrollar código malicioso, la recopilación de datos mediante fuentes abiertas puede llevarse a cabo utilizando recursos básicos y de libre acceso.

En la mayoría de los casos, basta con emplear motores de búsqueda como Google, aplicar operadores avanzados simples (site, filetype, intitle, inurl) y revisar perfiles públicos en redes sociales para construir un perfil relativamente detallado del objetivo. Este proceso, que en el ámbito de la ciberseguridad se conoce como fase de reconocimiento, puede realizarse en pocos minutos y sin dejar rastro evidente.

#### *2.5.1. Accesibilidad de las herramientas*

Uno de los factores que incrementa la facilidad de este tipo de delitos es que las herramientas necesarias son:

- Gratuitas.
- De uso cotidiano.

- Legales en su funcionamiento.
- Accesibles para cualquier usuario con conexión a Internet.

No se requiere software especializado ni conocimientos avanzados en programación. Incluso personas con habilidades digitales básicas pueden obtener datos relevantes si saben dónde buscar y cómo relacionar la información encontrada.

### *2.5.2. Importancia de la combinación de datos*

Otro elemento que facilita la comisión del delito es la posibilidad de combinar múltiples fragmentos de información aparentemente inofensivos. Por ejemplo:

- Un nombre completo obtenido en una red social.
- Un lugar de trabajo visible en LinkedIn.
- Fotografías familiares en Facebook.
- Un número de contacto publicado en Marketplace.

Por separado, estos datos pueden no parecer críticos; sin embargo, al integrarlos, permiten construir un perfil detallado que puede ser explotado para suplantación, fraude o ingeniería social.

### *2.5.3. Factores que incrementan la vulnerabilidad*

La facilidad para ejecutar este tipo de delitos aumenta considerablemente cuando se presentan las siguientes condiciones:

- Configuraciones de privacidad débiles o mal configuradas.
- Perfiles públicos indexados por motores de búsqueda.
- Publicación frecuente de información personal.
- Exposición de rutinas o ubicaciones en tiempo real.
- Falta de conciencia sobre los riesgos digitales.

En estos casos, el atacante no necesita vulnerar ningún sistema, sino simplemente aprovechar la información que la propia víctima ha hecho pública.

### *2.5.4. Reflexión crítica sobre la facilidad del delito*

Por lo tanto, puede afirmarse que, en determinados contextos, la ejecución de un delito informático basado en información de fuentes abiertas resulta relativamente sencilla. El mayor riesgo no radica necesariamente en la sofisticación técnica del atacante, sino en la combinación entre disponibilidad de información pública y desconocimiento por parte de los usuarios.

Esto evidencia una realidad preocupante: la barrera de entrada para este tipo de delitos es baja. Cualquier persona con intención maliciosa puede iniciar un proceso de recopilación de datos sin infringir inicialmente sistemas de seguridad, lo que dificulta la detección temprana del ataque.

En conclusión, el nivel de facilidad para la comisión de delitos basados en fuentes abiertas es elevado cuando existe una sobreexposición digital. La actividad

desarrollada demuestra que la protección frente a estos riesgos no depende únicamente de herramientas tecnológicas avanzadas, sino también de la gestión responsable de la información personal y del fortalecimiento de la cultura de ciberseguridad. La prevención comienza reduciendo la cantidad de datos accesibles públicamente y comprendiendo que, en el entorno digital, cada fragmento de información puede convertirse en una pieza clave dentro de un escenario delictivo.

## 2.6. Resumen Posibles Delitos

En conclusión, el análisis realizado demuestra que la información disponible públicamente en Internet puede convertirse en el punto de partida para múltiples modalidades delictivas, especialmente aquellas basadas en la manipulación psicológica, la ingeniería social y el aprovechamiento de la confianza digital. La recopilación de datos mediante fuentes abiertas no solo permite identificar información básica de un individuo, sino también construir perfiles detallados que facilitan la planificación de ataques personalizados.

A lo largo del desarrollo se evidenció que delitos como la suplantación de identidad, el phishing dirigido, los fraudes digitales y los riesgos físicos derivados de la exposición geográfica no requieren necesariamente vulneraciones técnicas complejas. En muchos casos, el elemento clave es la combinación estratégica de datos públicos que, aunque aislados parecen inofensivos, adquieren un alto valor cuando se integran en un mismo contexto.

