Guillermo Juan Pérez Prado

guillermojuan.perez@tajamar365.com

DISEÑO METODOLOGÍA OSINT

# Índice

## 1. Proceso de Investigación y Análisis de Información

### 1.1 Planificación

* 1.1.1 Definición de Objetivos
* 1.1.2 Alcance
* 1.1.3 Requerimientos de la Información
* 1.1.4 Consideraciones Legales y Éticas
* 1.1.5 Selección de Fuentes

### 1.2 Recolección

* 1.2.1 Ejecución
* 1.2.2 Métodos de Recolección
* 1.2.3 Herramientas OSINT Framework – Búsqueda por Categoría
* 1.2.4 Organización de la Información
* 1.2.5 Verificación de Datos

### 1.3 Análisis y Procesamiento

* 1.3.1 Procesamiento
* 1.3.2 Interpretación
* 1.3.3 Correlación
* 1.3.4 Evaluación
* 1.3.5 Síntesis

### 1.4 Diseminación de Resultados

* 1.4.1 Comunicación
* 1.4.2 Enfoque Accionable
* 1.4.3 Formato
* 1.4.4 Feedback

### 1.5 Aspectos Legales

* 1.5.1 Leyes de Protección de Datos y Privacidad
* 1.5.2 Términos de Servicio (ToS)
* 1.5.3 Acceso No Autorizado
* 1.5.4 Propiedad Intelectual
* 1.5.5 Difamación / Calumnia

### 1.6 Aspectos Éticos

* 1.6.1 Privacidad
* 1.6.2 Contexto
* 1.6.3 Precisión
* 1.6.4 Sesgo
* 1.6.5 No Abusar
* 1.6.6 Impacto

## 2. Caso Práctico: TechNova Solutions

### 2.1 Planificación

* 2.1.1 Definición de Objetivos
* 2.1.2 Alcance
* 2.1.3 Requerimientos de Información
* 2.1.4 Consideraciones Legales y Éticas
* 2.1.5 Selección de Fuentes

### 2.2 Recolección de Información

* 2.2.1 Ejecución
* 2.2.2 Métodos de Recolección
* 2.2.3 Herramientas Utilizadas
* 2.2.4 Organización (Uso de Maltego)
* 2.2.5 Verificación de Datos

### 2.3 Análisis y Procesamiento

* 2.3.1 Procesamiento
* 2.3.2 Interpretación
* 2.3.3 Correlación
* 2.3.4 Evaluación
* 2.3.5 Síntesis

### 2.4 Diseminación de Resultados

* 2.4.1 Comunicación
* 2.4.2 Enfoque Accionable
* 2.4.3 Formato
* 2.4.4 Feedback

### 2.5 Aspectos Legales y Éticos Aplicados

* 2.5.1 Aspectos Legales
* 2.5.2 Aspectos Éticos

### 2.6 Resultado Final

* 2.6.1 Conclusión del Caso

# Proceso de Investigación y Análisis de Información

## Planificación

• Definición de objetivos

Se deben determiner objetivos específicos, medibles, alcanzables, relevantes y limitados en el tiempo .Un objetivo bien definido, orienta todo el proceso y evita la recolección innecesaria de información y por tanto agiliza el proceso.

• Alcance

Delimitar el Proyecto, estableciendo fronteras temporales, geográficas y temáticas. Esto incluye definir el periodo de tiempo a estudiar, las áreas o regiones que serán analizadas y los temas o categorías relevantes. Un alcance bien definido optimiza recursos y mejora la precisión de los resultados. Además, un alcance demasiado amplio puede incluir información que sea ilegal obtener.

• Requerimientos de la información

Determinar qué tipo de datos se necesitan, cuantitativos o cualitativos, su nivel de detalle, el formato requerido, la frecuencia de actualización y las fuentes potenciales.  
También es esencial definir los criterios de calidad, veracidad y actualidad de los datos.

