UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

ANÁLISIS DE CIBER-AMENAZAS MEDIANTE TÉCNICAS DE OSINT Y CIBERINTELIGENCIA

AUTOR

BALON GARCIA ANDRES ALBERTO

EXAMEN COMPLEXIVO

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

ING. HAZ LÓPEZ LÍDICE VICTORIA, MSI.

Santa Elena, Ecuador

Año 2025

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino. Mgt.
DIRECTOR DE LA CARRERA

Ing. Lídice Haz López. Msi.
TUTOR

Ing. Jaime Orozco Iguasnia. Mgt.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez. Mgt.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **BALON GARCIA ANDRES ALBERTO**, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 05 días del mes de noviembre del año 2025

TUTOR

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ
Validar únicamente con FirmaEC

LÍDICE VICTORIA HAZ LÓPEZ

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Balon García Andres Alberto**

DECLARO QUE:

El trabajo de Titulación, **Análisis de Ciber-amenazas mediante Técnicas de OSINT y Ciberinteligencia** previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 16 días del mes de noviembre del año 2025

EL AUTOR

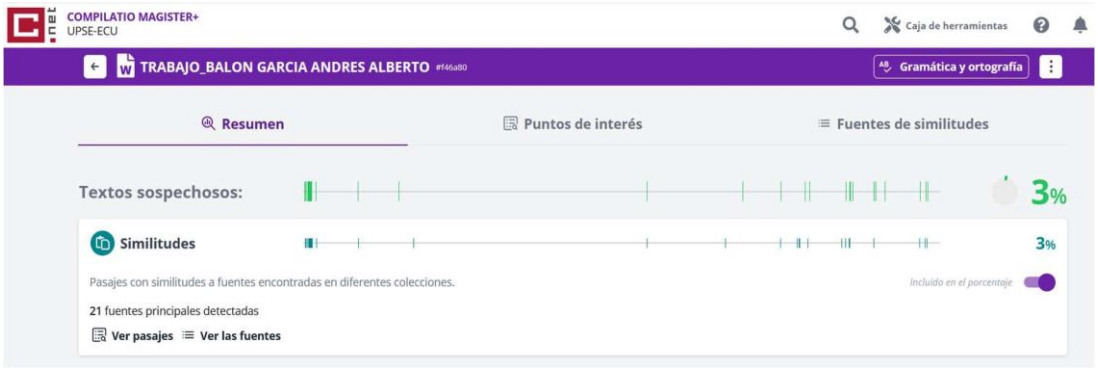
Balon García Andres Alberto

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado ANÁLISIS DE CIBER-AMENAZAS MEDIANTE TÉCNICAS DE OSINT Y CIBERINTELIGENCIA, presentado por el estudiante, **BALON GARCIA ANDRES ALBERTO** fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 3%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



TUTORA

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ
Validar únicamente con FirmaEC

LIDICE VICTORIA HAZ LÓPEZ

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Balon García Andres Alberto**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del presente trabajo de titulación con fines de difusión pública, además apruebo la reproducción dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 16 días del mes de noviembre del año 2025

EL AUTOR

Balon García Andres Alberto

AGRADECIMIENTO

En primer lugar, agradezco profundamente a Dios, por guiarme en cada paso de este camino académico, por darme la fortaleza, la paciencia y la sabiduría necesarias para culminar esta etapa de mi formación profesional.

A mi familia, por su constante apoyo, comprensión y motivación en los momentos más importantes. Su confianza y amor incondicional fueron fundamentales para alcanzar esta meta.

Extiendo un agradecimiento especial a mi tutora, la Ing. Lídice Haz López, Msi., por su orientación, compromiso y valioso acompañamiento durante el desarrollo de este trabajo. Su guía fue esencial para fortalecer mi aprendizaje y llevar este proyecto a buen término.

Finalmente, agradezco a mis compañeros y amigos por su colaboración y aliento a lo largo de este proceso, así como a los docentes de la Carrera de Tecnologías de la Información, quienes aportaron con sus conocimientos y experiencia a mi formación profesional.

Andres Alberto Balon García

DEDICATORIA

Dedico este logro a mi familia, por ser el motor que me impulsó a seguir adelante en cada momento.

A mi madre, por su amor, paciencia y por enseñarme que con esfuerzo todo es posible.

A mi padre, por su ejemplo de trabajo y dedicación, que me motivaron a nunca rendirme.

A ustedes les debo este logro, porque sin su apoyo y sacrificio nada de esto habría sido posible.

Andres Alberto Balon García

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El trabajo analiza la exposición de datos sensibles y la presencia de ciberamenazas mediante el uso de técnicas OSINT y ciberinteligencia. Su objetivo es identificar riesgos asociados a la publicación de información en fuentes abiertas y proponer acciones que fortalezcan la seguridad digital. La investigación se desarrolló a través de tres casos de estudio: una persona natural, una entidad privada y una entidad pública. Se aplicaron métodos de búsqueda, filtrado y análisis de información disponible en línea para evaluar el nivel de exposición y su impacto. Los resultados muestran que gran parte de los datos analizados permanecen accesibles públicamente y pueden ser aprovechados por actores maliciosos. Se concluye que el uso responsable de OSINT permite reconocer vulnerabilidades reales y fomenta una cultura preventiva para proteger la información personal y corporativa.

Palabras clave: OSINT, ciberinteligencia, ciberamenazas.

ABSTRACT

This work analyzes the exposure of sensitive data and the presence of cyber threats through the use of OSINT and cyber intelligence techniques. Its objective is to identify risks associated with the publication of information in open sources and to propose actions that strengthen digital security. The research was carried out through three case studies: a natural person, a private entity, and a public institution. Search, filtering, and data analysis methods were applied to evaluate the level of exposure and its impact. The results show that much of the information analyzed remains publicly accessible and can be exploited by malicious actors. It is concluded that the responsible use of OSINT helps to detect real vulnerabilities and promotes a preventive culture for the protection of personal and corporate information.

Keywords: OSINT, cyber intelligence, cyber threats.

INTRODUCCIÓN

La digitalización de los servicios y la expansión del uso de Internet han incrementado la cantidad de información personal e institucional expuesta en la red. Esta realidad ha creado un entorno donde los datos se convierten en un activo valioso, pero también en un objetivo frecuente para los ciberdelincuentes. Las filtraciones, el robo de identidad y el uso indebido de información pública muestran la necesidad de aplicar métodos que permitan identificar y reducir los riesgos digitales.

En este contexto, el uso de técnicas OSINT y ciberinteligencia se presenta como una alternativa para analizar la exposición de datos sin recurrir a métodos intrusivos. Estas técnicas aprovechan información disponible en fuentes abiertas para detectar vulnerabilidades, evaluar riesgos y generar conocimiento útil para la toma de decisiones.

El presente trabajo busca analizar la exposición de datos en distintos entornos mediante el uso de OSINT y ciberinteligencia. Para ello, se desarrollaron tres casos de estudio enfocados en una persona natural, una entidad privada y una institución pública. A través de este análisis se pretende demostrar cómo la información accesible en línea puede representar un riesgo si no se gestiona de forma adecuada.

El estudio también procura evidenciar la relación entre la gestión de datos y la seguridad digital, mostrando que la protección no depende solo de la tecnología, sino del uso responsable de la información. Comprender cómo se expone la huella digital permite adoptar medidas de prevención más efectivas y fortalecer la confianza en los entornos virtuales.

Los resultados obtenidos permiten comprender el impacto que tiene la exposición digital en la seguridad de los datos. Además, evidencian la importancia de fomentar una cultura de ciberseguridad basada en la prevención, la responsabilidad y el uso ético de la información. Este estudio busca aportar al fortalecimiento de las prácticas de protección digital tanto en el ámbito personal como institucional. Asimismo, resalta la importancia de aplicar buenas prácticas de ciberseguridad y mantenerse al tanto de los riesgos y cambios tecnológicos.

1. CAPITULO 1 FUNDAMENTACIÓN

1.1 Antecedentes

La digitalización de procesos en individuos, instituciones públicas y privadas ha generado una creciente cantidad de información expuesta de manera pública, muchas veces sin la debida conciencia de los riesgos que ello conlleva. Esta exposición de datos personales puede ser explotada por actores maliciosos para fines delictivos como el robo de identidad, ingeniería social, espionaje corporativo o ciberataques dirigidos [1].

El informe de IBM Security de 2023 revela que el costo promedio de una filtración de datos en el mundo ya es de 4.45 millones de dólares, lo que subraya la necesidad de controlar las amenazas y vulnerabilidades de manera efectiva [2]. Además, la exposición a estos ataques complica el cumplimiento de normativas como el Reglamento General de Protección de Datos (GDPR), presentando grandes desafíos para evitar riesgos.

Los ciberataques, sobre todo los de phishing, afectan la protección de datos personales y corporativos. En el primer trimestre de 2025, APWG registró 1 003 924 ataques de phishing, la cifra más alta desde fines de 2023 [3]. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) también indicó que el 43% de estos ataques estuvieron dirigidos a pequeñas y medianas empresas (PYMEs), que suelen tener recursos limitados para implementar sistemas de seguridad adecuados [4].

A pesar del potencial del OSINT en la identificación de ciberamenazas, varios estudios destacan las dificultades en su uso. Por ejemplo, en el artículo "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends", se subraya que el uso de OSINT sigue siendo limitado frente a otras técnicas más establecidas, en parte debido a la complejidad de manejar grandes volúmenes de datos sin estructura y a las dificultades para verificar la información [5].

Además, investigaciones recientes exploran el uso de OSINT para identificar riesgos en infraestructuras críticas. Por ejemplo, A. Vykopal et al. (2022) investigaron su papel en la detección de vulnerabilidades en infraestructuras

europeas, mientras que M. Atkinson et al. (2020) estudiaron cómo estas técnicas pueden revelar fugas de información sensible en redes sociales y foros públicos [6] [7].

1.2 Descripción de proyecto

El proyecto tiene como objetivo evaluar la exposición de datos sensibles mediante un entorno virtual basado en Kali Linux, utilizando técnicas y herramientas OSINT junto con enfoques de ciberinteligencia. Para el análisis se emplearon diversas utilidades especializadas, entre ellas Username Search, HaveIBeenPwned, Ghunt, Social Analyzer, DeHashed, Hunter.io, FOCA, Google Dorking e Investigator, las cuales permitieron la búsqueda, correlación y verificación de información en múltiples fuentes abiertas. El estudio se desarrolló en tres casos de investigación: persona natural, entidad pública y entidad privada, con el fin de identificar información expuesta en Internet y proponer medidas que fortalezcan la seguridad de los datos.

A través de un conjunto de métodos de búsqueda, filtrado y análisis, se exploran datos abiertos disponibles en sitios web, redes sociales, motores de búsqueda y dispositivos conectados a internet. El enfoque principal del proyecto no se basa en anticipar ciberataques, sino en localizar información que ya se encuentra expuesta públicamente, evaluando su impacto potencial y el riesgo que representa frente a posibles amenazas. De acuerdo con investigaciones recientes, la inteligencia de fuentes abiertas es esencial para mapear la huella digital y fortalecer la seguridad de la información desde un enfoque preventivo y no intrusivo [8].

La estructura del proyecto se inspira en la metodología presentada por Bazzell en Open Source Intelligence Techniques, adaptada al contexto de este trabajo. Esta versión contempla la identificación de recursos y técnicas de OSINT/ciberinteligencia, la recopilación y análisis de información expuesta, la evaluación contextual de la huella digital, así como la formulación de recomendaciones orientadas a mejorar la seguridad de la información [8]. Este enfoque permitió aplicar un método claro y organizado para alcanzar los objetivos del estudio. Asimismo, su aplicación contribuyó a mantener la coherencia entre los casos de estudio, permitiendo establecer patrones comunes en la exposición digital.

1.3 Objetivos del proyecto

Objetivo General

Analizar la exposición de datos sensibles y ciberamenazas en diferentes casos de estudio mediante la implementación de técnicas OSINT y Ciberinteligencia, con el fin de identificar riesgos que pueden perjudicar la integridad de los datos.

Objetivos Específicos

- Seleccionar las herramientas OSINT y técnicas de Ciberinteligencia más adecuadas para la recolección y análisis de datos públicos para cada caso de estudio.
- Analizar la exposición de datos sensibles en diferentes casos de estudio, mediante el uso de técnicas OSINT y Ciberinteligencia, evaluando las amenazas y vulnerabilidades asociadas a dicha exposición.
- Evaluar la efectividad de las herramientas y técnicas OSINT, así como de Ciberinteligencia en la detección precisa de la exposición de información sensible en los diferentes casos de estudio, analizando la relevancia y el alcance de los hallazgos.
- Proponer una guía de buenas prácticas de ciberseguridad basadas en los resultados obtenidos, enfocada en la protección de datos personales y seguridad de la información.

1.4 Justificación

La incorporación de técnicas de OSINT permite identificar información sensible ya expuesta en fuentes abiertas, como redes sociales, blogs, sitios web y foros, sin recurrir a métodos intrusivos. La Universidad Politécnica Salesiana señala que, de manera voluntaria o involuntaria, nos encontramos expuestos en Internet al aplicar OSINT, lo cual evidencia el riesgo real que representa esta exposición pasiva [9]. Por su parte, una guía académica reciente concluye que estas técnicas son “instrumentos valiosos para la recopilación de información relevante en línea” [10], y subraya que pueden revelar datos expuestos por errores humanos o falta de controles, lo que refuerza la importancia de revisar de forma periódica la información que permanece visible en la web.

Además, estudios de múltiples fuentes afirman que OSINT permite "tomar decisiones basadas en datos fiables", lo cual fortalece la capacidad de detectar y proteger información comprometida que ya está disponible públicamente [11]. En conjunto, más que prever amenazas, estas técnicas se centran en descubrir y analizar datos ya expuestos, lo cual facilita su protección efectiva.

La adaptabilidad de las herramientas OSINT permite su implementación desde la protección de datos personales, hasta en entidades gubernamentales y empresas privadas, fortaleciendo la protección de infraestructuras críticas. Según la Ley Orgánica de Protección de Datos Personales de Ecuador, que en su artículo 47 establece la responsabilidad proactiva en la implementación de mecanismos para la protección de datos personales, garantizando el cumplimiento de los principios, derechos y obligaciones establecidos en la normativa vigente [12].

Este proyecto está orientado al Plan Nacional de Desarrollo "Ecuador No Se Detiene" 2025-2029, descrito a continuación.

Eje social

Política 3.3.- "Potenciar las capacidades de inteligencia y contrainteligencia del estado que permita identificar, prevenir y neutralizar amenazas que puedan comprometer la seguridad y la estabilidad nacional." [13].

Objetivo 3.- "Garantizar un estado soberano, seguro, y justo promoviendo la convivencia pacífica y el respeto a los derechos humanos." [13].

Estrategia c.- "Incorporar tecnologías emergentes en la ciberinteligencia para identificar, monitorear y analizar amenazas, tendencias y oportunidades asociadas con innovaciones tecnológicas." [13].

1.5 Alcance de proyecto

El proyecto se desarrolla en un entorno virtual basado en Kali Linux y tiene como objetivo evaluar la exposición de datos sensibles en fuentes abiertas utilizando herramientas OSINT y técnicas de ciberinteligencia. El análisis se llevará a cabo en tres casos reales: una persona natural, una entidad pública y una organización privada. El propósito es identifica información pública que represente un riesgo de seguridad y propone recomendaciones orientadas a reducir dicha exposición

La investigación se estructura en cuatro fases. En la primera se seleccionan las herramientas y métodos OSINT más adecuados para la recolección de información en internet. En la segunda, se recopilan y analizan datos expuestos de los tres casos seleccionados, clasificándolos según su tipo y nivel de riesgo. La tercera fase se enfoca en evaluar el contexto de esa exposición digital, observando las diferencias entre los perfiles estudiados. Finalmente, se plantean recomendaciones prácticas para fortalecer la seguridad informacional, priorizando medidas de prevención y buenas prácticas en el uso de datos en línea.

Este trabajo no contempla el desarrollo de nuevas herramientas, ni la aplicación de técnicas intrusivas, ofensivas o automatizadas que vulneren sistemas. Tampoco se incluye el análisis en contextos de defensa nacional, infraestructura crítica o investigaciones de carácter judicial. El enfoque se limita al uso legal y ético de información públicamente accesible. Todas las actividades se realizarán en un entorno controlado, con fines académicos, sin intervenir ni alterar los sistemas o servicios analizados. La intención es demostrar cómo puede emplearse la inteligencia de fuentes abiertas con responsabilidad y dentro del marco normativo vigente.

Asimismo, el proyecto está sujeto a restricciones técnicas derivadas del uso de versiones gratuitas de herramientas OSINT. Muchas de estas plataformas limitan la cantidad de consultas, el tipo de datos disponibles y la frecuencia de uso, lo que puede afectar la profundidad del análisis. La investigación también dependerá de la disponibilidad y condiciones de uso de estos servicios, las cuales podrían cambiar durante el desarrollo del estudio.

Se tomarán en cuenta las normas legales vigentes y se respetarán los derechos de propiedad intelectual de las plataformas utilizadas, garantizando que cada procedimiento se realice dentro del marco permitido. Las recomendaciones finales estarán alineadas con un enfoque preventivo, respetuoso de la privacidad y de la legalidad en el manejo de datos expuestos en la red. El proyecto prioriza el uso ético de los recursos tecnológicos, buscando contribuir a la concientización sobre los riesgos asociados a la exposición digital y promoviendo prácticas responsables que reduzcan posibles vulnerabilidades.

2. CAPITULO 2 MARCO TEORICO Y METODOLOGIA DE PROYECTO

2.1 Marco legal

El presente trabajo se basa en la Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en el Registro Oficial el 26 de mayo de 2021. Esta ley regula el uso de los datos personales en Ecuador y establece que las instituciones deben aplicar medidas adecuadas para protegerlos. Su objetivo principal es garantizar los derechos de las personas y sancionar a quienes no cumplan con la normativa [14].

Según la LOPDP, el tratamiento de datos se rige por principios que aseguran un manejo correcto de la información. Entre ellos se encuentran la licitud y lealtad, que obligan a un uso legal y transparente; la finalidad, que limita el tratamiento a un propósito específico; y la minimización de datos, que permite recolectar solo lo necesario. Estos principios son la base para un manejo responsable de los datos [14].

También destacan los principios de seguridad y responsabilidad proactiva. El primero señala que se deben aplicar medidas que garanticen la confidencialidad, integridad y disponibilidad de la información. El segundo obliga a las instituciones a demostrar que cumplen con la ley mediante políticas, registros y controles. Con esto, la normativa busca que exista prevención y no solo reacción ante posibles incidentes [14].

La ley define como dato personal toda información que identifique o pueda identificar a una persona, como nombre, número de cédula, correo electrónico o teléfono. Además, clasifica como datos sensibles los relacionados con salud, origen étnico, ideología, identidad de género, orientación sexual, datos biométricos y genéticos. El mal uso de esta información puede afectar de manera directa los derechos de las personas [14].

El Artículo 47 establece que tanto instituciones públicas como privadas deben aplicar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad acorde al riesgo. Estas medidas deben proteger contra pérdida, alteración, acceso o divulgación no autorizada. Por ello, la LOPDP exige contar con políticas, controles y mecanismos de reporte de incidentes para el tratamiento de datos [14].

La **Tabla 1** resume los principales artículos de la Ley Orgánica de Protección de Datos Personales (LOPDP) que respaldan este trabajo. En ella se indica el tema central de cada artículo y cómo se aplica dentro del análisis, sirviendo como base legal para la evaluación de riesgos y el tratamiento adecuado de los datos personales, además de orientar las medidas que deben implementarse para garantizar un manejo responsable de la información.

Artículo	Descripción	Finalidad
Art. 4	Definiciones: establece los conceptos de dato personal y dato sensible.	Clasificar qué tipo de información se obtuvo (nombre, correo, imagen, etc.).
Art. 8	Consentimiento del titular: requiere autorización libre, específica, informada e inequívoca para tratar datos personales.	Requiere autorización del titular para tratar datos personales, salvo excepciones.
Art. 10	Principios del tratamiento: incluye finalidad, proporcionalidad, minimización y legitimidad; regula que los datos solo se usen para fines legítimos, necesarios y proporcionales al propósito.	Garantizar que el tratamiento de datos se limite a fines específicos, legítimos y proporcionales al objetivo perseguido.
Art. 37	Seguridad de los datos personales: obliga a aplicar medidas técnicas y organizativas adecuadas para proteger la información.	Asegurar la protección continua de los datos personales mediante controles técnicos y organizativos proporcionales al nivel de riesgo.
Art. 40	Análisis de riesgos, amenazas y vulnerabilidades.	Garantizar la detección, evaluación y mitigación de riesgos que puedan comprometer la seguridad de los datos personales.
Art. 42	Evaluación de impacto del tratamiento de datos personales (EIPD).	Indica que ciertos tratamientos deben analizar sus efectos antes de ejecutarse, evaluando los posibles riesgos.

Artículo	Descripción	Finalidad
Art. 43 y 46	Notificación de vulneraciones y gestión de incidentes de seguridad.	Exige registrar y mitigar vulneraciones de datos personales.
Art. 47	Obligaciones del responsable y encargado del tratamiento: mantiene la responsabilidad durante todo el ciclo de vida de los datos.	Reafirma el deber de seguridad en todo el ciclo de tratamiento.

Tabla 1: Artículos de la LOPDP relacionados con la protección y gestión de datos personales (Fuente: [14]).

2.2 Marco conceptual

2.2.1 Definición y evolución de la ciberseguridad

La ciberseguridad es una disciplina importante para la protección de los sistemas de información, redes y datos frente a amenazas digitales. Tiene como objetivo principal proteger la 'confidencialidad, integridad y disponibilidad' de la información, conocida como la triada CID. "La confidencialidad asegura que la información solo sea accesible por personal autorizado y previene divulgaciones no autorizadas. La integridad asegura que los datos sean precisos y completos protegiéndolos de alteraciones no autorizadas. La disponibilidad asegura que los sistemas y datos sean accesibles cuando se necesiten y se mantenga la continuidad operativa" [15].

La evolución de la ciberseguridad avanzó de la mano con los avances tecnológicos. El enfoque primordial para proteger estaba en los sistemas gubernamentales y militares, estos operaban en entornos de sistemas cerrados y controlados. La protección de datos no es un tema resiente, “ya que, con la llegada de la escritura, muchas civilizaciones antiguas buscaban proteger información valiosa que, si se usaba incorrectamente, podría poner en peligro el comercio o la guerra de la nación. Mas adelante, la era de la computación obligó y a su vez generó la necesidad de aplicar mecanismos de protección de datos registrados” [16]. Con el progreso de las tecnologías estas prácticas evolucionaron para responder a nuevas amenazas.

"Durante los años 70, surgieron los primeros virus informáticos, lo que llevó a la creación de software antivirus, esto con el fin de proteger los sistemas de información. En los años 80, la popularidad de las redes informáticas aumentó, lo que renovó el enfoque en la protección de la información personal a través de la autenticación y el cifrado de datos. Los años 90 marcaron la llegada del comercio electrónico y la globalización de los negocios, lo que inició al desarrollo de programas conocidos como firewalls y técnicas de detección de intrusiones." [17].

"Iniciando el siglo 21, con el incremento de los ataques cibernéticos y malware, las organizaciones comenzaron a automatizar la seguridad de transacciones financieras y agregar dos factores más para la autenticación. Los ataques se volvieron más activos, por lo que, en 2010, la proliferación de dispositivos móviles, aplicaciones en línea y computación en la nube transformaron completamente el paradigma de la ciberseguridad. Además, surgieron nuevos enfoques de seguridad activos en la nube, análisis de datos y hasta inteligencia artificial fueron empleados para prevenir ataques cibernéticos. " [18].

Actualmente, la ciberseguridad enfrenta complicaciones aún más desafiantes con la aparición de la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT), que han ampliado el alcance de posibles ataques y han llevado a que los sistemas modernos de ciberseguridad utilicen IA para procesar grandes cantidades de datos, buscar patrones y anomalías, así como prever comportamientos anormales que podrían sugerir un ataque. La llegada de la globalización y la digitalización perjudicaron este cambio. "Más notablemente, en conjunción con la pandemia de COVID-19 en 2020, la ciberseguridad emergió a la luz pública. El aumento del trabajo remoto y el uso de dispositivos móviles proporcionó un nuevo paradigma de trabajo para todas las empresas que tuvieron que ajustarse rápidamente a la situación" [18].

Desde este punto de vista, la ciberseguridad dejó de ser un problema técnico a ser ya una cuestión estratégica para estados y empresas. La expansión de las tecnologías de la información y la comunicación (TIC) en todas las ramas de la actividad económica contemporánea, ha provocado el aumentando de la exposición al riesgo en el ciberespacio, lo que requiere formas más integrales y de anticipación para la gestión de los riesgos de seguridad informática. "Hoy en día, la

ciberseguridad se asocia más a la operativa con la resiliencia, la reputación corporativa y la confianza que brindan clientes y socios. De igual manera, se ha vuelto un determinante e importante para la competitividad y sostenibilidad de las organizaciones en el mundo digital globalizado " [18].

2.2.2 Principales amenazas y vulnerabilidades en el ciberespacio

Los delitos cibernéticos han crecido en su complejidad y en su frecuencia. De acuerdo con "el Instituto Nacional de Ciberseguridad (INCIBE) demostró que surgieron 183 mil sistemas vulnerables en 2023 y, en su infraestructura, se gestionaron más de 83 mil incidentes de ciberseguridad que posicionan a ciudadanos y empresas como los más afectados. De estos incidentes, 237 estaban relacionados con infraestructuras de bancos, transportes y tecnologías de la información y la comunicación" [19].

Entre los delitos más comunes nos encontramos con phishing, ransomware y scareware. El phishing es el más utilizado, consiste en robar información confidencial de los usuarios, seguido del ransomware se refiere al poder recuperar datos que han sido secuestrados mediante cifrado y se pide un pago para su liberación. Y por último tenemos Scareware utiliza el miedo psicológico para enviar software malicioso para la descarga [20].

Además, se ha observado un incremento en la sofisticación de los ataques, aprovechando vulnerabilidades en sistemas desactualizados y la falta de formación en ciberseguridad. “En España, los incidentes cibernéticos crecieron un 24% en 2023, y se espera que alcancen casi 100,000 en 2024” [21].Este aumento resalta la necesidad de fortalecer las medidas de seguridad y promover una cultura de ciberseguridad en todos los niveles.

La continua expansión del entorno digital, junto con la falta de capacitación en ciberseguridad, sumada a la desactualización en los sistemas, ha permitido que los ataques y las vulnerabilidades adquieran más protagonismo y aumenten considerablemente en la actualidad. Según el Instituto Nacional de Ciberseguridad Incibe. “Los incidentes cibernéticos en España crecieron un 24% en 2023, y se proyecta que alcanzarán casi 100.000 en 2024” [21].

2.2.3 Modelos de protección y defensa

La protección de los sistemas informáticos frente a ciberamenazas requiere la implementación de modelos de defensa estratégicos, que integren tanto tecnología como procesos organizativos y políticas claras. Estos modelos no solo deben prevenir ataques, sino también detectar, contener y recuperarse frente a posibles incidentes de seguridad. A continuación, se presentan los principales enfoques adoptados en el campo de la ciberseguridad:

2.2.3.1 Defensa en profundidad

La defensa en profundidad implica la implementación de múltiples capas de seguridad en los sistemas de información, bajo la premisa de que ningún control es cien por ciento eficaz. “La metodología defensa en profundidad aplica seguridad en capas, coordinando varias líneas de defensa que cubren la profundidad del sistema” [22]. Esta estrategia busca reducir las superficies de ataque y aumentar la resiliencia operativa mediante la superposición de mecanismos de protección.

Se combinan controles como firewalls, IDS/IPS, autenticación multifactor, cifrado de datos y segmentación de redes, junto con medidas administrativas y físicas, para garantizar redundancia. Si una capa falla, las restantes siguen protegiendo el sistema. Este enfoque es esencial para disminuir la vulnerabilidad frente a ataques persistentes y sofisticados que buscan evadir los mecanismos convencionales.

2.2.3.2 Arquitectura Zero Trust

La arquitectura de Zero Trust o “confianza cero” se basa en el principio de nunca confiar, siempre verificar. "A diferencia de los modelos tradicionales que confiaban en los dispositivos o usuarios internos por defecto, Zero Trust elimina cualquier suposición de confianza, incluso dentro de las fronteras de la red corporativa. Cada intento de acceso debe atravesar un control meticuloso que evalúe la identidad, dispositivo, ubicación, contexto y riesgo. Esta arquitectura limita la superficie de ataque y reduce los movimientos laterales dentro de una red en caso de que un atacante obtenga acceso inicial" [23]. En la Figura 1 se ilustran los componentes lógicos que conforman esta arquitectura, mostrando la relación entre los puntos de control, decisión y cumplimiento de políticas.

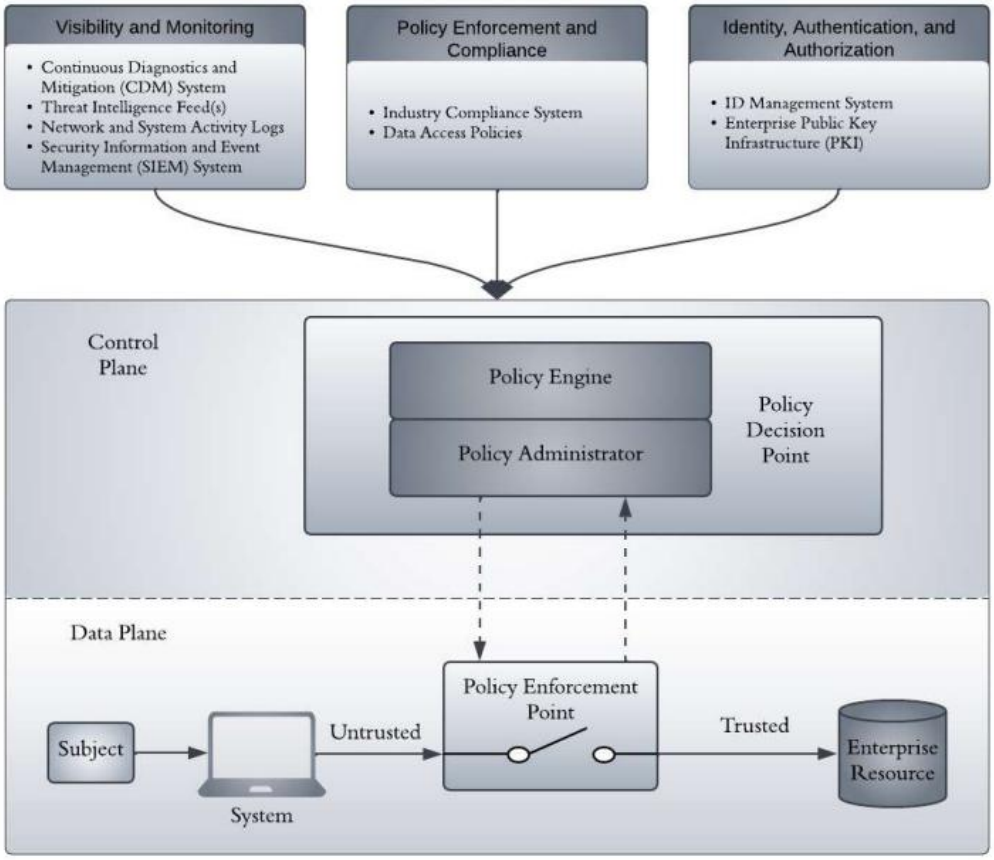


Figura 1: Componentes lógicos centrales de ZTA (basados en NIST SP 800-207). (Fuente [23])

2.2.3.3 Modelo de seguridad basado en riesgos

Este modelo se centra en la identificación y gestión de los riesgos cibernéticos en proporción al valor de los activos y el posible impacto de los incidentes. En lugar de implementar controles universales, la seguridad se adapta al nivel de amenaza y criticidad de la información. De esta manera, los recursos más importantes reciben medidas de protección mayores.

Como se muestra en la Figura 2, esta lógica es la base del modelo ARLI-CIB, que estructura el análisis de riesgo en etapas como identificación de activos, evaluación del impacto y probabilidad, aplicación de medidas según el riesgo identificado [24]. Este enfoque también ayuda a mantener una protección equilibrada, permitiendo asignar recursos de forma adecuada según la importancia de cada activo, asegurando así una gestión más coherente y eficiente del riesgo.

Figura 2: Marco conceptual del modelo de análisis de riesgo sobre ciberseguridad Fuente [23]

2.2.3.4 Marco de Ciberseguridad del NIST (NIST CSF)

El Marco de Ciberseguridad del NIST (NIST CSF) es una herramienta desarrollada por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos con el objetivo de ayudar a organizaciones de todo tipo a gestionar sus riesgos de ciberseguridad. Este marco se estructura en cinco funciones clave: Identificar, Proteger, Detectar, Responder y Recuperar, las cuales representan un ciclo continuo de mejora para la gestión de la seguridad.

Cada función contiene categorías y subcategorías que permiten evaluar el estado actual de la ciberseguridad en una organización y establecer objetivos de mejora según su nivel de madurez y necesidades particulares. Este enfoque permite que tanto pequeñas como grandes organizaciones adopten el marco en función de sus capacidades técnicas y recursos disponibles, facilitando una planificación más organizada y alineada con sus prioridades operativas [25].

Además, el NIST CSF proporciona un lenguaje común entre las áreas técnicas y de gestión, lo cual facilita la toma de decisiones estratégicas en torno a la ciberseguridad. La aplicación del marco no solo permite establecer prioridades en cuanto a inversión en controles y tecnologías, sino que también mejora la preparación ante incidentes y reduce el impacto de posibles ataques.

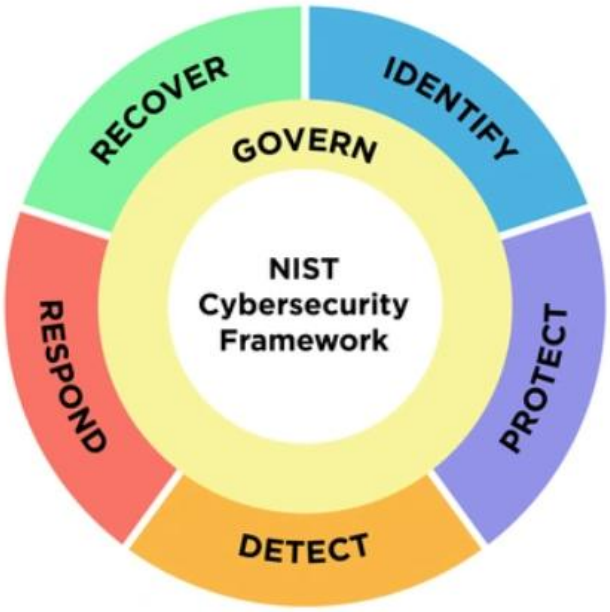


Figura 3: Modelo NIST CSF. (Fuente [25])

2.2.3.5 Modelo SOC (Centro de Operaciones de Seguridad)

Un Centro de Operaciones de Seguridad (SOC) es la unidad encargada de centralizar y coordinar la defensa cibernética de una organización mediante la vigilancia, detección, análisis y respuesta ante incidentes de seguridad. En el contexto español, el CCN-CERT define al SOC como un sistema basado en procesos y herramientas que garantiza una gestión integral del ciclo de vida de los incidentes, apoyado por servicios como vigilancia digital, prevención, detección, respuesta y recuperación. Estos centros se estructuran en función de la criticidad de los activos y se articulan en torno a un enfoque colaborativo entre distintos organismos públicos y privados, tal como se representa en la Figura 4, donde se observan las funciones principales que conforman el modelo SOC y como estas interactúan para mantener una protección continua.

Según el Centro Criptológico Nacional, el SOC se sitúa como núcleo de operaciones interconectadas que integran funciones como la operación, cumplimiento normativo, formación, prevención, vigilancia, detección, respuesta y recuperación. Este ecosistema permite una respuesta rápida y coordinada ante ciberataques, asegurando la continuidad operativa y el cumplimiento de las normativas de ciberseguridad en sectores clave. Su implementación resulta esencial para cualquier entidad que gestione infraestructuras críticas o información sensible, permitiendo afrontar amenazas de forma proactiva y eficiente [26].

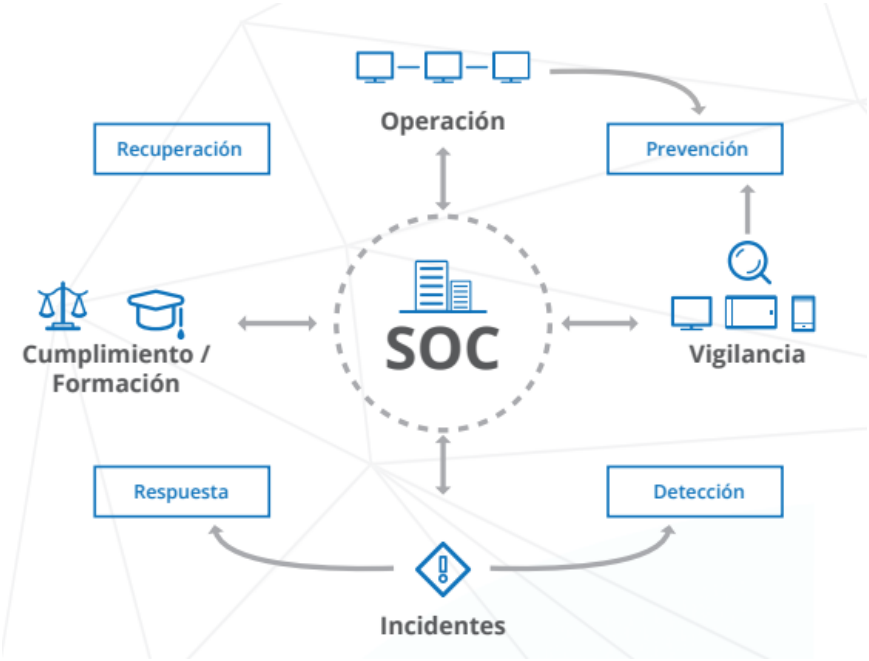


Figura 4: Componentes Funcionales de un Centro de Operaciones de Seguridad. (Fuente [26])

2.2.3.6 Modelo Zero Trust basado en comportamiento

El modelo Zero Trust basado en comportamiento aplica inteligencia artificial y aprendizaje automático para observar cómo se comportan los usuarios y dispositivos dentro de una red. A diferencia del modelo tradicional que confía en la identidad validada, este enfoque analiza patrones de uso. Si detecta una actividad fuera de lo normal como accesos desde lugares inusuales o acciones no habituales sobre archivos, puede activar medidas de seguridad adicionales como una autenticación reforzada [27]. La seguridad se ajusta a lo que ocurre realmente en el entorno, adaptándose a las variaciones que puedan surgir

Este modelo es útil para organizaciones que necesitan proteger datos sin depender solo de reglas fijas. Permite detectar amenazas internas o intentos de acceso no autorizados que no siempre se ven con controles convencionales. Además ayuda a reducir falsas alarmas y prioriza lo importante. Esto mejora el uso de recursos y permite actuar más rápido ante riesgos reales [27].

2.2.3.7 Modelo de seguridad orientado a la resiliencia cibernética

Este modelo se centra en que los sistemas puedan seguir operando y recuperarse rápidamente después de un incidente de seguridad. Usa copias de seguridad automatizadas, arquitecturas redundantes, planes de respuesta y simulacros periódicos para mantener la continuidad operativa de servicios críticos [28]. Es especialmente relevante cuando se reconoce que los ataques son inevitables y se necesita una estrategia que incorpore respuesta reactiva desde todos los niveles de la organización.

También promueve la revisión continua de los planes y ejercicios de recuperación. La participación de mandos, TI y operativos ayuda a consolidar una cultura de ciberresiliencia. Así se logra asegurar tanto la operatividad inmediata como la sostenibilidad a largo plazo frente a amenazas reales. Este enfoque requiere coordinación entre áreas técnicas y de gestión para que las decisiones ante incidentes sean rápidas y efectivas [28].

2.2.3.8 Modelo de segmentación y microsegmentación de red

La segmentación de red y la microsegmentación son técnicas importantes para mejorar la seguridad interna en infraestructuras digitales. La segmentación divide la red en zonas separadas, limitando el acceso entre ellas. En cambio, la microsegmentación aplica reglas más específicas para controlar cada aplicación, dispositivo o flujo de datos. Esto ayuda a detener ataques como el ransomware, ya que impide que un atacante que haya entrado en una parte del sistema acceda a otras áreas [29]. Además, contribuye al cumplimiento de normas y mejora la supervisión del tráfico interno.