Este escenario pone de manifiesto que la principal vulnerabilidad no siempre reside en fallos tecnológicos, sino en la sobreexposición de información personal y en la falta de conciencia sobre el alcance de la huella digital. La facilidad con la que puede recopilarse información mediante motores de búsqueda y redes sociales demuestra que el reconocimiento previo a un delito puede realizarse sin dejar evidencias visibles ni generar alertas de seguridad.

Asimismo, se observa que los delitos basados en fuentes abiertas suelen tener una alta tasa de éxito porque apelan a factores humanos como la confianza, la urgencia, el miedo o la familiaridad. Cuando un atacante utiliza datos reales del entorno de la víctima, el engaño se percibe como legítimo, lo que reduce la capacidad crítica del usuario.

Por tanto, la información pública mal gestionada no solo representa un riesgo potencial, sino que constituye un recurso estratégico para la ciberdelincuencia moderna. Esto evidencia la necesidad de adoptar medidas preventivas que reduzcan la exposición innecesaria de datos personales en Internet, fortalecer la cultura de ciberseguridad y promover una gestión consciente de la identidad digital.

En definitiva, la protección frente a estos delitos no depende exclusivamente de soluciones tecnológicas avanzadas, sino también de la responsabilidad individual en el uso de redes sociales y plataformas digitales. La prevención comienza con la comprensión de que cada dato compartido puede convertirse en una pieza clave dentro de un escenario delictivo.

## 2.7. Tabla Resumen de Posibles Delitos

Con el finde dar un mejor entendimisnto a continuación denoto una tabla resumen con los posibles delitos:

| Delito | Información utilizada | Método de ejecución | Nivel de riesgo | Facilidad de ejecución |
|---|---|---|---|---|
| Suplantación de identidad | Nombre, fotos, datos laborales, contactos | Creación de perfil falso en redes sociales | Muy alto | Alta |
| Phishing / Spear Phishing | Correo, empresa, eventos recientes | Correo o mensaje fraudulento personalizado | Alto | Alta |
| Vishing | Número de teléfono, nombre, banco | Llamada simulando entidad oficial | Alto | Media |
| Fraude en Marketplace | Teléfono, zona de residencia, anuncios | Comprobantes falsos, estafas de compraventa | Alto | Alta |
| Ingeniería social | Intereses, rutinas, relaciones personales | Manipulación psicológica personalizada | Muy alto | Alta |
| Robo domiciliario | Ubicación, rutinas, ausencias publicadas | Seguimiento de publicaciones en tiempo real | Alto | Media |
| Acoso / Stalking | Ubicación frecuente, rutinas, relaciones | Seguimiento físico basado en huella digital | Muy alto | Media |

*Fuente: Elaboración propia a partir del análisis OSINT realizado.*

# 3. Recomendaciones para prevenir delitos de fuentes abiertas

A partir del análisis realizado, se evidencia que gran parte de los riesgos identificados pueden mitigarse mediante la adopción de buenas prácticas de seguridad digital y una adecuada gestión de la privacidad en entornos online. A continuación, se presentan una serie de recomendaciones orientadas a reducir la exposición de información personal y prevenir posibles delitos informáticos.

## 3.1. Configuración adecuada de la privacidad en redes sociales

Una de las medidas preventivas más importantes para reducir el riesgo de delitos informáticos derivados de fuentes abiertas consiste en revisar y ajustar periódicamente la configuración de privacidad en redes sociales. Plataformas como Facebook, Instagram, LinkedIn o X (Twitter) concentran gran parte de la información personal que los usuarios comparten en su vida cotidiana, por lo que representan una de las principales fuentes de datos explotables mediante técnicas OSINT.

En muchos casos, los usuarios mantienen configuraciones predeterminadas que permiten un acceso amplio a sus publicaciones, fotografías y datos personales, sin ser plenamente conscientes del alcance real de dicha exposición. Por ello, resulta fundamental aplicar controles de privacidad que limiten la información disponible para personas desconocidas o potenciales atacantes.

### *3.1.1. Medidas recomendadas de configuración*

Entre las principales acciones preventivas se destacan las siguientes:

- Restringir la visibilidad de publicaciones únicamente a contactos de confianza: Es recomendable que las publicaciones personales, fotografías y estados no sean accesibles públicamente, sino únicamente por personas verificadas dentro del círculo social del usuario. Esto reduce la posibilidad de que terceros recopilen información sobre rutinas, intereses o actividades recientes.