• Consideraciones legales y éticas

Antes de iniciar, se deben identificar las leyes, regulaciones y normas éticas aplicables, ya que como se ha mencionado antes, es fácil excederse en y acabar incumpliendo la ley. Esto incluye el cumplimiento de normativas de protección de datos, el respeto a la privacidad y la propiedad intelectual, así como la transparencia en los métodos de obtención y uso de información.

• Selección de Fuentes

Es importante localizar y clasificar las fuentes primarias (originales), secundarias (interpretaciones o análisis) y terciarias (resúmenes o compilaciones) que pueden aportar información relevante. Tanto en la evaluación de su confiabilidad, acceso y pertinencia, como en la mención de las fuentes en la documentación.

Se debe analizar la credibilidad, actualidad, precisión y objetividad de cada fuente. Se debe verificar quién la emite, cuál es su propósito y si existen conflictos de interés.  
Fuentes institucionales, académicas o gubernamentales suelen ofrecer mayor fiabilidad.

## Recolección

• Ejecución:

Consiste en **recopilar la información** de las fuentes previamente identificadas, aplicando los métodos definidos en la planificación. Se debe documentar todo el proceso para **garantizar trazabilidad y reproducibilidad.**

**• Métodos: Se definen las técnicas de recolección que se utilizarán:**

**Pasivas: sin interactuar directamente con el objetivo (p. ej. búsquedas en Google, redes sociales).**

**Activas: implican interacción directa o rastreo más profundo (p. ej. escaneo de puertos, peticiones web)**

**• Herramientas: Software, scripts, automatización.**

**OSINT Framework – Herramientas de búsqueda por Categoría**

|  |  |
| --- | --- |
| **Nombre / Enlace** | **Descripción** |
| **📧 Email Address** | |
| **Hunter.io** | **Encuentra correos asociados a un dominio.** |
| **Have I Been Pwned** | **Comprueba si un correo ha sido filtrado.** |
| **EmailRep.io** | **Analiza reputación y riesgo de emails.** |
| **💻 IP & MAC Address** | |
| **Shodan** | **Buscador de dispositivos conectados a Internet.** |
| **IPinfo.io** | **Muestra información sobre direcciones IP.** |
| **MACVendors.com** | **Identifica el fabricante según dirección MAC.** |
| **🖼️ Images / Videos / Docs** | |
| **Google Reverse Image Search** | **Búsqueda inversa de imágenes.** |
| **TinEye** | **Encuentra versiones o fuentes de imágenes.** |
| **ExifTool** | **Extrae metadatos de imágenes y documentos.** |
| **🌐 Social Networks** | |
| **Social-Searcher** | **Busca menciones en redes sociales.** |
| **Namechk** | **Verifica disponibilidad de usuario en múltiples plataformas.** |
| **WhatsMyName** | **Rastrea alias en decenas de sitios.** |
| **Maigret (GitHub)** | **Identifica perfiles y analiza alias en múltiples redes.** |
| **Sherlock (GitHub)** | **Busca alias en cientos de sitios desde terminal.** |
| **👥 User & Identity Search** | |
| **Pipl (pago)** | **Buscador de personas con base de datos global.** |
| **PeekYou** | **Encuentra perfiles sociales asociados a un nombre.** |
| **WebMii** | **Muestra visibilidad online y redes vinculadas a un usuario.** |
| **ThatsThem** | **Búsqueda por nombre, email, IP o teléfono.** |
| **Spokeo** | **Agrega datos públicos, correos y redes sociales.** |
| **📞 Telephone Numbers** | |
| **TrueCaller** | **Identifica propietarios de números telefónicos.** |
| **Sync.me** | **Revela información pública de números.** |
| **Thatsthem.com** | **Permite buscar por teléfono, email o IP.** |
| **📄 Public Records** | |
| **OpenCorporates** | **Datos de empresas y registros públicos.** |
| **CourtListener** | **Acceso a registros judiciales en EE.UU.** |
| **GovData** | **Portal de datos abiertos gubernamentales.** |
| **🗺️ Geolocation Tools / Maps** | |
| **Google Maps** | **Búsqueda geográfica y localización.** |
| **GeoNames** | **Base de datos global de ubicaciones.** |
| **OpenStreetMap** | **Mapa colaborativo libre.** |
| **🔍 Search Engines** | |
| **Google** | **Búsquedas avanzadas con operadores.** |
| **DuckDuckGo** | **Motor privado sin rastreo.** |
| **Yandex** | **Excelente para búsqueda inversa de imágenes.** |
| **💬 Forums / Blogs / IRC** | |
| **BoardReader** | **Buscador de foros y comunidades.** |
| **Reddit** | **Análisis de hilos y usuarios.** |
| **4chan Search (4plebs)** | **Archivo de foros públicos de 4chan.** |
| **💰 Digital Currency** | |
| **Blockchain.com Explorer** | **Analiza transacciones y direcciones BTC.** |
| **Whale Alert** | **Monitorea grandes movimientos de criptomonedas.** |
| **CipherTrace** | **Investigación y análisis blockchain.** |
| **🛡️ OpSec** | |
| **PrivacyTools.io** | **Recursos y guías de privacidad digital.** |
| **Qubes OS** | **Sistema operativo enfocado en seguridad.** |
| **ProtonMail** | **Correo cifrado y privado.** |
| **🌑 Dark Web** | |
| **Ahmia** | **Buscador de servicios onion (Tor).** |
| **DarkSearch.io** | **Motor de búsqueda de la Dark Web.** |
| **OnionScan** | **Analiza servicios ocultos Tor.** |
| **🎓 Training** | |
| **Trace Labs OSINT Training** | **Recursos de formación OSINT práctica.** |
| **Bellingcat Training** | **Guías y cursos de investigación open source.** |
| **SANS SEC487** | **Curso profesional en técnicas OSINT.** |