La microsegmentación reduce la superficie de ataque al limitar los puntos vulnerables a los que un atacante puede llegar. Permite aplicar el principio de menor

privilegio de forma más precisa, controlando quién puede acceder a cada recurso. En ambientes dinámicos como la nube híbrida o los contenedores, ofrece una protección adaptable que escala según las necesidades actuales [29].

2.2.4 Ciberamenazas

Los avances tecnológicos y la dependencia de los sistemas de información han traído consigo una infinidad de riesgos; la seguridad de la información y los sistemas de infraestructura son vulnerables a ser atacados por alguna amenaza. Las amenazas cibernéticas son algunos de los problemas más urgentes hoy en día, empobreciendo no solo a las personas y organizaciones, sino también dañando información confidencial y debilitando su economía y reputación.

La **Figura 5** muestra el aumento de los principales tipos de ataques en los últimos años. El **phishing** y el **ransomware** presentan un crecimiento notable, mientras que el **malware** se mantiene estable y los ataques **DDoS** aumentan de forma gradual. Estos datos evidencian el crecimiento constante de las amenazas digitales y la importancia de fortalecer la seguridad, ya que reflejan una tendencia que afecta tanto a usuarios como a organizaciones. También demuestra que los atacantes continúan adaptando sus métodos y buscando nuevas formas de comprometer sistemas a nivel mundial, lo que confirma una evolución constante en sus tácticas y en el alcance de sus actividades.

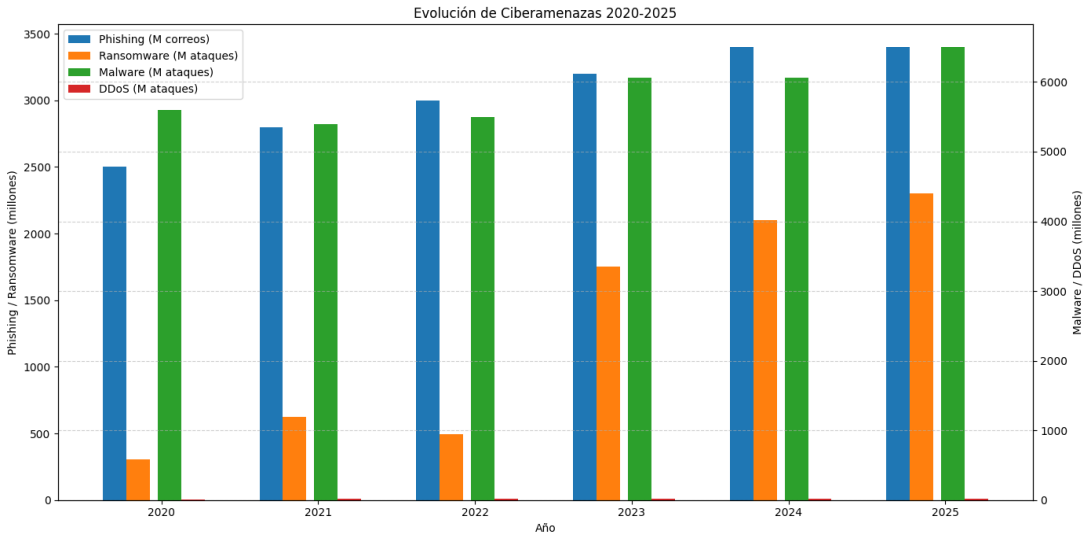


Figura 5: Evolución de ciberamenazas 2020-2025.

- **Phishing** presenta un crecimiento constante durante el período, comenzando en aproximadamente 2,500 millones de correos fraudulentos en 2020 y aumentando hasta cerca de 3,400 millones en 2025 [30].
- **Ransomware** muestra una tendencia al alza más marcada, partiendo de cerca de 300 millones de ataques en 2020 y alcanzando más de 2,300 millones en 2025, reflejando el crecimiento acelerado de esta amenaza en los últimos años [31] [32].
- **Malware** mantiene cifras altas y relativamente estables, fluctuando alrededor de los 5,400 a 6,300 millones de ataques, lo que indica su persistente prevalencia [33] [34].
- **DDoS** presenta valores mucho menores en comparación, pero también en aumento, desde 10 millones en 2020 hasta unos 22 millones en 2025, mostrando un incremento constante en la frecuencia de estos ataques [35] [36].

2.2.4.1 Tipos de ciberamenazas

En el ámbito de la ciberseguridad, es fundamental comprender las distintas formas en que pueden presentarse las amenazas digitales. Estas no solo varían en su método de ataque, sino también en su complejidad, alcance y objetivos. Desde técnicas automatizadas como el malware, hasta estrategias más elaboradas como las amenazas persistentes avanzadas, cada una representa un riesgo concreto para la integridad de los sistemas y la información. Además, conocer estas categorías permite identificar los posibles escenarios de ataque y adoptar las medidas necesarias. La siguiente tabla resume los principales tipos de ciberamenazas.

Tipo de Ciberamenaza	Descripción
Malware	Software diseñado para dañar, modificar o acceder sin permiso a sistemas. Incluye virus, troyanos y más.
Phishing	Suplantación de identidad para obtener datos sensibles mediante correos, SMS o llamadas falsas.

Tipo de Ciberamenaza	Descripción
Ransomware	Tipo de malware que bloquea archivos o sistemas y exige un rescate para desbloquearlos.
Ataques DoS / DDoS	Saturación de sistemas para interrumpir su funcionamiento. En DDoS se usan redes de bots.
Amenazas Persistentes Avanzadas (APT)	Ataques complejos y prolongados con fines de espionaje o sabotaje. Involucran varias fases.
Ingeniería Social	Manipulación psicológica para obtener información o acceso. Explotan la confianza y el error humano.

Tabla 2: Tipos de ciberamenazas. (Fuente [37])

2.2.4.2 Actores de amenazas

En el ámbito de la ciberseguridad, "los actores de amenazas son individuos o grupos que explotan vulnerabilidades en sistemas informáticos, redes y programas para llevar a cabo ciberataques como phishing, ransomware y malware, con el objetivo de causar daño intencional a dispositivos o sistemas digitales" [38]. Estos actores pueden tener diversas motivaciones, que van desde intereses económicos hasta causas ideológicas o geopolíticas. Dependiendo de su origen, capacidades y objetivos, los actores de amenazas se clasifican generalmente en hacktivistas, ciberdelincuentes y grupos patrocinados por estados, cada uno con tácticas y estrategias distintas.

En ecuador, se han identificado actores de amenazas que han llevado a cabo actividades significativas. Un ejemplo notable es el ataque perpetrado en 2015 contra el Banco del Austro, donde ciberdelincuentes lograron sustraer 12 millones de dólares mediante el uso indebido del sistema SWIFT para transferencias internacionales. Este incidente destaca la capacidad de los grupos patrocinados por estados para llevar a cabo operaciones cibernéticas complejas y de alto impacto, mostrando como este tipo de amenazas puede afectar directamente a entidades financieras y generar consecuencias reputacionales de la organización [39].

Además, Ecuador ha experimentado aumento notable en ciberataques en los últimos años. En 2023, se registraron más de 12 millones de intentos de ciberataques, afectando gravemente a sectores como el financiero, gubernamental y empresas medianas. Los ataques comunes incluyen malware, phishing, ransomware, exfiltración de datos y suplantación de identidad, todos con un impacto considerable en las organizaciones y su capacidad para operar de manera segura [40]. Esto incremento se debe a que los ciberdelincuentes han ampliado sus objetivos y métodos en el país.

Actor de amenaza	Descripción breve
Ciberdelincuentes	Grupos o individuos con fines económicos, que utilizan phishing, fraude, malware o ransomware para obtener beneficio.
Hacktivistas (ciberactivistas)	Actúan por motivaciones ideológicas mediante ataques como defacement o DDoS, sin buscar lucro económico directo.
Insiders (actores internos)	Empleados actuales o antiguos con acceso privilegiado que pueden causar daño por venganza, descuido o beneficio.
Ciberterroristas	Individuos u organizaciones que ejecutan ataques motivados políticamente o por temor, afectando infraestructura o reputación.
Grupos patrocinados por Estados	Organizados por gobiernos para espionaje, sabotaje o desestabilización, con recursos y tecnología avanzada.
Lobos solitarios	Actores individuales con alta pericia técnica que operan por ideología, notoriedad o desafío personal.

Tabla 3: Actores de amenazas. (Fuente [41])

2.2.4.3 Ciclo de ciberamenaza

El ciclo de vida de una ciberamenaza representa las etapas ordenadas que sigue un atacante desde la planificación inicial hasta la ejecución final del ataque. Conocer este proceso es clave para que las organizaciones puedan anticiparnos a actividades maliciosas antes de que causen daños serios. Las empresas que comprenden estas fases pueden establecer mecanismos de detección más efectivos y planes de respuesta más sólidos frente a incidentes de seguridad informática. Este modelo estructurado refleja el modo en que las amenazas modernas evolucionan dentro de los sistemas, por lo que es considerado una herramienta útil para el análisis de riesgos actuales [42].

Todo comienza con la fase de reconocimiento, donde el atacante se dedica a recolectar información sobre el objetivo sin interactuar directamente con él. Se busca identificar aspectos como direcciones IP visibles, servicios que se encuentran expuestos a internet y estructuras del sistema. Este paso permite conocer el entorno tecnológico de la víctima y preparar las acciones futuras. Aunque no se ejecuta aún ningún tipo de ataque, esta fase ya muestra una intención clara de violar la seguridad del sistema, y se puede dificultar limitando la información pública disponible y aplicando buenas prácticas de ocultamiento [42].

En la fase siguiente, llamada preparación, el atacante selecciona las herramientas y recursos necesarios para ejecutar el ataque. Esto incluye el desarrollo de archivos maliciosos o scripts, así como la configuración de servidores para controlar remotamente el sistema si el acceso se logra. A partir de esta etapa, el atacante adapta sus técnicas al entorno de la víctima, lo que vuelve más difícil anticiparse a sus acciones. Es una fase silenciosa pero fundamental, donde cualquier fallo puede llevar a la detección antes de que se logre una intrusión real [42].

Después de haber preparado el ataque, el paso siguiente es la entrega. Aquí, el atacante introduce el elemento malicioso en el sistema de la víctima. Esta entrega puede realizarse de múltiples formas, como correos electrónicos con enlaces falsos, sitios web comprometidos o dispositivos físicos conectados. La efectividad de esta fase depende del nivel de protección del entorno, así como de la formación del personal ante posibles engaños. La educación en ciberseguridad y el uso de filtros

avanzados de correo electrónico pueden reducir las probabilidades de éxito del atacante en esta etapa [42].

Una vez que el código malicioso ha sido introducido, se inicia la fase de explotación. El malware se ejecuta aprovechando una vulnerabilidad dentro del sistema para lograr acceso. Esta fase puede implicar acciones como la descarga automática de archivos, la apertura de puertas traseras o la manipulación de procesos internos. El objetivo es lograr control inicial del sistema sin que el usuario lo advierta. Las herramientas antivirus actualizadas y los sistemas de detección de intrusos son recursos esenciales para bloquear esta etapa antes de que escale [42].

Al conseguir acceso, se desarrolla la instalación, donde se colocan componentes que permiten al atacante mantener su presencia. Esto puede incluir la instalación de troyanos, programas de control remoto o mecanismos de acceso encubierto. Esta fase busca garantizar el acceso continuo incluso después de que el sistema haya sido reiniciado o actualizado. Para dificultar este paso, es importante tener controles de integridad del sistema y revisar constantemente los procesos y servicios activos [42].

En la fase de comando y control, el atacante establece una comunicación externa con el sistema comprometido. A través de este canal, puede enviar órdenes, extraer información o modificar el comportamiento del sistema según sus intereses. Esta etapa suele utilizar protocolos cifrados o tráfico disfrazado como si fuera legítimo, lo que complica su detección. El monitoreo del tráfico de red y la detección de patrones inusuales son métodos eficaces para detectar este tipo de actividad [42].

La última etapa es la de acción, donde el atacante ejecuta su objetivo final. Esto puede implicar la exfiltración de datos sensibles, la interrupción del servicio o el cifrado de archivos para exigir un rescate. El éxito de esta fase depende de lo discretas que hayan sido las anteriores. Si la amenaza ha pasado desapercibida hasta este punto, el impacto puede ser significativo, tanto operativamente como a nivel reputacional. En esta fase el atacante suele actuar con rapidez para maximizar los resultados antes de que se active cualquier respuesta defensiva. Por esta razón, la detección temprana durante cualquier fase previa es de gran importancia para limitar el daño [42].

2.2.5 Ciberinteligencia

El concepto de inteligencia en el ámbito de la ciberseguridad ha recorrido un largo camino desde su origen en el contexto militar hasta convertirse en una herramienta indispensable para la protección de activos digitales. Inicialmente, la inteligencia se asociaba únicamente a operaciones de defensa y espionaje en entornos estatales. Con la expansión de internet y el desarrollo de las tecnologías de la información, surgió la necesidad de trasladar estos métodos al entorno digital. Así nace la ciberinteligencia, como una disciplina destinada a identificar, analizar y prevenir amenazas cibernéticas que comprometan la seguridad de sistemas y datos.

La ciberinteligencia se entiende hoy como un proceso sistemático mediante el cual se recolecta, analiza y transforma información sobre amenazas digitales en conocimiento útil para la toma de decisiones. En palabras de Casanabria Casas, "la ciberinteligencia permite anticiparse a las acciones de un adversario, mediante el análisis de datos relacionados con vulnerabilidades, amenazas y riesgos del entorno virtual" [43]. Esto supone un cambio fundamental en la forma en que se abordan los incidentes de seguridad: ya no basta con reaccionar ante un ataque, sino que es necesario anticiparse a él a través del conocimiento.

2.2.5.1 Evolución de la inteligencia en ciberseguridad

El concepto de inteligencia en el ámbito de la ciberseguridad ha recorrido un largo camino desde su origen en el contexto militar hasta convertirse en una herramienta indispensable para la protección de activos digitales. Inicialmente, la inteligencia se asociaba únicamente a operaciones de defensa y espionaje en entornos estatales. Con la expansión de internet y el desarrollo de las tecnologías de la información, surgió la necesidad de trasladar estos métodos al entorno digital. Así nace la ciberinteligencia, como una disciplina destinada a identificar, analizar y prevenir amenazas cibernéticas que comprometan la seguridad de sistemas y datos.

La ciberinteligencia se entiende hoy como un proceso sistemático mediante el cual se recolecta, analiza y transforma información sobre amenazas digitales en conocimiento útil para la toma de decisiones. En palabras de Casanabria Casas, "la ciberinteligencia permite anticiparse a las acciones de un adversario, mediante el

análisis de datos relacionados con vulnerabilidades, amenazas y riesgos del entorno virtual" [43]. Esto supone un cambio fundamental en la forma en que se abordan los incidentes de seguridad: ya no basta con reaccionar ante un ataque, sino que es necesario anticiparse a él a través del conocimiento.

La evolución de esta disciplina ha sido impulsada por el crecimiento exponencial de los ataques informáticos, el uso de tecnologías más sofisticadas por parte de los ciberdelincuentes, y la creciente dependencia de las sociedades modernas respecto de los sistemas digitales. Como resultado, los enfoques tradicionales de seguridad se han visto rebasados, lo que ha llevado a la necesidad de desarrollar mecanismos más proactivos y adaptativos. "La ciberinteligencia no solo se limita al ámbito técnico, sino que también analiza comportamientos, patrones y contextos que permiten identificar actores, intenciones y capacidades" [44]. Esto la convierte en una herramienta estratégica de gran valor.

En términos históricos, la ciberinteligencia ha pasado de ser una práctica centrada en la protección de infraestructuras militares a convertirse en una necesidad transversal en sectores como el financiero, energético, educativo, y gubernamental. La digitalización global ha ampliado la superficie de ataque y ha hecho de la información un activo que requiere protección constante. El modelo de inteligencia tradicional ha sido adaptado a las características del ciberespacio, incorporando elementos como la inteligencia de fuentes abiertas (OSINT), la inteligencia de amenazas (threat intelligence) y la inteligencia basada en indicadores de compromiso.

Actualmente, se reconoce que el verdadero valor de la ciberinteligencia reside en su capacidad para reducir la incertidumbre frente a amenazas complejas, permitiendo a las organizaciones tomar decisiones fundamentadas sobre sus estrategias de defensa. No se trata únicamente de una función técnica, sino de una herramienta estratégica. Tal como señala la Escuela Nacional de Estudios Políticos y Estratégicos (ANEPE), "la ciberinteligencia actúa como una capacidad de anticipación que mejora la toma de decisiones frente al entorno dinámico del ciberespacio" [44], destacando así su importancia en contextos donde la información cambia constantemente.

2.2.5.2 Ciclo de inteligencia

El ciclo de la inteligencia es la colección de pasos para consolidar fragmentos dispersos de información en inteligencia procesable que ayuda a tomar decisiones informadas. Este enfoque es favorece a los dominios militar y de ciberseguridad ya que ayuda a mitigar incertidumbres sobre amenazas, actores y posibles escenarios de riesgo. Aunque hay algunas variaciones, generalmente consiste en cuatro fases principales: recolección, análisis, producción y diseminación, que se retroalimentan entre sí para lograr un proceso de mejora continua en la calidad de la inteligencia resultante.

El dicho "poner el caballo delante del carro" se aplica perfectamente aquí; la primera fase, la recolección, consiste en obtener sistemáticamente datos relevantes provenientes de diversas fuentes. Estas fuentes pueden dividirse en información técnica, humana, documentos y fuentes abiertas. La Secretaría de Seguridad y Protección Ciudadana de México señala que "durante esta etapa, el investigador se encarga de recolectar información desde distintas fuentes, basándose en las solicitudes que se plantean durante la fase de planificación" [45]. Esta tarea no solo involucra tecnología, sino también un buen criterio para seleccionar información pertinente y descartar datos irrelevantes.

La segunda etapa corresponde al análisis, un proceso fundamental en el que se interpreta clasifica y valida la información recopilada. Aquí es donde los datos se transforman en conocimiento útil. El análisis facilita la identificación de patrones ocultos, correlaciones y la predicción de tendencias que podrían pasar desapercibidas. Según Navarro Bonilla, “el análisis es la fase más crucial del ciclo, pues permite contextualizar la información y darle un significado que la convierta en conocimiento valioso” [46]. Para ello, se requiere tanto habilidad analítica como un entendimiento del entorno, junto con herramientas metodológicas que garanticen la objetividad.

A continuación, la producción de inteligencia consiste en la elaboración de informes u otros productos formales que contienen el resultado del análisis. Estos productos están orientados a responder preguntas específicas de los responsables de la toma de decisiones. Su utilidad depende tanto del contenido como de la forma en

que se presentan. Es fundamental que sean claros, pertinentes y oportunos. "La producción de inteligencia es el punto de confluencia entre el conocimiento técnico y la necesidad estratégica", afirma Navarro Bonilla [46].

La última fase, **la diseminación**, consiste en la entrega del producto de inteligencia a los destinatarios adecuados. Este paso es vital para que la inteligencia cumpla su función. No basta con generar información útil si no llega a quien debe utilizarla. Según la SSPC, "la difusión permite que la información procesada sea entregada de manera oportuna, segura y comprensible a quienes la requieren para la toma de decisiones" [45].

Este proceso suele incluir mecanismos de retroalimentación, mediante los cuales los usuarios pueden valorar la calidad y utilidad de los datos recibidos. El ciclo de inteligencia no es un proceso lineal, sino iterativo, flexible y adaptativo. Cada una de sus fases se interrelaciona con las demás y puede requerir ajustes en función del contexto. Su implementación adecuada permite a las organizaciones enfrentar amenazas de manera más informada, eficiente y proactiva.

Figura 6: Ciclo de inteligencia.

2.2.5.3 Niveles de inteligencia (estratégica, operativa, táctica)

La inteligencia se organiza en distintos niveles que facilitan el abordaje de amenazas y desafíos desde diversas perspectivas, cada una con enfoques y objetivos específicos. Estos niveles estratégico, operativo y táctico cumplen funciones diferenciadas dentro del proceso de toma de decisiones. Su adecuada integración resulta esencial para implementar acciones eficaces orientadas a la seguridad y al cumplimiento de los fines previamente establecidos.

La inteligencia estratégica se enfoca en el análisis de largo plazo y en la identificación de tendencias que puedan afectar la seguridad nacional o los intereses de una organización. Según Sherman Kent, "la inteligencia estratégica es el conocimiento que debe tener un estratega para trazar sus planes y llevarlos a cabo" [47]. Este nivel de inteligencia proporciona una visión amplia y profunda del entorno, permitiendo anticipar posibles escenarios y desarrollar políticas adecuadas para enfrentarlos

En **el nivel operativo**, la inteligencia se centra en la planificación y conducción de campañas o misiones específicas. Este nivel actúa como un puente entre la estrategia general y las acciones tácticas concretas. El documento "Operaciones Militares Cibernéticas" señala que "el nivel operacional vincula la estrategia y táctica mediante el establecimiento de objetivos operacionales necesarios para alcanzar el objetivo estratégico" [45]. La inteligencia operativa proporciona información detallada sobre el terreno, las capacidades del adversario y otros factores relevantes para la ejecución efectiva de las operaciones.

La inteligencia táctica, por su parte, se enfoca en el apoyo directo a las unidades en el campo, proporcionando información inmediata y específica para la ejecución de acciones concretas. Esta inteligencia se caracteriza por su inmediatez y por estar orientada a satisfacer las necesidades de los comandantes en situaciones específicas. El "Manual de Inteligencia Táctica" define la inteligencia de combate como "la información relativa al terreno, las condiciones meteorológicas y el enemigo que necesita un comandante para elaborar planes y llevar a cabo operaciones tácticas" [48]. Este nivel de inteligencia es indispensable para la toma de decisiones rápidas y efectivas en el campo de operaciones.

La interacción entre estos niveles de inteligencia es fundamental para el éxito de las operaciones y la seguridad en general. La inteligencia táctica proporciona información que alimenta el análisis operativo, el cual, a su vez, contribuye a la formulación de estrategias a largo plazo. Esta sinergia garantiza una respuesta coherente y coordinada frente a las amenazas, permitiendo una adaptación constante a las cambiantes condiciones del entorno.

2.2.5.4 Herramientas y plataformas de ciberinteligencia

En el ejercicio de actividades de ciberinteligencia existen diversas herramientas orientadas al análisis, estructuración e intercambio de información sobre amenazas, cuyo propósito es convertir la información en bruto en inteligencia procesable. Estas herramientas permiten automatizar la recolección de datos, facilitar el análisis gráfico de relaciones, integrar múltiples fuentes, visualizar amenazas y gestionar el intercambio estructurado de información. Existen plataformas que operan en niveles tácticos y estratégicos, incorporando estándares abiertos para apoyar la gestión colaborativa de indicadores y amenazas.

Nombre	Descripción (desde fuentes web)	Plataforma	Licencia
Maltego [49]	Maltego se destaca por mostrar gráficos complejos con interconexiones en vivo entre piezas de información.	Windows, macOS, Linux	Freemium (versión gratuita & de pago)
OpenCTI [50]	OpenCTI es una plataforma de ciberinteligencia que permite estructurar, almacenar, visualizar y compartir información sobre amenazas, vulnerabilidades y actores, bajo el estándar STIX2.	Linux, Docker	Open Source (AGPLv3)
MISP [51]	MISP (Malware Information Sharing Platform) es una plataforma de código abierto diseñada para el	Linux, Docker	Open Source (GPLv3)

Nombre	Descripción (desde fuentes web)	Plataforma	Licencia
	intercambio estructurado de indicadores de compromiso (IOCs), amenazas y tácticas TTP, facilitando la colaboración entre analistas y organizaciones.		

Tabla 4: Herramientas de ciberinteligencia.

2.2.6 OSINT (Open Source Intelligence)

La inteligencia de fuentes abiertas (OSINT) se refiere al proceso de recolectar, analizar y difundir información obtenida legalmente de fuentes públicas. Este tipo de inteligencia permite generar conocimiento estratégico sin recurrir a métodos encubiertos o ilegales. Su valor radica en la capacidad de transformar datos accesibles en información útil para la toma de decisiones. Es ampliamente utilizada en ámbitos como la ciberseguridad, inteligencia militar y análisis de riesgos. Según la legislación estadounidense, OSINT es la inteligencia producida a partir de información disponible públicamente, recopilada y difundida oportunamente con un propósito específico de inteligencia [52].

2.2.6.1 Definición y fundamentos de OSINT

OSINT (Inteligencia de Fuentes Abiertas) aplica los procesos de inteligencia a la recopilación de información que está fácilmente disponible en el dominio público. Estas fuentes abiertas ofrecen una gran cantidad de oportunidades que, una vez procesadas y analizadas adecuadamente, pueden ayudar en investigaciones sobre seguridad, evaluación de riesgos, perfiles digitales, monitoreo de amenazas y más.

Además, el uso de OSINT permite obtener información desde diversas fuentes públicas para identificar patrones, vínculos y posibles vulnerabilidades. Al correlacionar datos de distintas plataformas, se obtiene una visión más clara del entorno digital analizado. Esto convierte al OSINT en un recurso clave para la ciberseguridad, ya que aporta información útil para evaluar riesgos y anticipar amenazas potenciales. Su aplicación también facilita comprender mejor la dinámica

del entorno digital y reconocer elementos que podrían pasar desapercibidos a simple vista, ampliando así el alcance de análisis dentro de un marco conceptual de seguridad.

Fuente OSINT	Descripción y utilidad
Redes sociales. [53] [55]	Información sobre ubicación, relaciones, opiniones y actividades. Base para análisis conductual y geolocalización.
Sitios web y blogs. [53]	Reflejan eventos actuales y clima social. Útiles para contextualizar riesgos y actores relevantes.
Foros y comunidades en línea. [54] [55]	Detectan discursos de odio, amenazas emergentes, influenciadores y planificación de acciones.
Registros públicos y bases oficiales. [54]	Incluyen datos fiscales, mercantiles, catastrales y civiles. Vitales para verificar estructuras legales o relaciones personales.
Búsquedas avanzadas (Google Dorks). [53] [55]	Localizan archivos, configuraciones o documentos sensibles mediante operadores booleanos sin técnicas intrusivas.
Registros de dominios / WHOIS. [54]	Revelan propietarios de sitios, servidores y relaciones entre dominios. Esenciales en investigaciones cibernéticas.
Archivos y multimedia. [54]	A través de metadatos se puede conocer origen, modificaciones, ubicación y equipos usados.
Geolocalización y mapas. [53] [55]	Permiten rastrear movimientos, identificar ubicaciones clave y verificar eventos sobre el terreno.

Tabla 5: Tipos de fuentes OSINT.

2.2.6.2 Técnicas de recolección, filtrado y análisis de datos públicos

El proceso de OSINT (Inteligencia de Fuente Abierta) está respaldado por el propósito analítico y la recuperación de información pública. Este proceso implica mucho más que simplemente buscar datos; requiere técnicas metodológicas bien definidas enfocadas en convertirlos en conocimiento útil. Como se señaló en OSINT.com.ar, "la técnica OSINT consiste en recopilar datos que son accesibles públicamente en internet u otras fuentes, analizarlos y procesarlos para convertirlos en inteligencia" [9].

En cuanto a la primera etapa del proceso, la **recopilación** de datos que implica en realizar búsqueda en diversas redes sociales y sitios web institucionales, foros y bases de datos, esto se trata más de recuperar datos cargados de valor. Esta etapa también requiere herramientas que permitan la automatización, especialmente cuando la cantidad de información es alta. Por ejemplo, la Universidad Politécnica Salesiana informa que "el proceso de recopilación de datos OSINT incluye herramientas automatizadas como scrapers, motores de búsqueda avanzados y otro software relevante para permitir la adquisición de grandes cantidades de información de manera adecuada" [56].

Con esta información, se avanza a la parte de **filtrado**, donde se elimina información que es irrelevante, o contenido duplicado y defectuoso. Aquí se observa la confiabilidad y exactitud de la información. "El filtrado tiene como objetivo central reducir el ruido de la información recolectada, identificando qué datos aportan valor al análisis y cuáles deben descartarse por irrelevantes o poco confiables" [56]. Este paso resulta fundamental, ya que permite validar el análisis posterior y garantiza que se base en información sólida.

Luego se avanza con la última, extrayendo los hallazgos para establecer alguna relación y llegar a una conclusión con sentido. Tales vínculos y conclusiones son el resultado final, además de tener la información clara, se requiere que esta esté organizada de forma definida y profunda, permitiendo un análisis coherente. "El **análisis** OSINT debe permitir al investigador generar conocimiento, anticiparse a riesgos y tomar decisiones basadas en evidencia verificada, especialmente en el campo de la ciberseguridad" [9].

En su totalidad, estos tres pasos reconocimiento, filtrado y análisis forman el núcleo de la metodología OSINT. Tanto las herramientas empleadas como la formación del analista tienen un impacto en la calidad del proceso. La correcta aplicación de estos métodos no solo mejora la eficacia de la inteligencia producida, sino que también garantiza el cumplimiento de los estándares éticos y legales, particularmente en el ciberespacio y en contextos de mitigación de amenazas.

2.2.6.3 Herramientas de OSINT

Las herramientas de OSINT (Open Source Intelligence) constituyen un conjunto de recursos tecnológicos diseñados para recopilar, procesar y analizar información disponible públicamente en internet. Estas herramientas permiten a analistas, investigadores y profesionales de la ciberseguridad acceder a datos dispersos en múltiples plataformas digitales, facilitando la transformación de información no estructurada en inteligencia procesable. A continuación, se presentan a través de una tabla el conjunto de herramientas que nos ayudaran en la recolección de datos:

Nombre	**Descripción (fuente web)**	**Plataforma**	**Licencia**
Username Search [55]	Permite buscar un nombre de usuario o correo en más de 600 redes sociales y sitios de citas, mostrando resultados de forma inmediata.	Web	Freemium / Pago
HaveIBeenPwned [57]	Servicio que permite verificar si una cuenta de correo electrónico ha estado involucrada en una brecha de datos.	Web	Gratuita / pago
Ghunt [58],	Permite investigar información pública sobre cuentas Google: fotos, calendario, ubicaciones y otros datos asociados al perfil.	Linux (CLI)	Código abierto

Nombre	Descripción (fuente web)	Plataforma	Licencia
Social Analyzer [59]	Examina perfiles sociales para detectar cuentas duplicadas, actividad anómala o relaciones sospechosas.	CLI (Python)	Código abierto
DeHashed [60]	Motor de búsqueda de datos filtrados (emails, IPs, contraseñas, etc.), útil para ciberinvestigaciones.	Web	Freemium / Pago
Hunter.io [61]	Herramienta para encontrar emails asociados a dominios corporativos, útil para campañas OSINT o análisis organizacional.	Web / API	Freemium
FOCA [62]	Extrae metadatos de documentos públicos (PDF, DOCX, etc.), revelando rutas de red, usuarios, software usado.	Windows	Gratuita
Google Dorking [63]	Técnica OSINT que usa operadores avanzados en Google para encontrar información sensible expuesta.	Web (Buscador)	Gratuita
SpiderFoot [64]	SpiderFoot automatiza la recopilación de información y la vigilancia sobre un objetivo, ya sea una IP, dominio, host o nombre comercial	Windows, Linux, Web	Open Source (GPL/GPL v3),

Tabla 6: Conjunto de herramientas OSINT.

2.3 Marco teórico

2.3.1 Impacto de las herramientas OSINT en la detección de amenazas

Las herramientas OSINT se han vuelto fundamentales en la ciberseguridad moderna, permitiendo la detección temprana de amenazas mediante la recopilación y análisis de datos públicos. Según el artículo de IBM titulado "OSINT: La Inteligencia Abierta que Revoluciona la Ciberseguridad", OSINT permite a los equipos de seguridad identificar vulnerabilidades y amenazas potenciales desde múltiples fuentes, como redes sociales y bases de datos públicas. Esta capacidad de monitoreo preventivo ayuda a fortalecer las defensas de las organizaciones antes de que ocurra un ataque [65].

De forma complementaria, "El Papel Creciente de OSINT en la Ciberseguridad" de GCS Network resalta cómo el monitoreo de foros en la dark web y otras plataformas permite detectar signos tempranos de ataques. Analizar estos espacios ayuda a identificar patrones sospechosos como la venta de exploits o filtraciones de datos. Este enfoque permite actuar antes de que los atacantes comprometan activos clave como bases de datos o sistemas de control industrial, evitando incidentes graves como el robo de información confidencial o la interrupción de servicios esenciales, lo que podría resultar en grandes pérdidas para la organización [65] [66].

2.3.2 Importancia de las herramientas OSINT en la ciber-inteligencia

Las herramientas OSINT ayudan a los analistas a recopilar y revisar información pública como noticias y redes sociales, para encontrar patrones que indiquen riesgo como la difusión de datos sensibles o comportamientos inusuales. Al combinar estos datos con información privada, se pueden elaborar informes más completos y responder rápido a incidentes. Un estudio realizado por D. Mider en 2024 analizó más de 130 herramientas OSINT y señaló que estas permiten procesar grandes cantidades de datos disponibles en línea, detectar vulnerabilidades y alertar sobre posibles amenazas antes de que causen problemas [67] .

IBM destaca que la accesibilidad y rentabilidad de OSINT lo convierte en una opción estratégica frente a métodos tradicionales. Las herramientas OSINT, al analizar fuentes públicas como redes sociales y foros, permiten obtener inteligencia

sin grandes costos, lo que facilita una respuesta rápida a amenazas emergentes. Esto es de gran importancia para detectar ataques de phishing o vulnerabilidades nuevas y adaptarse a un entorno de seguridad en constante cambio, sin la necesidad de grandes inversiones en tecnologías propietarias [65].

2.3.3 OSINT fundamental para la seguridad de infraestructuras críticas

El uso de OSINT en la protección de infraestructuras críticas ha demostrado resultados positivos. En "OSINT: La Defensa Estratégica para Infraestructuras Críticas", GCS Network explica que las herramientas OSINT permiten el monitoreo en tiempo real de vulnerabilidades en infraestructuras esenciales, como redes de energía y sistemas de transporte. Este enfoque ayuda a protegerlas de posibles ataques y a garantizar su estabilidad, aumentando la resiliencia ante amenazas cibernéticas [66].

En "IBM y OSINT: Cumpliendo con Normativas y Fortaleciendo la Resiliencia", explica cómo OSINT ayuda a las organizaciones a detectar vulnerabilidades y cumplir con normativas de seguridad. Al identificar brechas en infraestructuras críticas, como redes de energía o transporte, OSINT permite implementar controles preventivos antes de que los atacantes las exploten, mejorando la resiliencia y garantizando la estabilidad de los sistemas esenciales. Este enfoque proactivo es clave para prevenir ciberataques que podrían causar daños significativos, como apagones masivos o fallos en servicios vitales [65].

2.4 Metodología de proyecto

2.4.1 Metodología de investigación

El tipo de investigación que se realizará es experimental, ya que implica la manipulación de variables en un entorno controlado para evaluar el desempeño de las herramientas OSINT en la detección de ciberamenazas. Según Tamayo y Tamayo, la investigación experimental se caracteriza por la creación de condiciones específicas en las que se manipulan ciertas variables independientes para observar sus efectos sobre variables dependientes, permitiendo establecer relaciones causales [68]. Este enfoque resulta ideal cuando se requiere probar hipótesis de manera precisa, ya que permite observar directamente como responden las herramientas.

Además, se aplicará una metodología descriptiva, la cual se basa en la observación de los fenómenos tal como ocurren en su entorno natural, sin manipular las variables. Su objetivo principal es describir las características, procesos o comportamientos de los hechos estudiados para obtener una comprensión clara de su estado actual [68].

En este proyecto, este enfoque permitirá analizar cómo se comportan las herramientas OSINT en contextos reales y registrar sus resultados de manera objetiva. De esta forma, la descripción de los resultados complementará las pruebas experimentales, aportando una visión más completa del rendimiento y utilidad de las herramientas evaluadas.

En este contexto, el uso de un ambiente controlado permite ejecutar pruebas sin el riesgo de comprometer sistemas externos, garantizando la seguridad en la experimentación con diversas configuraciones de las herramientas. Esto posibilita analizar con detalle el comportamiento y la efectividad de cada herramienta, lo cual es importante para obtener conclusiones sólidas y recomendaciones basadas en evidencias. Al trabajar en un entorno seguro, los resultados obtenidos serán confiables y podrán extrapolarse para su aplicación en situaciones reales de ciberseguridad.

2.4.2 Técnicas e instrumentos de recolección de datos

Para el análisis de ciberamenazas mediante técnicas de inteligencia de fuentes abiertas (OSINT) y ciberinteligencia, se emplearán métodos orientados a la recopilación automatizada de información, el análisis contextual de entidades digitales y la identificación de posibles relaciones entre elementos expuestos. La recopilación automatizada permitirá extraer datos desde fuentes públicas de forma estructurada y eficiente. Las técnicas de recolección en el ámbito OSINT incluyen el análisis de redes sociales, el uso de Google Dorking y la consulta de registros públicos. Estas prácticas permiten obtener información disponible en fuentes abiertas y verificar posibles exposiciones de datos relevantes para la investigación.

El análisis de entidades facilitará la identificación de elementos clave como: dominios, credenciales, correos o documentos expuestos y permitirá comprender su

relevancia dentro del contexto digital de cada caso de estudio. Además, cuando sea pertinente, se explorarán conexiones entre estos elementos que puedan indicar patrones de exposición, vulnerabilidades o riesgos asociados. Todas estas actividades se desarrollarán dentro de un entorno virtualizado basado en Kali Linux, que proporciona un marco seguro y ético para la recolección y el análisis de información accesible públicamente.

2.4.3 Análisis de recolección de datos

La recolección de datos en este estudio se realizó a partir de fuentes abiertas disponibles en internet, aprovechando herramientas OSINT y de ciber inteligencia que permiten identificar información sensible expuesta en distintos entornos digitales. El análisis incluyó correos electrónicos institucionales y personales, credenciales filtradas, metadatos técnicos y registros en plataformas públicas que evidenciaban posibles riesgos de seguridad. Una vez recopilados, los datos fueron clasificados y depurados, descartando información redundante o irrelevante y priorizando aquella con mayor impacto en los casos de estudio.

Luego se aplicaron procesos de correlación y validación cruzada con distintas herramientas, lo que permitió confirmar la veracidad de los hallazgos y reducir los falsos positivos. Este análisis aseguró que la información usada fuera confiable e importante para la evaluación de riesgos. Finalmente, la organización de los datos en tablas y matrices facilitó una interpretación clara de las amenazas detectadas en los tres escenarios estudiados.

2.4.4 Metodología de desarrollo

La metodología del proyecto se basa en el enfoque planteado por Bazzell en Open Source Intelligence Techniques para el análisis de inteligencia en fuentes abiertas (OSINT). De forma complementaria, se emplea el Ciclo de Inteligencia, ampliamente utilizado en ámbitos militares, policiales y de ciberseguridad, con el objetivo de convertir datos públicos en conocimiento estratégico útil y aplicable al contexto del análisis[8] [69].

El Ciclo de Inteligencia está compuesto por seis etapas: planificación y dirección, recolección, procesamiento, análisis y producción, difusión y retroalimentación

[69]. Para este trabajo, dichas etapas se han adaptado y reorganizado en cuatro fases los cuales son: identificación de recursos y técnicas OSINT/ciberinteligencia, recopilación y análisis de datos expuestos, evaluación contextual de la exposición digital y recomendaciones para mejorar la seguridad de la información, manteniendo un enfoque ético, controlado y alineado con los objetivos establecidos.

Fase 1: Identificación de recursos y técnicas OSINT/ciberinteligencia

Esta fase se centra en la selección de métodos de recopilación de información disponibles en fuentes abiertas, orientados a identificar datos expuestos públicamente. Corresponde principalmente a la etapa de planificación y dirección del ciclo de inteligencia, donde se definen las fuentes, técnicas y objetivos.

Se consideran herramientas propias de la inteligencia de fuentes abiertas y procedimientos de ciberinteligencia que permiten obtener información desde sitios web, redes sociales, motores de búsqueda, documentos públicos y plataformas institucionales. La elección de cada recurso se basa en criterios de aplicabilidad, confiabilidad, legalidad y capacidad para proporcionar indicadores sobre exposición digital. Además, se analiza la pertinencia técnica de las herramientas y su alcance frente a distintos tipos de casos, de modo que el proceso sea coherente con los objetivos del proyecto y las limitaciones de acceso a la información.