- Limitar el acceso público a la lista de amigos o contactos: Mostrar públicamente las conexiones sociales facilita ataques de ingeniería social, ya que un atacante puede identificar familiares, compañeros de trabajo o amistades cercanas para diseñar fraudes dirigidos. Ocultar esta información dificulta la construcción de redes de confianza falsas.

- Ocultar datos sensibles como número de teléfono, correo electrónico o fecha de nacimiento: Este tipo de datos puede ser utilizado directamente para suplantación de identidad, fraudes o ataques de phishing. Por ello, es fundamental que no estén visibles en perfiles públicos ni disponibles para desconocidos.

- Desactivar la indexación del perfil en motores de búsqueda externos: Muchas redes sociales permiten que los perfiles sean encontrados a través de Google u otros buscadores. Desactivar esta opción reduce la visibilidad global del perfil y limita la recopilación masiva de información mediante búsquedas automatizadas.

### *3.1.2. Importancia de la revisión periódica*

La privacidad en redes sociales no debe considerarse un ajuste único, sino un proceso continuo. Las plataformas actualizan con frecuencia sus políticas, opciones de visibilidad y configuraciones predeterminadas, lo que puede provocar que información antes restringida se vuelva accesible nuevamente.

Asimismo, es recomendable revisar publicaciones antiguas, ya que contenido compartido años atrás puede seguir disponible y ser utilizado en el presente con fines maliciosos.

### *3.1.3. Impacto preventivo en delitos informáticos*

Una configuración adecuada de la privacidad reduce significativamente la cantidad de información accesible a terceros desconocidos, dificultando la ejecución de ataques basados en OSINT. Al limitar la exposición de datos personales, se disminuyen las probabilidades de delitos como:

- Suplantación de identidad.
- Phishing personalizado.
- Fraudes digitales.
- Acoso o seguimiento.

En conclusión, la gestión responsable de la privacidad en redes sociales constituye una barrera esencial frente a la recopilación de información en fuentes abiertas. Adoptar configuraciones restrictivas, controlar la visibilidad del perfil y reducir la

exposición de datos sensibles son medidas fundamentales para proteger la identidad digital y prevenir posibles delitos informáticos en un entorno cada vez más conectado.

## 3.2. Control de la información publicada

Más allá de la configuración técnica de la privacidad, una de las medidas más efectivas para prevenir delitos informáticos derivados de fuentes abiertas es el control consciente de la información que se publica en Internet. Cada fotografía, comentario o actualización de estado forma parte de la huella digital del usuario y puede ser recopilada, almacenada y analizada por terceros.

Antes de compartir cualquier contenido en redes sociales o plataformas digitales, es recomendable realizar una evaluación crítica preguntándose si esa información podría ser utilizada de manera indebida o combinada con otros datos para construir un perfil detallado del individuo. Este ejercicio de reflexión preventiva constituye una de las principales barreras frente a ataques basados en ingeniería social.

### *3.2.1. Buenas prácticas en la publicación de contenido*

Entre las principales recomendaciones para un adecuado control de la información publicada se destacan:

- Evitar publicar ubicaciones en tiempo real: Compartir la ubicación exacta mientras se está presente en un lugar específico puede facilitar situaciones de riesgo, como seguimiento, acoso o vigilancia no autorizada. Es preferible publicar este tipo de información una vez que el evento ha concluido.
- No difundir planes de viaje mientras se está fuera del domicilio: Informar públicamente sobre ausencias prolongadas puede exponer la vivienda a robos o intrusiones. Desde el punto de vista de la seguridad física, esta práctica incrementa la vulnerabilidad del entorno personal.
- No mostrar documentos personales en fotografías: Fotografías aparentemente inocentes pueden incluir información sensible visible en segundo plano, como documentos de identidad, tarjetas bancarias, boletos de viaje, credenciales laborales o direcciones. Estos datos pueden ser utilizados para suplantación de identidad o fraude.
- Limitar la exposición de menores o familiares: La publicación constante de información sobre hijos, pareja o familiares amplía el círculo de posibles víctimas y facilita ataques dirigidos. Además, en el caso de menores, la sobreexposición digital puede tener consecuencias a largo plazo en su privacidad y seguridad.