• Organización: Utilización de Maltego para **organizar, relacionar y visualizar los datos obtenidos** de manera estructurada y comprensible. Representando entidades y relaciones en forma de grafo facilita la identificación de patrones, conexiones y vínculos ocultos entre diferentes elementos investigados.

• Verificación:

Comparar los datos obtenidos en distintas plataformas o bases de datos para identificar coincidencias o discrepancias.

Se analiza la coherencia temporal, se revisan fechas, ubicaciones y contextos de publicación para comprobar si la información es actual, coherente y relevante con el objetivo de la investigación.

Se clasifica según su nivel de credibilidad (alta, media, baja) en función de su origen, reputación y precisión histórica.

Los datos críticos se verifican por al menos dos fuentes independientes(Cross-validation). Este principio es esencial para evitar sesgos o falsos positivos.

Imágenes, vídeos y documentos se analizan mediante herramientas de verificación digital para detectar manipulaciones o falsificaciones (ejemplo: metadatos, geolocalización, sombras, tiempo).

Se documenta la verificación indicando la fuente, fecha, método y resultado, permitiendo trazar el proceso de validación y mantener transparencia analítica.

**OSINT Framework – Herramientas para la Verificación de Información**

|  |  |  |
| --- | --- | --- |
| **Tipo** | **Herramienta / Enlace** | **Descripción breve** |
| **🔍 Análisis de metadatos** | **ExifTool FotoForensics Metadata2Go** | **Permiten revisar metadatos, fechas, cámaras, y detectar alteraciones o ediciones en archivos multimedia.** |
| **🖼️ Verificación de imágenes y videos** | **InVID-WeVerify Google Reverse Image TinEye** | **Compara imágenes y videos para identificar duplicados, manipulaciones o contextos falsos.** |
| **🌐 Comprobación de dominios y correos** | **Have I Been Pwned EmailRep.io Hunter.io WHOIS Lookup** | **Comprueba la autenticidad y registros de dominios y correos electrónicos.** |
| **🕓 Cronología y contexto** | **Wayback Machine Archive.today WhoisXML** | **Verifica la existencia histórica y cambios en sitios web o contenidos digitales.** |
| **📰 Evaluación de fuentes** | **Hoaxy NewsGuard CrowdTangle** | **Analiza la fiabilidad, reputación y propagación de la información en medios o redes.** |