Fase 2: Recopilación y análisis de datos expuestos

Durante este proceso se aplican criterios básicos de ciberinteligencia para reconocer relaciones entre elementos visibles, posibles indicios de vulnerabilidades, riesgos de privacidad, casos de suplantación de identidad y la presencia de información en repositorios filtrados o accesibles públicamente. Esta revisión inicial permite identificar patrones relevantes dentro de los recolectados, ofreciendo una primera aproximación del nivel de exposición, lo que prepara el análisis de la siguiente fase.

Fase 3: Evaluación contextual de la exposición digital

Esta fase constituye un punto clave dentro del desarrollo metodológico, ya que traduce los datos recopilados en conocimiento aplicable. A través de este enfoque se busca comprender no solo la cantidad de información expuesta, sino también el contexto en el que dicha exposición ocurre y las implicaciones que puede tener

según el tipo de actor involucrado. La evaluación considera factores técnicos, legales y de privacidad, con el propósito de determinar el nivel de riesgo que representan los datos identificados en fuentes abiertas. Asimismo, permite establecer patrones de vulnerabilidad y vincular la información encontrada con los principios de la Ley Orgánica de Protección de Datos Personales (LOPDP), garantizando una interpretación coherente con el marco normativo vigente.

Esta fase corresponde a la etapa de análisis y producción del ciclo, donde se realiza una revisión detallada de la información. Se estudian diferentes tipos de entidades reales para entender cómo varía la exposición digital según el perfil del sujeto u organización. Cada caso se examina considerando su huella digital visible en fuentes abiertas, identificando patrones de riesgo y elementos que puedan representar una amenaza potencial. Esta evaluación permite establecer el nivel de criticidad de la información expuesta y valorar su posible impacto desde un enfoque preventivo.

Fase 4: Recomendaciones para mejorar la seguridad de la información

Esta fase se relaciona con la etapa de difusión y retroalimentación del ciclo de inteligencia. A partir de los resultados obtenidos, se formulan recomendaciones orientadas a mitigar los riesgos detectados en los diferentes casos de estudio. Las propuestas incluyen medidas de privacidad digital, pautas de gestión de datos y estrategias de concientización adaptadas a cada entorno. También se enfatiza la necesidad de fortalecer la capacitación en ciberseguridad y promover una cultura preventiva que impulse el uso responsable de las tecnologías.

El objetivo es fomentar el aprovechamiento de OSINT y la ciberinteligencia como herramientas prácticas para la gestión del riesgo digital, destacando su valor en la protección de la información y la reducción de vulnerabilidades en espacios personales, empresariales e institucionales. Además, se busca impulsar una comprensión más amplia sobre la importancia de analizar de forma constante la información expuesta en línea y adoptar hábitos que fortalezcan la seguridad digital en el día a día. Con ello, se pretende promover un uso más consciente de las tecnologías y facilitar la adopción de medidas que eviten incidentes derivados de la exposición innecesaria de datos.

CAPITULO 3. PROPUESTA

3.1 Fase 1: Identificación de recursos y técnicas OSINT/ciberinteligencia.

En la primera fase del proyecto, se desarrolló el proceso de planificación de la investigación OSINT, estableciendo los lineamientos generales, objetivos y alcance de los casos seleccionados. Se definieron los criterios para la recolección de información y se seleccionaron las fuentes abiertas más relevantes, considerando la pertinencia de los datos y su relación con el contexto de cada caso. Asimismo, se estableció la metodología de análisis y los parámetros éticos de la investigación, garantizando un uso responsable de la información recopilada. Esta fase sentó las bases necesarias para estructurar de manera ordenada los escenarios de persona natural, entidad privada y entidad pública, que se abordaron en las etapas posteriores.

Las técnicas OSINT se enfocaron en la recolección de información pública mediante reconocimiento pasivo, búsqueda avanzada en fuentes abiertas y análisis de metadatos. Estas acciones permitieron obtener datos iniciales de los casos seleccionados sin generar interacción directa. Por otra parte, las técnicas de ciberinteligencia se orientaron al análisis y correlación de la información obtenida, con el fin de identificar patrones, posibles riesgos y relaciones entre los elementos encontrados. Esta combinación permitió establecer una base sólida para las etapas siguientes del proyecto, donde los datos recolectados fueron evaluados y transformados en conocimiento útil.

La aplicación conjunta de estas técnicas permitió mantener un equilibrio entre la planificación y el análisis previo a la obtención de información. En esta fase se identificaron los recursos, fuentes y métodos que se emplearían en cada caso. De esta manera, la fase de identificación se centró en definir cómo y con qué herramientas se llevaría a cabo la investigación, garantizando una estructura ordenada para las etapas posteriores del proyecto. Además, se establecieron criterios de selección y validación de las fuentes para asegurar la fiabilidad de los datos recolectados. Este enfoque metodológico permitió optimizar el proceso analítico y garantizar la coherencia entre los resultados obtenidos y los objetivos planteados.

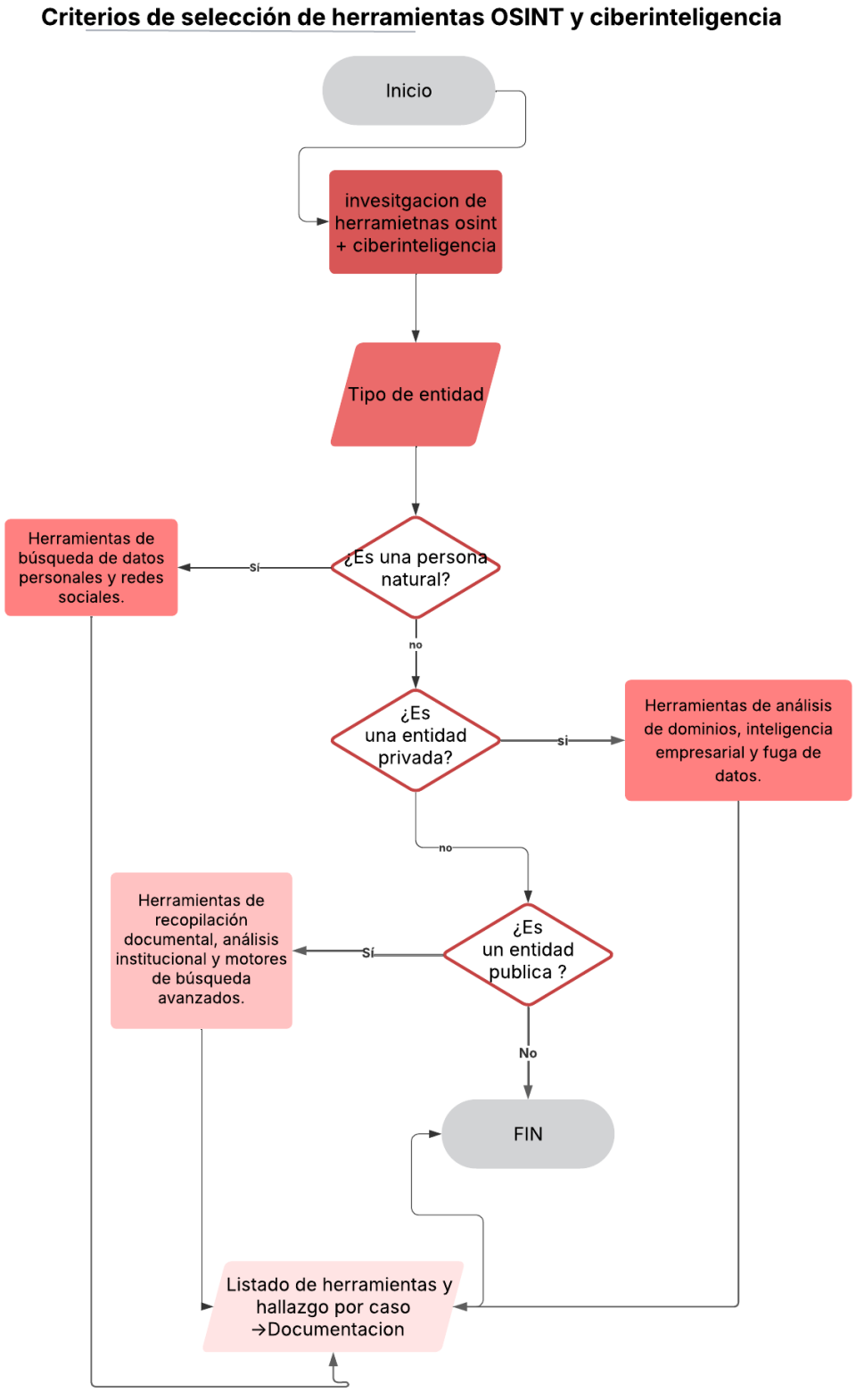


Figura 7: Proceso de selección de herramientas OSINT y de ciberinteligencia según tipo de entidad.

El diagrama de la figura 7 muestra el proceso donde se inicia con la selección de las herramientas OSINT y de ciberinteligencia más adecuadas para el caso en estudio. Esta elección no es aleatoria, sino que responde a un criterio de efectividad: cada herramienta se seleccionó en función de los mejores resultados que ofrece dentro de su ámbito de aplicación, ya sea en la detección de filtraciones de datos personales, en el reconocimiento de configuraciones técnicas expuestas o en la identificación de amenazas visibles en entornos digitales.

Durante esta fase se realizaron pruebas con distintas herramientas OSINT y de ciberinteligencia, seleccionando aquellas que ofrecieron mejores resultados y se ajustaron a los objetivos del proyecto. Se definió la estructura que guiaría su uso, el orden de aplicación y los criterios para determinar en qué casos cada recurso resultaba más adecuado. Este proceso permitió mantener coherencia en el trabajo y asegurar que las herramientas elegidas respondieran a los propósitos del estudio. También se incluyó la descripción general de las fuentes abiertas utilizadas, delimitando su uso dentro de un marco ético y responsable.

La fase de identificación sirvió también para unificar el formato de registro de la información y planificar la documentación de los pasos que se realizarían en etapas posteriores. Se elaboraron plantillas con campos definidos para anotar las herramientas utilizadas, los métodos aplicados y la naturaleza de los datos encontrados. Esta planificación permitió anticipar posibles ajustes en la estructura del proyecto y facilitar la revisión del material recopilado. Asimismo, se establecieron pautas básicas para mantener la trazabilidad del proceso, garantizando que toda la información registrada tuviera un origen verificable y se mantuviera bajo control durante el desarrollo del proyecto.

En la siguiente Tabla 7, se presenta el conjunto de herramientas utilizadas durante el desarrollo del proyecto. Cada una fue seleccionada en función de su capacidad para identificar, correlacionar y analizar información expuesta en fuentes abiertas. La tabla detalla los casos de estudio, las versiones de las herramientas empleadas, la justificación de su uso y las técnicas aplicadas tanto de OSINT como de ciberinteligencia, permitiendo evidenciar su aporte en la detección y evaluación de riesgos digitales.

Caso de estudio	Herramienta	Versión	Justificación	Técnicas OSINT	Técnicas de ciberinteligencia
Caso 1: Análisis de riesgos derivados de la exposición de datos personales mediante técnicas OSINT dirigido a personas naturales	HaveIBeenPwned	Gratuita	Permite verificar si los correos personales han sido expuestos en filtraciones y estimar el alcance de la fuga de datos.	Búsqueda de brechas y filtraciones públicas.	Evaluación de exposición de correos y estimación de riesgo asociado.
	Usersearch	Suscripción	Relaciona un correo con perfiles sociales para rastrear identidades.	Perfilado social y rastreo de alias.	Análisis de vínculos entre identidades digitales.
	Ghunt	Gratuita	Detecta actividad y vínculos en servicios Google.	Descubrimiento de información en servicios Google y geolocalización.	Corroboración de identidad y validación de datos recolectados.
	Social Analyzer	Gratuita	Vincula alias o correos con cuentas sociales.	Búsqueda en redes sociales y correlación de alias.	Análisis de relaciones y patrones de exposición social.
	Dehashed	Suscripción	Expone contraseñas, mostrando posibles compromisos previos y evidenciando credenciales sensibles presentes en filtraciones públicas y registros históricos.	Consulta de bases de datos filtradas.	Priorización de riesgos por reutilización de credenciales.

Caso de estudio	Herramienta	Versión	Justificación	Técnicas OSINT	Técnicas de ciberinteligencia
Caso 2: Evaluación de riesgos por exposición de datos personales en una entidad privada	Dehashed	Gratuita	Detecta filtraciones de accesos corporativos, señalando posibles riesgos internos.	Búsqueda de filtraciones corporativas.	Identificación de accesos comprometidos y riesgos internos.
	Investigator	Gratuita (GitHub)	Permite evaluar configuraciones visibles en sitios privados para detectar puntos débiles.	Enumeración de configuraciones públicas.	Identificación de superficie de ataque y vectores de riesgo.
	Maltego CE	Community	Mapea conexiones entre correos, dominios y redes que amplían la superficie de exposición.	Análisis de correlación de entidades mediante grafos.	Análisis de vínculos y correlación visual de actores y activos.
	SpiderFoot	Gratuita	Automatiza la recolección de datos expuestos en infraestructuras corporativas.	Recolección automatizada de información pública.	Correlación de resultados y priorización de hallazgos.
	Hunter.io	Gratuita (limitada)	Recupera direcciones de empleados, mostrando posibles vectores de spear phishing.	Enumeración de correos asociados a un dominio.	Identificación de posibles objetivos para ataques dirigidos.
	Deep Research (Gemini)	Gratuito	Utiliza la inteligencia artificial para realizar investigaciones complejas de forma automática.	Búsqueda asistida y filtrado inteligente de fuentes abiertas.	Análisis contextual y agrupación de hallazgos relevantes.

Caso de estudio	Herramienta	Versión	Justificación	Técnicas OSINT	Técnicas de ciberinteligencia
Caso 3: Análisis de riesgos OSINT por exposición de datos personales en una entidad pública	Maltego	Community	Permite identificar relaciones entre correos, dominios y documentos públicos, evidenciando conexiones que muestran la magnitud de la exposición digital de la entidad.	Reconocimiento pasivo y correlación de datos públicos.	Análisis de superficie de exposición digital.
	FOCA	Gratuita	Revela metadatos presentes en documentos oficiales, como usuarios internos o rutas del sistema, lo que ayuda a detectar fugas de información no intencionadas.	Análisis de metadatos en documentos públicos.	Extracción de información interna y detección de posibles puntos de fuga.
	Google Dorking	Gratuita	Localiza documentos y datos expuestos en la web mediante búsquedas avanzadas, mostrando información que la entidad publicó sin control adecuado, identificar archivos confidenciales y configuraciones.	Búsquedas avanzadas mediante operadores específicos.	Identificación de fugas de información y exposición documental.

Tabla 7: Herramientas y Técnicas OSINT y de Ciberinteligencia aplicadas en los casos de estudio.

3.2 Fase 2: Recopilación y análisis de datos expuestos

En esta fase se desarrollaron los tres casos de estudio aplicando técnicas de OSINT y ciberinteligencia con el objetivo de evaluar la exposición digital y las posibles vulnerabilidades presentes en diferentes entidades. Cada caso se enfocó en un escenario particular, donde se emplearon herramientas y metodologías específicas para la recolección, análisis y correlación de información pública. A partir de los resultados obtenidos, se identificaron incidentes de seguridad relevantes y se documentaron hallazgos que reflejan riesgos potenciales para las organizaciones analizadas.

3.2.1 Caso de estudio 1: Análisis de riesgos derivados de la exposición de datos personales mediante técnicas OSINT dirigido a personas naturales.

En este caso se evaluó el nivel de exposición digital de una persona natural mediante una dirección de correo que fue expuesta **(gisa**********@gmail.com)**, utilizando herramientas OSINT como Have I Been Pwned, DeHashed, GHunt, Social Analyzer y UserSearch. Estas herramientas permitieron identificar filtraciones de datos, rastrear información pública vinculada a servicios de Google y detectar la posible asociación del correo con perfiles en redes sociales y plataformas de mensajería. El propósito fue determinar el grado de visibilidad del identificador en entornos digitales y la facilidad con la que puede ser relacionado con otros servicios.

Los hallazgos confirmaron la presencia del correo en distintas brechas de seguridad que comprometieron datos sensibles como nombres, contraseñas cifradas y referencias de perfil. Además, se constató actividad pública en el ecosistema Google (perfil, calendario y mapas), así como la existencia de perfiles abiertos en redes sociales. Este conjunto de resultados muestra cómo un único identificador puede concentrar información dispersa en diversas plataformas, permitiendo reconstruir parcialmente la huella digital de un usuario. En la **Tabla 8,** se resumen los incidentes identificados, junto con la herramienta utilizada, el procedimiento aplicado y los principales hallazgos documentados. Estos resultados resaltan la importancia de revisar con frecuencia la información visible en Internet para evitar posibles riesgos.

DATOS DEL CASO			
Título del caso de estudio:	Análisis de riesgos derivados de la exposición de datos personales mediante técnicas OSINT aplicadas a información disponible públicamente.	**Tipo de Prueba**	Análisis OSINT y evaluación de ciberexposición
Realizado por:	Andres Balon García	**Fecha inicio:**	25/07/2025
Nº de prueba aplicadas:	3	**Fecha fin:**	25/07/2025
HERRAMIENTAS APLICADAS			
Hardware:	Computadora, conexión a internet		
Software:	Have I Been Pwned, DeHashed, GHunt, Social Analyzer, Usersearch.io		
Virtualización:	Kali Linux		
Fuentes de Información	Internet / Plataformas públicas		
Prueba 1: Have I Been Pwned (HIBP) + DeHashed			
DESCRIPCION DE LA PRUEBA 1			
Objetivo de la prueba:	Identificar filtraciones de datos históricas y actuales vinculadas al correo electrónico gisas*****@gmail.com, correlacionando credenciales, alias y datos de ubicación.	**Técnica empleada**	Búsqueda de brechas y filtraciones públicas.

Nivel de complejidad:	Fácil	**Tiempo de ejecución:**	5 minutos
Categoría de análisis:	Exposición de credenciales y brechas de datos.	**Fase:**	Fase 2: Recopilación y análisis de datos expuestos
PROCEDIMIENTO APLICADO:	1. Acceder a la web de Have I Been Pwned. 2. Introducir el correo electrónico objetivo en el campo de búsqueda. 3. Registrar plataformas comprometidas, año de la filtración y tipo de datos expuestos. 4. Acceder a DeHashed y crear una cuenta gratuita o iniciar sesión. 5. Introducir el correo en el buscador avanzado de DeHashed. 6. Exportar información de contraseñas (cifradas o texto plano), alias y direcciones IP encontradas. 7. Correlacionar coincidencias entre ambas fuentes y evaluar riesgos de credential stuffing, rastreo geográfico y suplantación.		
DETALLE TÉCNICO:	Ver anexo 1 prueba 1 Anexo 1. Procedimiento técnico		
Prueba 2 – GHunt			
DESCRIPCION DE LA PRUEBA 2			

Objetivo de la prueba:	Detectar servicios activos de Google asociados al correo objetivo y obtener metadatos de perfil.	**Técnica empleada**	Descubrimiento de información en servicios Google.
Nivel de complejidad:	Medio	**Tiempo de ejecución:**	20 minutos
Categoría de análisis:	Perfilado digital y enumeración de servicios en Google.	**Fase:**	Fase 2: Recopilación y análisis de datos expuestos
PROCEDIMIENTO APLICADO:	**Instalación y configuración en Kali Linux:** 1. Actualizar sistema y dependencias: 2. Clonar repositorio oficial. 3. Instalar Poetry (gestor de dependencias): 4. Sincronizar dependencias y bloquear versiones: 5. Activar entorno virtual. 6. Iniciar GHunt para menú de configuración: 7. En Firefox, instalar extensión GHunt Companion, sincronizar con GHunt y autenticar con credenciales de Google. 8. Seleccionar método 1 de sincronización para capturar tokens de acceso. 9. Revisar resultados obtenidos: imagen de perfil, eventos públicos, actividad en Google Maps y Chat. 10. Extraer Gaia ID y anotar servicios asociados para análisis posterior.		
DETALLE TÉCNIXO:	Ver anexo 1 prueba 2 Anexo 1. Procedimiento técnico		
Prueba 3 – Social Analyzer y Usersearch			

DESCRIPCION DE LA PRUEBA 3			
Objetivo de la prueba:	Localizar perfiles públicos en redes sociales y mensajería vinculados al correo objetivo.	**Técnica empleada**	Búsqueda en redes sociales y correlación de alias.
Nivel de complejidad:	Medio	**Tiempo de ejecución:**	25 minutos
Categoría de análisis:	Perfilado psicológico y vectores de ingeniería social.	**Fase:**	Fase 2: Recopilación y análisis de datos expuestos
PROCEDIMIENTO APLICADO:	Social Analizer 1. Clonar repositorio oficial 2. Instalar Docker Compose 3. Ejecutar despliegue de contenedores 4. Acceder vía navegador 5. Ingresar username o alias objetivo para escaneo. Usersearch 1. Acceder al panel principal de UserSearch.AI. 2. Seleccionar el tipo de búsqueda “Correo electrónico (Email)”. 3. Ingresar el correo objetivo en el campo de consulta. 4. Ejecutar la búsqueda y esperar los resultados. 5. Revisar coincidencias en plataformas detectadas y exportar la información relevante.		
DETALLE TÉCNIXO:	Ver anexo 1 prueba 3 Anexo 1. Procedimiento técnico		

Resultados	**Validación**
▪ Se expusieron nombre, correo, IP, género, ubicación, contraseñas cifradas con MD5 y redes sociales. ▪ Se identificaron contraseñas en texto plano, alias y ubicaciones aproximadas, junto con otros datos asociados. ▪ Presencia de imagen de perfil, eventos públicos y actividad en Google Maps y Chat. ▪ Perfiles públicos en Pinterest y canal abierto en Telegram.	
Conclusiones	
▪ El análisis OSINT confirmó que el correo evaluado aparece en múltiples filtraciones históricas, exponiendo credenciales cifradas y en texto plano, lo que evidencia una alta vulnerabilidad del identificador digital. Esta repetida aparición en brechas públicas refleja un historial de compromisos que se ha ido acumulando con el tiempo, dejando un rastro amplio de información vinculada al mismo correo. ▪ La correlación entre HIBP, DeHashed y GHunt permitió verificar la existencia de servicios activos asociados al ecosistema Google, incluyendo imagen de perfil, metadatos y actividad pública, lo cual incrementa la visibilidad del usuario en plataformas abiertas. Los elementos encontrados muestran que el correo mantiene interacción con distintos servicios, haciendo posible reconstruir aspectos adicionales del entorno digital asociado. ▪ La presencia de perfiles en redes sociales y plataformas de mensajería vinculados al mismo correo demuestra una elevada trazabilidad digital, facilitando la asociación entre identidad, actividad en línea y alias utilizados. Esta conexión entre servicios y alias refuerza la posibilidad de seguir el rastro digital del usuario en diferentes espacios públicos de la red. ▪ La combinación de datos expuestos como nombre, ubicación aproximada, alias, intereses y contraseñas comprometidas confirma un riesgo significativo de ingeniería social y suplantación, debido a la cantidad de información que puede ser reconstruida mediante fuentes abiertas. La variedad y relación entre estos datos permite construir un perfil amplio y detallado, lo que amplía la superficie de exposición del usuario en entornos digitales.	▪ Valido ☒ ▪ Inválido ☐ ▪ No concluyente ☒

Tabla 8: Reporte OSINT de exposición digital en un individuo.

3.2.2 Caso 2: Evaluación de riesgos por exposición de datos personales en una entidad privada

En las entidades privadas, el análisis de riesgos derivados de la exposición de datos personales mediante OSINT se centra en correos institucionales, configuraciones visibles y servicios en la nube. A diferencia de los usuarios individuales, las organizaciones suelen contar con sistemas más robustos que dificultan la filtración directa de información sensible de clientes. Sin embargo, la identificación de cuentas de empleados o directivos expuestas en brechas pasadas, así como datos publicados de forma accidental en entornos públicos, representa un riesgo que puede ser aprovechado para ataques externos.

El uso de herramientas como Hunter.io, Spiderfoot, Maltego, Dehashed e Investigator permitió detectar correos y datos filtrados de empleados. Durante la evaluación realizada en una entidad financiera ecuatoriana, se detectaron tres incidentes principales: exposición de 68 correos institucionales, participación de múltiples cuentas en filtraciones previas y un bucket público de Amazon S3 que contenía información sensible en texto claro, como nombres completos, número de cuenta, cédula y correo electrónico. Aunque estos datos posteriormente fueron retirados, su exposición temporal originada por un tercero externo a la entidad, el cual constituye un riesgo elevado para la seguridad y confidencialidad de la información.

El análisis del caso permitió comprender mejor cómo las entidades privadas manejan la información expuesta en sus entornos digitales. Las técnicas OSINT aplicadas facilitaron la identificación de patrones de publicación y el reconocimiento de datos vinculados a cuentas corporativas. Este proceso ayudó a evaluar de forma clara las prácticas internas de gestión de información y a entender cómo se originan algunos incidentes de exposición.

A continuación, se presenta el reporte de resultado del caso número 2, el cual detalla las pruebas realizadas, los procedimientos aplicados y los hallazgos obtenidos. Este reporte organiza los incidentes identificados en diferentes etapas del análisis, mostrando cómo la información recopilada en fuentes abiertas permite dimensionar el riesgo de filtraciones y su impacto potencial en la seguridad de la organización.

DATOS DEL CASO			
Título del caso de estudio:	Evaluación de riesgos por exposición de datos personales en una entidad privada	Tipo de Prueba	Análisis OSINT y evaluación de exposición digital
Realizado por:	Andres Balon García	Fecha inicio:	26/07/2025
Nº de prueba aplicadas:	4	Fecha fin:	26/07/2025

Prueba 1: Identificación de correos institucionales expuestos			
DESCRIPCION DE LA PRUEBA 1			
Objetivo de la prueba:	Identificar direcciones de correo institucional expuestas en fuentes abiertas y brechas de seguridad, correlacionando información asociada como nombres, cargos y números telefónicos.	**Técnica empleada**	Enumeración de correos asociados a un dominio.
Nivel de complejidad:	Medio	**Tiempo de ejecución:**	90 minutos
Categoría de análisis:	Recolección de correos electrónicos y evaluación de vectores de phishing.	**Fase:**	Fase 2: Recopilación y análisis de datos expuestos
PROCEDIMIENTO APLICADO:	**A) Hunter.io – Domain Search** 1. Abrir navegador y acceder a hunter.io → Domain Search. 2. Ingresar el dominio institucional y ejecutar búsqueda.		

	3. Verificar patrón de nomenclatura (p. ej., inicial+apellido@dominio). 4. Registrar nombre, cargo (si aparece) y fuentes que sustentan cada correo. 5. Usar Email Verifier para muestrear direcciones y validar deliverability (solo verificación, sin envío). 6. Enlistar en un archivo csv y normalizar campos (correo, nombre, cargo, fuente, fecha). **B) SpiderFoot – Descubrimiento automatizado** 1. Ingresar al terminal de Kali Linux y lanzar la interfaz web local 2. Abrir spiderfoot desde el navegador. 3. Nuevo Scan → Target: bancoguayaquil.com (o el dominio autorizado). 4. Activar módulos relevantes como.: correos, breaches públicas, redes sociales, paste sites, subdominios. 5. Ejecutar y, al finalizar, filtrar entidades Email Address / Person / Phone Number.
DETALLE TÉCNIXO:	Ver anexo 2 prueba 1 Anexo 2. Procedimiento técnico

Prueba 2: Búsqueda de información con la ayuda de Deep Research – Gemini			
DESCRIPCION DE LA PRUEBA 2			
Objetivo de la prueba:	Evaluar la capacidad de herramientas de inteligencia artificial (IA) para recopilar y analizar información pública relacionada con directivos y empleados de la entidad privada, con el fin de identificar posibles riesgos reputacionales o de exposición de datos	**Técnica empleada**	Búsqueda asistida y filtrado inteligente de fuentes abiertas
Nivel de complejidad:	Fácil	**Tiempo de ejecución:**	5 minutos

Categoría de análisis:	Búsqueda avanzada de información y perfilamiento digital.	**Fase:**	Fase 2: Recopilación y análisis de datos expuestos
PROCEDIMIENTO APLICADO:	1. Ingresar al entorno de Gemini Deep Research desde una cuenta autenticada. 2. Iniciar una consulta dirigida con términos relacionados a directivos o cargos de la entidad. 3. Revisar los resultados generados por la IA, priorizando coincidencias verificables en portales públicos, medios y registros corporativos. 4. Analizar el informe automatizado de Debida Diligencia Mejorada (DDM) generado por la IA, enfocándose en el uso de datos personales, menciones públicas y riesgos reputacionales. 5. Registrar los hallazgos relevantes, excluyendo cualquier información privada o no verificable.		
DETALLE TÉCNIXO:	Ver anexo 2 prueba 2 Anexo 2. Procedimiento técnico		
Prueba 3 – Exposición de correos institucionales filtrados en brechas			
DESCRIPCION DE LA PRUEBA 3			
Objetivo de la prueba:	Detectar correos institucionales involucrados en filtraciones históricas y dimensionar el riesgo de reutilización de credenciales.	**Técnica empleada**	Búsqueda de filtraciones corporativas y análisis de correlación de entidades mediante grafos.
Nivel de complejidad:	Medio	**Tiempo de ejecución:**	25 minutos
Categoría de análisis:	Exposición de credenciales y brechas de datos.	**Fase:**	Fase 2: Recopilación y análisis de datos expuestos
PROCEDIMIENTO APLICADO:	**A) Maltego – Inserción masiva de correos + Transformación HIBP** 1. Abrir Maltego CE en Kali Linux. 2. Crear un nuevo Graph en blanco.		

	3. Importar todos los correos recolectados previamente con Hunter.io y SpiderFoot: 4. Copiar/pegar uno a uno como entidad Email Address. 5. Una vez agregados los correos al grafo, seleccionarlos todos. 6. Ejecutar la transformación integrada de Have I Been Pwned (HIBP): 7. Para cada correo, Maltego devuelve nodos adicionales: • Nombre de la brecha, • Año, • Tipo de datos comprometidos (emails, contraseñas hash/planas, teléfonos, direcciones, etc.). 8. Analizar el grafo visualmente para identificar cuentas más expuestas (muchas brechas asociadas). 9. Exportar el grafo a PDF/PNG para anexar en el reporte y guardar los resultados en CSV para correlación con DeHashed. **B) DeHashed – Validación y detalle de fugas** 1. Acceder a deHashed con usuario registrado. 2. Buscar cada correo (o directamente por @dominio.com) en la barra de búsqueda. 3. Filtrar resultados por fecha de fuga, tipo de datos expuestos y número de incidentes. 4. Exportar coincidencias (si el plan lo permite) o registrar manualmente: • Fecha de brecha, • Servicio afectado, • Si existen contraseñas cifradas o en texto plano, • Otros metadatos vinculados (IP, teléfono). 5. Correlacionar resultados con el grafo de Maltego, marcando coincidencias entre HIBP y DeHashed.
DETALLE TÉCNIXO:	Ver anexo 2 prueba 3 Anexo 2. Procedimiento técnico
Prueba 4: Investigator (exposición en almacenamiento nube)	
DESCRIPCION DE LA PRUEBA 4	

Objetivo de la prueba:	Identificar exposición de servicios o buckets públicos con datos sensibles (p. ej., S3), validar su accesibilidad, documentar el riesgo asociado y registrar los elementos visibles sin interactuar con contenido no destinado al público.	**Técnica empleada**	Búsqueda OSINT en índices de buckets públicos y validación de accesibilidad.
Nivel de complejidad:	Medio	**Tiempo de ejecución:**	25 minutos
Categoría de análisis:	Exposición de información financiera y personal.	**Fase:**	Fase 2: Recopilación y análisis de datos expuestos
PROCEDIMIENTO APLICADO:	1. Acceder al portal Investigator. 2. Ingresar el dominio de la entidad en el buscador principal. 3. Verificar de forma sistemática las diferentes opciones que ofrece la plataforma como: certificados, subdominios, pastes, dorks en buscadores, almacenamiento en la nube, etc. y registrar únicamente la información relevante. 4. Durante la revisión de la sección de almacenamiento en nube, se identificó un bucket público de Amazon S3 que contenía información sensible (nombres, correos electrónicos, números de identificación y cuentas bancarias). 5. Se documentó la URL y la evidencia mediante capturas de pantalla, sin interactuar ni descargar archivos, únicamente constatando la visibilidad pública.		
DETALLE TÉCNIXO:	Ver anexo 2 prueba 4 Anexo 2. Procedimiento técnico		
HERRAMIENTAS APLICADAS			

<table>
<tr><td>Hardware:</td><td colspan="2">Computadora, conexión a internet</td></tr>
<tr><td>Software:</td><td colspan="2">SpiderFoot, Hunter.io, DeHashed, Maltego, Investigator</td></tr>
<tr><td>Virtualización:</td><td colspan="2">Kali Linux</td></tr>
<tr><td>Fuentes de Información</td><td colspan="2">Internet
Plataformas públicas</td></tr>
<tr><td colspan="2">Resultados</td><td>Validación</td></tr>
<tr><td colspan="2">▪ Correos institucionales expuestos en múltiples filtraciones.
▪ Contraseñas cifradas y datos personales asociados (nombre, teléfono, cargo).
▪ Exposición de datos personales en bucket S3.
▪ Información pública adicional identificada mediante IA, indicando riesgos reputacionales.</td><td rowspan="3">▪ Valido ☒
▪ Inválido ☐
▪ No concluyente ☐</td></tr>
<tr><td colspan="2">Conclusiones</td></tr>
<tr><td colspan="2">▪ La reutilización de correos institucionales y credenciales filtradas aumenta la exposición de empleados y directivos.
▪ Las filtraciones de datos personales y financieros incrementan el riesgo de ataques dirigidos, fraude y daño reputacional, ya que la información expuesta facilita la identificación de posibles objetivos dentro del entorno institucional.
▪ La exposición temporal de buckets públicos constituye una vulnerabilidad crítica que debe ser mitigada de inmediato.
▪ La información adicional identificada por herramientas de IA demuestra la necesidad de gestionar y limitar la visibilidad pública de datos corporativos.</td></tr>
</table>

Tabla 9: Reporte OSINT sobre exposición de datos en una entidad privada.

3.2.3 Caso de estudio 3: Evaluación de riesgos por exposición de datos personales en portales institucionales de una entidad pública

En las instituciones públicas, el análisis de riesgos derivados de la exposición de datos personales mediante OSINT se centra en documentos oficiales, portales institucionales y configuraciones técnicas. A diferencia de las entidades privadas, gran parte de la información se publica de manera intencional como parte de políticas de transparencia, lo que incrementa las probabilidades de que datos sensibles queden accesibles sin los controles adecuados. Listados de personal, correos electrónicos institucionales o configuraciones visibles en documentos oficiales pueden ser utilizados por actores maliciosos para diseñar ataques de ingeniería social, suplantación de identidad o fraudes electrónicos.

El uso de herramientas como Google Dorking, FOCA e Investigator permitió localizar documentos institucionales con información personal y técnica, extraer metadatos que exponen detalles internos de la infraestructura y detectar archivos históricos que contienen bases de datos de ciudadanos aún disponibles en línea. Estos hallazgos ponen en evidencia deficiencias en la gestión de los documentos digitales, en el control de metadatos y en la aplicación de políticas de protección de datos. La exposición de información de este tipo no solo representa un riesgo para la institución, sino también para la seguridad y la privacidad de los ciudadanos.

El caso permitió analizar cómo las instituciones públicas gestionan y publican su información digital. El uso de técnicas OSINT ayudó a identificar patrones en la organización y acceso de los documentos oficiales. Estos resultados ofrecieron una visión más clara sobre las prácticas de manejo documental y la exposición de datos en entornos institucionales.

A continuación, en la **tabla 10**, el cual detalla los incidentes identificados, los procedimientos aplicados y la evidencia recolectada. El reporte organiza los hallazgos en diferentes pruebas realizadas con técnicas OSINT, mostrando cómo la publicación inadecuada de documentos y la falta de controles de seguridad generan riesgos significativos para la infraestructura institucional y la confianza ciudadana, lo que evidencia la necesidad de mejorar el control sobre la información publicada para evitar futuras exposiciones y posibles inconvenientes derivados. .

DATOS DEL CASO			
Título del caso de estudio:	Evaluación de riesgos por exposición de datos personales en portales institucionales de una entidad pública	Tipo de Prueba	Análisis OSINT y evaluación de ciberexposición institucional
Realizado por:	Andres Balon García	Fecha inicio:	27/07/2025
Nº de prueba aplicadas:	3	Fecha fin:	27/07/2025
Prueba 1: Detección y mapeo de documentos institucionales mediante Machines (Maltego).			
DESCRIPCION DE LA PRUEBA 1			
Objetivo de la prueba:	Identificar archivos oficiales publicados en el dominio institucional que contienen datos personales y documentar los elementos encontrados.	**Técnica empleada**	Reconocimiento pasivo y correlación de entidades mediante herramientas OSINT (Maltego).
Nivel de complejidad:	Medio	**Tiempo de ejecución:**	15 minutos
Categoría de análisis:	Exposición de información pública, recolección de identificadores y detección de datos personales.	**Fase:**	Fase 2: Recopilación y análisis de datos expuestos

PROCEDIMIENTO APLICADO:	1. Ejecutar la herramienta Maltego, preinstalada en la máquina virtual Kali Linux. 2. Ubicar la opción “Machines” dentro de la interfaz principal. 3. Seleccionar la *machine* preconfigurada “Company Stalker”. 4. Ingresar el dominio institucional solicitado por la herramienta para iniciar el análisis. 5. Revisar el grafo generado, priorizando nodos relacionados con archivos PDF, XLS o CSV. 6. Descargar únicamente los documentos públicos relevantes para su verificación. 7. Identificar la presencia de datos personales (nombres, correos, teléfonos, cargos). 8. Documentar los hallazgos y evaluar los riesgos asociados a phishing, suplantación o uso indebido de la información expuesta.
DETALLE TÉCNIXO:	Ver anexo 3 prueba 1 Anexo 3. Procedimiento técnico

Prueba 2: Extracción de metadatos en documentos institucionales			
DESCRIPCION DE LA PRUEBA 2			
Objetivo de la prueba:	Detectar exposición de información técnica y operativa mediante el análisis de metadatos en documentos oficiales publicados.	**Técnica empleada**	Análisis de metadatos en documentos públicos.
Nivel de complejidad:	Medio	**Tiempo de ejecución:**	20 minutos
Categoría de análisis:	Exposición de infraestructura interna y usuarios.	**Fase:**	Fase 2: Recopilación y análisis de datos expuestos

PROCEDIMIENTO APLICADO:	1. Descargar e instalar FOCA desde el repositorio oficial. 2. Ejecutar FOCA en un entorno Windows. 3. Crear un nuevo proyecto dentro de la herramienta. 4. Introducir el dominio de la entidad pública (ejemplo: dominio.gob.ec). 5. Permitir que FOCA descargue automáticamente documentos asociados al dominio. 6. Analizar los metadatos extraídos de los archivos PDF, DOC y XLS. 7. Identificar correos electrónicos, nombres de usuario, rutas de archivos internos, nombres de equipos, versiones de software y autores. 8. Documentar posibles riesgos de explotación (fuerza bruta, path traversal, ingeniería social).
DETALLE TÉCNIXO:	Ver anexo 3 prueba 2 Anexo 3. Procedimiento técnico

Prueba 3: Exposición de documentos con datos personales			
DESCRIPCION DE LA PRUEBA 3			
Objetivo de la prueba:	Identificar documentos PDF publicados en el dominio que expongan información personal de ciudadanos.	**Técnica empleada**	Búsquedas avanzadas mediante operadores específicos.
Nivel de complejidad:	Medio	**Tiempo de ejecución:**	15 minutos
Categoría de análisis:	Exposición sensible de información personal.	**Fase:**	Fase 2: Recopilación y análisis de datos expuestos

PROCEDIMIENTO APLICADO:	1. Abrir navegador web y acceder a Google 2. Ejecutar la consulta avanzada: 3. Revisar los primeros resultados devueltos. 4. Descargar los documentos PDF que contienen listados con información personal. 5. Identificar la presencia de datos sensibles como nombres, números de cédula, direcciones y teléfonos. 6. Confirmar que la información se encontraba de acceso público sin autenticación. 7. Evaluar riesgos de uso indebido en campañas de fraude, suplantación o ingeniería social. 8. Documentar el hallazgo como vulnerabilidad crítica.
DETALLE TÉCNIXO:	Ver anexo 3 prueba 3 Anexo 3. Procedimiento técnico
HERRAMIENTAS APLICADAS	
Hardware:	Computadora, conexión a internet
Software:	Google Dorking, FOCA, Maltego
Virtualización:	Kali Linux, Windows
Fuentes de Información	Internet / Plataformas públicas

Resultados	**Validación**
▪ Google indexaba documentos PDF del dominio con acceso público sin autenticación. ▪ Los archivos contenían datos personales como nombres, cédulas, direcciones y teléfonos, además de otra información asociada a los registros institucionales.	▪ Válido ☒ ▪ Inválido ☐ ▪ No concluyente ☐

▪ Se identificaron formularios institucionales visibles desde Google con información sensible. ▪ Algunos documentos fueron retirados después de la revisión, confirmando exposición real. ▪ Se encontraron PDFs con datos de salud y registros administrativos sin anonimización, expuestos directamente desde el sitio web institucional correspondiente.	
Conclusiones	
▪ La entidad mantiene documentos institucionales expuestos públicamente que contienen datos personales y sensibles, lo que evidencia una falta de control sobre los procesos de publicación y gestión de archivos digitales. ▪ La indexación de documentos por parte de Google demuestra que la información estuvo disponible sin autenticación, permitiendo que nombres, cédulas, teléfonos, direcciones y datos administrativos sean accesibles para cualquier usuario. ▪ El análisis de metadatos confirmó la presencia de información técnica como nombres de usuarios, rutas internas y software utilizado, lo que incrementa la superficie de ataque y facilita la elaboración de vectores de ataque. ▪ La exposición de formularios, listados y documentos sin anonimización revela un manejo inadecuado del ciclo de vida documental, afectando la confidencialidad y el tratamiento adecuado de datos personales según la normativa vigente. ▪ La cantidad de documentos expuestos demuestra que la entidad mantiene información accesible sin control, lo que permite que datos personales y detalles internos queden relacionados de forma no intencionada.	