### *3.2.2. La combinación de información como factor de riesgo*

Uno de los aspectos más críticos es que la información no se analiza de manera aislada. Un atacante puede combinar múltiples publicaciones para inferir:

- Horarios habituales.
- Nivel socioeconómico.
- Relaciones personales.
- Lugares frecuentados.

- Actividades regulares.

Aunque cada publicación individual pueda parecer inofensiva, su acumulación genera un perfil detallado que puede ser explotado en ataques personalizados.

### *3.2.3. Relación con la ingeniería social*

La prudencia en la publicación de información personal constituye una de las principales barreras frente a la ingeniería social, ya que este tipo de ataques se fundamenta en la manipulación del factor humano más que en vulnerabilidades técnicas. La ingeniería social explota emociones como la confianza, la urgencia, el miedo o la curiosidad, utilizando información real del entorno de la víctima para construir escenarios creíbles y difíciles de detectar.

En este sentido, la información compartida públicamente en redes sociales y plataformas digitales representa una fuente valiosa para los atacantes. Datos como el lugar de trabajo, estudios, intereses, eventos recientes o relaciones personales pueden ser utilizados para diseñar mensajes altamente personalizados. Cuanto mayor sea la cantidad de información disponible, mayor será la capacidad del delincuente para adaptar su discurso y generar una falsa sensación de legitimidad.

Por ejemplo, un atacante que conoce detalles sobre la vida cotidiana del objetivo puede simular comunicaciones provenientes de contactos cercanos, instituciones académicas, entidades bancarias o incluso compañeros de trabajo. Este nivel de personalización incrementa considerablemente la probabilidad de éxito del engaño, ya que la víctima tiende a confiar cuando el mensaje incluye referencias reales y contextuales.

Reducir la cantidad de información expuesta públicamente limita de manera directa el material disponible para este tipo de manipulación psicológica. Cuando el usuario controla cuidadosamente lo que publica, dificulta que un atacante pueda construir un perfil detallado, disminuyendo así el riesgo de suplantación de identidad, fraudes digitales o campañas de phishing dirigidas.

Asimismo, es importante comprender que la ingeniería social no requiere necesariamente grandes volúmenes de datos; en ocasiones, pequeños fragmentos de información pueden ser suficientes para iniciar un ataque. Por ello, la prevención debe basarse en una gestión consciente y responsable de la identidad digital.

En conclusión, el control crítico de la información publicada constituye una medida preventiva esencial en la protección frente a delitos informáticos basados en ingeniería social. La seguridad en el entorno digital no depende únicamente de herramientas tecnológicas avanzadas, sino también del comportamiento responsable del usuario. Adoptar una actitud reflexiva antes de compartir contenido en línea permite disminuir significativamente la exposición innecesaria de datos personales y reducir la probabilidad de convertirse en víctima de engaños y manipulaciones en el ciberespacio.

## 3.3. Eliminación o solicitud de retirada de contenidos

En el entorno digital actual, uno de los principales desafíos relacionados con la privacidad es la permanencia de la información en Internet. Una vez que un dato personal ha sido publicado, puede ser replicado rápidamente, almacenado en múltiples plataformas o indexado por motores de búsqueda, dificultando su eliminación completa. Esta característica convierte a la red en un espacio donde la gestión de la identidad digital resulta compleja, especialmente cuando la información expuesta es no deseada o puede representar un riesgo para la seguridad de una persona.

Ante la detección de contenido personal publicado sin consentimiento o de información que pueda ser utilizada con fines maliciosos, existen distintos mecanismos que permiten solicitar su retirada o, al menos, reducir su visibilidad. Una de las primeras acciones recomendadas consiste en contactar directamente con el administrador del sitio web donde se encuentra alojado el contenido. En muchos casos, páginas externas, blogs, foros o portales públicos ofrecen canales de comunicación para solicitar la eliminación o modificación de información sensible, especialmente si se demuestra que vulnera la privacidad del afectado.

En el caso de redes sociales, la mayoría de plataformas digitales cuentan con herramientas internas para reportar publicaciones, perfiles falsos o contenido inapropiado. Estos mecanismos permiten denunciar situaciones como suplantación de identidad, difusión de datos personales, acoso o publicación de imágenes sin autorización. Aunque el proceso suele ser accesible para cualquier usuario, la efectividad depende de las políticas internas de cada red social y del tiempo de respuesta que estas plataformas manejen.