## Análisis y Procesamiento

Los datos brutos recolectados deben limpiarse, correlacionarse y contextualizarse para producir conclusiones relevantes.

Procesamiento: Limpieza y normalización de los datos. Eliminación de duplicados, errores o información irrelevante.

Interpretación: Comprender el sentido de la información, su origen, intención y relación con los objetivos iniciales.

Correlación: Vincular diferentes elementos (IPs, usuarios, dominios, imágenes, fechas) para detectar patrones, vínculos o comportamientos.

Evaluación: Valorar la fiabilidad de las fuentes y la veracidad de los datos obtenidos.

Síntesis: Integrar todos los hallazgos para generar una narrativa coherente o conclusiones estratégicas.

**OSINT Framework – Herramientas Análisis y procesamiento**

|  |  |  |
| --- | --- | --- |
| **Paso** | **Herramienta / Enlace** | **Descripción breve** |
| **🧹 Procesamiento** | **Lampyre OpenRefine Excel / Google Sheets** | **Limpieza, normalización y depuración de datos. Eliminación de duplicados, errores o información irrelevante.** |
| **🧠 Interpretación** | **KH Coder NVivo RapidMiner** | **Comprensión del sentido, origen e intención de la información. Análisis semántico y de contenido.** |
| **🔗 Correlación** | **Maltego SpiderFoot Analyst’s Notebook** | **Vincula diferentes elementos (IPs, usuarios, dominios, fechas) para detectar patrones o comportamientos.** |
| **📊 Evaluación** | **Hoaxy NewsGuard Cognite** | **Valora la fiabilidad y veracidad de las fuentes o datos obtenidos. Asigna niveles de confianza.** |
| **🧩 Síntesis** | **Maltego Export Tableau Power BI** | **Integra los hallazgos y genera conclusiones estratégicas mediante informes o visualizaciones.** |

## Diseminación de Resultados

• Comunicación: Adaptación del mensaje según la audiencia.

• Accionable: Enfocar la información en resultados prácticos o decisiones.

• Formato: Reportes, dashboards, presentaciones, artículos, etc.

• Feedback: Revisión, mejora continua y retroalimentación del público o pares.

**OSINT Framework – Herramientas para la Diseminación de Resultados**

**La fase de diseminación de resultados busca comunicar eficazmente los hallazgos obtenidos durante el proceso OSINT. El objetivo es transformar la información analizada en conocimiento útil, claro y orientado a la acción, adaptando su formato y nivel de detalle al público objetivo.**

|  |  |  |
| --- | --- | --- |
| **Aspecto** | **Herramienta / Enlace** | **Descripción breve** |
| **💬 Comunicación** | **Microsoft Word Canva Notion** | **Adaptación del mensaje según la audiencia. Uso de lenguaje claro, estructurado y con énfasis en los hallazgos clave.** |
| **🎯 Accionable** | **Trello Miro Monday.com** | **Transforma los resultados en información práctica para la toma de decisiones o implementación de medidas.** |
| **📊 Formato** | **Power BI Tableau Google Data Studio PowerPoint** | **Presentación de resultados mediante reportes, dashboards, presentaciones o artículos técnicos.** |
| **🔁 Feedback** | **Google Forms Slack Notion Comments Microsoft Teams** | **Recopila retroalimentación del público o del equipo para mejorar continuamente los productos de inteligencia.** |

## Aspectos Legales

• Leyes de Protección de Datos y Privacidad

Toda actividad de recopilación y tratamiento de información deberá cumplir con las leyes de protección de datos personales vigentes (como el RGPD u otras normativas nacionales).