Tabla 10: Reporte OSINT sobre exposición de datos en una entidad pública.

3.3 Fase 3: Evaluación contextual de la exposición digital

3.3.1 Evaluación técnica de la exposición digital mediante MITRE ATT&CK en los casos de estudio

En este apartado se presentan los resultados obtenidos al correlacionar los hallazgos recopilados con herramientas OSINT, con el marco de referencia MITRE ATT&CK, aplicado a los tres casos de estudio analizados. La tabla de cada caso resume las técnicas detectadas, la fase de la kill chain en la que se ubican, una breve descripción de su funcionamiento y el riesgo asociado según el contexto particular. De esta manera, se evidencian los vectores de ataque más probables y se establece una relación directa entre la exposición digital identificada y las tácticas empleadas por actores maliciosos.

3.3.1.1 Caso de estudio 1: Análisis de riesgos derivados de la exposición de datos personales mediante técnicas OSINT dirigido a personas naturales.

En este caso se identificaron técnicas de acceso inicial y reconocimiento relacionadas con correos expuestos en filtraciones. Los riesgos principales corresponden a phishing dirigido, spear phishing y uso de credenciales válidas en intentos de acceso. El análisis confirma que la exposición de datos personales facilita diferentes fases de un ataque, como se muestra en la Tabla 11. Además, se evidenció una relación directa entre la cantidad de información expuesta y el nivel de riesgo detectado. Estos resultados permiten comprender mejor cómo pequeños descuidos en la publicación de datos pueden derivar en amenazas más complejas.

Rendimiento y Confiabilidad de Plataformas OSINT			
Herramienta	**Efectividad**	**Tiempo de recuperación**	**Limitaciones**
Have I Been Pwned (HIBP)	**Alta** - Precisa para verificar correos en brechas confirmadas	1 minutos	Solo trabaja con fugas ya divulgadas públicamente
DeHashed	**Alta** - Permite correlacionar correos con contraseñas expuestas y más metadatos	2 minutos	Varias funciones avanzadas requieren suscripción paga

Rendimiento y Confiabilidad de Plataformas OSINT			
Herramienta	**Efectividad**	**Tiempo de recuperación**	**Limitaciones**
GHunt	**Media** - Muy útil para ecosistema Google, pero solo permite analizar correos gmail	3 minutos	Depende de cookies/tokens; más lento en resultados
Social Analyzer	**Media** - Detecta perfiles públicos asociados a usernames	15 minutos	Posibles falsos positivos por coincidencias con homónimos
UserSearch	**Alta -** Permite rastrear la existencia de un mismo username en múltiples plataformas sociales	4 minutos	No siempre confirma si el perfil está activo; depende de búsquedas por nombre de usuario

Resultados – MITRE ATT&CK en el Caso 1				
Técnica	**Nombre**	**Fase MITRE ATT&CK**	**Descripción resumida**	**Riesgo asociado al caso**
T1566	Phishing	Initial Access	Envío de correos con enlaces/archivos maliciosos para comprometer al usuario.	El correo expuesto en filtraciones puede recibir phishing dirigido.
T1566.002	Spearphishing Link	Initial Access	Enlaces fraudulentos que simulan servicios legítimos para robar credenciales.	Posible uso de correos filtrados en campañas personalizadas.
T1078	Valid Accounts	Initial Access, Persistence	Uso de credenciales legítimas robadas.	Riesgo directo por contraseñas filtradas en Deezer/Wattpad/Cutout.Pro.

Técnica	Nombre	Fase MITRE ATT&CK	Descripción resumida	Riesgo asociado al caso
T1036	Masquerading	Defense Evasion	Archivos o procesos renombrados para parecer benignos y evadir detección.	Ataques posteriores usando cuentas expuestas pueden usar técnicas de camuflaje.
T1589	Gather Victim Identity Information	Reconnaissance	Recolección de información personal y credenciales expuestas en filtraciones públicas.	Los datos expuestos (correo, ubicación, IP) facilitan campañas de OSINT hostil.
T1590	Gather Victim Network Information	Reconnaissance	Identificación de dominios, IPs y redes asociadas a la víctima, mediante información filtrada o disponible públicamente	Los correos y datos filtrados permiten mapear servicios usados por la víctima.
T1591.002	Business Relationships	Reconnaissance	Recolección de información sobre relaciones con terceros y proveedores, incluyendo vínculos operativos.	Riesgo de supply chain o phishing que simule plataformas legítimas.

Tabla 11: Relación entre la Efectividad de las Herramientas OSINT y los Riesgos Categorizados según MITRE ATT&CK.

3.3.1.2 Caso 2: Evaluación de riesgos por exposición de datos personales en una entidad privada

En la Tabla 12 se muestran los resultados del caso de una entidad privada. Se detectaron técnicas asociadas a acceso inicial, reconocimiento y recolección de información, destacando el uso de correos filtrados, credenciales expuestas y almacenamiento en la nube sin protección. Estos hallazgos representan riesgos para empleados y clientes, con la posibilidad de ingeniería social, ataques de credenciales y fuga de datos sensibles.

Rendimiento y Confiabilidad de Plataformas OSINT			
Herramienta	**Efectividad**	**Tiempo de recuperación**	**Limitaciones**
Hunter.io	**Alta** – Precisa para enumerar correos institucionales	2 minutos	API limitado en versión gratuita
SpiderFoot	**Media** – Buen alcance para vínculos OSINT, pero genera ruido	90 miuntos	Requiere filtrado manual; resultados dispersos y puede tardar días en obtener los resultados
Maltego (transform HIBP)	**Media** – Útil para correlación de brechas con correos	40 minutos	Configuración compleja y demanda tiempo de normalización
DeHashed	**Alta** – Permite correlacionar correos con contraseñas expuestas	3 minutos	Varias funciones avanzadas requieren suscripción paga
Investigator	**Media-** Localiza buckets S3 y archivos expuestos rápidamente	60 minutos	Alcance limitado a servicios compatibles

Resultados – MITRE ATT&CK en el Caso 2				
Técnica (ID)	**Nombre**	**Fase MITRE ATT&CK**	**Descripción resumida**	**Riesgo asociado al caso**
T1566	Phishing	Initial Access	Envío de correos	Los 68 correos identificados

Resultados – MITRE ATT&CK en el Caso 2				
Técnica (ID)	**Nombre**	**Fase MITRE ATT&CK**	**Descripción resumida**	**Riesgo asociado al caso**
			fraudulentos a empleados o clientes.	pueden ser blanco de phishing o spear phishing.
T1566.001	Spearphishing Attachment	Initial Access	Correos con archivos maliciosos adjuntos.	Riesgo de ataques dirigidos a directivos con información filtrada.
T1566.002	Spearphishing Link	Initial Access	Enlaces maliciosos que simulan servicios financieros.	Clientes o empleados podrían ser engañados con sitios falsos.
T1078	Valid Accounts	Initial Access / Persistence	Uso de credenciales expuestas en brechas previas.	Correos en DeHashed facilitan ataques (credential stuffing/password spraying).
T1589	Gather Victim Identity Information	Reconnaissance	Obtención de datos personales y laborales de empleados.	La exposición de nombres, cargos y teléfonos facilita ingeniería social.
T1530	Data from Cloud Storage Object	Collection	Acceso a datos en servicios en la nube (ej. Amazon S3).	El bucket público expuso información personal y bancaria sensible.

Tabla 12: Análisis Integrado del rendimiento de herramientas OSINT y aplicación del marco MITRE ATT&CK en una entidad privada.

3.3.1.3 Caso de estudio 3: Evaluación de riesgos por exposición de datos personales en portales institucionales de una entidad pública

En el caso de la institución pública se detectaron técnicas asociadas a reconocimiento, descubrimiento y obtención de credenciales, vinculadas a la exposición de directorios, documentos y metadatos. Los riesgos más destacados son la recopilación masiva de información, el uso de credenciales expuestas y la suplantación institucional. Esta situación refleja que la información publicada sin control puede aprovecharse en fraudes y ataques, tal como se detalla en la Tabla 13.

Rendimiento y Confiabilidad de Plataformas OSINT			
Herramienta	**Efectividad**	**Tiempo de recuperación**	**Limitaciones**
Google Dorking	**Alta** – Localiza documentos y directorios públicos con rapidez	5–10 minutos	Depende de indexación de Google
FOCA	**Alta** – Extrae metadatos y estructura de documentos institucionales	10 minutos	Requiere validación manual de resultados
Maltego (Machines)	**Alta –** Automatiza el descubrimiento de entidades, relaciones entre dominios, correos y documentos públicos	10 minutos	Alcance limitado a servicios, la versión gratuita solo permite usar un conjunto reducido de transformaciones

Resultados – MITRE ATT&CK en el caso 3				
Técnica (ID)	**Nombre**	**Fase MITRE ATT&CK**	**Descripción resumida**	**Riesgo asociado al caso**
T1589	Gather Victim Identity Information	Reconnaissance	Obtención de datos de empleados y ciudadanos.	El directorio institucional publicado contiene nombres, cargos y correos.
T1596	Search Open Websites / Domains	Reconnaissance	Uso de sitios públicos para recolectar datos.	Documentos PDF y formularios expuestos en el portal institucional.

Resultados – MITRE ATT&CK en el caso 3				
Técnica (ID)	**Nombre**	**Fase MITRE ATT&CK**	**Descripción resumida**	**Riesgo asociado al caso**
T1083	File and Directory Discovery	Discovery	Identificación de rutas internas y estructuras técnicas.	FOCA reveló rutas de sistemas, versiones de software y usuarios.
T1552	Unsecured Credentials	Credential Access	Exposición de correos y credenciales en metadatos.	Riesgo de ataques de fuerza bruta o diccionarios personalizados.
T1119	Automated Collection	Collection	Extracción automática de grandes volúmenes de datos.	Documentos y formularios accesibles permiten recopilación masiva.
T1656	Impersonation	Initial Access / Social Engineering	Suplantación de identidad institucional.	Los datos expuestos pueden usarse en fraudes que simulen ser del organismo.

Tabla 13: Análisis técnico del uso de herramientas OSINT y técnicas MITRE ATT&CK asociadas a la exposición de datos en portales públicos.

Nota: Para esta fase se tomó como referencia el marco **MITRE ATT&CK**, el cual permitió contextualizar los hallazgos dentro de un modelo reconocido de tácticas y técnicas de ciberataque. Este enfoque facilitó la correlación entre las vulnerabilidades detectadas y los posibles vectores de ataque, aportando una visión más estructurada del análisis realizado [70].

Gracias a ello, fue posible identificar patrones comunes y comprender mejor cómo se desarrollan los incidentes dentro de cada fase del ataque, lo que ayudó a definir con mayor precisión las áreas que requieren mejora y fortalecimiento en la seguridad institucional, proporcionando además una base metodológica solida para orientar decisiones y priorizar acciones correctivas.

3.3.2 Evaluación de riesgos y análisis de exposición según la Ley Orgánica de Protección de Datos Personales (LOPDP).

Se evaluó la exposición digital en los tres casos de estudio: persona natural, entidad privada y entidad pública. El objetivo fue identificar qué tipos de datos personales estaban públicos en fuentes abiertas, que tan accesibles eran esos datos y qué impacto podría generar su uso indebido. Para cuantificar el riesgo se empleó una escala de dos factores: probabilidad e impacto, calculado mediante la relación NR = P × I. La probabilidad se refiere a la facilidad de acceso a la información mediante fuentes abiertas, según los criterios detallados en la **Tabla 14**, mientras que el impacto considera las posibles consecuencias sobre la privacidad, reputación o seguridad de los datos expuestos, conforme a la **Tabla 15**.

Por último, la **Tabla 16** presenta la clasificación del nivel de riesgo resultante, que integra ambos factores, y permite determinar la criticidad en la exposición del dato. Los resultados obtenidos se condensaron en una matriz de evaluación, donde se muestra el nivel de riesgo asignado a los distintos datos, incorporando además una referencia legal a la Ley Orgánica de Protección de Datos Personales (LOPDP) para contextualizar el tratamiento y la protección de la información expuesta.

La evaluación de riesgos se basa en la Norma ISO 31000:2018 de Gestión del Riesgo, que establece un enfoque sistemático para identificar, analizar y valorar los riesgos considerando la relación entre probabilidad e impacto [71]. Este marco permitió definir las categorías y niveles utilizados en la matriz, asegurando coherencia metodológica con estándares internacionales y con la Ley Orgánica de Protección de Datos Personales (LOPDP).

El desarrollo de esta etapa permitió relacionar los hallazgos obtenidos con el marco legal vigente en materia de protección de datos. La aplicación del modelo de evaluación facilitó interpretar de forma práctica los resultados de cada caso, determinando qué tipo de información requiere mayor control. Además, el uso de la escala de riesgo permitió comparar los niveles de exposición y establecer prioridades de corrección según su impacto. Esto permitió obtener una visión más completa del nivel real de exposición, además de fortalecer el análisis al vincular los resultados con medidas concretas de mitigación y cumplimiento normativo.

Escala de valoración del riesgo

Probabilidad (P)

Mide qué tan fácil es encontrar o acceder al dato mediante fuentes abiertas.

Valor	Nivel de probabilidad	Descripción
1	Muy baja	Difícil de obtener o explotar públicamente.
2	Baja	Requiere búsqueda avanzada o datos complementarios.
3	Media	Disponible parcialmente o bajo ciertas condiciones.
4	Alta	Fácilmente localizable y reutilizable en OSINT.
5	Muy alta	Ampliamente expuesto, con alta facilidad de explotación.

Tabla 14: Escala de probabilidad de exposición de datos en fuentes abiertas

Impacto (I)

Evalúa la gravedad del impacto reputacional, psicológico o de privacidad que podría generarse si la información es expuesta o utilizada indebidamente.

Valor	Nivel de impacto	Descripción
1	Insignificante	Sin consecuencias relevantes.
2	Bajo	Afecta de forma menor o temporal.
3	Moderado	Causa molestias o riesgos limitados.
4	Alto	Daños notables en la reputación o seguridad.
5	Crítico	Compromiso severo de la integridad o privacidad.

Tabla 15: Escala de valoración del impacto de exposición de datos personales

Nivel de riesgo (NR)

Se calcula mediante la fórmula:

$$NR = P \times I$$

Rango	Clasificación	Descripción
1–5	Bajo	Riesgo mínimo o controlado.
6–10	Medio	Riesgo moderado; requiere monitoreo.
11–15	Alto	Riesgo considerable; debe mitigarse.
16–25	Crítico	Riesgo inaceptable; requiere acción inmediata.

Tabla 16: Clasificación del nivel de riesgo resultante

El análisis de riesgo permite entender con mayor detalle cómo ciertos tipos de información pública pueden representar un nivel de exposición más alto. Este enfoque ayudó a distinguir entre los datos que requieren medidas inmediatas y aquellos que pueden mantenerse bajo observación. La matriz elaborada durante la evaluación permitió visualizar las áreas más sensibles dentro de cada caso, lo que facilitó una interpretación más completa de los resultados. De esta manera, el modelo aplicado no solo clasificó los riesgos, sino que también aportó una base práctica para futuras acciones de mejora en el manejo de datos.

La correcta aplicación de la escala de riesgo constituye un paso importante dentro del proceso de gestión de ciberseguridad, ya que permite visualizar objetivamente los niveles de amenaza y su posible afectación. La aplicación de la escala también permite comprobar que la relación entre probabilidad e impacto ofrece una visión equilibrada del riesgo. Al integrar estos factores, el proceso de evaluación no solo cuantifica la exposición, sino que facilita su interpretación en el contexto de la Ley Orgánica de Protección de Datos Personales. Esto refuerza la importancia de mantener un control constante sobre la información disponible en fuentes abiertas.

3.3.2.1 Caso de estudio 1: Amenazas derivados de la exposición de datos personales mediante técnicas OSINT dirigido a personas naturales.

El análisis de información correspondiente a una persona natural permitió identificar diversos elementos expuestos en fuentes abiertas, entre ellos correos electrónicos, contraseñas, alias digitales y fotografías personales. Los resultados evidencian que la reutilización de credenciales en distintos servicios y la vinculación de nombres de usuario entre plataformas pueden facilitar la correlación de identidades y el rastreo de actividades en línea. Este tipo de información, aunque accesible públicamente, puede ser utilizada en campañas de suplantación, phishing o ingeniería social. Por ello, es necesario fortalecer las medidas de seguridad digital personales, promoviendo el uso de contraseñas únicas, la autenticación multifactor y una gestión responsable de la identidad en redes sociales. Estos hallazgos reflejan el nivel de exposición individual en el entorno digital y la importancia de reconocer las vulnerabilidades derivadas del uso cotidiano de plataformas en línea.

De igual forma, la exposición de imágenes, perfiles en redes y servicios vinculados a cuentas de Google puede permitir la elaboración de perfiles digitales detallados que revelen hábitos, ubicaciones y relaciones personales. La combinación de estos datos, incluso sin vulnerar sistemas, amplía las posibilidades de uso indebido de la información. Este hallazgo subraya la importancia de la concienciación sobre el manejo de datos personales y la necesidad de aplicar prácticas preventivas que reduzcan la huella digital. Mantener una presencia controlada en línea y revisar periódicamente la información pública disponible son acciones clave para disminuir la probabilidad de exposición y fortalecer la privacidad individual.

Como se muestra en la Tabla 17, se presentan los resultados del análisis de riesgos aplicados a una persona natural. En ella se identifican los principales datos personales expuestos durante la investigación, el tipo de riesgo asociado y la referencia legal correspondiente según la LOPDP. Esta tabla resume cómo la exposición de información como correos electrónicos, alias digitales o contraseñas puede afectar la privacidad individual y facilitar ataques de suplantación o fraude. Además, evidencia la necesidad de aplicar medidas preventivas que reduzcan la exposición de datos en entornos públicos.

Tipo de Dato	Descripción de la amenaza	Referencia legal LOPDP	Evaluación de probabilidad	Evaluación de impacto	Nivel de riesgo	Clasificación
Correo electrónico personal	Exposición del correo en fuentes abiertas que permite intentos de contacto malicioso.	**Art. 4** (dato personal identificable), **Art. 37** (seguridad de datos).	**Media (3):** Frecuente exposición en fugas y OSINT.	**Critico (5):** Acceso no autorizado y phishing.	15	Alto
Nombre completo	Identificación básica, facilita búsquedas dirigidas en fuentes abiertas.	**Art. 4** (dato personal general), **Art. 10** (principio de minimización).	**Alta (4):** Amplia disponibilidad pública.	**Moderado (3):** Genera exposición moderada, pero requiere otros datos para representar una amenaza.	12	Alto
Contraseñas / credenciales	Exposición o reutilización de credenciales en distintos servicios.	**Art. 37** (medidas de seguridad técnicas y organizativas).	**Muy alta (5):** Exposición recurrente en fugas.	**Critico (5):** Compromiso total de cuentas.	25	Crítico
Alias digitales / usernames	Reutilización del mismo alias que permite rastrear presencia digital en varias plataformas y servicios relacionados.	**Art. 40** Análisis de riesgos, amenazas y vulnerabilidades.	**Alta (4):** Reutilizados y útil para correlacionar.	**Moderado (3):** Permiten relacionar perfiles o servicios asociados a una misma persona.	12	Alto

Tipo de Dato	Descripción de la amenaza	Referencia legal LOPDP	Evaluación de probabilidad	Evaluación de impacto	Nivel de riesgo	Clasificación
Imagen de perfil (fotografía)	Representación visual de identidad personal, su publicación puede revelar rasgos físicos, entorno, ubicación aproximada o hábitos.	**Art. 4** Identificador personal.	**Media (3):** Exposición frecuente en redes.	**Alta (4):** Riesgo reputacional o de suplantación de identidad.	12	Alto
Servicios activos de Google (Gaia ID, Maps, etc.)	Rastreo transversal de actividades personales que puede mostrar interacciones, ubicaciones, uso de aplicaciones y conexiones entre cuentas asociadas al mismo ecosistema.	**Art. 40** Análisis de riesgos, amenazas y vulnerabilidades.	**Media (3):** Detectables por metadatos y correlaciones.	**Alta (4):** Rastreo y vinculación de cuentas.	12	Alto
Cuentas en redes sociales	Exposición adicional de la identidad digital, riesgo de acoso o ataques de ingeniería social	**Art. 10** (Principio de finalidad y minimización), **Art. 42** Evaluación de impacto del tratamiento de datos personales.	**Muy alta (5):** Alta visibilidad y correlación entre plataformas.	**Alta (4):** Riesgo de suplantación y pérdida de privacidad.	20	Crítico

Tabla 17: Exposición de datos personales y evaluación de riesgos asociados en usuarios individuales.

3.3.2.2 Caso de estudio 2: Evaluación de vulnerabilidades por exposición de datos personales en una entidad privada

El estudio realizado en una entidad privada permitió observar la existencia de información institucional disponible en espacios digitales públicos, lo que puede implicar riesgos en la gestión de datos de empleados y clientes. Se identificaron elementos como correos institucionales, credenciales de acceso y nombres asociados a cargos laborales en documentos o repositorios abiertos. Esta información puede ser aprovechada para ejecutar campañas de ingeniería social o intentos de suplantación. Estos hallazgos resaltan la necesidad de reforzar los controles internos sobre el manejo de credenciales y la publicación de información corporativa en entornos digitales.

También se identificó la presencia de teléfonos institucionales, números de identificación y datos financieros en fuentes abiertas. Aunque en algunos casos su difusión responde a fines administrativos o de contacto, la ausencia de medidas de protección adecuadas puede aumentar los riesgos de fraude o uso no autorizado. La exposición simultánea de información laboral y personal amplía la superficie de ataque y puede dificultar la gestión de incidentes de seguridad. Por tanto, resulta importante que las empresas adopten políticas de protección de datos, realicen auditorías periódicas y apliquen buenas prácticas conforme a los principios de seguridad, proporcionalidad y minimización establecidos en la LOPDP.

En la Tabla 18 se detallan las amenazas detectadas en una entidad privada, evidenciando la exposición de datos de empleados y clientes a través de brechas y servicios en la nube. La información se clasifica según el tipo de dato comprometido, el nivel de riesgo estimado y la disposición legal aplicable. Este registro permite visualizar los principales puntos de riesgo institucional y su relación con las obligaciones establecidas en la LOPDP. También ayuda a reconocer los procesos que requieren un mejor control en el manejo de la información y el uso de plataformas digitales, permitiendo orientar acciones que reduzcan la posibilidad de exposición de datos y mejoren las prácticas de seguridad dentro de la entidad. De esta manera, se refuerza la gestión preventiva y el cumplimiento normativo.

Tipo de Dato	Descripción de la amenaza	Referencia legal LOPDP	Evaluación de probabilidad	Evaluación de impacto	Nivel de riesgo	Clasificación
Nombre completo + cargo	Identificación básica vinculada a una organización; puede usarse para ingeniería social o suplantación	**Art. 4** (dato personal general) **Art. 10** (principio de finalidad).	**Alta (5):** Común en sitios institucionales y redes profesionales.	**Moderado (3):** Facilita identificar roles y puede favorecer intentos de contacto no autorizado.	15	Alto
Correo institucional	Exposición del correo laboral que permite intentos de contacto malicioso, campañas de phishing y otros tipos de comunicación fraudulenta.	**Art. 4** (dato personal general), **Art. 10** (principio de minimización).	**Alta (4):** Frecuente en portales institucionales, comunicados o bases de contacto.	**Moderado (3):** Su exposición no compromete directamente la seguridad, pero puede ser un punto de entrada para phishing.	12	Alto
Teléfono institucional	Divulgación del número laboral que facilita intentos de contacto indebido y comunicaciones no autorizadas	**Art. 4** (dato personal identificador) **Art. 10** (principio de proporcionalidad).	**Media (3):** Publicación en portales oficiales.	**Moderado (3):** Posibles llamadas no autorizadas o ingeniería social	9	Medio

Tipo de Dato	Descripción de la amenaza	Referencia legal LOPDP	Evaluación de probabilidad	Evaluación de impacto	Nivel de riesgo	Clasificación
Credenciales (usuario/contraseña)	Exposición o reutilización de credenciales internas.	**Art. 40** Análisis de riesgos, amenazas y vulnerabilidades.	**Muy Alta (5):** Las credenciales suelen filtrarse con frecuencia en fugas públicas (breaches) o reutilizarse en varios servicios.	**Critico (5):** Permiten acceso directo a sistemas internos, robo de información o suplantación total del usuario.	25	Critico
Número de identificación personal (cédula/RUC)	Dato único que permite relacionar información disponible en distintas fuentes públicas o filtradas.	**Art. 4** (dato identificador) **Art. 8** (Consentimiento del titular).	**Medio (3):** Accesible en registros públicos o bases filtradas.	**Alta (4):** Puede usarse en consultas públicas y vinculación básica de información.	12	Alto
Cuenta bancaria	Exposición del número de cuenta bancaria, lo que puede ser utilizado en intentos de fraude	**Art. 4** (dato financiero sensible) **Art. 37** (seguridad reforzada y confidencialidad).	**Bajo (2):** No suele estar pública; puede filtrarse en documentos, correos o bases de datos. Su obtención requiere esfuerzo.	**Alto (4)** Puede facilitar solicitudes de pago fraudulentas, reclamaciones indebidas o intentos de suplantación	8	Medio

Tabla 18: Evaluación de riesgos por exposición de datos personales en una entidad privada.

3.3.2.3 Caso de estudio 3: Evaluación de riesgos por exposición de datos personales en portales institucionales de una entidad pública

El análisis aplicado a la entidad pública permitió identificar la presencia de información personal publicada en portales institucionales sin mecanismos de control claramente definidos. Esta situación, frecuente en organismos que buscan mantener la transparencia y la comunicación con la ciudadanía, puede generar riesgos en materia de confidencialidad y protección de datos. Durante la revisión se encontraron documentos y bases con nombres, correos personales, teléfonos y formularios con datos identificativos accesibles públicamente. La disponibilidad de este tipo de información incrementa la posibilidad de uso indebido o de ataques de ingeniería social dirigidos a funcionarios o ciudadanos.

Por otro lado, la publicación de datos técnicos y metadatos asociados a documentos institucionales refleja la necesidad de fortalecer los procedimientos internos de revisión antes de compartir información en línea. Estos elementos, aunque no constituyen una vulnerabilidad directa, pueden servir para mapear estructuras internas o identificar servicios en uso. Además, la exposición simultánea de información personal y técnica puede afectar la confianza digital y el cumplimiento de los principios de proporcionalidad y minimización establecidos en la LOPDP. En este sentido, se recomienda promover prácticas preventivas que incluyan auditorías periódicas, anonimización de información y controles de acceso adecuados para proteger la privacidad de los datos en los portales públicos.

La Tabla 19 presenta los riesgos derivados de la publicación de información personal en portales institucionales de una entidad pública. Se describen los tipos de datos encontrados. Los resultados reflejan cómo la exposición masiva de datos ciudadanos puede vulnerar principios de confidencialidad y proporcionalidad previstos en la LOPDP. Además, permite identificar las áreas donde es necesario aplicar controles más adecuados para el tratamiento de la información, especialmente en la gestión de documentos y formularios en línea. De esta manera, se promueve una administración más segura de los datos y un cumplimiento más claro de las disposiciones establecidas por la ley, fortaleciendo la responsabilidad institucional en la protección de la información pública.

Tipo de Dato	Descripción de la amenaza	Referencia legal LOPDP	Evaluación de probabilidad	Evaluación de impacto	Nivel de riesgo	Clasificación
Nombres completos y cargos (directorio institucional)	Posible uso en suplantación o ingeniería social hacia funcionarios.	Art. 4 (dato personal general), Art. 10 (principio de finalidad).	**Muy alta (5):** Datos disponibles en portales institucionales.	**Moderado (3):** Facilitan contacto o fraude dirigido.	15	Alto
Correos electrónicos institucionales	Uso indebido en campañas de spear phishing o contacto no autorizado.	Art. 4 (Dato personal identificador), Art. 37 (Seguridad de los datos personales).	**Muy alta (5):** Publicados en directorios y documentos oficiales.	**Moderado (3):** Pueden requerir contexto adicional para representar un riesgo.	15	Alto
Correos electrónicos personales	Exposición del correo que facilita intentos de contacto malicioso.	Art. 4 (dato personal identificable), Art. 37 (seguridad de datos).	**Muy alta (5):** Detectables en fugas públicas o archivos expuestos.	**Alto (4):** Riesgo directo de phishing o robo de identidad.	20	Crítico
Teléfonos institucionales	Uso indebido para contactos no autorizados o ingeniería social.	Art. 10 (Principio de finalidad y proporcionalidad).	**Media (3):** Publicación frecuente en portales oficiales.	**Moderado (3):** Permite llamadas no solicitadas al área o funcionario	9	Medio
Teléfonos personales	Riesgo de acoso o fraude por exposición de número privado, afectando la privacidad.	Art. 4 (Dato personal identificador). Art. 37 (seguridad de datos personales).	**Alta (4):** Expuestos en documentos institucionales o bases filtradas.	**Alta (4):** Impacto directo a la privacidad del titular.	16	Crítico

Tipo de Dato	Descripción de la amenaza	Referencia legal LOPDP	Evaluación de probabilidad	Evaluación de impacto	Nivel de riesgo	Clasificación
Estructura organizacional interna	Permite identificar jerarquías, áreas sensibles y responsables.	Art. 40 (análisis de riesgos y vulnerabilidades).	**Alta (4):** Información detectada en documentos públicos.	**Alto (4):** Facilita ataques dirigidos y reconocimiento interno.	16	Crítico
Metadatos técnicos (usuarios, rutas, software, impresoras, etc.)	Permiten mapear infraestructura interna o usuarios del sistema.	Art. 37 (Seguridad de los datos personales), Art. 47 (Obligaciones del responsable y encargado).	**Alta (4):** Detectables mediante análisis OSINT técnico (FOCA).	**Crítico (5):** Riesgo de explotación técnica o acceso no autorizado.	20	Crítico
Base histórica de ciudadanos (nombres, cédulas, correos, teléfonos, datos médicos/laborales, etc.)	Compromiso masivo de datos personales y sensibles.	Art. 4 (Datos personales y sensibles), Art. 8 (Consentimiento del titular), Art. 37 (Seguridad de los datos personales).	**Alta (4):** Documentos accesibles públicamente sin autenticación.	**Crítico (5):** Daño legal, ético y reputacional.	20	Crítico
Formulario con nombre, cédula, teléfono, correo personal	Recolección sin medidas de seguridad o control de acceso, exponiendo información personal.	Art. 10 (Principio de minimización), Art. 37 (Seguridad de los datos personales)	**Muy alta (5):** Accesible desde el portal sin restricciones.	**Alto (4):** Facilita phishing, suplantación de identidad y ataques de ingeniería social.	20	Crítico

Tabla 19: Evaluación de riesgos por exposición de datos personales en una entidad pública.

3.4 Fase 4: Recomendaciones para mejorar la seguridad de la información

La fase 4 presenta recomendaciones orientadas a fortalecer la seguridad de la información según los hallazgos obtenidos. Estas acciones buscan reducir la exposición de datos personales, mitigar riesgos detectados en los casos de estudio y fomentar buenas prácticas digitales. Se proponen medidas preventivas y correctivas que promueven una gestión segura, responsable y acorde con las normativas de protección de datos.

3.4.1 Medidas preventivas y buenas prácticas

Caso 1: Análisis de riesgos derivados de la exposición de datos personales mediante técnicas OSINT dirigido a personas naturales.

En el análisis de riesgos de las personas naturales se identificó que la exposición de información personal en internet es un factor crítico que facilita ataques digitales. Las contraseñas débiles, la poca conciencia sobre la privacidad en redes sociales y la falta de monitoreo de filtraciones incrementan la vulnerabilidad. Por ello, se proponen medidas enfocadas en fortalecer los hábitos de seguridad digital, con prácticas sencillas pero efectivas. La siguiente tabla resume las principales recomendaciones para proteger la información personal y reducir los riesgos asociados.

Se evidenció que la falta de conocimiento sobre seguridad digital sigue siendo uno de los factores más comunes que facilitan ataques en internet. Muchos usuarios comparten información sin considerar las consecuencias o reutilizan contraseñas en varios servicios. Por ello, resulta fundamental fomentar la educación digital y la concientización sobre el valor de la privacidad. Promover el uso responsable de las plataformas y enseñar prácticas sencillas de protección puede marcar una gran diferencia en la prevención de amenazas cotidianas y en la construcción de una identidad digital más segura.

En la **Tabla 20** se presentan las principales medidas preventivas y buenas prácticas recomendadas para personas naturales. Estas acciones buscan reducir la exposición de datos personales en línea y fortalecer la seguridad digital individual. Las recomendaciones incluyen el uso de contraseñas seguras, la activación de

autenticación multifactor y la correcta configuración de privacidad en redes sociales. También se sugiere realizar revisiones periódicas de posibles filtraciones de datos, con el fin de detectar a tiempo incidentes que puedan comprometer la información personal. La aplicación de estas medidas ayuda a crear hábitos más seguros y a minimizar los riesgos de suplantación o robo de identidad.

Recomendación /Medida preventiva	**Justificación**	**Implementación propuesta**	**Objetivo esperado**
Uso de contraseñas fuertes y únicas	Muchas personas reutilizan contraseñas, lo que facilita ataques en caso de filtraciones.	Utilizar combinaciones seguras de caracteres, cambiarlas de forma periódica y evitar su reutilización. Apoyarse en gestores de contraseñas para administrarlas de manera segura.	Reducir el riesgo de accesos no autorizados a cuentas personales.
Autenticación multifactor (MFA)	El robo de credenciales es común en filtraciones masivas.	Activar MFA en correos, redes sociales y cuentas financieras mediante aplicaciones o sistemas de verificación en dos pasos.	Añadir una segunda capa de protección, incluso si la contraseña es comprometida.
Configuración de privacidad en redes sociales	Datos expuestos públicamente facilitan la ingeniería social.	Revisar la configuración de privacidad de cada red, limitar la visibilidad de publicaciones, fotos y listas de contactos mediante ajustes de seguridad integrados en las plataformas sociales.	Evitar que atacantes recopilen información personal para suplantación o fraudes.
Monitoreo de filtraciones de datos	Los correos personales suelen aparecer en brechas sin que el usuario lo sepa.	Realizar revisiones periódicas con herramientas de verificación de brechas y cambiar contraseñas cuando se detecten incidentes.	Reducir riesgos derivados de brechas pasadas y proteger cuentas actuales.

Tabla 20: Buenas prácticas digitales para la protección de datos personales.

Caso 2: Evaluación de vulnerabilidades por exposición de datos personales en una entidad privada.

El caso de la entidad privada mostró vulnerabilidades relacionadas con la exposición de correos institucionales en brechas previas y en fuentes públicas. También se identificó un bucket S3 con datos sensibles, aunque este último no fue gestionado directamente por la institución, sino por un tercero. Aun así, la presencia de información asociada a la entidad representa riesgos de suplantación de identidad, phishing y pérdida de confianza de los clientes.

Las medidas propuestas están orientadas a mejorar la gestión de credenciales, fortalecer la seguridad en la nube y reducir la exposición de información crítica. Además, la aplicación de estas medidas refuerza la seguridad y el cumplimiento normativo dentro de la entidad. Mantener un buen control de accesos y supervisar los servicios en la nube ayuda a proteger la información sensible. También es clave capacitar al personal para evitar errores comunes. En conjunto, estas acciones fortalecen la protección frente a posibles ataques.

En la **Tabla 21** se resumen las principales medidas de ciberseguridad recomendadas para la entidad privada, derivadas del análisis realizado. Estas acciones buscan corregir las debilidades detectadas en el manejo de credenciales, el uso de servicios en la nube y la exposición de datos personales. Cada recomendación incluye su justificación, forma de implementación y el objetivo esperado, con el fin de orientar a la organización hacia una gestión más segura de la información y promover practicas internas que reduzcan la posibilidad de incidentes. Además, este conjunto de medidas ofrece una guía practica para fortalecer los controles existentes y mejorar la protección general del entorno digital institucional.

Su aplicación permitirá reducir los riesgos de suplantación, accesos no autorizados y pérdida de confianza por parte de los clientes, al fortalecer los controles básicos que protegen las cuentas institucionales y la información sensible. Esto también ayudará a mejorar la respuesta ante incidentes, disminuir errores comunes en la gestión de datos y mantener un entorno mas organizado y seguro dentro de la entidad. De igual forma, contribuirán a mantener una operación más ordenada y a evitar problemas derivados de una gestión inadecuada.

Recomendación /Medida preventiva	Justificación	Implementación propuesta	Objetivo esperado
Gestión de correos institucionales expuestos	Se detectaron 68 correos institucionales con datos asociados, lo que facilita phishing e ingeniería social.	Implementar MFA obligatoria, rotación de credenciales y monitoreo de fugas de datos en plataformas libres.	Prevenir accesos no autorizados y reducir riesgos de suplantación.
Respuesta frente a correos filtrados en brechas pasadas	Varias cuentas ya estuvieron en fugas previas, lo que habilita ataques de credential stuffing.	Usar contraseñas seguras y únicas, activar alertas de acceso y reforzar la capacitación interna sobre manejo de credenciales.	Minimizar el impacto de fugas anteriores y proteger credenciales activas.
Protección contra ingeniería social y phishing	Los datos filtrados incluyen nombres, cargos y teléfonos de empleados.	Implementar filtros de correo y sistemas de detección de mensajes fraudulentos, junto con simulaciones de phishing y comunicación preventiva con clientes.	Reducir el éxito de ataques de spear phishing y fraudes financieros.
Gestión de exposición en almacenamiento en la nube (Amazon S3)	Se detectó un bucket público con datos bancarios y personales sensibles.	Configurar controles de acceso seguros en la nube, auditar con herramientas de seguridad y establecer alertas ante cambios de configuración.	Evitar nuevas exposiciones de información sensible en servicios en la nube.
Minimización de exposición de datos personales	Datos filtrados como teléfonos y correos amplían la superficie de ataque.	Limitar la publicación de información personal, anonimizar datos personales en documentos	Proteger la privacidad de clientes y empleados, preservando la confianza en la entidad.

Tabla 21: Medidas de ciberseguridad entidades privadas.

Caso 3: Evaluación de riesgos por exposición de datos personales en portales institucionales de una entidad pública.