Por otro lado, desde una perspectiva legal, en determinadas jurisdicciones existe el derecho de supresión, también conocido como “derecho al olvido”, especialmente reconocido dentro del marco normativo europeo (GDPR). Este derecho permite a los ciudadanos solicitar la eliminación de información personal que resulte irrelevante, excesiva o perjudicial, otorgando un mayor control sobre los datos que permanecen accesibles públicamente. Sin embargo, su aplicación puede presentar dificultades, ya que debe equilibrarse con otros principios como la libertad de información o el interés público.

Asimismo, cuando la eliminación directa del contenido no es posible, una alternativa relevante consiste en solicitar a motores de búsqueda como Google la desindexación de enlaces que vulneren la privacidad. Esto implica que el contenido no aparecerá en los resultados de búsqueda, reduciendo significativamente su accesibilidad para terceros. Aunque esta medida no elimina la información desde su fuente original, sí limita su difusión y disminuye el riesgo asociado a su exposición.

A pesar de la existencia de estos procedimientos, es importante señalar que la eliminación total de información en Internet no siempre es viable, debido a la facilidad con la que los datos pueden ser copiados, almacenados o redistribuidos en diferentes espacios digitales. Por esta razón, estos mecanismos deben entenderse como herramientas de mitigación más que como soluciones absolutas.

En conclusión, aunque el control completo sobre la información publicada en Internet resulta complejo, existen alternativas técnicas y legales para solicitar la retirada o

reducción de contenidos no deseados. Estos procedimientos representan un componente esencial dentro de la protección de la identidad digital y refuerzan la importancia de adoptar medidas preventivas desde el inicio, evitando la sobreexposición de datos personales en plataformas públicas.

### 3.4. Protección de documentos y datos personales

Una de las prácticas más comunes que incrementan el riesgo de exposición digital es la publicación de documentos en formato PDF u otros archivos descargables que contienen información sensible. En muchos casos, los usuarios comparten currículums vitae, certificaciones, formularios o documentos académicos sin considerar que estos pueden ser indexados por motores de búsqueda y permanecer accesibles públicamente durante largos periodos de tiempo.

Los currículums, por ejemplo, suelen incluir datos como nombre completo, número de identificación, dirección, correo electrónico, número telefónico y trayectoria laboral detallada. Esta información resulta especialmente valiosa para atacantes que deseen ejecutar suplantación de identidad, fraudes o campañas de phishing personalizado. Una vez que un documento es publicado en una plataforma abierta o en un sitio web sin restricciones adecuadas, puede ser localizado fácilmente mediante operadores de búsqueda como filetype:pdf, lo que facilita su recopilación sistemática.

En caso de que sea estrictamente necesario compartir este tipo de documentos, se recomienda adoptar medidas de minimización de datos. Esto implica eliminar información innecesaria que no aporte valor al propósito del documento, utilizar versiones resumidas que omitan datos sensibles y controlar cuidadosamente los permisos de acceso cuando se comparta mediante plataformas en la nube. Asimismo, es recomendable verificar periódicamente si existen archivos personales indexados públicamente utilizando motores de búsqueda, con el fin de detectar posibles exposiciones no autorizadas.

La protección de documentos digitales forma parte de una estrategia más amplia de gestión responsable de la identidad en línea. Reducir la cantidad de información estructurada disponible públicamente disminuye significativamente las posibilidades de que terceros construyan perfiles detallados con fines maliciosos.

### 3.5. Educación en ciberseguridad y concienciación

La prevención de delitos informáticos no depende únicamente de configuraciones técnicas o herramientas de protección, sino también del nivel de conocimiento y conciencia del usuario. En muchos casos, la vulnerabilidad principal no se encuentra en los sistemas tecnológicos, sino en el factor humano. Por ello, la educación en ciberseguridad constituye un elemento esencial dentro de cualquier estrategia de protección digital.

Desarrollar una cultura de ciberseguridad implica comprender que cada acción en línea puede tener consecuencias, y que la información compartida puede ser utilizada de formas no previstas. Esto requiere adoptar una actitud crítica frente a solicitudes inesperadas de información personal, especialmente cuando provienen de correos electrónicos, mensajes o llamadas que apelan a la urgencia o al miedo.