Evitar recolectar datos sensibles sin justificación legal.

No almacenar ni compartir información personal sin autorización expresa.

Asegurar la confidencialidad y protección de los datos recopilados.

• Términos de Servicio (ToS)

El acceso a plataformas digitales y fuentes abiertas debe realizarse respetando los Términos de Servicio establecidos por cada sitio web o aplicación.

No se deben utilizar herramientas o métodos que violen dichos términos.

Revisar periódicamente las políticas de uso de las plataformas empleadas.

• Acceso No Autorizado

Las prácticas OSINT se limitan exclusivamente a información pública y accesible sin vulnerar sistemas protegidos.

Está prohibido intentar eludir mecanismos de seguridad o autenticación.

Cualquier intento de acceso no autorizado constituye una falta grave y puede implicar responsabilidades penales.

• Propiedad Intelectual

Toda la información, material o contenido utilizado debe respetar las leyes de propiedad intelectual y derechos de autor.

Citar las fuentes utilizadas en informes y análisis.

No reproducir contenido protegido sin el permiso correspondiente.

• Difamación / Calumnia

Los informes deben basarse en datos verificables y contrastados.

Evitar emitir juicios de valor o afirmaciones no comprobadas.

La publicación de información falsa o engañosa puede acarrear sanciones legales y disciplinarias.

## Aspectos Éticos

• Privacidad

Aunque la información sea pública, debe protegerse la privacidad individual.

No divulgar datos personales que puedan causar daño o exposición indebida.

Limitar la recolección de información al propósito legítimo del análisis.

• Contexto

La información debe interpretarse dentro de su contexto original.

No alterar el sentido de las fuentes ni presentar los datos de forma engañosa.

Mantener una representación fiel y objetiva de los hechos.

• Precisión

El trabajo OSINT requiere verificación y validación rigurosa.

Contrastar la información con múltiples fuentes confiables.

Evitar la difusión de datos no confirmados o especulativos.

• Sesgo

Los analistas deben ser conscientes de los posibles sesgos personales o de las fuentes.

Mantener una postura neutral durante el proceso de análisis.

Documentar cualquier limitación o posible sesgo detectado.

• No Abusar

El OSINT debe emplearse únicamente con fines legítimos y profesionales.

Queda prohibido el uso de información para acosar, discriminar o manipular.

Toda actividad debe alinearse con los objetivos institucionales y las leyes aplicables.

• Impacto

Antes de publicar o compartir resultados, se debe evaluar el posible impacto social, reputacional o emocional.

Considerar las consecuencias de la difusión de información.

Priorizar siempre la responsabilidad ética sobre la exposición pública.

# Ejemplo ficticio

**Planificación**

**Definición de Objetivos**

* **Objetivo general:** Analizar la presencia digital de la empresa **“TechNova Solutions”** para detectar posibles indicios de fraude o actividades engañosas.
* **Objetivos específicos:**
  + Verificar la legitimidad de su sitio web y dominios asociados.
  + Identificar redes sociales y comprobar autenticidad.
  + Analizar correos corporativos y su reputación.
  + Evaluar coherencia entre presencia digital y actividad comercial declarada.

**Alcance**

* **Temporal:** Enero 2023 – Octubre 2025.
* **Geográfico:** Latinoamérica y España.
* **Temático:** Legitimidad corporativa, identidad digital, reputación y huella en línea.  
  Un alcance bien definido evita recopilar información innecesaria o ilegal.

**Requerimientos de Información**

* **Datos requeridos:** cuantitativos (fechas, registros, IPs) y cualitativos (contenido, contexto, reputación).
* **Criterios:** actualidad, fiabilidad, veracidad.
* **Fuentes:** institucionales, académicas, corporativas, redes sociales y bases de datos OSINT.