En el escenario de la entidad pública, los riesgos detectados se vinculan principalmente con el manejo de datos de los ciudadanos y la publicación de documentos oficiales. El incumplimiento de normativas como la LOPDP, la falta de segmentación en las redes y la exposición de metadatos representan amenazas importantes para la seguridad institucional. Las buenas prácticas recomendadas buscan garantizar el uso responsable de la información, prevenir fugas de datos y fortalecer la cooperación entre organismos. La tabla siguiente resume las acciones sugeridas para mejorar la seguridad en este contexto.

Se comprobó que muchos de los riesgos detectados provienen de la falta de controles internos para la publicación de información institucional. La capacitación del personal, el uso de herramientas de revisión previa y la cooperación entre organismos resultan esenciales para mantener la seguridad de los datos públicos. Fomentar una cultura de responsabilidad digital en el sector público no solo ayuda a prevenir incidentes, sino que también garantiza una gestión más transparente y segura de la información gubernamental.

La aplicación de estas medidas también requiere una planificación continua y la revisión periódica de los procedimientos institucionales. La adopción de controles básicos, como la verificación de documentos antes de su publicación y el uso de canales seguros para el intercambio de información, puede reducir los riesgos de exposición. Con ello, las instituciones públicas podrán mantener un entorno digital más confiable y alineado con las disposiciones legales vigentes.

En la **Tabla 22** se resumen las principales medidas de ciberseguridad recomendadas para las instituciones públicas Las recomendaciones abarcan desde la eliminación de metadatos en documentos oficiales hasta la colaboración con equipos de respuesta ante incidentes (CERT/CSIRT). Su aplicación contribuye a reducir la posibilidad de fugas de información y fortalecer la confianza de la ciudadanía en los servicios digitales del Estado. Además, fomenta una cultura de protección de datos dentro de las entidades públicas y promueve la adopción de buenas prácticas en todos los niveles de gestión.

Recomendación /Medida preventiva	Justificación	Implementación propuesta	Objetivo esperado
Cumplimiento estricto de la LOPDP	Entidades públicas manejan datos sensibles de ciudadanos; incumplir puede generar sanciones.	Crear normas internas de protección de datos, designar delegados de cumplimiento y realizar auditorías periódicas del tratamiento de información.	Asegurar el tratamiento responsable de datos personales y cumplir con la ley.
Eliminación de metadatos en documentos públicos	Documentos PDF/Word subidos a portales oficiales pueden exponer autores, ubicaciones o sistemas internos.	Aplicar herramientas de limpieza de metadatos y establecer un flujo de revisión antes de publicar archivos institucionales.	Prevenir fugas indirectas de información sensible a través de documentos oficiales.
Cooperación interinstitucional (CERT/CSIRT)	Las entidades públicas suelen ser blanco de APTs y necesitan coordinación nacional.	Fortalecer la colaboración con el CERT Ecuador y otros CSIRT sectoriales.	Mejorar la detección, mitigación y respuesta ante ciberamenazas avanzadas.
Anonimización de datos personales en publicaciones institucionales	La exposición de directorios, correos y nombres completos en portales públicos facilita ataques de ingeniería social y suplantación de identidad.	Implementar procesos automáticos de anonimización o enmascaramiento de datos antes de publicar documentos o bases de datos en línea.	Proteger la privacidad de los ciudadanos y reducir la explotación de datos personales en campañas de fraude o ataques dirigidos.

Tabla 22: Medidas de ciberseguridad para instituciones del sector público.

3.4.2 Consideraciones éticas y legales en el uso de OSINT

El uso de OSINT debe realizarse dentro de un marco que combine la ética profesional con el cumplimiento legal. Aunque la información provenga de fuentes abiertas, su uso indebido puede afectar la privacidad de las personas y generar consecuencias negativas para organizaciones. Por este motivo, es importante que el análisis de datos públicos se haga con responsabilidad, siguiendo criterios de legalidad y proporcionalidad en cada caso.

En Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPDP) regula el manejo de información personal y establece sanciones para quienes la recolecten o difundan sin autorización. Esta normativa obliga a limitar la recolección a lo estrictamente necesario, evitando el almacenamiento excesivo o la difusión de datos que no guarden relación con el objetivo del análisis. Además, promueve principios como la transparencia y la responsabilidad en el tratamiento de los datos personales, lo que refuerza la confianza en las prácticas de investigación digital. Así, se protege la integridad de la información y se respeta el derecho a la privacidad de los ciudadanos.

Desde la perspectiva ética, el analista tiene la responsabilidad de utilizar los datos únicamente con fines legítimos, como la investigación académica, la auditoría de seguridad o la prevención de incidentes cibernéticos. Los resultados deben enfocarse en la protección de sistemas e individuos, evitando exponer vulnerabilidades de forma que puedan ser aprovechadas por actores maliciosos. También se debe mantener la imparcialidad durante el proceso, sin alterar ni manipular los resultados para obtener conclusiones sesgadas.

Asimismo, es recomendable que los hallazgos se compartan únicamente con las áreas competentes dentro de una organización, en lugar de publicarlos abiertamente. Esta práctica evita que la información sensible sea utilizada con fines inadecuados y contribuye a mantener un nivel adecuado de confidencialidad, especialmente cuando se trata de datos que podrían exponer vulnerabilidades internas. Finalmente, la ética profesional implica actuar con transparencia, prudencia y compromiso, asegurando que el uso de OSINT contribuya a generar un entorno digital más seguro, responsable y confiable para todos.

CONCLUSIONES

- El proyecto demostró que las técnicas OSINT y de ciberinteligencia son efectivas para identificar información expuesta en distintos entornos digitales. En los tres casos analizados se registraron 196 activos expuestos, entre ellos 167 correos institucionales, 4 brechas del correo personal, 15 documentos con metadatos sensibles, 8 perfiles digitales vinculados y varios correos personales adicionales, además de recursos expuestos como un formulario institucional o un bucket S3 con información financiera. La revisión conjunta de estos datos permitió identificar patrones de riesgo y comprender mejor las vulnerabilidades detectadas, lo que facilita aplicar medidas para reducir la exposición de la información
- El análisis realizado mostró que la exposición de información pública es una problemática común y persistente. Esta situación se origina principalmente por la falta de control y la escasa conciencia sobre los riesgos que conlleva compartir datos personales sin restricciones. Dichos descuidos representan oportunidades para actores maliciosos que pueden explotar la información. En consecuencia, se incrementa la probabilidad de sufrir ataques cibernéticos y pérdida de confianza digital.
- La metodología aplicada permitió recopilar, organizar y evaluar datos de forma estructurada, generando una visión clara sobre los niveles de exposición detectados en cada caso. Se confirmó que el grado de vulnerabilidad no depende únicamente del tipo de actor analizado, sino también de las medidas de protección implementadas. Asimismo, se evidenció la importancia de gestionar los datos personales con responsabilidad. Esto permitió evaluar con precisión los riesgos conforme a la LOPDP.
- El uso combinado de técnicas OSINT y procesos de ciberinteligencia facilitó la detección temprana de riesgos en diferentes entornos digitales. Además, impulsó el desarrollo de una cultura de seguridad que promueve la prevención y la protección proactiva de la información. Este enfoque integral fomenta la resiliencia ante amenazas cibernéticas en los sectores público y privado, evidenciando la importancia de la ciberinteligencia en los entornos digitales.

RECOMENDACIONES

- Se recomienda que tanto usuarios como organizaciones realicen revisiones periódicas de su huella digital utilizando técnicas y herramientas OSINT. Este proceso permite identificar información expuesta antes de que sea aprovechada por terceros y facilita la corrección temprana de vulnerabilidades. La supervisión constante refuerza la protección de credenciales y datos personales. Así se mejora la prevención frente a incidentes de seguridad en entornos digitales.
- Se sugiere fortalecer la capacitación en ciberseguridad dentro de entornos laborales, educativos e institucionales. Una mayor conciencia sobre las amenazas digitales contribuye a la adopción de buenas prácticas en el manejo de la información. Estas actividades deben incluir simulaciones de phishing y sesiones de sensibilización sobre el valor de la privacidad. Promover la formación continua ayuda a reducir errores humanos y a consolidar una cultura de seguridad.
- Es necesario establecer políticas y buenas prácticas de ciberseguridad orientadas a la publicación, almacenamiento y tratamiento de datos personales. Dichas medidas deben ser aplicadas en todos los sectores con base en los principios de proporcionalidad y minimización de la LOPDP. Su correcta implementación permitirá reducir la exposición innecesaria de información en entornos digitales. Con ello se garantiza la protección de la privacidad y la integridad de los datos.
- Se recomienda que tanto instituciones públicas como privadas integren progresivamente la ciberinteligencia dentro de sus estrategias de seguridad. Este enfoque permitirá fortalecer la prevención y la detección de amenazas de forma más eficiente. Además, contribuye a la creación de un ecosistema digital más seguro y confiable. La incorporación de procesos de inteligencia mejora la capacidad de respuesta ante incidentes. Así se garantiza una protección constante de la información.

REFERENCIAS

[1] C. Sausalito, «CYBERCRIME MAGAZINE,» 10 junio 2019. [En línea]. Available: https://cybersecurityventures.com/cybersecurity-market-report/. [Último acceso: 25 sep 2024].

[2] IBM Security, «Cost of a Data Breach Report 2024,» 2024. [En línea]. Available: https://www.ibm.com/security/data-breach. [Último acceso: 2024 sep 25].

[3] Anti-Phishing Working Group, «Number of ransomware attacks worldwide from 2016 to 2022,» Anti-Phishing Working Group, Cambridge, Massachusetts, Estados Unidos., 2025.

[4] European Union Agency for Cybersecurity (ENISA), «ENISA Threat Landscape 2022: Mapping the Threats,» 2022. [En línea]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022. [Último acceso: 25 sep 2024].

[5] K. Y. F. W. S. J. Watson, «The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends,» *IEEE Access,* 2021.

[6] J. F. y. M. O. R. Santos, «Effectiveness of OSINT in Detecting Malicious Cyber Activities,» pp. 113745-113759, 2021.

[7] A. V. e. al., «Using OSINT to Safeguard Critical Infrastructures,» de *2022 International Conference on Cybersecurity*, 2022.

[8] M. Bazzell, Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, USA: CreateSpace Independent Publishing Platform, 2021.

[9] Diego Leonardo Chimbo Chillogalli, Rodolfo Xavier Bojorque Chasi, «Estudio de herramientas OSINT para ciberseguridad,» 2023.

[10] A. M. Z. P. e. al., «Guía básica teórica y práctica de uso de herramientas OSINT,» *Polo del Conocimiento, Revista Tecnológica,* vol. 10, nº 3, 2025.

[11] J. A. Calderón, «OSINT (Open Source Intelligence),» 2022. [En línea]. Available: https://es.scribd.com/document/472880241/OSINT. [Último acceso: 1 Noviembre 2024].

[12] Asamblea Nacional del Ecuador, «Registro Oficial Suplemento 459,» 26 Mayo 2021. [En línea]. Available: https://www.lexis.com.ec/biblioteca/ley-organica-proteccion-datos-personales. [Último acceso: 12 Noviembre 2024].

[13] Asamblea Nacional del Ecuador, «Plan Nacional de Desarrollo Ecuador No Se Detiene 2025 – 2029,» 2025. [En línea]. Available: https://www.planificacion.gob.ec/wpcontent/uploads/2025/08/PlanNacionalDeDesarrollo25-29_EcuadorNoSeDetiene.pdf.

[14] Ministerio de Telecomunicaciones y de la Sociedad de la Información, «Ley Orgánica de Protección de Datos Personales,» 2021. [En línea]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf. [Último acceso: 2025 Agosto 27].

[15] J. I. A. O. P. N. S. J. T. López Díaz, «Ciberseguridad para todos: orígenes, concepto y alcance,» *ININEE Ciencia Revista de Divulgación Científica,* vol. 2, nº 4, pp. 39-48, 2025.

[16] R. L. Galvá, «La seguridad de la información: Desde la antigüedad hasta el Internet de las cosas,» *Revista Seguridad, Ciencia & Defensa,* Vols. %1 de %2Vol. 4,, nº 4, p. 60–69, 2018.

[17] R. L. Villagra, «Evolución tecnológica y ciberseguridad,» *Tema de Investigación Central de la Academia,* p. 85–99, 2019.

[18] M. F. Boné-Andrade, «Evaluación de la evolución de la ciberseguridad en sistemas empresariales modernos,» *Multidisciplinary Collaborative Journal,* vol. 1, nº 2, p. 25–38, 2023.

[19] Cadena SER, «Incibe detecta al año 183.000 sistemas vulnerables y lleva a cabo un simulacro para probar sus propias defensas,» *Cadena SER,* 18 Septiembre 2024.

[20] El País, «Se buscan expertos en ciberseguridad,» *El País,* 29 Noviembre 2024.

[21] El País, «Fraudes digitales, nadie está a salvo,» *El País,* 8 Diciembre 2024.

[22] J. M. Y.-H. T. J. P.-G. y. M. C. O. Z. Alfonso A. Guijarro-Rodríguez, «Aplicación de seguridad en capas en entornos informáticos como estrategia de defensa en profundidad,» *Revista Espacios,* vol. 39, nº 42, pp. 19-30, 2018.

[23] Q. Z. Y. Ge, «Zero Trust for Cyber Resilience,» *arXiv ,* 5 Diciembre 2023.

[24] J. Arteaga, «El análisis de riesgos en la ciberseguridad,» Real Instituto Elcano, 14 enero 2020. [En línea]. Available: https://media.realinstitutoelcano.org/wpcontent/uploads/2021/11/comentario-arteaga-analisis-de-riesgos-en-ciberseguridad.pdf.

[25] NIST (Instituto Nacional de Estándares y Tecnología), «Marco de Ciberseguridad del NIST: Versión 2.0 (traducción al español),» 26 Febrero 2024. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf.

[26] CCN-CERT (Centro Criptológico Nacional – Equipo de Respuesta a Incidentes de Seguridad), «Infografía Red Nacional de SOC,» 2021. [En

línea]. Available: https://www.ccn.cni.es/es/docman/documentos-publicos/489-infografia-red-nacional-de-soc. [Último acceso: 28 julio 2025].

[27] SafePaaS, «Guía de seguridad Zero Trust para la empresa digital,» SafePaaS, 25 Mayo 2025. [En línea]. Available: https://www.safepaas.com/es/articles/zero-trust-security-guide-for-the-digital-enterprise/.

[28] N. A. R. S., «Ciberresiliencia: integración entre seguridad de la información y continuidad de negocio,» *Revista Sistemas,* nº 159, Julio 2021.

[29] C. Osuna Miranda, «Segmentación y microsegmentación de redes,» Pers.eus, 3 Marzo 2025. [En línea]. Available: https://www.pers.eus/articulos-tecnicos/segmentacion-y-microsegmentacion-de-redes/.

[30] Anti-Phishing Working Group (APWG), «Phishing Activity Trends Report,» Anti-Phishing Working Group, 23 Diciembre 2021. [En línea]. Available: https://apwg.org/trendsreports/.

[31] Cybersecurity Ventures, «Ransomware Damage Report,» Cybersecurity Ventures, 15 Marzo 2024. [En línea]. Available: https://cybersecurityventures.com/ransomware-damage-report/.

[32] SonicWall, «2024 SonicWall Cyber Threat Report,» SonicWall, 1 Febrero 2024. [En línea]. Available: https://www.sonicwall.com/resources/white-papers/2024-sonicwall-cyber-threat-report/.

[33] AV-TEST GmbH, «Malware Statistics,» AV-TEST GmbH, 30 Abril 2024. [En línea]. Available: https://www.av-test.org/en/statistics/malware/.

[34] Verizon, «Data Breach Investigations Report 2023,» Verizon, 6 Junio 2023. [En línea]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[35] Arbor Networks, «ATLAS Global DDoS Attack Data,» Arbor Networks, 15 Octubre 2023. [En línea]. Available: https://www.arbornetworks.com/atlas.

[36] NETSCOUT Systems, Inc., «Threat Intelligence Report,» NETSCOUT Systems, Inc., 30 Septiembre 2023. [En línea]. Available: https://www.netscout.com/threatreport.

[37] A. Mata, Ciberseguridad para todos, Ediciones de la U, 2025.

[38] IBM, «¿Qué es un actor de amenazas?,» [En línea]. Available: https://www.ibm.com/es-es/topics/threat-actor. [Último acceso: 2025 05 08].

[39] Trend Micro, «Ecuadorean Bank Loses $12 million via SWIFT,» 20 Mayo 2016. [En línea]. Available: https://www.trendmicro.com/vinfo/nz/security/news/cyber-attacks/ecuadorean-bank-loses-12m-via-swift.

[40] Movistar Empresas, « Security Forum analizó el escenario y tendencias de ciberseguridad en el país,» 09 Febrero 2024. [En línea]. Available: https://www.telefonica.com.ec/security-forum-de-movistar-empresas-analizo-el-escenario-y-tendencias-de-ciberseguridad-en-el-pais/.

[41] M. Á. C. V. y. D. C. Serrano, El Libro del Hacker, España: Anaya Multimedia (colección Títulos Especiales), 2021.

[42] Panda Security, «Entendiendo los Ciber-Ataques. Parte I,» 2015. [En línea]. Available: https://www.pandasecurity.com/rfiles/enterprise/solutions/ad360/1704-WHITEPAPER-CKC-ES.pdf.

[43] A. C. Casas, «La ciberinteligencia: un eslabón clave para la seguridad,» 2022.

[44] C. I. y E. Estratégicos (Centro de Investigaciones y Estudios Estratégicos), «Ciberinteligencia: Contextualización, aproximación conceptual, características y desafíos,» 2018.

[45] Secretaría de Seguridad y Protección Ciudadana de México, «Ciclo de Inteligencia,» 2020. [En línea]. Available: https://www.gob.mx/cms/uploads/attachment/file/535136/Ciclo_Inteligencia.pdf.

[46] D. N. Bonilla, «El ciclo de inteligencia y sus límites,» *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol,* nº No. 48, p. 67–82, 2004.

[47] S. Kent, Inteligencia Estratégica, Pleamar, 1994.

[48] J. A. S. d. l. Peña, «Inteligencia Táctica,» p. 213–216, 2012.

[49] Maltego Technologies, «Maltego,» [En línea]. Available: https://docs.maltego.com.

[50] OpenCTI, «Open Cyber Threat Intelligence Platform,» OpenCTI Project, [En línea]. Available: https://filigran.io/platforms/opencti/. [Último acceso: 19 Septiembre 2025].

[51] C. Wagner, A. Dulaunoy, G. Wagener y A. Iklody, «MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform,» *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (WISCS '16),* 2016.

[52] United States Congress, «Public Law 109-163, Section 931,» U.S. Government Publishing Office (GPO), Washington, D.C., 2006.

[53] R. M. González, «Técnicas OSINT para investigación en Internet.,» 2025. [En línea]. Available:

https://mpdf.robertomurillo.net/wp-content/uploads/2025/05/Ciberpatrulla-Tecnicas-Osint-para-Investigacion-en-Internet.pdf.

[54] Ciberseguridade Galicia, «Open source Intelligence (OSINT),» Blog oficial de Ciberseguridade Galicia, 9 Febrero 2024. [En línea]. Available: https://ciberseguridadegalicia.gal/es/recursos/articulos/open-source-intelligence-osint.

[55] Artículo 19 México y Centroamérica, «Artículo 19 México y Centroamérica,» https://articulo19.org/wp-content/uploads/2023/07/Informe-OSINT-Mexico.pdf, 2023.

[56] J. Gutierrez, Metodología OSINT para investigar en internet, Madrid: Ciberpatrulla – Julián Gutiérrez, 2021.

[57] T. Hunt, «Have I Been Pwned: Check if your email has been compromised in a data breach,» haveibeenpwned.com, [En línea]. Available: https://haveibeenpwned.com.

[58] mxrch, «GHunt – OSINT Tool for Google Accounts,» Github, 2020. [En línea]. Available: https://github.com/mxrch/GHunt.

[59] P. Osman, «Social-analyzer – API and CLI for analyzing social media profiles,» Github, 2021. [En línea]. Available: https://github.com/PawanOsman/social-analyzer.

[60] DeHashed, «World's Largest Search Engine for Hacked Data,» dehashed.com, [En línea]. Available: https://www.dehashed.com.

[61] Hunter.io, «Find email addresses in seconds,» Hunter.io, [En línea]. Available: https://hunter.io.

[62] ElevenPaths, «FOCA – Metadata extraction tool,» GitHub, [En línea]. Available: https://github.com/ElevenPaths/FOCA.

[63] OWASP Foundation, «Google Hacking (Google Dorking),» OWASP, [En línea]. Available: https://owasp.org/www-community/Google_Hacking.

[64] SpiderFoot, «SpiderFoot,» SpiderFoot Documentation, [En línea]. Available: https://github.com/smicallef/spiderfoot.

[65] IBM, «OSINT: La Inteligencia Abierta que Revoluciona la Ciberseguridad,» 2023. [En línea]. Available: https://osint.org/the-integral-role-of-osint-in-modern-cyberdefense/. [Último acceso: 1 Noviembre 2024].

[66] GCS Network, «El Papel Creciente de OSINT en la Ciberseguridad,» 21 Diciembre 2022. [En línea]. Available: https://securityboulevard.com/2022/12/osint-in-cybersecurity-effectively-leveraging-open-source-intelligence-to-drive-enterprise-security-value-in-2023/. [Último acceso: 1 Noviembre 2024].

[67] D. Mider, «"Open source intelligence on the internet: functionalities and challenges",» *Internal Security Review,* nº No. 31, 2024.

[68] M. T. y. Tamayo, El proceso de la investigación científica, 5ª ed., México: Limusa, 2004.

[69] P. H. D. M. G. M. W. S. D. O. P. G. R. D. Mark Phythian, Understanding the Intelligence Cycle, M. Phythian, Ed., London: Routledge, 2013.

[70] MITRE Corporation, «MITRE ATT&CK Framework,» MITRE Corporation, 2013. [En línea]. Available: https://attack.mitre.org/. [Último acceso: 22 10 2025].

[71] International Organization for Standardization, ISO 31000:2018, Gestión del riesgo — Directrices, Ginebra: Organización Internacional de Normalización (ISO), 2018.

ANEXOS

Anexo 1: Análisis de riesgos derivados de la exposición de datos personales mediante técnicas OSINT

1. OBJETIVOS

OBJETIVO: Analizar los riesgos derivados de la exposición de datos personales de un individuo en plataformas digitales mediante técnicas OSINT, evaluando la información sensible disponible públicamente, además de su posible impacto en la seguridad personal y digital del usuario afectado.

Examinar el caso de estudio identificando la presencia y actividad del correo gisas*****@gmail.com en distintas plataformas tecnológicas, así como los datos personales accesibles mediante fuentes abiertas.

2. RECURSOS NECESARIOS

- Computadora
- Kali Linux
- Social Analizer
- Have I Been Pwnd
- Dehashed
- Ghunt
- Usersearch

3. ESCENARIO DEL CASO

Contexto: La dirección de correo electrónico gisasanza@gmail.com fue sometida a un proceso de análisis de ciberinteligencia basado en técnicas OSINT con el objetivo de identificar su nivel de exposición en internet y las plataformas sociales. El correo fue rastreado a través de herramientas como Have I Been Pwned, DeHashed, GHunt, Usersearch y Social analizer, además de una verificación manual en redes sociales. Estas acciones permitieron reconstruir parte de su huella digital y evaluar los riesgos derivados de filtraciones previas, presencia pública, y vinculación a plataformas personales o profesionales. El estudio revela que el uso reiterado de un mismo identificador digital, como lo es una cuenta de correo principal, puede comprometer severamente la privacidad y facilitar vectores de ataque si no existen medidas preventivas de seguridad.

Problema: Durante el análisis realizado se identificó que el correo electrónico analizado está vinculado a múltiples plataformas en línea, algunas de ellas con exposición directa de datos sensibles o con registros de participación en filtraciones de datos masivas. La combinación de estos elementos revela un nivel de exposición preocupante ya que, si llegara en manos de un actor malicioso, puede derivar en campañas dirigidas de phishing, ataques de ingeniería social o acceso a cuentas personales. La falta de anonimización, así como el uso reiterado del mismo identificador (correo electrónico), facilita la trazabilidad del perfil digital del usuario, poniendo en riesgo su seguridad.

4. RESOLUCIÓN

Análisis de Exposición Digital de un Identificador Personal mediante Técnicas OSINT

Incidente 1: Incidente combinado: Exposición en brechas de seguridad y registros públicos

El análisis OSINT realizado sobre la dirección de correo electrónico gisa******@gmail.com evidenció su compromiso en diversas brechas de datos y su aparición en registros públicos indexados en bases de datos filtradas. A través de la plataforma **Have I Been Pwned** se identificó su implicación en tres incidentes relevantes. Estos resultados confirman que la cuenta ha sido expuesta en diferentes servicios en línea, lo que incrementa el riesgo de suplantación o uso indebido de la información asociada.

Plataforma	Año	Datos filtrados (según las imágenes)
Dubsmash	Diciembre 2018	Direcciones de correo electrónico, Nombres de usuario, Hashes de contraseña, Ubicaciones geográficas, Nombres, Contraseñas, Números de teléfono, Idiomas hablados.
Canva	Mayo 2019	Direcciones de correo electrónico, Nombres de usuario, Nombres, Ciudades de residencia (asociadas a ubicaciones geográficas), Contraseñas (almacenadas como hashes bcrypt).

Plataforma	Año	Datos filtrados (según las imágenes)
Wattpad	Junio 2020	Biografías, Fechas de nacimiento, Direcciones de correo electrónico, Géneros, Ubicaciones geográficas, Direcciones IP, Nombres, Contraseñas, Perfiles de redes sociales, URL de sitios web de usuarios, Nombres de usuario.
Trello	Enero 2024	Direcciones de correo electrónico, Nombres, Nombres de usuario.

Tabla 23: Dominios expuestos según Have I been Pwnd

Complementariamente, la consulta en DeHashed reveló información adicional vinculada al mismo identificador, incluyendo contraseñas expuestas, algunas sin cifrado, alias digitales empleados en otras plataformas y ubicaciones aproximadas. Estos resultados evidencian el nivel de detalle que pueden ofrecer las bases de datos filtradas y cómo permiten reconstruir parte de la actividad digital asociada a una cuenta comprometida.

Riesgos e implicaciones identificados:

Credential stuffing: La exposición masiva de direcciones de correo electrónico, nombres de usuario y contraseñas hasheadas (incluso con algoritmos más robustos como bcrypt y PBKDF2) crea una base de datos valiosa para ataques automatizados. La reutilización de contraseñas podría comprometer otras cuentas, incluidas las financieras o corporativas.

Riesgo de phishing y spear phishing: Al combinar la dirección de correo electrónico con el nombre, usuario, biografías y perfiles de redes sociales, los atacantes pueden crear mensajes falsos muy creíbles. El objetivo es manipular a la víctima para robarle más información o acceder a sus cuentas.

Reconstrucción y Suplantación de Identidad: La disponibilidad de múltiples datos de validación como nombres, fechas de nacimiento, géneros, ubicaciones geográficas, números de teléfono e URLs de sitios web de usuarios facilita enormemente la elaboración de un perfil detallado. Esta información puede ser utilizada para validar la identidad de forma fraudulenta en servicios de atención al cliente o para abrir cuentas a nombre de la víctima.

Rastreo geográfico: La exposición de ubicaciones geográficas permite saber las zonas habituales de actividad. Esta información podría usarse para hacer ataques de fraude telefónico o para identificar rutinas de la persona.

Persistencia de la información filtrada: Datos antiguos como los de Dubsmash (2018), que expusieron millones de correos y contraseñas, fueron vendidos inicialmente en la dark web y después circularon en repositorios públicos. Aunque el incidente tenga varios años, la permanencia de estos registros mantiene vigente el riesgo de uso indebido.

Incidente 2: Reconocimiento de cuenta activa en el ecosistema Google mediante GHunt

El análisis realizado con la herramienta GHunt confirmó que el correo electrónico gisas********@gmail.com está asociado a una cuenta activa de Google con un perfil asociado en Google Maps. Estos resultados permiten establecer una relación directa entre la identidad digital y su presencia en plataformas abiertas, lo que incrementa la exposición de información personal y amplía el riesgo de que terceros accedan a datos adicionales.

Elemento Encontrado	Descripción del Hallazgo
Cuenta de Google	Confirmación de cuenta activa con Gaia ID y foto de perfil personalizada.
Página de Perfil (Maps)	Perfil público de "Gisbell Asanza" en Google Maps (Guía Local Nivel 3).
Actividad Geográfica	7 reseñas y 113 respuestas públicas. Las reseñas señalan actividad en Quito, Ecuador y Magnum Gym, Argentina.
Servicios Activos	El servicio de Google Maps está activado para este perfil.

Tabla 24: Exposición de datos personales a través de servicios de Google

Riesgos e Implicaciones

Los datos obtenidos del ecosistema de Google permiten un análisis de riesgos más enfocado y preciso:

Rastreo y Perfilamiento de Rutinas: La actividad en Google Maps revela ubicaciones geográficas específicas y negocios de interés (ej. gimnasios en Ecuador y Argentina). Esto permite inferir rutinas de viaje, trabajo o residencia, facilitando ataques físicos o de ingeniería social altamente localizados.

Spear Phishing Avanzado: El nombre completo ("Gisbell Asanza"), el correo electrónico y la foto de perfil personalizada ofrecen un contexto de identidad muy sólido. Un atacante puede usar esta información para crear correos electrónicos o mensajes extremadamente convincentes que aparenten provenir de servicios de Google, gimnasios o contactos en esas ubicaciones.

Suplantación de Identidad Digital: La foto de perfil y el nombre completo pueden ser utilizados para crear perfiles falsos muy creíbles en redes sociales, lo que facilita el engaño a amigos, familiares o colegas de la víctima.

Incidente 3: Identificación de perfiles públicos en redes sociales

Mediante el uso combinado de UserSearch y Social Analyzer, se identificó la vinculación del correo electrónico o un alias asociado (gisas**** y Gisbell) con múltiples perfiles y servicios.

Plataforma/Servicio	Estado de Conexión	Enlace/Detalles
Google	Conexión encontrada	Perfil activo (visto en Incidente 2).
Trello	Conexión de correo	Perfil de usuario o registro de la cuenta.
Dropbox	Conexión de correo/Nombre	Perfil de usuario o registro de la cuenta.
Microsoft	Conexión de correo	Perfil de usuario o registro de la cuenta.

Plataforma/Servicio	Estado de Conexión	Enlace/Detalles
Adobe	Conexión de correo	Perfil de usuario o registro de la cuenta.
Mecanografía	Conexión de correo	Servicio no detallado.
Facebook	Posible Perfil	Búsqueda por nombre de usuario gisasanza.
Pinterest	Posible Perfil	Búsqueda por nombre de usuario gisas****.
Instagram	Posible Perfil	Búsqueda por nombre de usuario gisas****.
TikTok	Posible Perfil	Búsqueda por nombre de usuario gisas****.

Tabla 25: Resultados OSINT de vinculación entre correo y plataformas

Riesgos e implicaciones:

Expansión de superficie de ataque: La presencia del usuario en varias plataformas, incluyendo entornos de trabajo, almacenamiento, redes sociales y servicios de diseño, incrementa los vectores por los que un atacante puede realizar campañas de phishing o suplantación de identidad. La información contextual que cada plataforma aporta, como roles, relaciones y proyectos, al combinarse facilita la creación de mensajes dirigidos y creíbles.

Falta de anonimización y trazabilidad: El uso constante del mismo alias o de variaciones del nombre real (Gisbell Asanza) permite vincular actividades en ámbitos profesionales, personales y creativos. Esta continuidad en los identificadores digitales facilita rastrear la huella del usuario y reunir información que podría ser aprovechada en un ataque.

Ataques de ingeniería social: La existencia de múltiples perfiles que contienen fragmentos de información personal ofrece a los atacantes material suficiente para construir relatos verosímiles y dirigidos. Un suplantador puede, por ejemplo, presentarse como un colaborador en Trello o un contacto en LinkedIn, utilizar los datos visibles para generar confianza y engañar a la víctima.

5. PROCEDIMIENTO TÉCNICO

Prueba 1: Verificación de exposición en filtraciones públicas mediante Have I Been Pwned

Objetivo: Determinar si la dirección de correo electrónico analizada ha sido comprometida en brechas de datos conocidas, identificando los servicios afectados, la naturaleza de la información filtrada y los posibles riesgos asociados.

Procedimiento:

Ingresar al sitio web oficial: https://haveibeenpwned.com. En el campo de búsqueda, introducir la dirección de correo electrónico que será analizado.

Análisis de resultados: Observar si la cuenta ha sido parte de alguna brecha de datos, tomar nota de los servicios comprometidos y verificar los tipos de datos filtrados: correos, contraseñas, IPs, nombres, ubicaciones, etc.

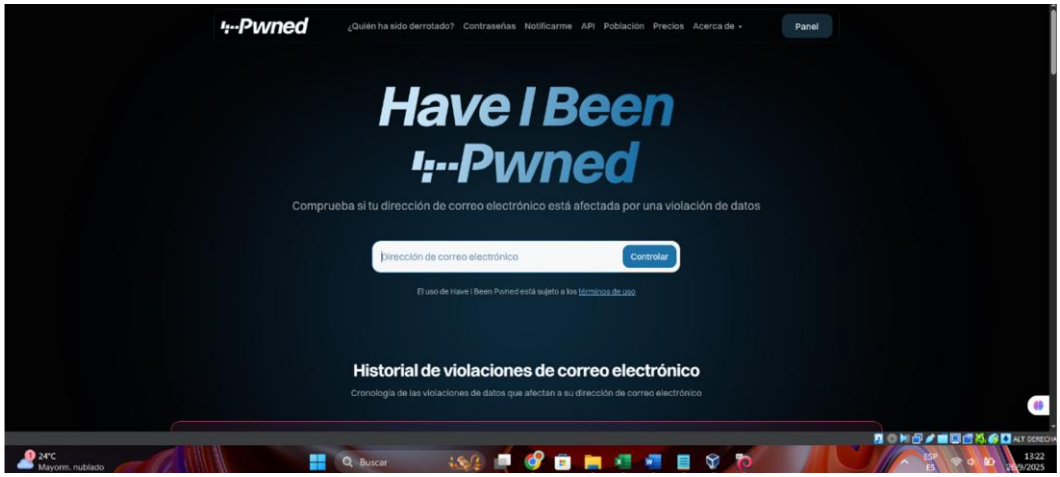


Figura 8: Página oficial de Have I Been Pwned.

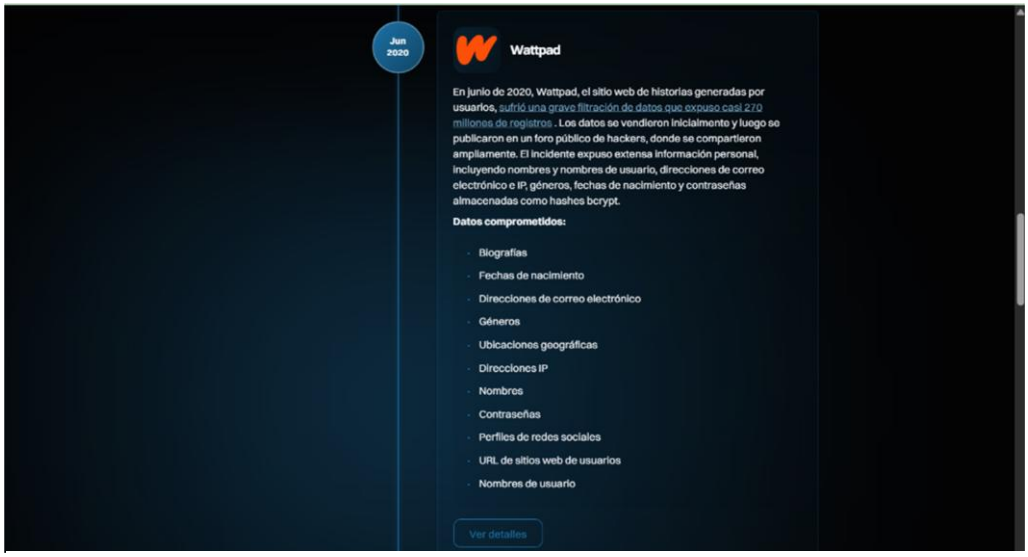
En los resultados obtenidos con la herramienta **Have I Been Pwned**, mostrados en la figura 9, se evidencia que la cuenta de correo analizada estuvo involucrada en **cuatro violaciones de datos**. Este hallazgo indica que la dirección fue comprometida en distintas brechas, exponiendo información como nombres, direcciones IP y contraseñas cifradas. Las filtraciones ocurrieron en diferentes plataformas, reflejando una exposición continua de datos personales en el entorno digital.

Figura 9: Resultado de búsqueda en Have I Been Pwned.

En enero de 2024, se extrajeron datos de Trello y se publicaron para su venta en un foro popular de *hackers*. Esta exposición incluyó más de 15 millones de direcciones de correo electrónico, junto con nombres y nombres de usuario.

Figura 10: Detalles de filtración de datos de Trello.

En junio de 2020, Wattpad sufrió una grave filtración que expuso hasta 270 millones de registros. Los datos comprometidos fueron extensos, incluyendo direcciones de correo electrónico, contraseñas almacenadas como *hashes* Bcrypt, biografías, fechas de nacimiento, géneros, ubicaciones IP y perfiles de redes sociales. La información permite crear perfiles detallados del usuario, lo que facilita ataques personalizados.



Figuras 11: Detalles de filtración de datos de Wattpad.

En el caso de Canva, la brecha ocurrió en mayo de 2019 y afectó a 137 millones de usuarios, exponiendo direcciones de correo electrónico, nombres, ubicaciones, contraseñas cifradas con Bcrypt y nombres de usuario. Además, el registro indica que parte de esta información fue publicada en foros de la red, lo que amplió su difusión y aumentó el riesgo de reutilización de credenciales en otros servicios. Este tipo de exposición prolongada facilita que los datos comprometidos sean incorporados en nuevas bases de filtraciones, incrementando su disponibilidad para actividades ilícitas y la probabilidad de intentos de acceso no autorizado en otras plataformas.

Figura 12: Detalles de la filtración de 137 millones de cuentas de Canva.

Aunque la brecha de Dubsmash ocurrió en diciembre de 2018, fue revelada posteriormente. El incidente expuso 162 millones de registros, incluyendo direcciones de correo electrónico, nombres, contraseñas (con el *hash* PikbZF), números de teléfono, idiomas hablados y nombres de usuario. Esta exposición de datos puede usarse en fraudes o campañas de *phishing* dirigidas.

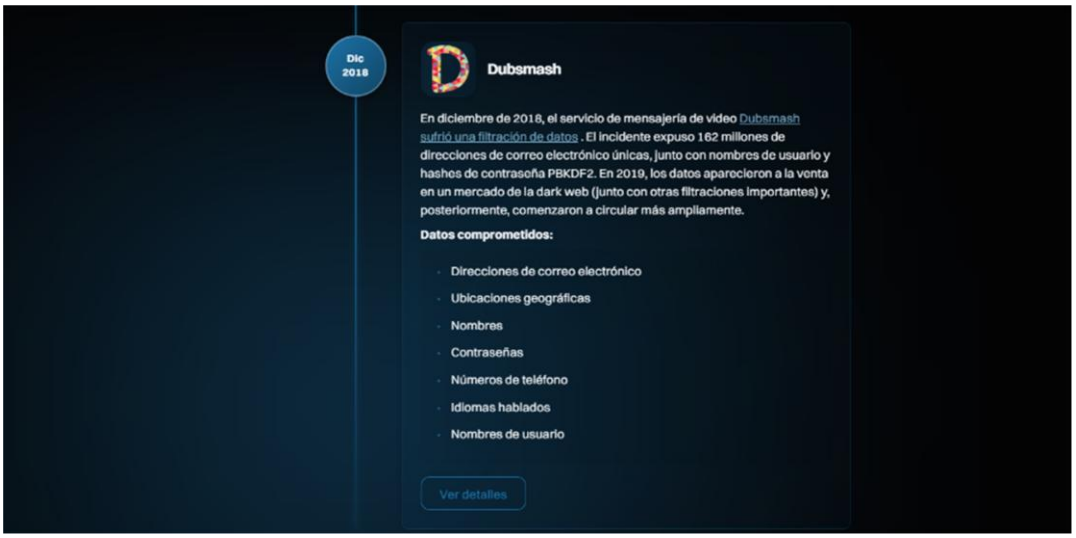


Figura 13: Detalles de filtración de datos de Dubsmash.