Asimismo, resulta fundamental verificar la autenticidad de enlaces y comunicaciones antes de interactuar con ellos, evitando hacer clic en direcciones sospechosas o proporcionar credenciales sin confirmar la legitimidad del remitente. La implementación de mecanismos adicionales de protección, como la autenticación en dos factores (2FA), añade una capa extra de seguridad que dificulta el acceso no autorizado incluso cuando las credenciales han sido comprometidas.

La concienciación del usuario reduce considerablemente la efectividad de ataques basados en ingeniería social, ya que estos dependen en gran medida de la reacción emocional y de la falta de verificación previa. Un usuario informado es menos propenso a caer en engaños, reconocerá señales de alerta y adoptará medidas preventivas antes de que el ataque se materialice.

En conclusión, la educación en ciberseguridad constituye un pilar fundamental para la protección de la identidad digital. Más allá de las soluciones tecnológicas, es la formación y el comportamiento responsable del individuo lo que determina en gran medida su nivel de exposición frente a delitos informáticos.

Y con este último punto se da por finalizado el desarrollo de este laboratorio.

## CONCLUSIONES DE LA ACTIVIDAD

Para concluir este trabajo, se puede afirmar que el desarrollo de la actividad permitió comprender de manera práctica el alcance y la relevancia de las técnicas de inteligencia en fuentes abiertas (OSINT) aplicadas al análisis de la huella digital de una persona en Internet. A través del uso de motores de búsqueda, operadores avanzados de Google y la exploración de redes sociales, se evidenció cómo es posible recopilar información personal accesible públicamente y transformarla en un conjunto de datos útil para evaluar riesgos en materia de ciberseguridad y privacidad.

A diferencia de un enfoque meramente teórico, en el cual los conceptos relacionados con delitos informáticos o exposición digital se estudian de forma abstracta, la implementación práctica permitió observar de manera directa cómo un ciberdelincuente podría iniciar un proceso de reconocimiento previo a un ataque utilizando únicamente información disponible en Internet. El proceso comenzó con búsquedas generales del objetivo, seguido del uso de operadores específicos como site, filetype, intitle e inurl, lo que permitió localizar perfiles, documentos públicos y rastros digitales dispersos en distintas plataformas.

En el análisis inicial se observó que gran parte de la información encontrada corresponde a datos aparentemente inofensivos, como fotografías públicas, nombres completos o ubicaciones generales. Sin embargo, este tipo de información presenta una limitación importante: por sí sola no siempre parece peligrosa, pero adquiere un valor considerable cuando se combina con otros elementos disponibles en línea.

Por esta razón, resultó fundamental evaluar la sensibilidad de los datos recopilados y su posible utilización en contextos delictivos. La actividad permitió identificar que información como correos electrónicos, números de contacto, ubicaciones frecuentes o documentos personales puede convertirse en un recurso clave para delitos como la

suplantación de identidad, el phishing personalizado, la ingeniería social o incluso riesgos físicos derivados de la exposición geográfica.

Un aspecto especialmente relevante evidenciado en este trabajo es la diferencia entre dos enfoques dentro del análisis OSINT:

- Recopilación básica de información pública: permite obtener una primera aproximación general sobre la presencia digital del objetivo.
- Análisis contextual y combinado de datos: permite identificar riesgos reales cuando diferentes piezas de información se relacionan entre sí, generando un perfil detallado que puede ser explotado por atacantes.

Ambos enfoques son complementarios: mientras el primero muestra la cantidad de datos accesibles, la segunda evidencia es el verdadero impacto que puede tener dicha exposición en términos de seguridad.

Asimismo, el análisis realizado permitió reflexionar sobre la facilidad con la que pueden ejecutarse ciertos delitos informáticos sin necesidad de conocimientos técnicos avanzados. En muchos casos, basta con herramientas gratuitas y accesibles para construir un escenario de ataque convincente basado únicamente en información pública.

Finalmente, se abordaron los procedimientos y dificultades existentes para eliminar o restringir contenidos no deseados en redes sociales y motores de búsqueda. Este punto evidenció que, aunque existen mecanismos como denuncias, configuraciones de privacidad o solicitudes de desindexación, el control total sobre la información publicada en Internet resulta complejo debido a la permanencia y replicación constante de los datos en el entorno digital.