**Consideraciones Legales y Éticas**

* Cumplir con el **RGPD** y las leyes nacionales de protección de datos.
* No obtener información privada ni acceder a sistemas restringidos.
* Transparencia en la recolección y uso de datos.

**Selección de Fuentes**

* **Primarias:** Sitios web, redes sociales oficiales, registros WHOIS.
* **Secundarias:** Artículos periodísticos, bases de datos corporativas.
* **Terciarias:** Compilaciones, resúmenes o reportes de terceros.  
  Las fuentes se evalúan por **credibilidad, actualidad, precisión y objetividad**.

**Recolección de Información**

**Ejecución**

Se recopila la información de las fuentes previamente identificadas, documentando cada paso (fecha, fuente, enlace, descripción, nivel de fiabilidad).

**Métodos**

* **Pasivos:** Búsquedas avanzadas, revisión de redes sociales, WHOIS Lookup.
* **Activos:** Validación directa mediante *Hunter.io*, *EmailRep.io*, entre otras.

**Herramientas Utilizadas**

| **Categoría** | **Herramienta** | **Descripción** |
| --- | --- | --- |
| 📧 Email | Hunter.io / Have I Been Pwned | Verifica correos asociados a un dominio y filtraciones. |
| 💻 IP | Shodan / IPinfo.io | Busca dispositivos conectados y ubicación IP. |
| 🌐 Web | WHOIS Lookup / OpenCorporates | Consulta registros de dominios y empresas. |
| 👥 Redes Sociales | Sherlock / Maigret | Rastrea perfiles por alias en múltiples plataformas. |
| 🖼️ Imágenes | TinEye / ExifTool | Analiza metadatos y fuentes de imágenes. |
| 🗺️ Geolocalización | Google Maps / GeoNames | Verifica direcciones o ubicaciones asociadas. |

**Organización**

Se emplea **Maltego** para representar entidades y relaciones (dominios, IPs, correos, redes) en forma de grafo, facilitando la identificación de vínculos entre elementos investigados.

**Verificación**

* Se comparan datos en distintas fuentes (cross-validation).
* Se comprueba coherencia temporal y contextual.
* Se analizan metadatos y procedencia de imágenes con **ExifTool** y **TinEye**.
* Se clasifican datos según su **nivel de credibilidad (alta, media, baja)**.

**Ejemplo de verificación:**

* El dominio *technova-solutions.com* fue creado hace 3 meses, pero la empresa afirma existir hace 5 años.
* Correos corporativos filtrados en *Have I Been Pwned*.
* Imágenes del sitio web son tomadas de bancos de imágenes libres.
* En redes sociales se detectan seguidores falsos y fechas incoherentes.

**Análisis y Procesamiento**

**Procesamiento**

* Limpieza y normalización de datos con **OpenRefine**.
* Eliminación de duplicados y corrección de errores.

**Interpretación**

* Identificación de inconsistencias entre la información pública y la actividad declarada.
* Se infiere que la empresa presenta una **huella digital artificial**.

**Correlación**

* En **Maltego**, se vincula el correo “contact@technova-solutions.com” con otra empresa (*NovaTech Global*) registrada en Panamá, compartiendo la misma IP.
* Esto sugiere una **infraestructura digital duplicada o fraudulenta**.

**Evaluación**

* Fuentes gubernamentales: alta fiabilidad.
* Publicaciones en foros o redes: baja fiabilidad.
* Nivel de riesgo estimado: **alto**.

**Síntesis**

Los hallazgos apuntan a que **TechNova Solutions** es una empresa de fachada creada recientemente con posible intención fraudulenta.  
El análisis cruzado de fuentes y metadatos permitió construir una narrativa coherente y fundamentada.