Verificación de exposición avanzada mediante DeHashed

Objetivo: Ampliar el análisis de exposición de un correo electrónico identificando coincidencias en bases de datos filtradas, nombres de usuario relacionados, contraseñas antiguas o reutilizadas, direcciones IP y otros datos vinculados. Acceder al portal de búsqueda DeHashed: https://www.dehashed.com e ingresar la dirección de correo electrónico en el campo de búsqueda. Verificar los resultados obtenidos: revisar coincidencias en registros filtrados y los tipos de datos expuestos**.**

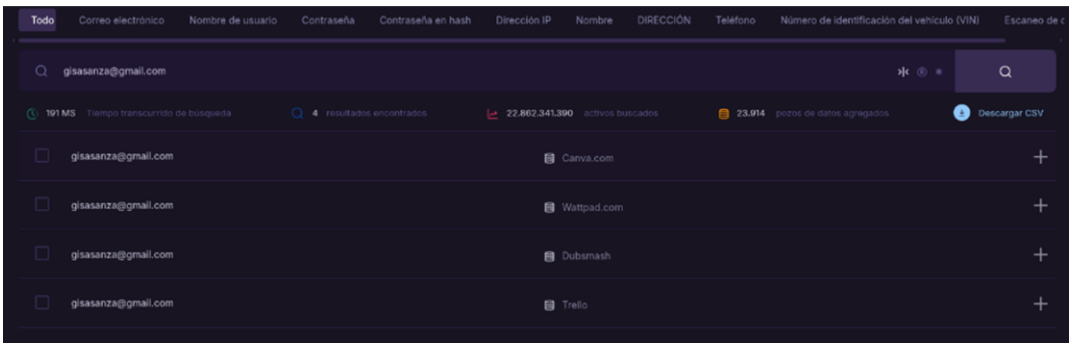


Figura 14: Resultado de búsqueda de exposición de datos en DeHashed.

DeHashed identificó múltiples coincidencias relacionadas con la cuenta analizada, como direcciones de correo, nombres de usuario y contraseñas en formato hash. En la figura se observa parte de esta información visible en la interfaz de resultados, aunque el acceso a los detalles completos requiere una suscripción al servicio. Esta evidencia confirma la exposición del correo en bases de datos filtradas y muestra cómo las plataformas especializadas pueden revelar información sensible proveniente de diferentes incidentes de seguridad.

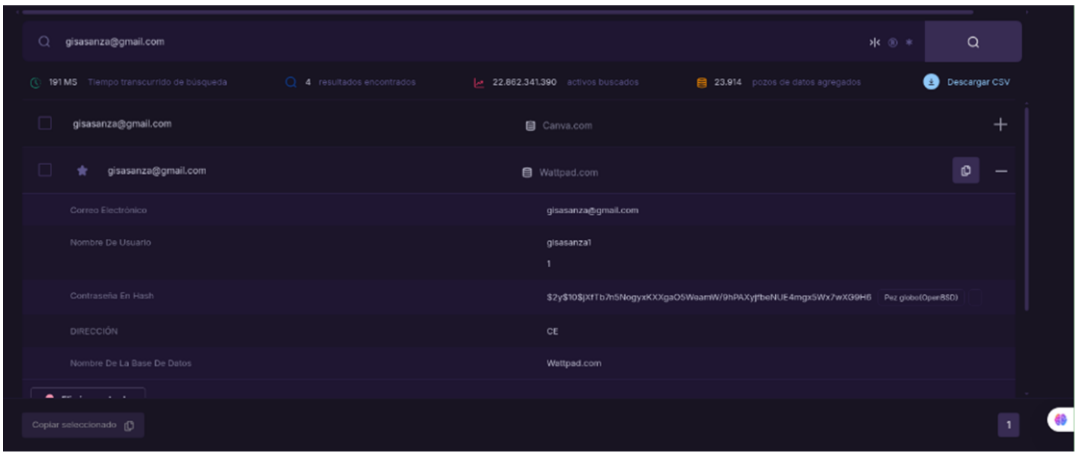


Figura 15: Información extraída por DeHashed.

.

Prueba 2: Reconocimiento de perfil público en el ecosistema Google con GHunt

Objetivo: Identificar información pública vinculada a una cuenta de Google a través de su dirección de correo, con el fin de evaluar el nivel de exposición del usuario en servicios como Google Calendar, Google Maps, YouTube, Google Photos o Google Chat.

Proceso de instalación de Ghunt

Para preparar el entorno en Kali Linux se ejecuta el comando sudo apt update && sudo apt install git python3 python3-pip python3-venv -y, que actualiza el sistema e instala Git y las dependencias básicas de Python. Esto garantiza que el sistema cuente con las herramientas necesarias para clonar el repositorio de GHunt y gestionar correctamente los paquetes en un entorno virtual, evitando conflictos con otros proyectos y asegurando una instalación más estable.

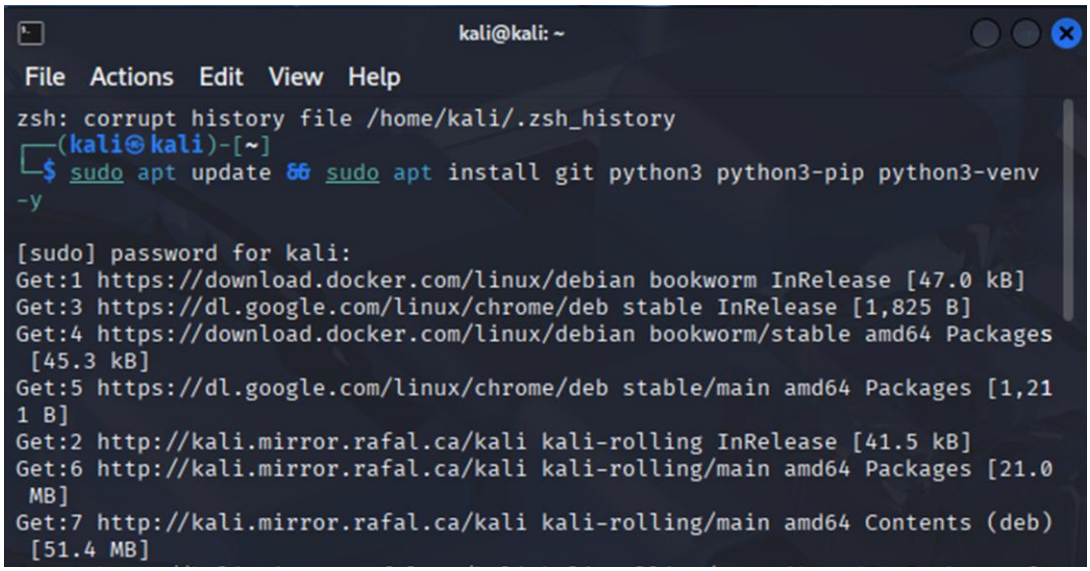


Figura 16: Actualización del sistema e instalación de Git y Python en la terminal de Kali Linux.

Se debe copiar el enlace de clonación de los archivos necesarios para el funcionamiento de GHunt desde su repositorio oficial en GitHub. Esto permite descargar el proyecto directamente en el equipo y acceder a todos sus componentes originales para realizar la instalación de forma correcta. Al clonar el repositorio, se obtiene una copia exacta del código fuente junto con sus dependencias y configuraciones iniciales. Este paso asegura trabajar con una versión actualizada y confiable de la herramienta, evitando errores causados por archivos modificados o versiones no oficiales. Finalmente, disponer de la fuente original facilita futuras actualizaciones o correcciones dentro del entorno de trabajo.

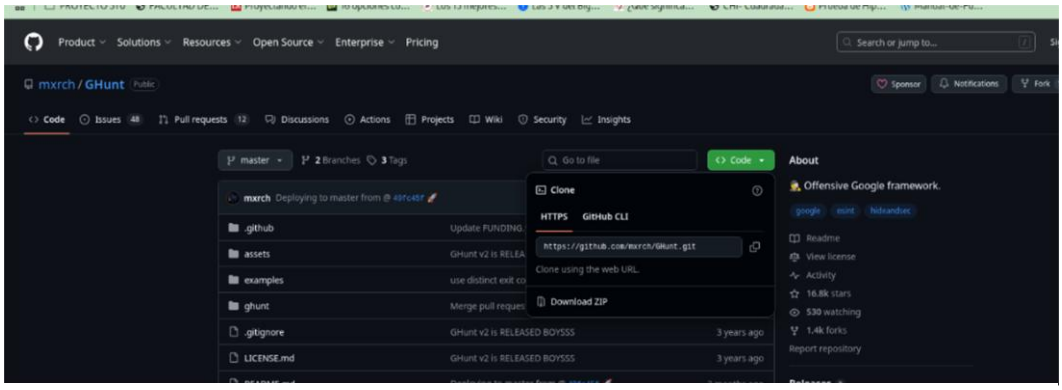


Figura 17: Repositorio oficial de GHunt en GitHub.

Realizar la clonación desde la terminal de Kali Linux y no dirigimos a la carpeta de Ghunt

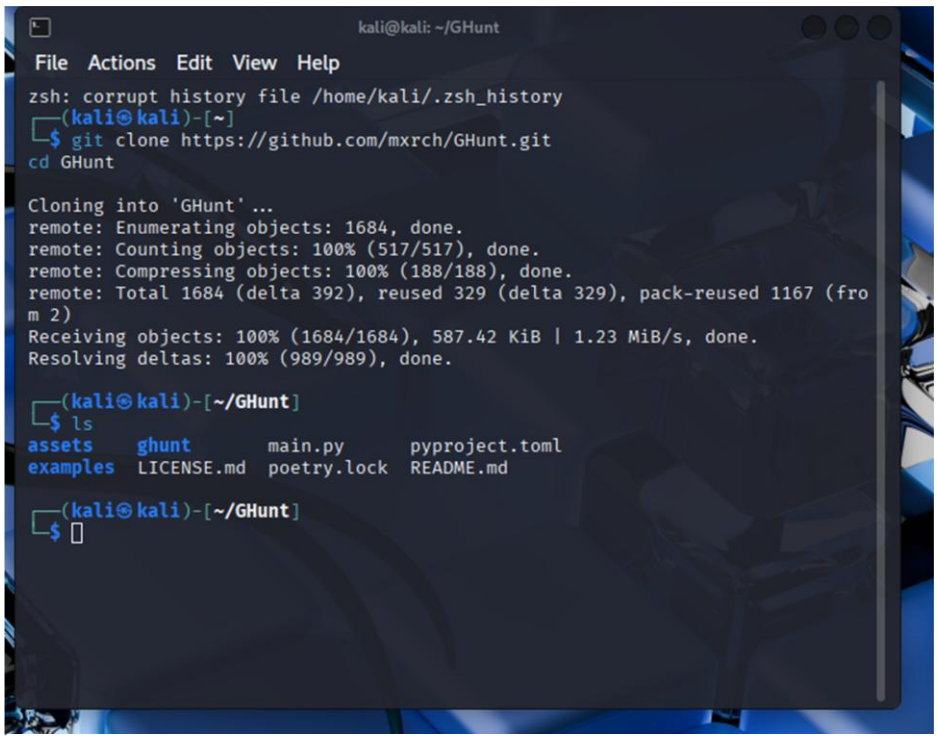


Figura 18: Clonación del repositorio de GHunt en Kali Linux.

Instalar Poetry, herramienta necesaria para gestionar e instalar las dependencias del proyecto GHunt de forma automática y en un entorno virtual aislado.

Figura19: Instalación de dependencias de Python para GHunt.

Una vez instalado Poetry y estando dentro del directorio del proyecto, es necesario sincronizar el archivo de dependencias de Poetry para asegurar que todas las versiones estén correctamente definidas. Para ello ejecutamos: poetry lock y procedemos con la instalación de las dependencias

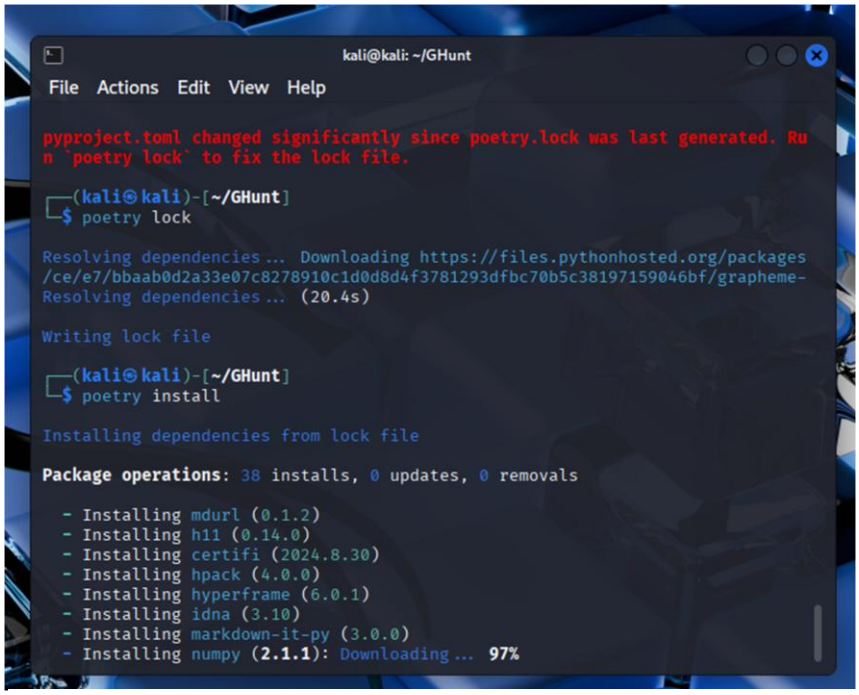


Figura 20: Instalación de dependencias de GHunt con Poetry.

Después de instalar las dependencias con Poetry, se debe activar el entorno virtual utilizando el comando:

source/home/kali/cache/pypoetry/virtualenvs/ghuntdfGbE8NUpy3.13/bin/activae.

Este proceso permite aislar las librerías del proyecto, garantizando que los paquetes y herramientas usados por GHunt no afecten el funcionamiento de otras aplicaciones del sistema.

Figura 21: Activación del entorno virtual de GHunt.

Si está todo está instalado correctamente iniciamos GHunt y nos aparecerá el menú de configuración.

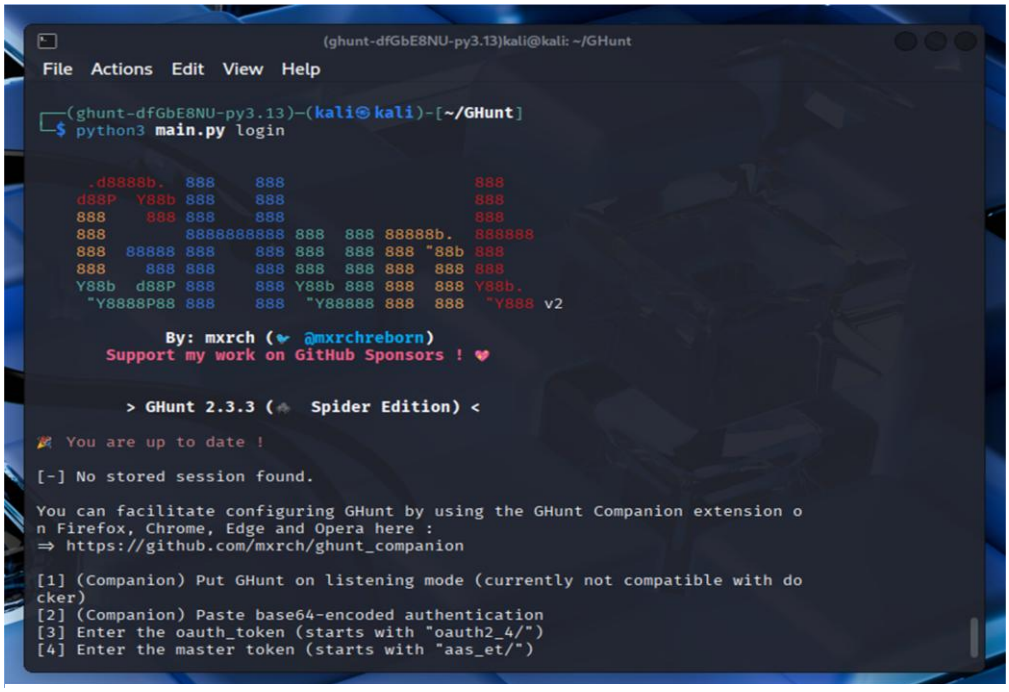


Figura 22: Lanzamiento y ejecución de la herramienta GHunt.

Nos dirigimos al menú de complementos de nuestro navegador Firefox, buscamos "GHunt Companion", añadimos y por último hacemos clic en la opción sincronizar con Ghunt. Una vez completado este paso, la herramienta queda vinculada al entorno de trabajo y lista para ejecutar las búsquedas de información asociadas a cuentas de Google.

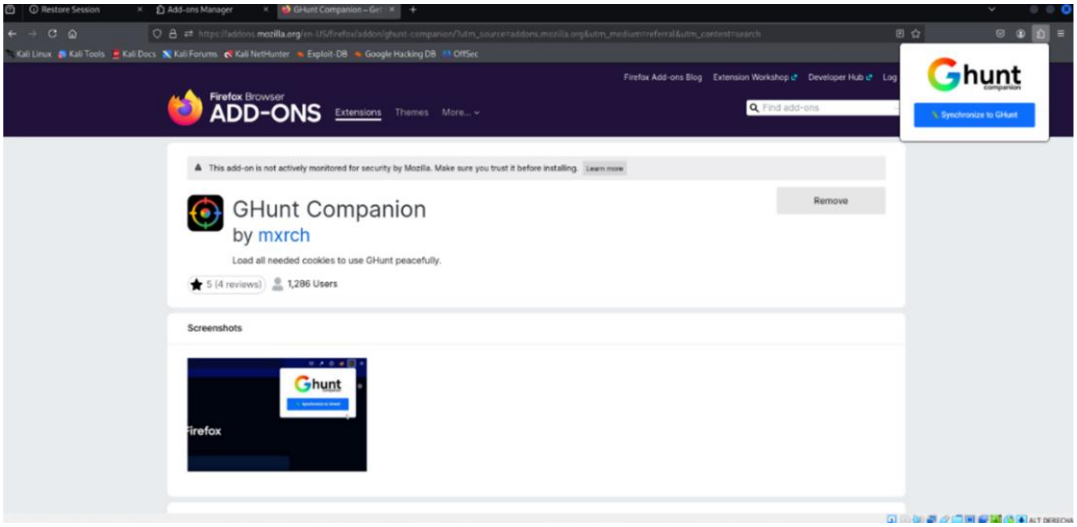


Figura 23: Instalación de la extensión GHunt Companion en Firefox.

Nos solicitará iniciar sesión con nuestras credenciales de Google

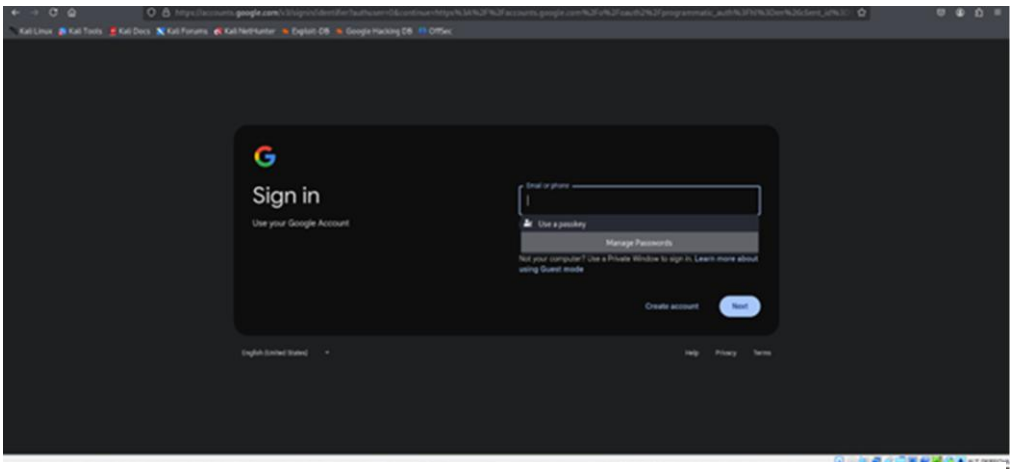


Figura 24: Autenticación en la cuenta de Google para el uso de GHunt.

Una vez verificado nuestras credenciales se abrirá el menú de opciones para sincronizarse con Ghunt desde el terminal de Kali Linux.

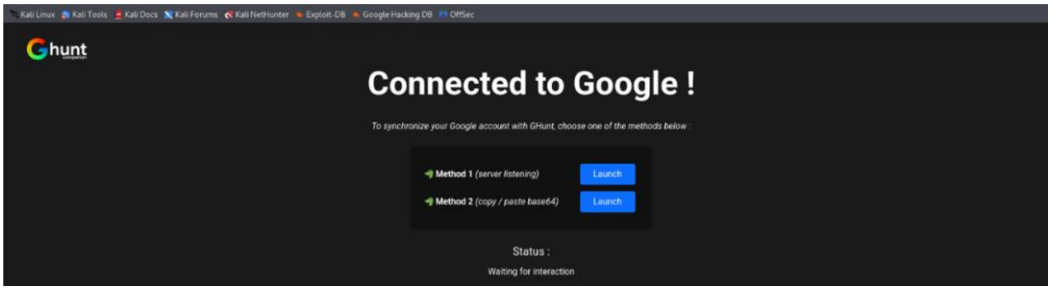


Figura 25: Sincronización de GHunt con la cuenta de Google.

En el terminal de Kali y en nuestro navegador, seleccionamos el método 1 para sincronizar GHunt con la extensión y establecer la conexión necesaria para la captura automática de tokens.

Figura 26: Sincronización de GHunt desde la terminal.

Una vez sincronizados, GHunt estará listo para investigar cualquier correo electrónico que pertenezca a dominios compatibles, como Gmail.

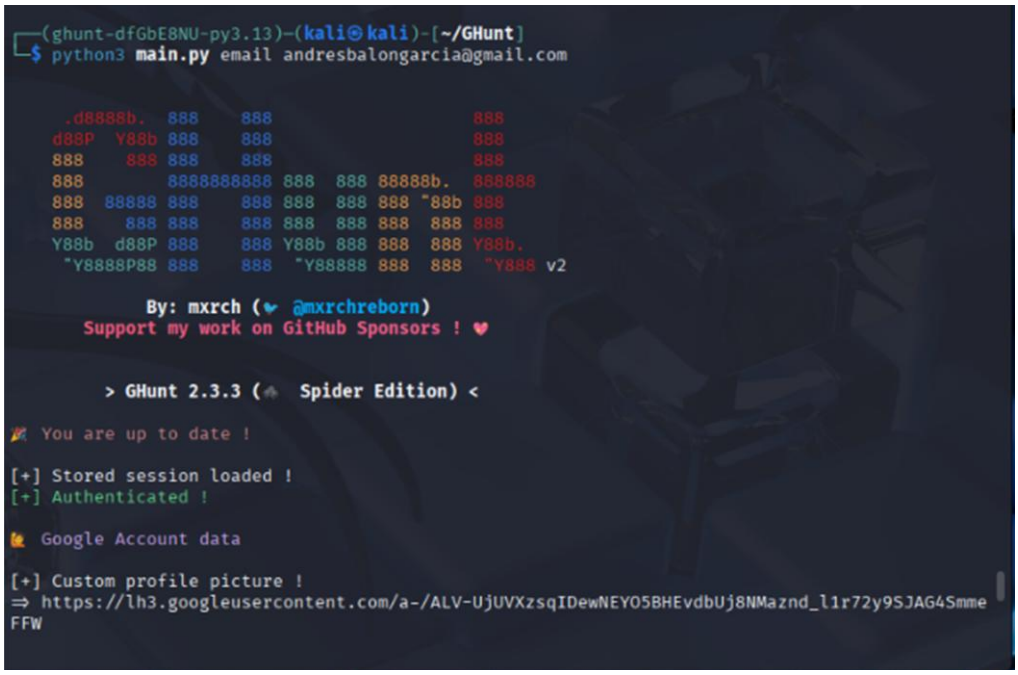


Figura 27: Uso de GHunt para recopilar información de una cuenta de Google.

Las imágenes muestran la información recolectada mediante GHunt sobre una cuenta de Google. Incluyen datos como el nombre del propietario, la foto de perfil pública, los servicios de Google activos (como YouTube o Meet), y el identificador único (Gaia ID). Esta información permite confirmar que el correo está vinculado a una cuenta activa dentro del ecosistema Google.

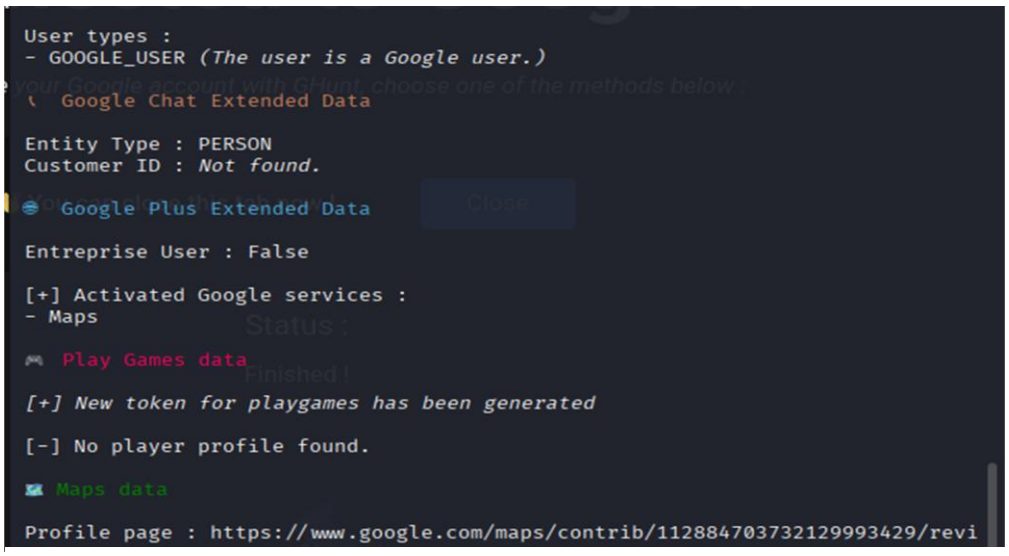


Figura 28: Resultados del escaneo de GHunt en una cuenta de Google.

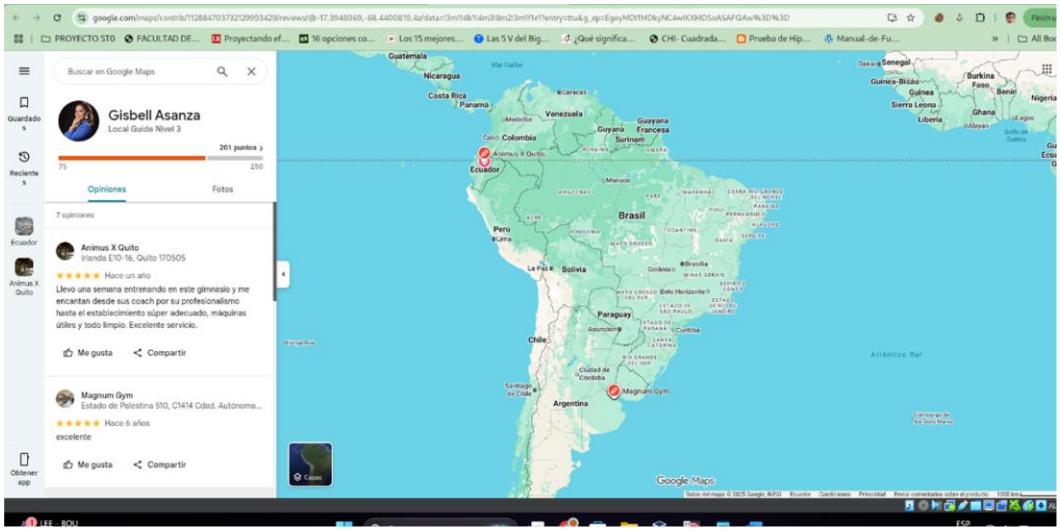


Figura 29: Hallazgo de geolocalización y opiniones en Google Maps.

Prueba 3: Identificación de perfiles públicos mediante Social Analyzer y usersearch

Instalación de social analyzer

Clonar los ficheros desde el repositorio oficial de github clonación de ficheros desde el repositorio oficial de GitHub de **Social Analyzer** (https://github.com/qeeqbox/social-analyzer) permite obtener el código fuente más actualizado del proyecto directamente desde su fuente original. Este proceso garantiza la integridad del software y facilita su instalación, personalización y uso en entornos locales para realizar análisis de perfiles y búsqueda de información en diversas plataformas digitales.

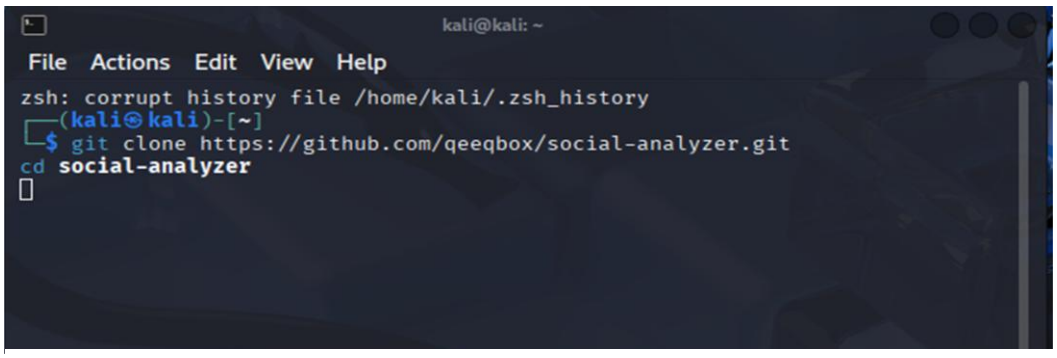


Figura 30: Clonando el repositorio de Social-Analyzer en la terminal de Kali Linux.

Instalar Docker Compose que permite definir y ejecutar aplicaciones complejas en múltiples contenedores utilizando un archivo docker-compose.yml, facilitando la instalación y despliegue de herramientas como Social-Analyzer.

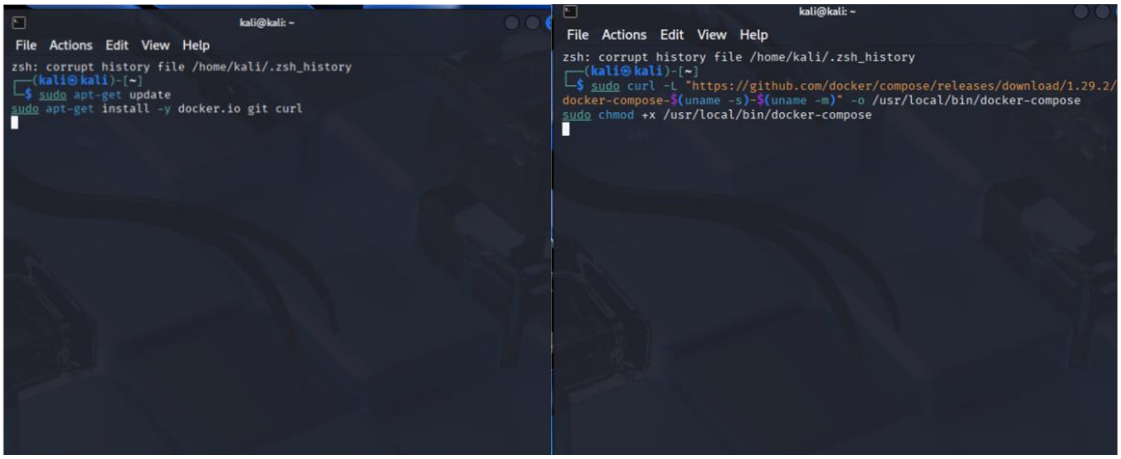


Figura 31: Configuración de docker y docker compose en Kali Linux.

Una vez instalado, ejecutar Docker compose dentro de la carpeta social-analyzer con el comando sudo docker compose up

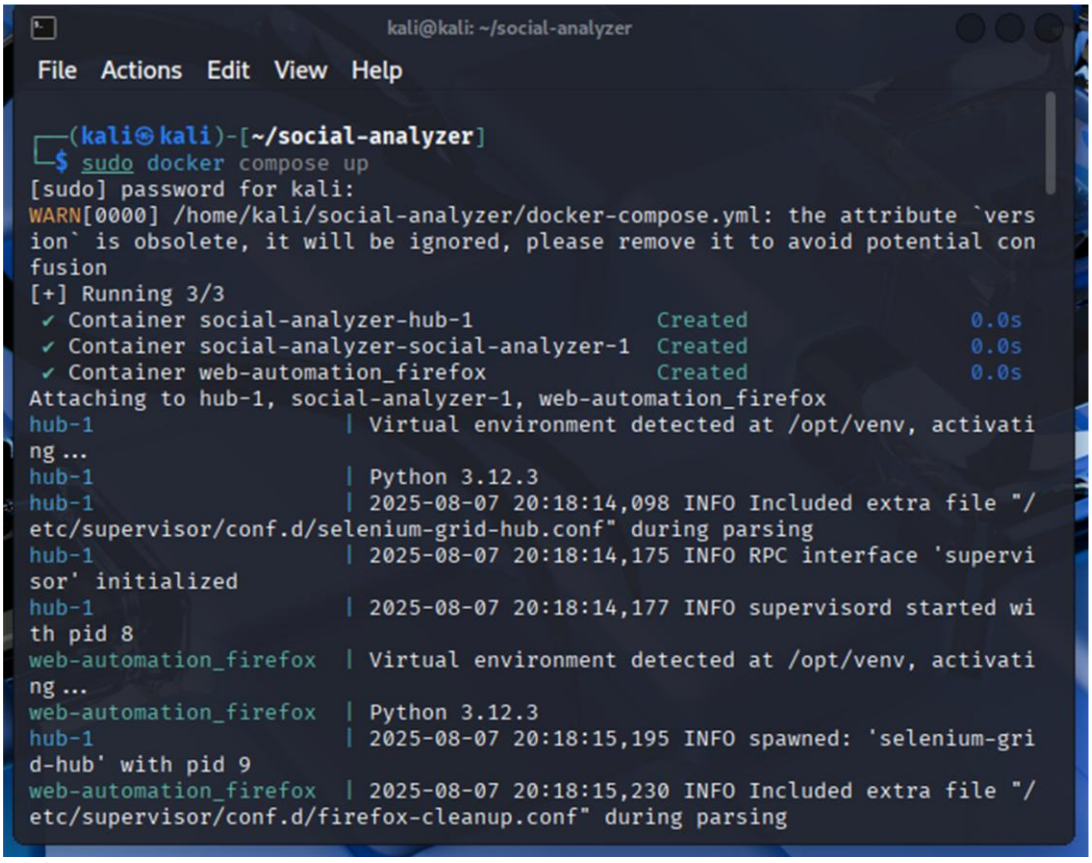


Figura 32: Iniciando el servicio de Social-Analyzer con Docker Compose.

Después de ejecutar sudo docker compose up, esperamos a que se inicien todos los contenedores. Luego, desde el navegador, accedemos a la dirección http://localhost:9005/app.html para utilizar la herramienta desde su panel web, luego ingresamos el username para su respectivo escaneo.

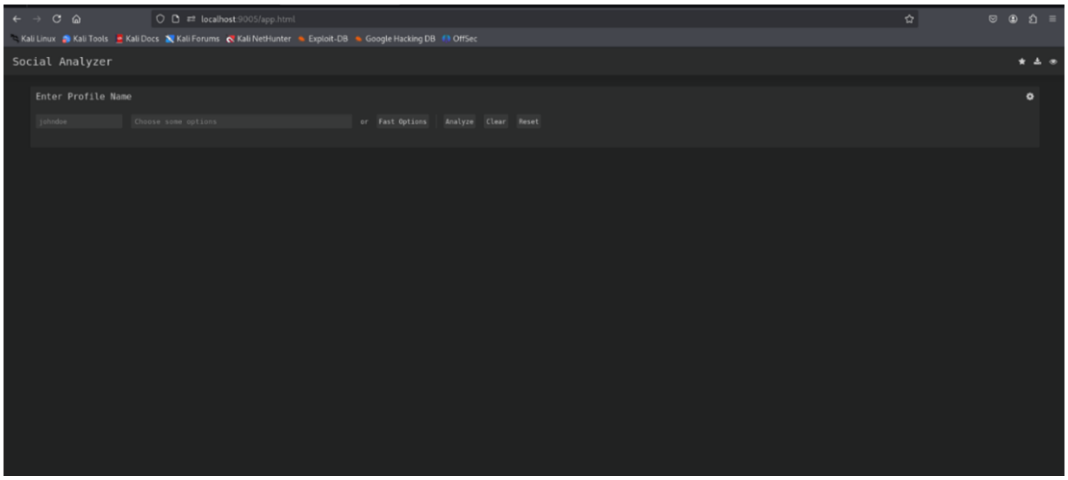


Figura 33: Interfaz de la herramienta Social-Analyzer lista para analizar un perfil.

Social Analyzer detectó un uso constante del mismo alias en distintas plataformas. Se identificaron cuentas activas en TikTok y Pinterest registradas a nombre de Gisbell Asanza, junto con un enlace vinculado a Telegram. Además, se hallaron coincidencias de usuario en Facebook, Instagram, Twitter y Reddit, lo que evidencia una presencia amplia y sostenida en diversas redes sociales, posiblemente bajo la misma identidad digital.

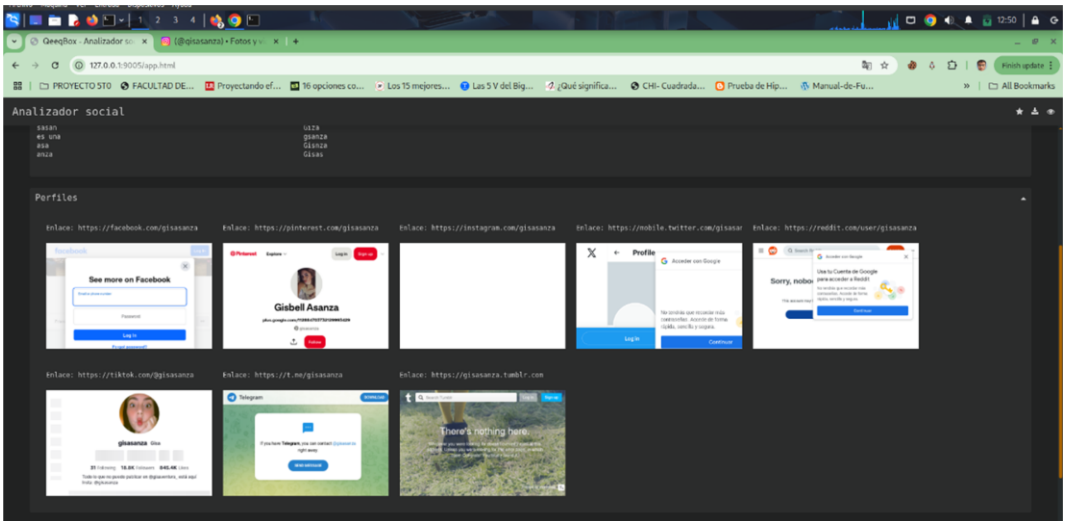


Figura 34: Resultados del análisis de perfiles en redes sociales con Social-Analyzer.

Búsqueda con Usersearch.ai

Ingresar al panel de UserSearch.AI y selecciona el tipo de búsqueda “Correo electrónico”. En el campo de consulta se introduce el correo objetivo y se verifica el saldo de créditos disponibles antes de ejecutar la búsqueda.

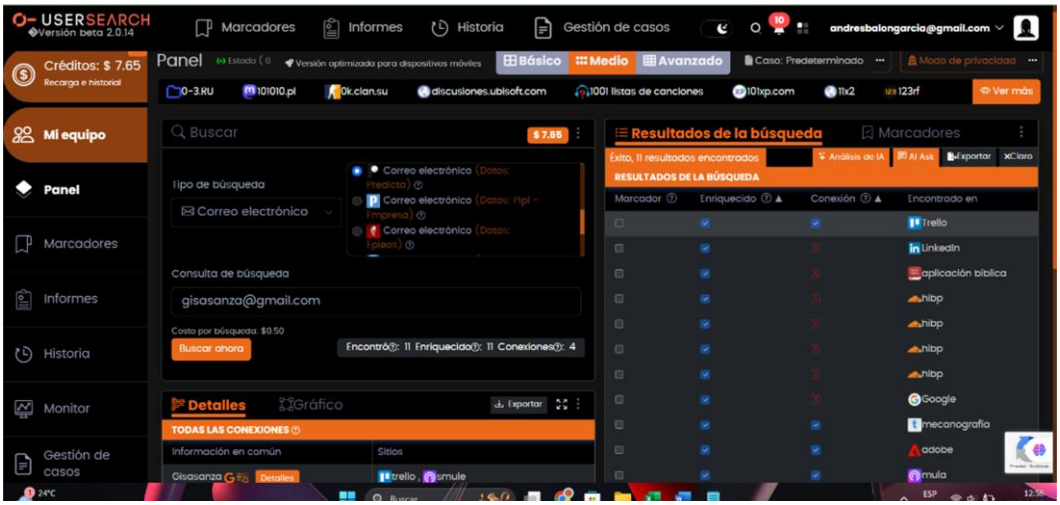


Figura 35: Inicio del proceso OSINT de búsqueda por email en Usersearch.