En síntesis, esta actividad permitió aplicar de manera práctica los fundamentos de la inteligencia en fuentes abiertas, consolidando habilidades para identificar riesgos asociados a la exposición de datos personales, evaluar posibles delitos derivados y proponer medidas preventivas. Más allá de los resultados obtenidos, el trabajo evidencia la importancia de desarrollar una cultura de ciberseguridad basada en la gestión responsable de la identidad digital.

En conclusión, el análisis demuestra cómo la información disponible públicamente en Internet puede convertirse en el punto de partida de múltiples delitos informáticos, resaltando la necesidad de adoptar medidas de protección, concienciación y control de la privacidad como elementos esenciales en la sociedad digital actual.

## BIBLIOGRAFÍA

A continuación, la bibliografía implementada en este desarrollo:


- Tema 1. Una perspectiva global de la seguridad. Seguridad en los Sistemas de Información (COLGII) - PER 15746 - Enero 2026.
- Tema 7. Técnicas de protección de sistemas. Seguridad en los Sistemas de Información (COLGII) - PER 15746 - Enero 2026.

- Tema 10. Auditoría y ataques Web. Seguridad en los Sistemas de Información (COLGII) - PER 15746 - Enero 2026.
- Clases virtuales con el profesor Ing. Diego Osorio Reina.
- Google. (s. f.). Eliminar resultados de búsqueda sobre ti en Google. Google Support. Recuperado el 17 de febrero de 2026, de https://support.google.com/websearch
- Facebook. (s. f.). Configuración de privacidad y seguridad en Facebook. Meta Help Center. Recuperado el 17 de febrero de 2026, de https://www.facebook.com/help
- Instagram. (s. f.). Centro de ayuda: privacidad, seguridad y denuncias. Meta Help Center. Recuperado el 17 de febrero de 2026, de https://help.instagram.com
- LinkedIn. (s. f.). Administrar la visibilidad del perfil público. LinkedIn Help Center. Recuperado el 17 de febrero de 2026, de https://www.linkedin.com/help/linkedin
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR). Official Journal of the European Union. https://eur-lex.europa.eu
- National Institute of Standards and Technology. (2017). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). U.S. Department of Commerce. https://nvlpubs.nist.gov
- ENISA. (2021). OSINT tools and techniques for cybersecurity. European Union Agency for Cybersecurity. Recuperado el 17 de febrero de 2026, de https://www.enisa.europa.eu
- Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking (2nd ed.). Wiley.
- Mitnick, K. D., & Simon, W. L. (2011). The Art of Deception: Controlling the Human Element of Security. Wiley.
- Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press.
- Solove, D. J. (2007). The Future of Reputation: Gossip, Rumor, and Privacy on the Internet. Yale University Press.
- United Nations Office on Drugs and Crime. (2013). Comprehensive Study on Cybercrime. United Nations. https://www.unodc.org


## AGRADECIMIENTO


Finalmente, deseo expresar mi más sincero agradecimiento al profesor Ing. Diego Osorio Reina, por los conocimientos, orientación y acompañamiento brindados durante el desarrollo de esta actividad. Sus explicaciones y aportes en el área de seguridad informática y análisis de riesgos digitales fueron fundamentales para comprender la importancia de la protección de la información en entornos abiertos.

Gracias a los conceptos abordados en clase, fue posible desarrollar esta actividad de manera estructurada, aplicando correctamente técnicas de búsqueda en fuentes abiertas (OSINT), análisis de huella digital y evaluación de riesgos asociados a la exposición de datos personales en Internet. La guía metodológica proporcionada permitió abordar el trabajo paso a paso, desde la recopilación de información hasta la identificación de posibles delitos y la formulación de recomendaciones preventivas.

Sin duda, esta experiencia fortaleció significativamente mi formación académica, ampliando mi comprensión sobre cómo la información disponible públicamente puede convertirse en un recurso tanto para fines legítimos como para la comisión de delitos informáticos. Esta actividad no solo consolidó conceptos teóricos sobre ciberseguridad, sino que también permitió reflexionar sobre la responsabilidad individual en la gestión de la identidad digital y la importancia de adoptar medidas de protección en la sociedad actual.

**¡¡¡Mil gracias profesor!!!**

**Respetuosamente,**

**Alejandro De Mendoza**