**Diseminación de Resultados**

**Comunicación**

El informe final se redacta en **Microsoft Word**, con lenguaje claro y visualizaciones extraídas de **Maltego**.  
Se enfatizan hallazgos clave, riesgos y recomendaciones.

**Accionable**

* Se recomienda **no establecer relaciones comerciales** con la empresa.
* Notificar a autoridades de consumo y registrar el dominio en listas de vigilancia.

**Formato**

* **Dashboard en Power BI** para mostrar redes y correlaciones.
* **Presentación PowerPoint** para exposición ejecutiva.

**Feedback**

* Se distribuye el informe a los equipos de seguridad y se recopila retroalimentación a través de **Google Forms** y **Notion Comments**

**Aspectos Legales y Éticos**

**Aspectos Legales**

**• Leyes de Protección de Datos y Privacidad**

Toda actividad de recopilación y tratamiento de información deberá cumplir con las leyes de protección de datos personales vigentes (como el **RGPD** u otras normativas nacionales).

* Evitar recolectar datos sensibles sin justificación legal.
* No almacenar ni compartir información personal sin autorización expresa.
* Asegurar la confidencialidad y protección de los datos recopilados.

**• Términos de Servicio (ToS)**

El acceso a plataformas digitales y fuentes abiertas debe realizarse respetando los **Términos de Servicio** de cada sitio o aplicación.

* No usar herramientas que violen dichos términos.
* Revisar periódicamente las políticas de uso de las plataformas empleadas.

**• Acceso No Autorizado**

Las prácticas OSINT se limitan exclusivamente a **información pública y accesible**.

* Está prohibido eludir mecanismos de seguridad o autenticación.
* Cualquier intento de acceso no autorizado constituye una falta grave y puede implicar sanciones penales.

**• Propiedad Intelectual**

Toda información o contenido utilizado debe respetar las **leyes de propiedad intelectual y derechos de autor**.

* Citar las fuentes en los informes.
* No reproducir contenido protegido sin permiso.

**• Difamación / Calumnia**

Los informes deben basarse en datos **verificables y contrastados**.

* Evitar juicios de valor o afirmaciones no comprobadas.
* La publicación de información falsa puede acarrear sanciones legales y disciplinarias.

**Aspectos Éticos**

**• Privacidad**

Aunque la información sea pública, debe protegerse la **privacidad individual**.

* No divulgar datos personales que puedan causar daño o exposición indebida.
* Limitar la recolección de datos al propósito legítimo del análisis.

**• Contexto**

La información debe interpretarse **dentro de su contexto original**.

* No alterar el sentido de las fuentes ni presentar los datos de forma engañosa.
* Mantener una representación fiel y objetiva de los hechos.

**• Precisión**

El trabajo OSINT requiere **verificación y validación rigurosa**.

* Contrastar la información con múltiples fuentes confiables.
* Evitar la difusión de datos no confirmados o especulativos.

**• Sesgo**

Los analistas deben ser conscientes de sus posibles **sesgos personales o de fuente**.

* Mantener neutralidad durante el análisis.
* Documentar cualquier limitación o posible sesgo detectado.

**• No Abusar**

El OSINT debe usarse únicamente con **fines legítimos y profesionales**.

* Prohibido el uso de la información para acosar, discriminar o manipular.
* Todas las acciones deben alinearse con las leyes y políticas institucionales.

**• Impacto**

Antes de publicar o compartir resultados, se debe evaluar el **impacto social, reputacional o emocional**.

* Considerar consecuencias antes de difundir la información.
* Evitar causar perjuicios innecesarios a personas o entidades.

**Resultado Final**

**Conclusión:** La investigación OSINT permitió descubrir que “TechNova Solutions” era una fachada digital creada recientemente con fines posiblemente fraudulentos. La trazabilidad de la información, la verificación cruzada y el análisis visual en **Maltego** fueron claves para determinar la falta de legitimidad de la empresa, cumpliendo en todo momento con los principios **legales y éticos** del análisis OSINT.