La plataforma descuenta créditos y muestra un resumen con las coincidencias encontradas tras el análisis. Los resultados iniciales incluyen actividad vinculada a servicios como Google, LinkedIn, Adobe y Microsoft, visibles en la sección de resultados generales. Además, se pueden observar detalles adicionales como la fecha de detección, el tipo de dato encontrado y la posible relación con otras cuentas asociadas, lo que facilita un análisis más completo del perfil digital.

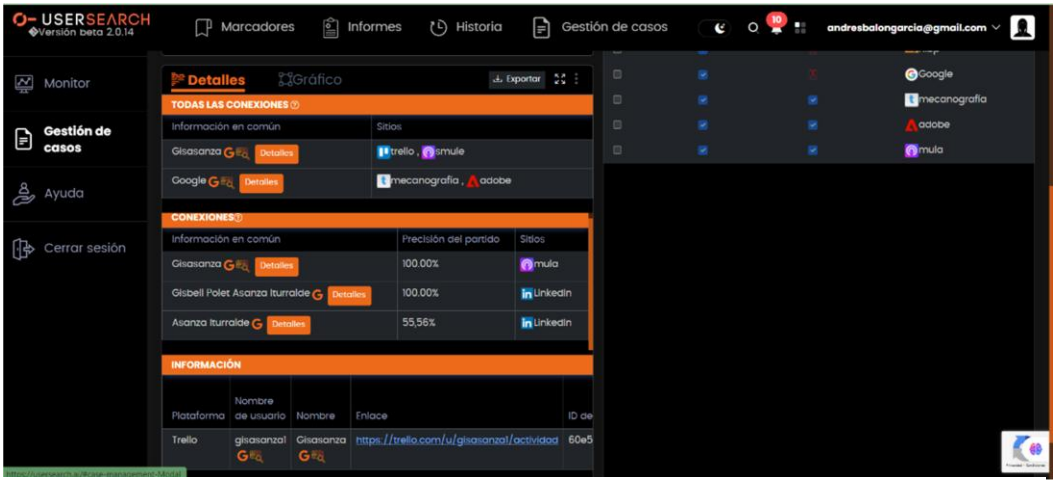


Figura 36: Análisis de Conexiones Digitales Encontradas por Email en Usersearch.ai.

En el panel “Detalles” se revisan coincidencias exactas asociadas al correo, como un usuario en Trello y perfiles de LinkedIn, con precisión del 100%. Además, se muestra información complementaria como nombre de usuario, plataforma y enlace directo de cada hallazgo.

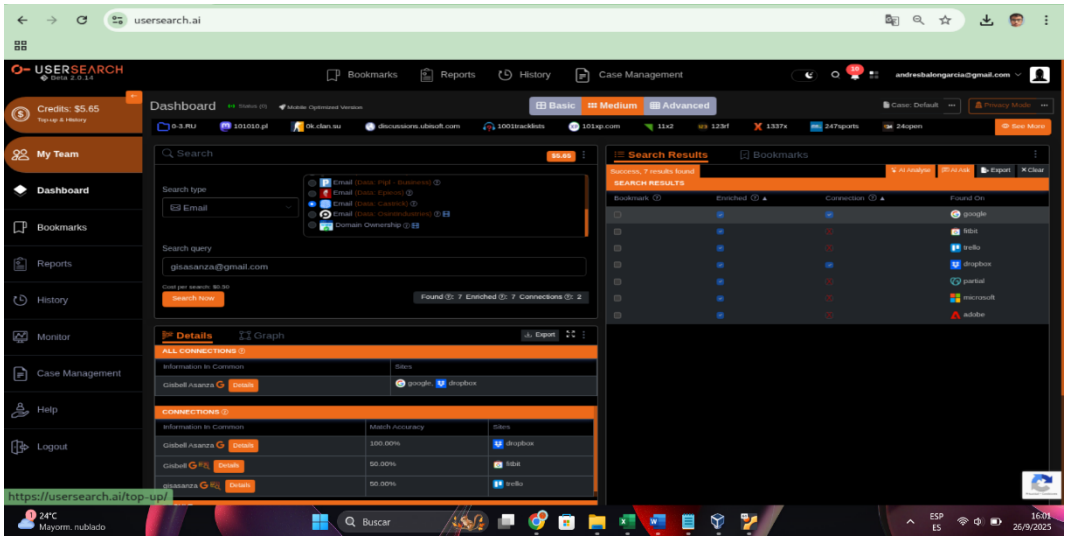


Figura 37: Resultados de coincidencias en UserSearch.ai asociados a un correo electrónico

Anexo 2: Evaluación de riesgos por exposición de datos personales en una entidad privada

• OBJETIVOS

Analizar los riesgos derivados de la exposición de datos personales en entidades privadas mediante técnicas OSINT y herramientas de ciberinteligencia, evaluando las vulnerabilidades presentes en plataformas tecnológicas y su posible impacto en la seguridad de la información.

1. RECURSOS NECESARIOS

- Computadora
- Kali Linux
- Spiderfoot
- Hunter io
- Dehashed
- Maltego
- Investigator
- Deep Research (Gemini)

2. ESCENARIO DEL CASO

Escenario – Exposición de datos y servicios en una entidad financiera

Contexto: La entidad analizada es una de las instituciones financieras más grandes y consolidadas del Ecuador, con una trayectoria que la ha posicionado como un referente en el sector bancario. Ofrece una amplia variedad de productos y servicios tanto para clientes individuales como corporativos, lo que la convierte en un actor importante dentro del sistema financiero nacional. Su funcionamiento depende de una infraestructura tecnológica que soporta millones de transacciones diarias y administra información sensible de gran valor. Las plataformas digitales son un medio esencial para la interacción con los usuarios, ya que permiten realizar operaciones en línea y recibir atención de manera ágil. Por el volumen de datos que maneja y la importancia de sus procesos, resulta necesario mantener medidas de seguridad que aseguren la protección de la información y la continuidad de las operaciones.

Problema: Durante la revisión de la infraestructura digital de la entidad se identificaron exposiciones que representan un riesgo para la seguridad de la información. Se encontraron correos institucionales relacionados con empleados y directivos que aparecían en brechas de datos que fueron expuestos, y direcciones filtradas en fugas previas. Además, se detectó la exposición temporal de información sensible en un bucket público de Amazon S3 que incluía datos personales y financieros. Estos incidentes, de no ser gestionados oportunamente, pueden facilitar ataques de phishing, suplantación de identidad o fraude, lo que compromete tanto la operación interna como la confianza de clientes y empleados.

3. RESOLUCIÓN

Incidente 1: Identificación de correos institucionales expuestos

Hallazgos:

Durante la fase de recolección de información mediante Hunter.io y SpiderFoot**,** se identificaron un total de 68 direcciones de correo electrónico relacionadas con la entidad:

- **59 correos institucionales** pertenecientes a empleados y directivos del banco.
- **9 correos genéricos** (ejemplo: soporte@, info@, contacto@) vinculados a servicios internos y atención al cliente.

Muchos de estos correos estaban acompañados de información sensible como:

- Nombre completo del empleado.
- Cargo o área de trabajo.
- Teléfono interno o de oficina.
- Enlaces a fuentes públicas donde aparecían mencionados.

Riesgos e implicaciones:

Phishing y suplantación de identidad: La exposición de correos institucionales junto con datos de identificación personal permite elaborar campañas de phishing dirigidas contra el personal o los clientes.

Ingeniería social: La información asociada facilita ataques de manipulación, donde un actor malintencionado puede hacerse pasar por un empleado o directivo para solicitar información o accesos.

Afectación reputacional: El uso indebido de correos corporativos puede generar desconfianza en los canales oficiales de la entidad y deteriorar la imagen institucional.

Incremento de contacto no deseado: La publicación de estos datos puede provocar un aumento de correos fraudulentos y llamadas no solicitadas a empleados y usuarios.

Incidente 2 – Exposición de correos institucionales filtrados en brechas

A través de herramientas como: Maltego y DeHashed se identificaron múltiples direcciones de correo institucional de la entidad privada que han estado involucradas en filtraciones de datos previas.

Por ejemplo:

csf@[redacted] (1 fuga reportada)
jalmeida@[redacted] (3 fugas reportadas)

aenderica@[redacted] (4 fugas reportadas)
cjimenez@[redacted] (4 fugas reportadas)
kherrera1@[redacted] (1 fuga reportada)

Riesgos e implicaciones

Phishing y spear phishing: Las direcciones filtradas pueden emplearse en campañas de engaño selectivo contra el personal de la entidad o sus clientes. **Credential stuffing:** La reutilización de contraseñas comprometidas posibilita intentos de acceso no autorizado a sistemas internos o externos. **Ingeniería social corporativa:** Al conocerse nombres y cargos, los atacantes pueden construir perfiles creíbles para suplantar identidades dentro de la organización.

Riesgo persistente: Aunque muchas contraseñas estaban cifradas, la información filtrada (nombres, teléfonos y correos) sigue circulando en repositorios y foros, manteniendo vigente la amenaza de nuevos intentos de ataque.

Incidente 3 – Exposición temporal de datos en Amazon S3

Con la ayuda de la herramienta Investigator, se identificó temporalmente información sensible publicada por un tercero en una página web externa, relacionada con la entidad financiera. Entre los datos expuestos se encontraba una cuenta bancaria, acompañada de información de contacto como correo electrónico y número telefónico.

Aunque el banco no fue responsable de esta publicación, el hallazgo ilustra cómo incluso datos de terceros vinculados a la institución pueden representar un riesgo de ingeniería social y phishing. La página fue retirada posteriormente, pero el incidente evidencia la importancia de considerar el ecosistema digital completo de la organización al realizar análisis de ciberamenazas y ciberinteligencia defensiva. Entre la información encontrada se incluían:

- Número de cuenta bancaria.
- Nombre completo del titular.
- Número de identificación personal.
- Correo electrónico y número telefónico de contacto.

Riesgos e implicaciones:

Fraude financiero e identidad: La filtración de datos bancarios y personales permite la ejecución de fraudes, robo de identidad o creación de perfiles falsos. **Phishing avanzado:** Los atacantes pueden aprovechar la información real para diseñar mensajes altamente creíbles dirigidos a clientes o empleados.

Extorsión y exposición pública: La disponibilidad de datos financieros sensibles incrementa el riesgo de chantaje o divulgación maliciosa.

Daño reputacional: Aun cuando el incidente provino de un tercero, la asociación de los datos con la entidad afecta su credibilidad y confianza ante el público.

4. PROCEDIMIENTO TÉCNICO

Prueba 1: Identificación de correos institucionales expuestos

A) Recolección de correos con hunter io

Una vez dentro de la plataforma, se puede utilizar la función **"Finder"** para buscar direcciones de correo electrónico asociadas a un dominio específico. Esta herramienta permite identificar contactos corporativos visibles en sitios web o registros públicos, lo que facilita analizar posibles vectores de riesgo y exposición de datos laborales. Los resultados obtenidos deben revisarse con criterio ético y únicamente con fines de evaluación de seguridad, evitando el uso indebido de la información recolectada.

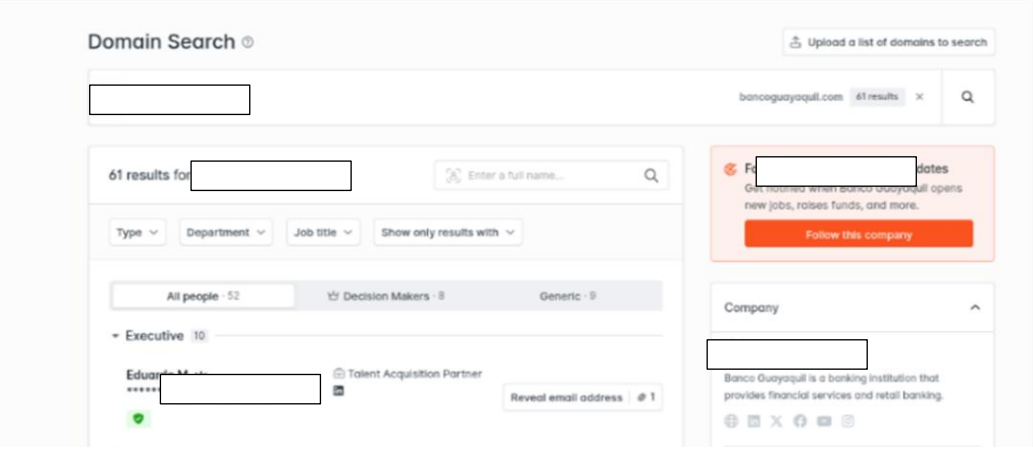


Figura 38: Resultados de la búsqueda de correos electrónicos por dominio usando Hunter.io

Enumerar todos los correos electrónicos encontrados, indicando además las diferentes direcciones o fuentes en las que fueron localizados.

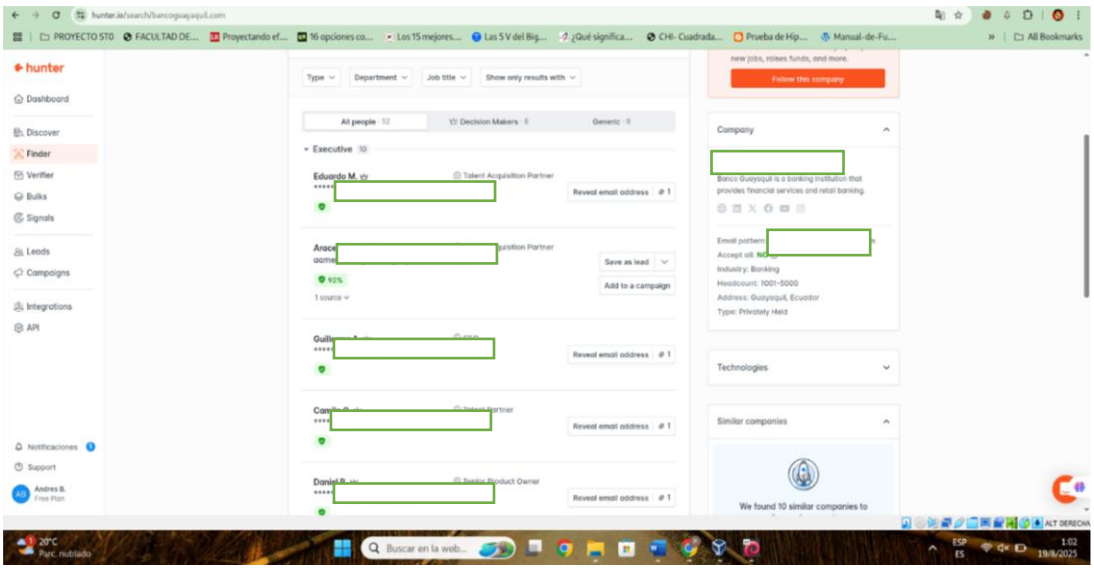


Figura 39: Vista detallada de los correos electrónicos obtenidos por hunter.io

La mayoría de estos correos se encuentran en la plataforma LinkedIn, donde además es posible acceder a información más detallada, como títulos universitarios, cargos laborales y especialidades profesionales. En varios perfiles también se observan vínculos hacia otros espacios digitales, como páginas institucionales o redes de contacto, lo que amplía la visibilidad pública de los empleados y permite establecer relaciones entre distintos entornos profesionales asociados a la entidad.

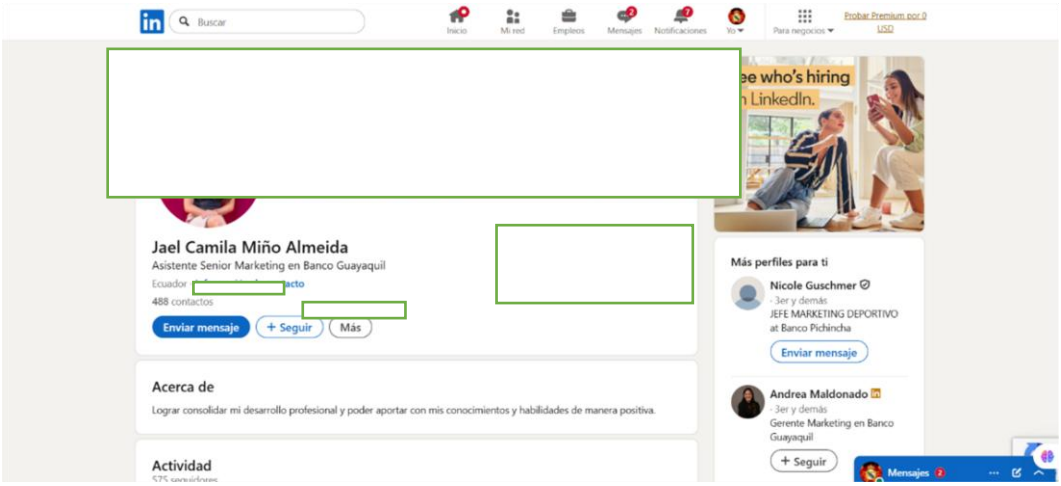


Figura 40: Perfil de un empleado en una red social profesional

Adicionalmente, algunos de estos correos también pueden localizarse en blogs personales o en páginas web corporativas, lo que amplía la exposición de datos y facilita la obtención de un perfil más completo de los usuarios

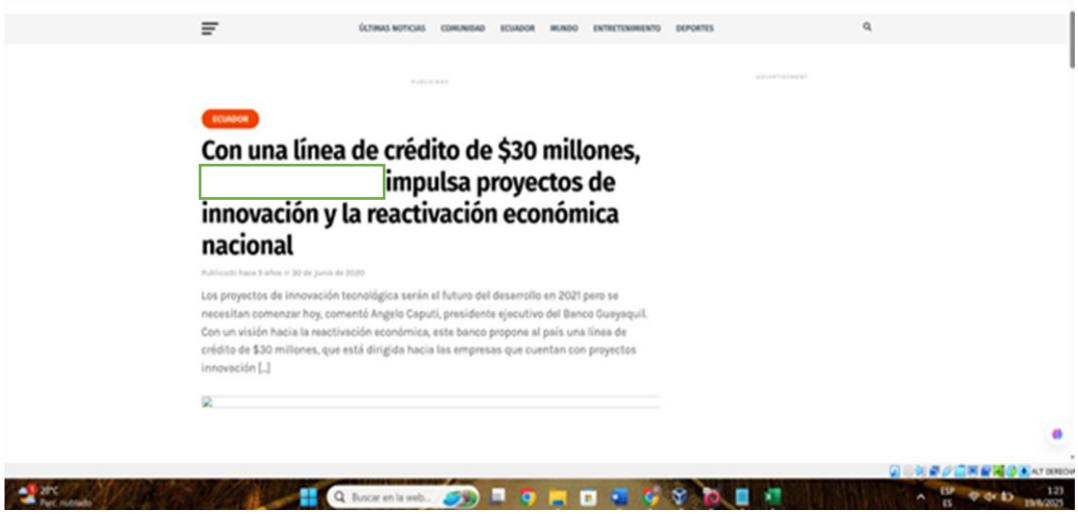


Figura 41: Recopilación de información de fuentes abiertas como artículo de noticias y otros sitios web

Posteriormente, se debe enumerar en un archivo .csv todos los correos electrónicos localizados, asociándolos con la información complementaria disponible, como nombres, apellidos, cargos y números telefónicos en caso de estar disponibles, para su respectivo análisis.

B) Recolección con spiderfoot

Iniciar Inicie Kali Linux, abra una terminal y ejecute el comando: *spiderfoot -l 127.0.0.1:5001* para arrancar la herramienta SpiderFoot. Este proceso habilita la interfaz web en el puerto 5001 de la dirección local. Luego, abra un navegador y acceda al enlace *http://127.0.0.1:5001* para interactuar con la plataforma y realizar los análisis correspondientes.

SpiderFoot es una herramienta de automatización OSINT que permite recopilar información de diversas fuentes públicas. A través de su interfaz web, el usuario puede configurar escaneos personalizados, definir objetivos específicos y seleccionar los módulos de análisis más adecuados. Además es una de las herramientas, la cual viene preinstalada en el entorno virtual de Kali Linux.

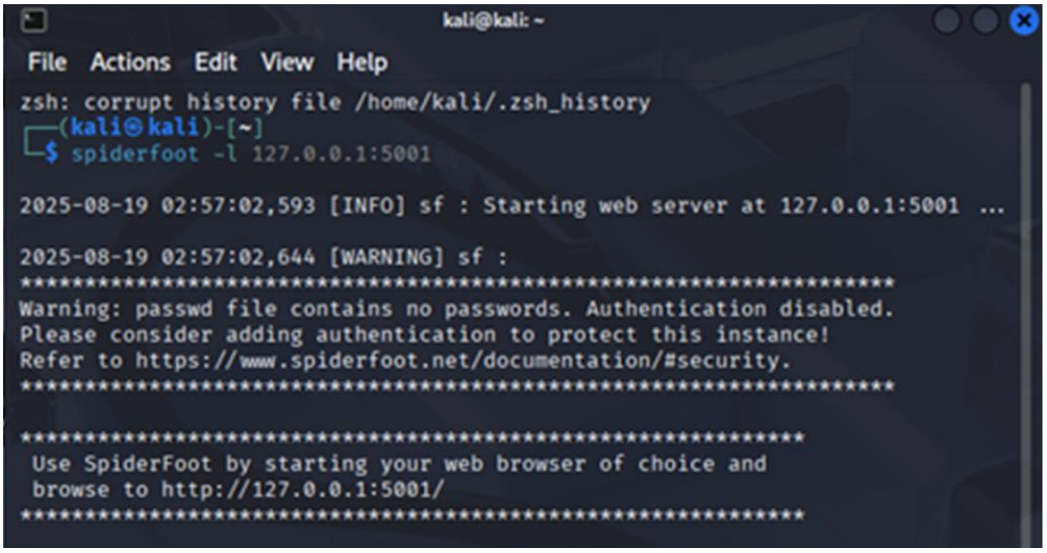


Figura 42: Iniciando el servidor web de SpiderFoot en la terminal de Kali

Al iniciar un nuevo escaneo, la herramienta ofrece cuatro modalidades: All, Footprint, Investigate y Passive. Para este caso, se seleccionó la opción Footprint, ya que permite obtener una visión general del perímetro de red del objetivo, identificar identidades asociadas y recopilar diversa información mediante el rastreo web y la consulta en motores de búsqueda especializados. Esta modalidad resulta especialmente útil en las primeras fases de reconocimiento, ya que brinda una panorámica completa del entorno digital del objetivo y facilita la detección de posibles vínculos o activos expuestos que pueden ser analizados con mayor profundidad en etapas posteriores.

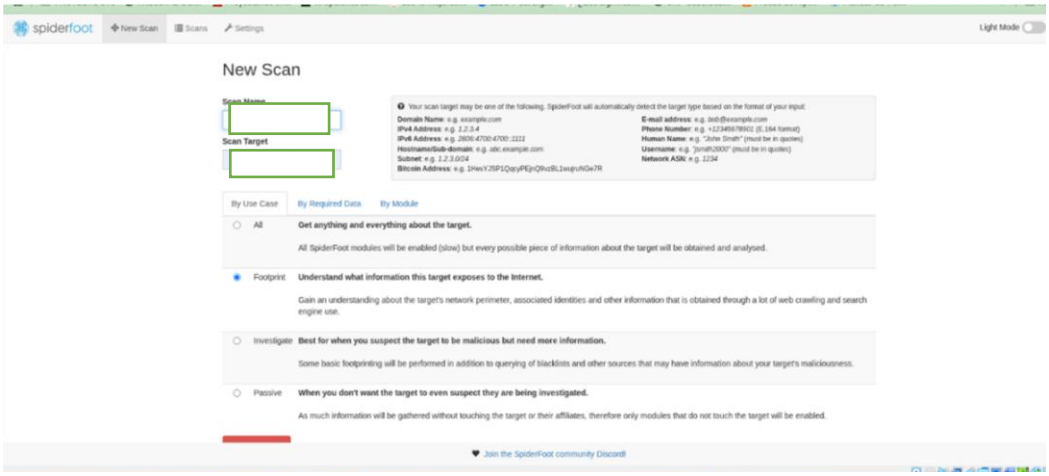


Figura 43: Configuración de un nuevo escaneo de un dominio con SpiderFoot

Luego se seleccionan los datos requeridos dentro de SpiderFoot, priorizando aquellos relacionados con la exposición de información personal y corporativa tal como se observa en la Figura 44. En este caso, se eligieron principalmente correos electrónicos, nombres, cargos y números telefónicos para identificar posibles filtraciones vinculadas a empleados y directivos. Adicionalmente, se incluyeron dominios, registros DNS, direcciones IP y tecnologías web asociadas a la entidad, con el fin de evaluar la superficie de ataque y detectar riesgos de suplantación o phishing. Finalmente, se consideraron datos sobre brechas de seguridad, fugas en sitios de filtración y exposición en buckets públicos, ya que estos representan un factor crítico en la protección de la información sensible.

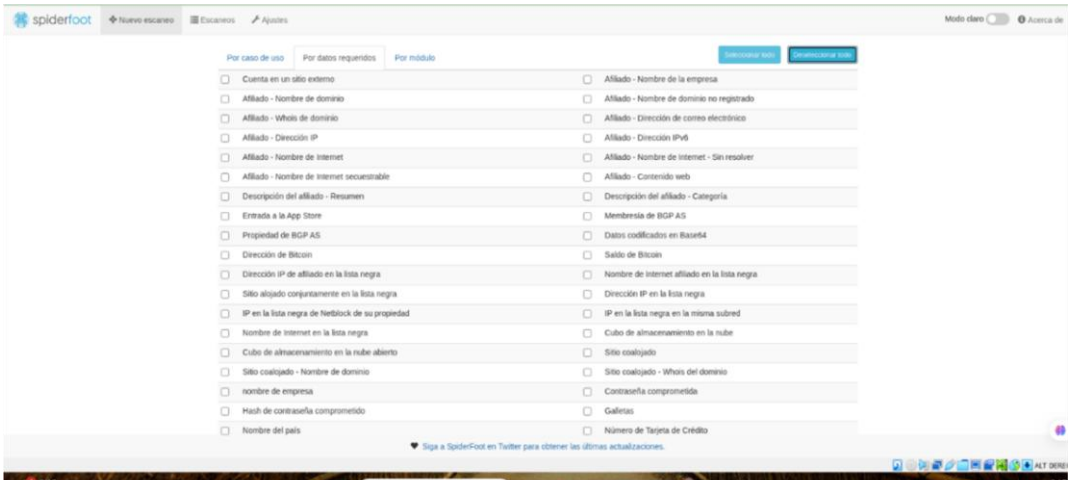


Figura 44: Lista de tipo de datos para un escaneo en SpiderFoot

Luego se eligen los módulos que se muestran en la figura 45, seleccionando de manera precisa aquellos que resultan más relevantes para la investigación. En esta etapa se debe priorizar la obtención de información personal como correos electrónicos, números de teléfono, nombres y cargos de empleados, así como datos técnicos relacionados con la organización, tales como direcciones IP, dominios, registros DNS y tecnologías utilizadas en los servidores.

También es importante incluir fuentes que permitan detectar posibles filtraciones de datos, brechas de seguridad o información expuesta en repositorios y sitios de filtración pública. Esta selección garantiza que el análisis posterior sea más enfocado y permita identificar vulnerabilidades reales en la superficie de ataque de la entidad evaluada.

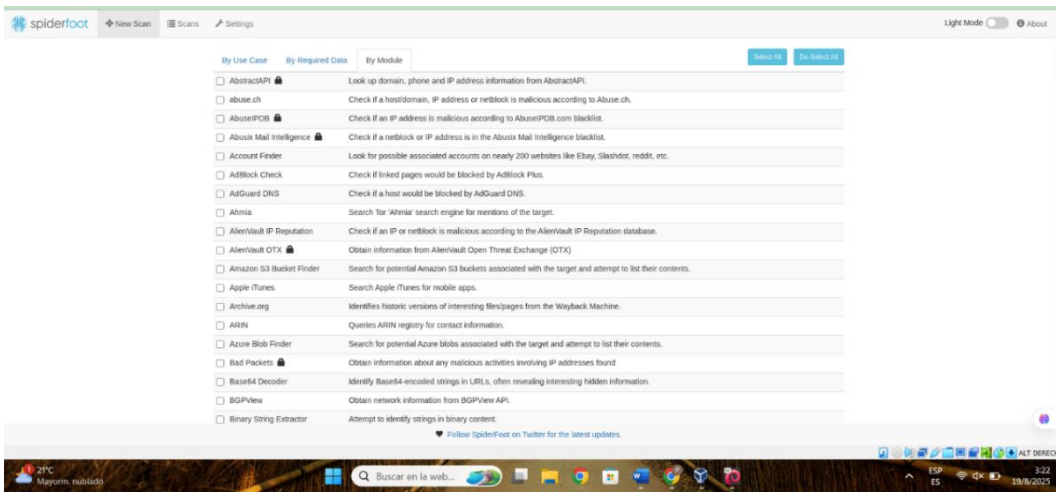


Figura 45: Lista de los módulos de escaneo de SpiderFoot

Una vez definidos los parámetros de recolección de datos, se procede a ejecutar el proceso mediante la opción Run Scan. En este punto, SpiderFoot inicia el escaneo automatizado conforme a las condiciones y fuentes previamente seleccionadas. El motor de búsqueda del framework comienza a correlacionar información desde múltiples orígenes (OSINT, bases de datos públicas, motores de búsqueda, registros DNS, servicios de reputación, etc.), generando en tiempo real hallazgos que van desde datos de contacto y credenciales expuestas hasta indicadores de compromiso o infraestructura asociada a la organización.

En este caso, el análisis se centrará únicamente en la recolección de información relevante para la investigación, priorizando datos sensibles como correos electrónicos, credenciales expuestas u otros elementos asociados a la entidad evaluada. Al completarse el escaneo, los resultados quedan centralizados en el panel de análisis, donde es posible filtrar, clasificar y evaluar la información obtenida para determinar su nivel de criticidad y relevancia frente a la superficie de ataque.

Durante el escaneo se identificaron relaciones entre dominios y correos institucionales vinculados, lo que ayudó a detectar posibles puntos de exposición. Esta función facilita el análisis de riesgos y complementa el trabajo con otras herramientas OSINT. En conjunto, el proceso demuestra la utilidad de SpiderFoot en la evaluación inicial de la seguridad digital.

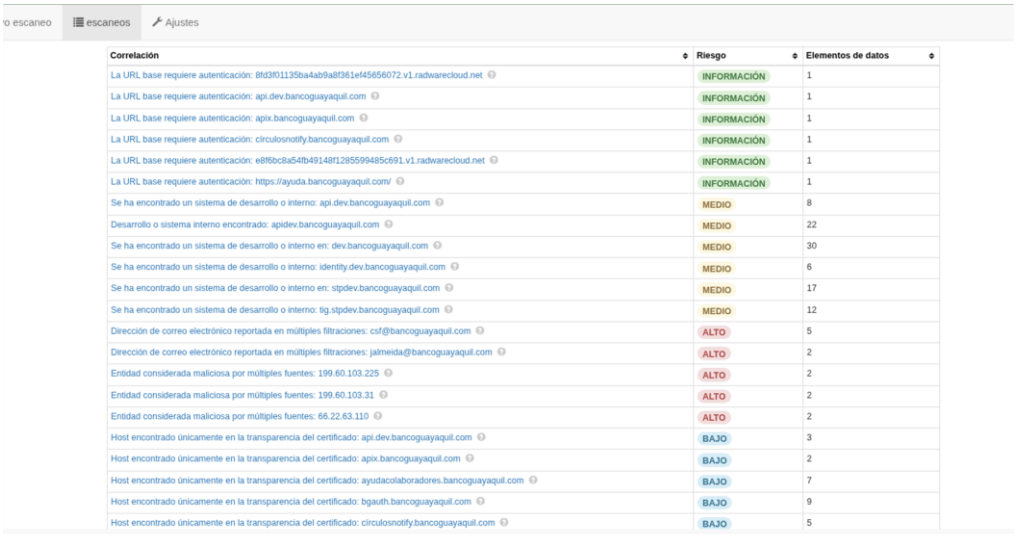


Figura 46: Resultados del análisis de seguridad de un dominio en SpiderFoot

Los correos electrónicos identificados en los resultados del escaneo serán extraídos y organizados de manera estructurada. Posteriormente, se enlistarán en el archivo CSV previamente creado, lo que permitirá mantener un registro centralizado y ordenado. Esta exportación facilita el análisis posterior, ya que los correos quedan almacenados en un formato compatible con otras herramientas de ciberinteligencia, permitiendo correlacionar información, detectar posibles patrones y evaluar riesgos de exposición de datos sensibles.

Prueba 2: Búsqueda de información con la ayuda de Deep Research – Gemini

Esta prueba consistió en la utilización del asistente Gemini con la función *Deep Research* para evaluar su capacidad en la recopilación y análisis automatizado de información pública disponible en fuentes abiertas. El objetivo fue determinar la precisión, pertinencia y profundidad de los resultados obtenidos frente a técnicas tradicionales de OSINT.

La herramienta permitió generar un informe sobre un perfil de riesgo, consolidando información reputacional y profesional obtenida de fuentes verificables. Se observó un buen nivel de contextualización en las respuestas, aunque dependiente de la claridad de las instrucciones y del acceso a información pública. La prueba evidenció el potencial de la inteligencia artificial aplicada al análisis OSINT.

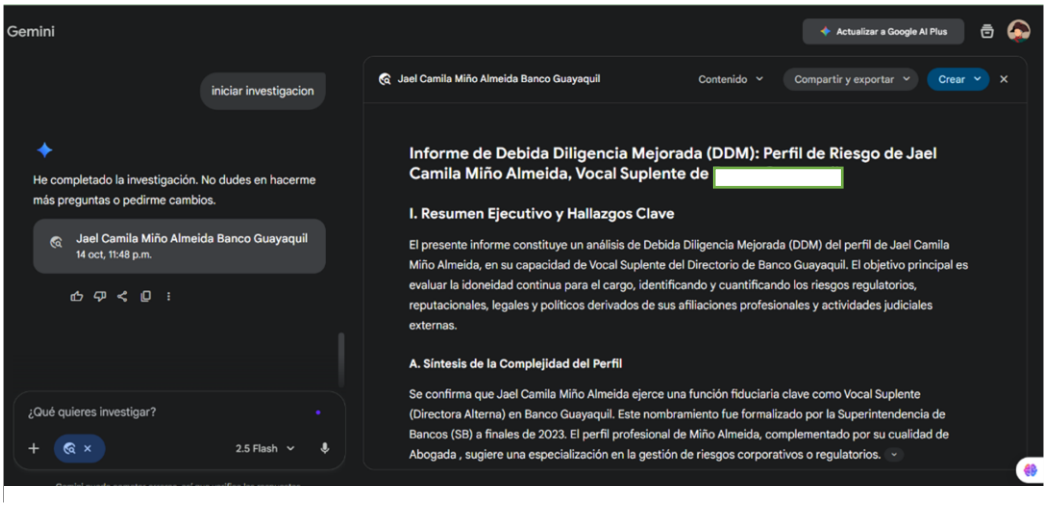


Figura 47: Evidencia de la búsqueda automatizada con Deep Research – Gemini

Prueba 3: Exposición de correos institucionales filtrados en brechas

Una vez preparado el archivo CSV con los correos institucionales, se importó la lista en Maltego para su análisis. El objetivo fue verificar si dichas direcciones habían sido expuestas previamente. Se eligió Maltego como herramienta, ya que permite analizar los datos de manera conjunta, evitando la necesidad de revisar cada correo de forma individual.

A) Maltego – Inserción masiva de correos + Transformación HIBP

Abrir Maltego CE/XL en Kali Linux. El primer paso consiste en ejecutar Maltego desde Kali Linux. Esta herramienta viene preinstalada en la distribución, por lo que basta con buscarla en el menú de aplicaciones o iniciarla desde la terminal con el comando maltego. Una vez abierta, el sistema solicitará iniciar sesión o crear una cuenta para acceder a las funciones principales. Tras completar este proceso, se mostrará la interfaz de trabajo donde se pueden crear nuevos gráficos y comenzar con el análisis de relaciones entre entidades.

Al iniciarse, la plataforma cargará el entorno gráfico donde se realizan los análisis, permitiendo trabajar con grafos y aplicar transformaciones sobre entidades.En caso de requerir una actualización de la herramienta, se recomienda ejecutar los siguientes comandos en la terminal:

sudo apt update, sudo apt install --only-upgrade maltego.

Crear un nuevo Graph en blanco. Una vez dentro de la aplicación, se procede a crear un nuevo grafo en blanco. Este espacio servirá como área de trabajo donde se insertarán los correos institucionales y se aplicarán las transformaciones necesarias. El grafo es esencial, ya que organiza la información de manera visual, facilitando la identificación de relaciones y patrones entre los datos importados.

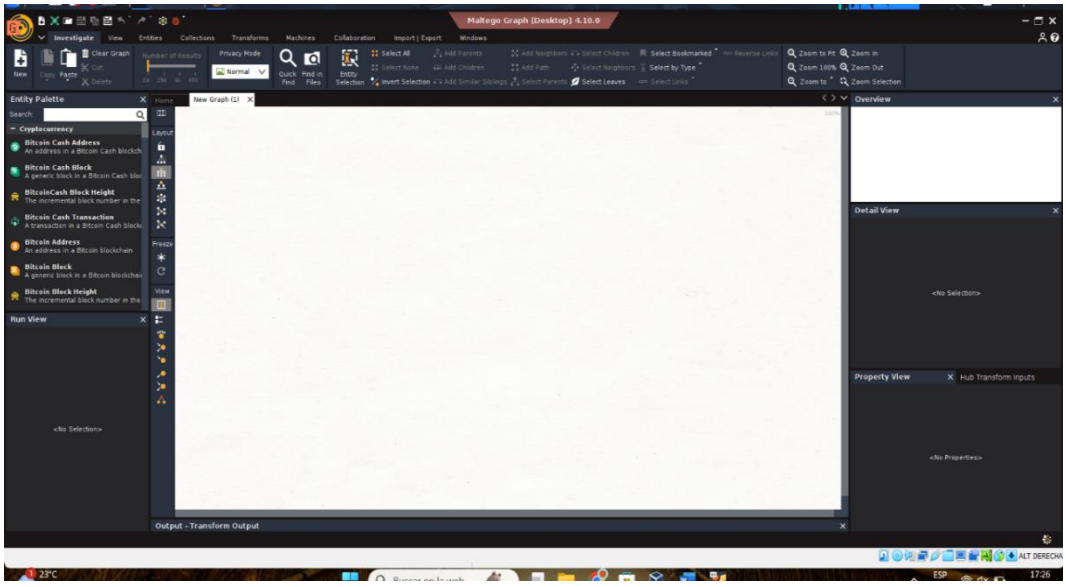


Figura 48: Interfaz de Maltego lista para comenzar un nuevo análisis OSINT

Importar todos los correos recolectados previamente con Hunter.io y SpiderFoot. Para trabajar de forma más eficiente, en lugar de ingresar los correos electrónicos uno por uno, Maltego permite realizar una importación masiva desde un archivo CSV. Este procedimiento se inicia seleccionando la opción **Import → Import Graph** desde el menú principal y eligiendo el archivo previamente preparado con la lista de correos institucionales.

Una vez cargado el archivo, el asistente de importación (Graph Import Wizard) guía al usuario a través de varios pasos. Primero se selecciona el archivo de origen y se configuran las opciones de conectividad, definiendo si se desea importar solo entidades o también relaciones entre ellas. Generalmente, para este caso basta con importar las entidades de tipo **Email Address**.

En la sección **Mapping Configuration**, como se observa en la imagen, es necesario asignar la columna del archivo a un tipo de entidad. Para ello, se selecciona la

columna que contiene las direcciones de correo (Column1) y se configura como **Email Address**. Esto asegura que Maltego reconozca los registros como correos electrónicos válidos y habilite las transformaciones correspondientes.

Por último, después de configurar el mapeo, se procede a los ajustes finales en el asistente y se hace clic en **Finish**. El grafo se genera automáticamente con todas las direcciones de correo cargadas como entidades, listas para ejecutar transformaciones, como la conexión con la base de datos de Have I Been Pwned (HIBP). Este método es más rápido, consistente y reduce errores respecto a la inserción manual.

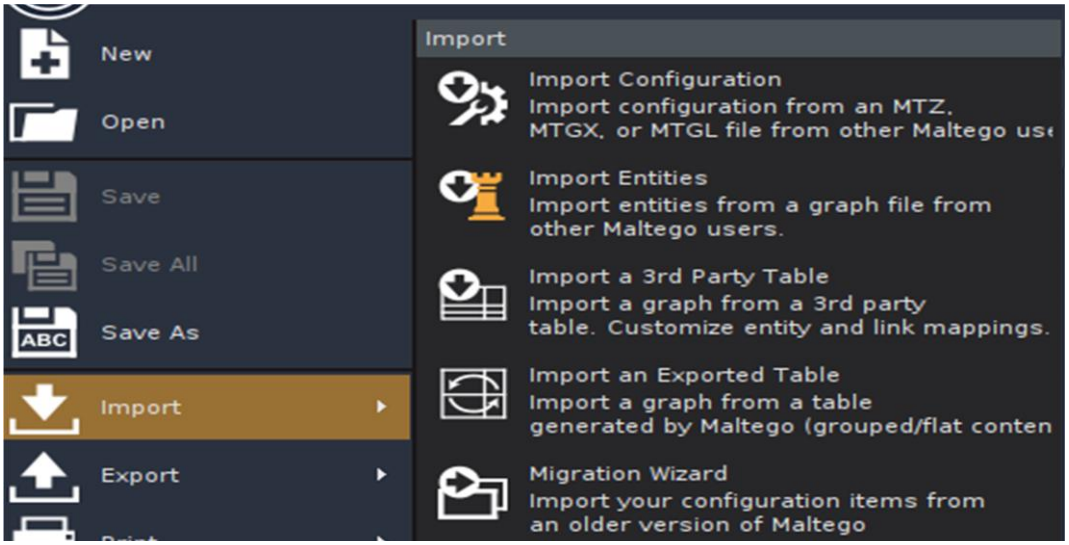


Figura 49: Menú de importación de datos en la herramienta de análisis Maltego.

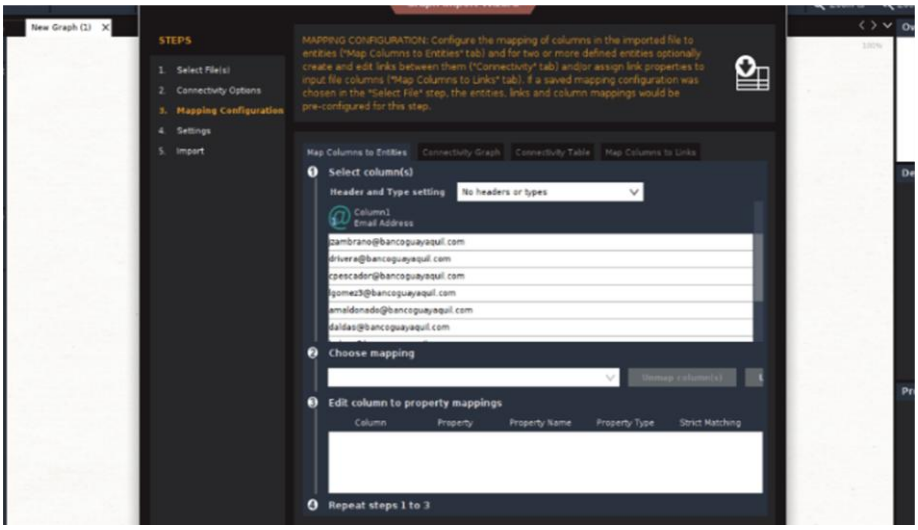


Figura 50: Configurando el mapeo de datos importados en Maltego

Una vez agregados los correos al grafo, seleccionarlos todos. Cuando se han cargado todas las entidades correspondientes a correos, se procede a seleccionarlas en su totalidad. Esto permite que la transformación que se ejecute posteriormente se aplique de manera masiva, evitando tener que ejecutar los procesos uno por uno. De esta forma, se optimiza el tiempo y se asegura uniformidad en el análisis.

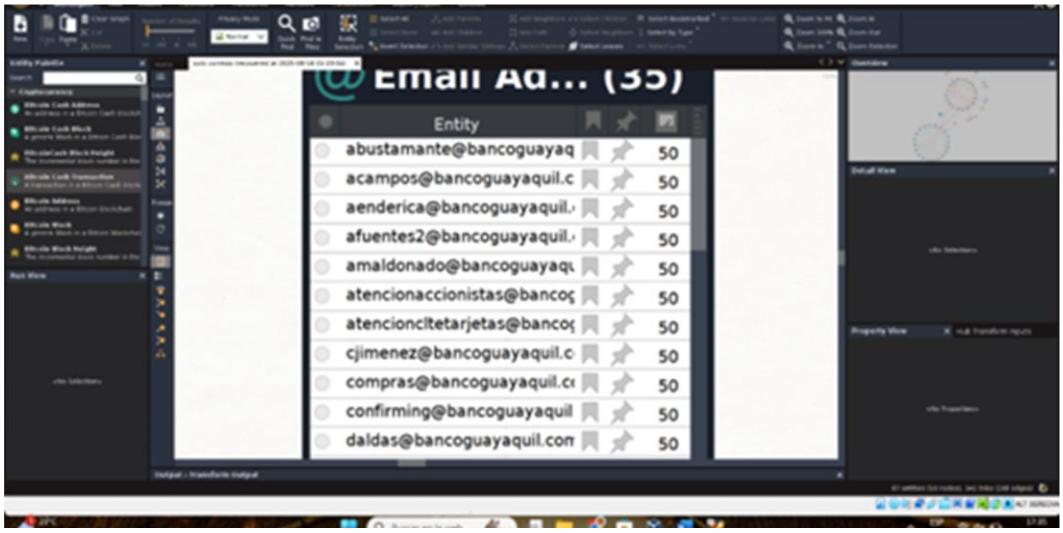


Figura 51: Visualización de correos electrónicos importados en Maltego

Ejecutar la transformación integrada de Have I Been Pwned (HIBP). Con las entidades seleccionadas, se accede al menú contextual y se elige: Run Transform → Email Address → To Breach (HIBP). Este módulo consulta la base de datos de Have I Been Pwned para comprobar si los correos han estado involucrados en filtraciones. Si es la primera ejecución, será necesario configurar una API Key obtenida desde el portal oficial de HIBP.

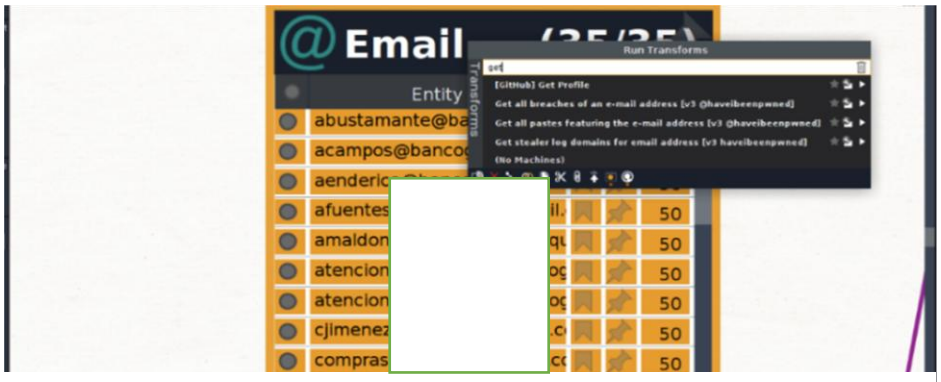


Figura 52: Ejecutando la transformación de HIBP sobre una lista de correos.

Para cada correo, Maltego devuelve nodos adicionales. El resultado de la transformación genera nodos relacionados con cada dirección de correo. Estos nodos pueden incluir el nombre de la brecha, el año en que ocurrió y el tipo de información comprometida (como contraseñas, teléfonos o direcciones). Esta información es crítica para determinar el nivel de exposición de cada cuenta y las posibles amenazas derivadas.

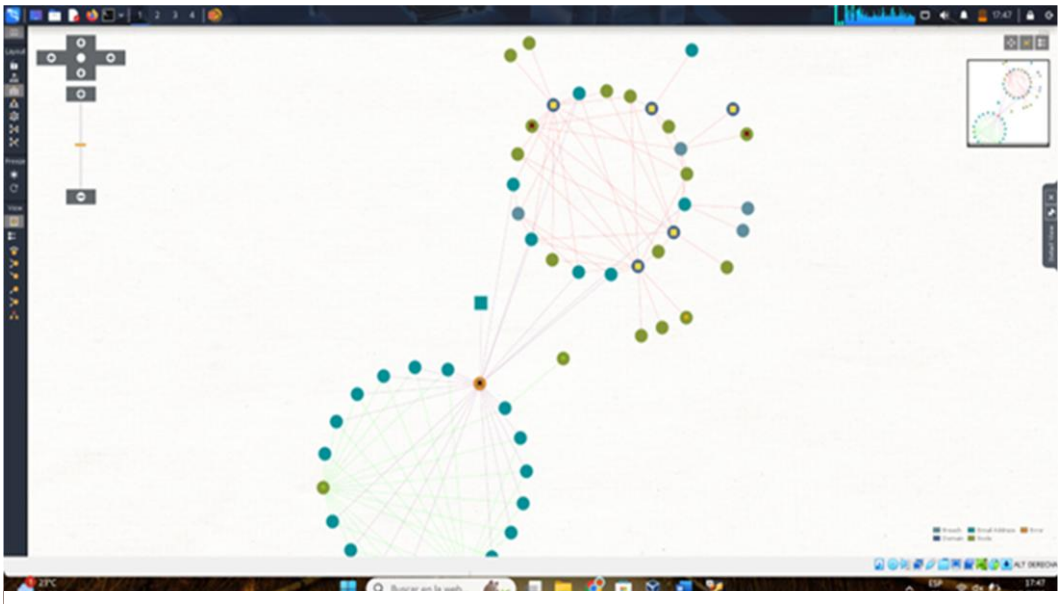


Figura 53: Análisis de inteligencia de fuentes abiertas y su representación visual en Maltego.

Analizar el grafo visualmente para identificar cuentas más expuestas. Con el grafo generado, se realiza un análisis visual que permite identificar rápidamente cuáles cuentas aparecen en más brechas y, por ende, se consideran más expuestas. Este método facilita reconocer patrones y establecer prioridades de mitigación en función del grado de compromiso de los correos.

Exportar el grafo a PDF/PNG y guardar los resultados en CSV. El grafo puede exportarse como archivo PDF o PNG para su incorporación en el informe final, permitiendo visualizar de forma clara las relaciones detectadas. Además, los resultados generados deben guardarse en formato CSV, lo que facilita su revisión, filtrado y comparación con otras fuentes de datos, como DeHashed. Esto permite enriquecer el análisis de exposición y obtener una visión de los posibles riesgos.

B) DeHashed – Validación y detalle de fugas

Acceder a dehashed con usuario registrado: El proceso inicia ingresando a DeHashed https://dehashed.com/ con una cuenta válida, lo que habilita búsquedas y, según el plan, exportaciones. Esta plataforma indexa brechas y "pastes" que estuvieron disponibles públicamente en distintos momentos. Es importante dejar constancia de fecha y hora de acceso, dado que algunas fuentes que fueron públicas durante la investigación pueden haber sido eliminadas o desindexadas posteriormente por sus autores u hospedadores.

Realizar una búsqueda por dominio: DeHashed devuelve coincidencias históricas asociadas a filtraciones y listados difundidos públicamente basándose en el dominio de la empresa. En varios casos observamos que los enlaces de origen referenciados por la plataforma habían sido públicos al momento de la verificación inicial, pero más tarde fueron retirados, quedando disponibles solo los metadatos indexados por el servicio.

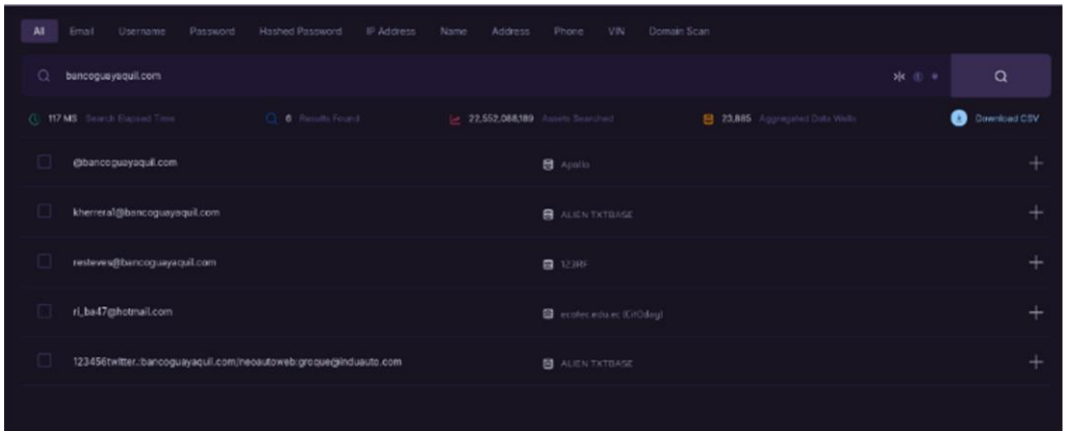


Figura 54: Exposición de credenciales en inteligencia de brechas

Exportar coincidencias si el plan lo permite o registrar manualmente los detalles. Cuando la suscripción lo permite, se exportan los resultados a CSV; de lo contrario, se documentan manualmente los campos clave: fecha de la brecha, servicio afectado, si existen contraseñas cifradas o en texto plano y otros metadatos (IP, teléfono). En todos los casos se registra el identificador o URL de referencia y se capturan pantallas como evidencia pasiva, señalando explícitamente si la fuente original estuvo pública y después fue removida, sin interactuar ni descargar datos.

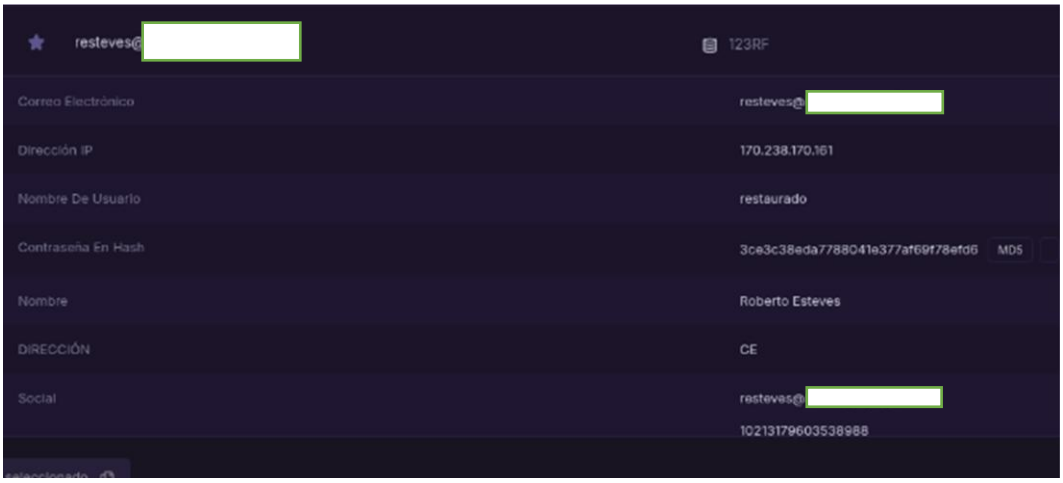


Figura 55: Fuga de datos de correo institucional obtenidos con DeHashed.

Correlacionar resultados con el grafo de Maltego, marcando coincidencias entre HIBP y DeHashed. Los hallazgos se contrastan con el grafo de Maltego generado con HIBP para identificar cuentas recurrentemente expuestas y brechas coincidentes. Esta correlación permite calificar el riesgo por volumen y criticidad de los datos comprometidos. En las notas del anexo se destaca cada coincidencia y se indica el estado de la fuente (pública en el momento de análisis vs. actualmente retirada), preservando trazabilidad y contexto temporal del hallazgo.

Prueba 4: Uso de Investigator para recolección de información

Acceder al portal Investigator. El análisis comenzó ingresando al portal de Investigator https://abhijithb200.github.io/investigator/, una herramienta que centraliza diversas fuentes OSINT para la búsqueda de información relacionada con dominios y organizaciones. El acceso a la plataforma se realizó a través de su página principal, lo que permitió disponer de un entorno de consulta especializado en la identificación de posibles vectores de exposición.

Ingresar el dominio de la entidad en el buscador principal: Una vez dentro de la herramienta, se utilizó el buscador principal para el dominio institucional de la entidad financiera. Este procedimiento permitió a Investigator rastrear información asociada con el dominio como: registros históricos, subdominios o documentos

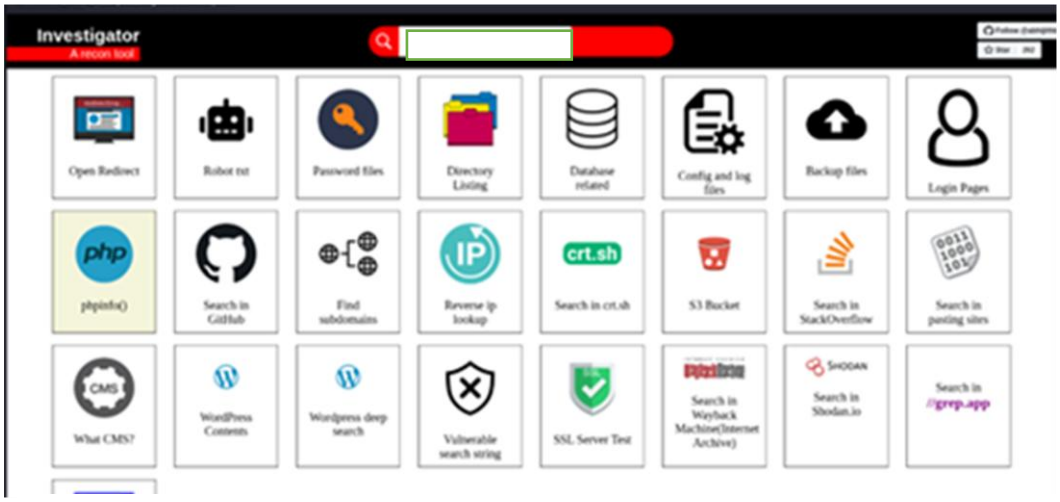


Figura 56: Interfaz de la herramienta OSINT Investigator.

Verificar las diferentes opciones de búsqueda que ofrece la plataforma: Investigator ofrece múltiples fuentes y categorías de búsqueda que deben ser revisadas de forma sistemática. Entre estas se encuentran los certificados digitales, los subdominios vinculados, los pastes en foros públicos, dorks en motores de búsqueda y posibles referencias en servicios de almacenamiento en la nube. De esta revisión únicamente se documentó la información considerada relevante para la investigación, descartando datos sin relación directa con la entidad.

Identificación de un bucket público en Amazon S3: Durante la revisión de la categoría de almacenamiento en la nube, se identificó un bucket público alojado en Amazon S3. Este contenedor incluía información sensible que abarcaba nombres completos, dirección de correo electrónico, número de identificación y dato bancario asociado a clientes de la entidad financiera privada. Cabe destacar que este bucket fue accesible de manera pública en el momento de la investigación; sin embargo, posteriormente fue eliminado, dejando de estar disponible en línea.

Aunque el bucket estaba vinculado con la entidad financiera, no se comprobó que la exposición proviniera de sus sistemas. Era una publicación de un tercero, posiblemente un cliente, que compartió información de forma pública. Los datos incluían nombres, correos y referencias bancarias asociadas a la entidad, lo que originó la vinculación en el análisis. El caso se registró como una exposición indirecta con posible impacto reputacional.

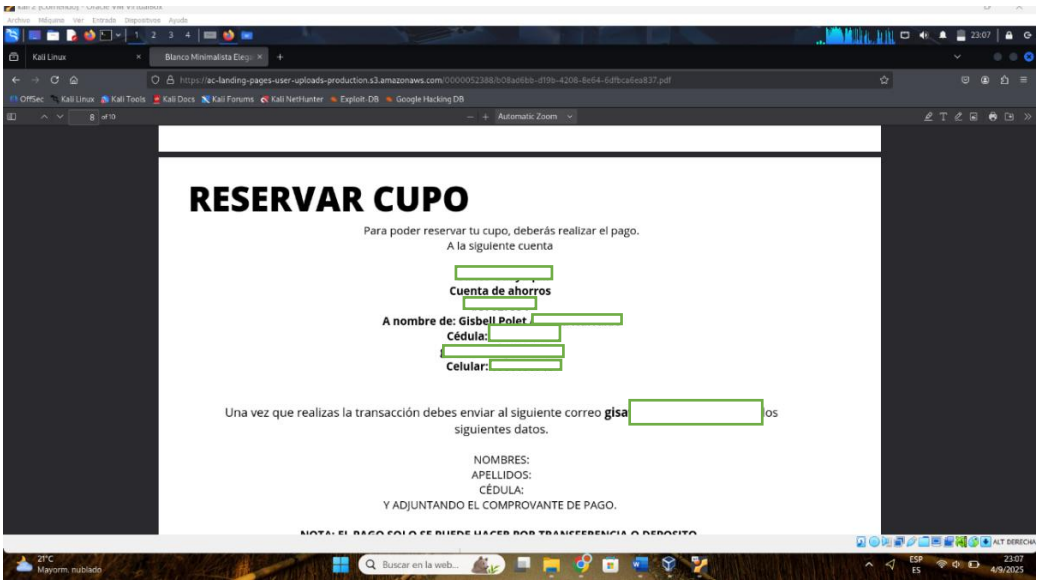


Figura 57: Información sensible de pago expuesta mediante google dorking.

Anexo 3: Evaluación de riesgos por exposición de datos personales en portales institucionales de una entidad pública

1. OBJETIVOS

Analizar los riesgos derivados de la exposición de datos personales en entidades públicas mediante técnicas OSINT y herramientas de ciberinteligencia, evaluando las vulnerabilidades presentes en plataformas tecnológicas, identificando la información sensible que se encuentra disponible de forma abierta y determinando su posible impacto en la seguridad de la información, tanto a nivel institucional como en los usuarios involucrados.

2. RECURSOS NECESARIOS

- Computadora
- Kali Linux
- FOCA
- Google Dorking
- Maltego

3. ESCENARIO DEL CASO

Escenario: Problemas de seguridad de datos personales en una entidad pública del Ecuador

Contexto: Una entidad pública del Ecuador gestiona y publica información a través de múltiples plataformas digitales, incluyendo portales web de acceso ciudadano, servicios en línea y repositorios de documentos.

En el cumplimiento de sus funciones, la institución maneja bases de datos, reportes internos, documentos oficiales y registros electrónicos que contienen información personal y técnica. Parte de esta información se encuentra disponible en internet por obligación de transparencia, mientras que otra debería permanecer bajo estrictas medidas de seguridad.

En el entorno actual, las amenazas cibernéticas contra organismos públicos han incrementado, y los atacantes suelen aprovechar cualquier debilidad para obtener datos que permitan realizar fraudes, campañas de phishing o intrusiones en sistemas internos. Por ello, es importante que las plataformas digitales de las instituciones públicas no solo cumplan con sus objetivos de servicio y transparencia, sino que también apliquen buenas prácticas de seguridad y protección de datos.

Problema: Durante una investigación de ciberinteligencia, mediante técnicas de recolección de información pública y herramientas de análisis, se identificaron incidentes que comprometen la seguridad de datos, además evidencian deficiencias técnicas en su portal web oficial. Estos hallazgos podrían ser explotados para realizar ataques de ingeniería social, robo de identidad, campañas de phishing o incluso para comprometer la infraestructura interna.

4. RESOLUCIÓN

Incidente 1: Detección y mapeo de documentos institucionales mediante Maltego.

Durante la investigación se empleó Maltego (versión CE/XL) utilizando la *machine* Company Stalker para mapear relaciones entre el dominio institucional, entidades asociadas, correos electrónicos y archivos publicados (PDF, XLS, CSV). La máquina automatiza transformaciones que permiten identificar nodos relacionados con documentos y dominios, filtrar por extensiones de archivo y revelar conexiones

entre correos, subdominios y recursos públicos que normalmente aparecen en directorios o repositorios del sitio institucional.

El análisis con Maltego permitió localizar grafos que contenían referencias a documentos oficiales—incluyendo un Directorio Institucional en formato PDF—y relacionarlos con direcciones de correo y cargos mostrados en el grafo. Aunque parte de la información puede estar publicada por transparencia, desde la perspectiva de seguridad estos hallazgos exponen nombres, cargos, teléfonos, correos (institucionales y personales) y la estructura organizacional, facilitando posibles ataques de phishing, spear-phishing o suplantación de identidad. **Riesgos e implicaciones:**

Ingeniería social y suplantación: La información identificada en los grafos de Maltego permite reconstruir relaciones entre correos, cargos y dependencias institucionales, lo que facilita la elaboración de mensajes creíbles y dirigidos a empleados o autoridades.

Ataques dirigidos: Conocer la estructura organizacional y los contactos asociados posibilita planificar ataques específicos hacia personal con funciones críticas, como responsables de tecnología o directivos.

Perfilamiento de la entidad: El mapeo automatizado de documentos y dominios expone la interconexión entre distintos recursos públicos, lo que permite a un atacante obtener una visión general del ecosistema digital de la institución. **Riesgo reputacional:** La visibilidad de datos personales y corporativos en fuentes abiertas puede afectar la percepción de seguridad institucional y la confianza de los usuarios en los servicios públicos.

Incidente 2: Exposición de metadatos y rutas internas mediante FOCA

Utilizando la herramienta FOCA (Fingerprinting Organizations with Collected Archives), se extrajeron metadatos de varios documentos PDF publicados por la entidad pública. La herramienta permitió identificar al menos 99 correos institucionales, así como otros elementos técnicos valiosos como el nombre del autor del documento, el nombre del equipo de trabajo donde fue creado, rutas de sistemas de archivos, versiones de software, usuarios y dispositivos utilizados.

Estos metadatos revelan detalles sobre la infraestructura técnica y operativa de la institución. Por ejemplo, exponer rutas internas facilita ataques como path traversal o inclusión de archivos locales (LFI). Asimismo, la información puede ser aprovechada para crear diccionarios de usuarios internos e intentar ataques de fuerza bruta contra sistemas autenticados. Esta exposición representa una amenaza importante cuando no existe control sobre la publicación de documentos ni procedimientos claros de limpieza de metadatos antes de su divulgación.

Riesgos e implicaciones:

Exposición de infraestructura interna: Los metadatos revelan detalles del entorno informático, como sistemas operativos, versiones de software y configuraciones internas, que pueden facilitar ataques de enumeración o explotación de vulnerabilidades específicas.

Reconocimiento técnico: La información obtenida puede ser usada para realizar un mapeo de la red o desarrollar ataques dirigidos a servidores y estaciones de trabajo.

Fuerza bruta y diccionarios personalizados: Los nombres de usuarios extraídos permiten construir listas de credenciales válidas para intentos de acceso no autorizado.

Ausencia de control documental: La falta de procedimientos de limpieza de metadatos evidencia debilidades en la gestión de información pública y aumenta el riesgo de filtraciones accidentales.

Incidente 3: Formulario institucional con datos personales expuesto públicamente

Durante la investigación, se localizó un formulario oficial de aportes ciudadanos accesible en línea desde un dominio institucional. Dicho documento contenía información personal sensible de un ciudadano, incluyendo:

- Nombre completo
- Número de cédula
- Número de teléfono celular
- Dirección de correo electrónico personal
- Sugerencias del ciudadano

La exposición de estos datos sin medidas de resguardo constituye una vulnerabilidad crítica que infringe principios de la Ley Orgánica de Protección de Datos Personales (LOPDP), como confidencialidad, proporcionalidad y temporalidad. Además, demuestra la ausencia de controles internos para la anonimización o depuración de documentos antes de su publicación en plataformas públicas.

Riesgos e implicaciones:

Robo de identidad y fraude electrónico: La información expuesta puede ser utilizada para crear perfiles falsos o realizar transacciones ilícitas.

Phishing y spear phishing: Los datos personales permiten diseñar mensajes falsos altamente creíbles dirigidos al ciudadano afectado o a terceros.

Pérdida de confianza institucional: La exposición de información privada en un portal oficial afecta la percepción de seguridad y transparencia del organismo. **Sanciones legales y responsabilidad administrativa:** El incidente puede derivar en sanciones por incumplimiento de la LOPDP y otras normativas de protección de datos.

5. PROCEDIMIENTO TÉCNICO

Prueba 1: Detección y mapeo de documentos institucionales mediante Machines (Maltego).

Uso de la opción "Machines" dentro de la interfaz principal de Maltego. Maltego también dispone de una opción llamada Machines, que son flujos de trabajo preconfigurados que automatizan transformaciones y consultas sobre una o varias entidades, permitiendo al analista ejecutar tareas repetitivas de forma automática y estructurada dentro de un proceso de análisis OSINT.

Como se muestra en la figura 58 maltego dispone de 11 machines activos, puesto que cada Machine cumple una función específica: **Company Stalker** localiza correos vinculados a un dominio, **Footprint L1** mapea la infraestructura básica de una organización, **Footprint L2** amplía el análisis con subdominios y servicios expuestos, **Footprint L3** realiza un reconocimiento más profundo, **Person Email** busca información relacionada con una cuenta de correo

Estas permiten ejecutar secuencialmente las transformaciones sin hacerlo manualmente, facilitando la detección de relaciones entre dominios, correos o documentos públicos. Con su uso, el analista acelera el reconocimiento y obtiene una visión más clara de la información en fuentes abiertas, reduciendo errores y tiempo de trabajo.

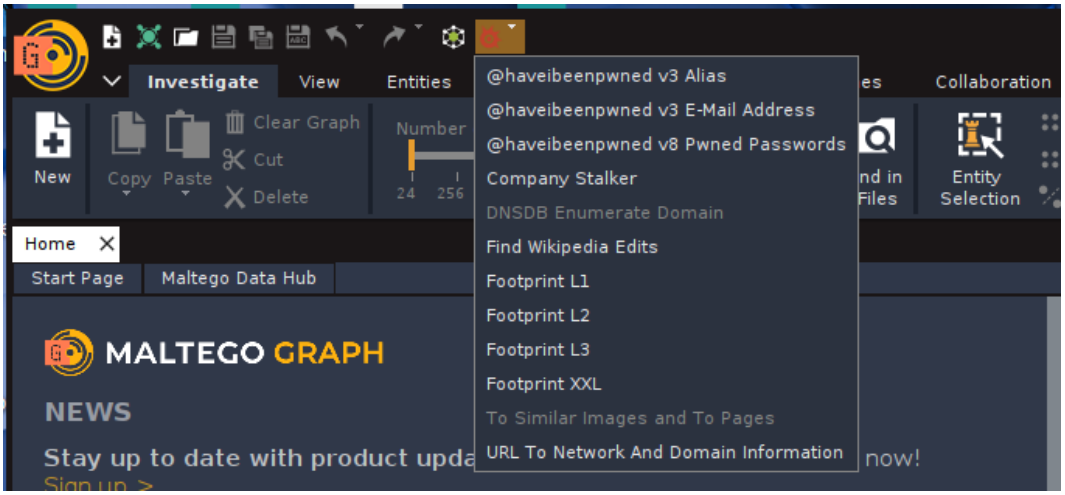


Figura 58: Machines de Maltego para análisis OSINT.

Ejecutar la máquina Company Stalker. Durante su ejecución nos solicitará ingresar el dominioa investigar tal como se muestra en la imagen 59, luego Maltego inicia una serie de transformaciones que permiten identificar correos electrónicos, subdominios, enlaces públicos y archivos expuestos en diferentes formatos. El resultado se representa posteriormente mediante un grafo donde se muestran las relaciones encontradas entre los elementos del dominio.

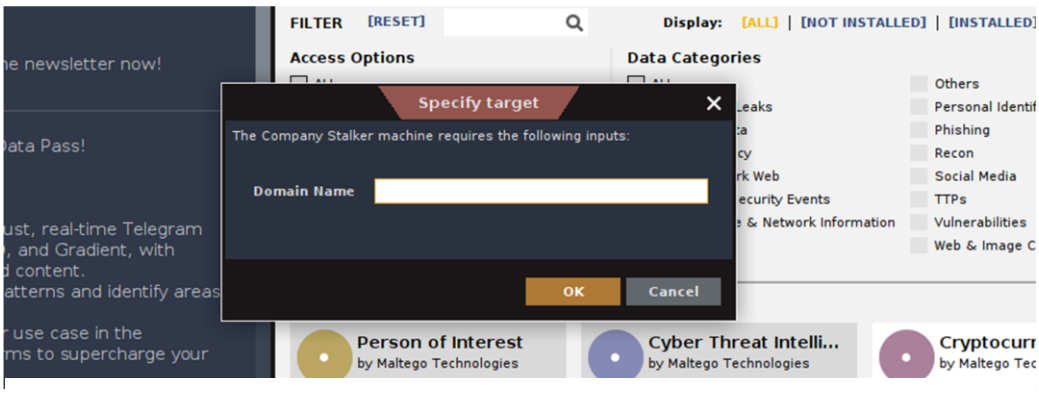


Figura 59: Ejecución de la Machine Company Stalker en Maltego.

procede a revisar los nodos generados como se muestra en la Figura 60, priorizando aquellos clasificados como File o URL, especialmente los que contengan extensiones PDF, XLS o CSV, y términos como “directorio”, “personal” o “contactos”. Estos resultados permiten ubicar documentos que podrían contener datos sensibles que se encuentren disponibles de manera pública.

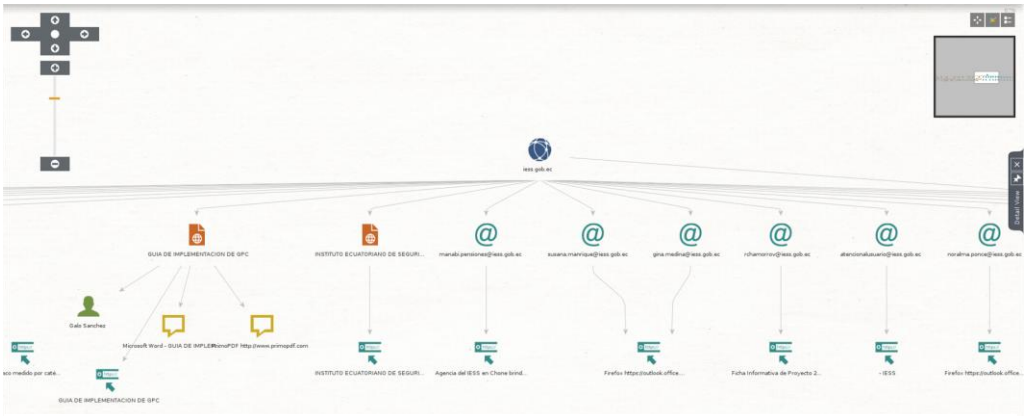


Figura 60: Resultados del análisis de dominio con la Machine Company Stalker en Maltego

Prueba 2: FOCA – Extracción y análisis de metadatos

1. Descargar e instalar FOCA desde el repositorio oficial.

El proceso inicia con la descarga de FOCA desde su repositorio oficial en GitHub, siguiendo las instrucciones proporcionadas por los desarrolladores. Aunque se planeaba ejecutarla únicamente en Kali Linux, la instalación presentó dificultades por dependencias y compatibilidad, ya que la herramienta fue diseñada principalmente para entornos Windows.

Debido a que FOCA fue desarrollada inicialmente para funcionar de forma nativa en Windows, se optó por instalarla en dicho sistema operativo para garantizar su estabilidad y correcto funcionamiento. Esta decisión permitió continuar con el análisis sin afectar la validez metodológica ni los resultados obtenidos, manteniendo la integridad del proceso y asegurando el uso adecuado de la herramienta.

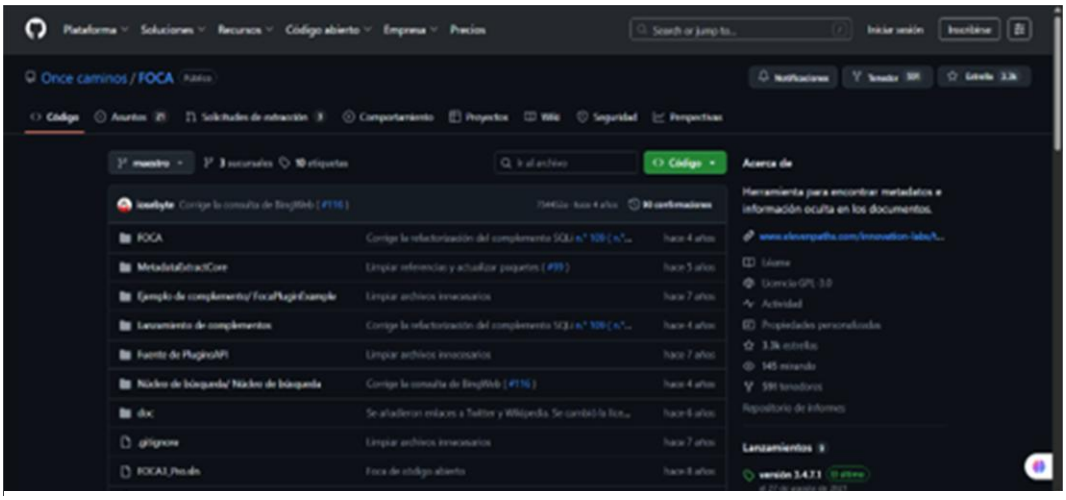


Figura 61: Repositorio oficial de FOCA en GitHub

Ejecutar FOCA en Windows. Una vez descargado el archivo comprimido en formato ZIP, se procede a descomprimirlo para acceder al ejecutable de la herramienta. Al finalizar este proceso, se obtiene la carpeta con los archivos necesarios para su funcionamiento, incluido *FOCA.exe*, tal como se observa en la **Figura 62**, donde aparecen las librerías y componentes internos de la herramienta. Con esta estructura desplegada, FOCA queda lista para su ejecución en Windows, permitiendo iniciar el análisis de metadatos en documentos publicados por la entidad y detectar información sensible expuesta de manera no intencional.

Nombre	Fecha de modificación	Tipo	Tamaño
de	23/4/2025 22:37	Carpeta de archivos	
DNSDictionary	23/4/2025 22:37	Carpeta de archivos	
Plugins	23/4/2025 22:37	Carpeta de archivos	
BaseSDK.dll	23/4/2025 22:37	Extensión de la ap...	17 KB
com.rusanu.dataconnectiondialog.dll	23/4/2025 22:37	Extensión de la ap...	14 KB
DiarioSDKNet.dll	23/4/2025 22:37	Extensión de la ap...	11 KB
DotNetZip.dll	23/4/2025 22:37	Extensión de la ap...	448 KB
EntityFramework.dll	23/4/2025 22:37	Extensión de la ap...	4.878 KB
EntityFramework.SqlServer.dll	23/4/2025 22:37	Extensión de la ap...	579 KB
FOCA.exe	23/4/2025 22:37	Aplicación	2.608 KB
FOCA.exe.config	23/4/2025 22:37	Archivo de origen ...	3 KB
Google.Apis.Core.dll	23/4/2025 22:37	Extensión de la ap...	66 KB
Google.Apis.Customsearch.v1.dll	23/4/2025 22:37	Extensión de la ap...	45 KB
Google.Apis.dll	23/4/2025 22:37	Extensión de la ap...	75 KB
Google.Apis.PlatformServices.dll	23/4/2025 22:37	Extensión de la ap...	5 KB
Heijden.Dns.dll	23/4/2025 22:37	Extensión de la ap...	39 KB
HtmlAgilityPack.dll	23/4/2025 22:37	Extensión de la ap...	162 KB

Figura 62: Archivos internos de FOCA tras la descompresión del paquete ZIP.

Crear un nuevo proyecto dentro de la herramienta. Al iniciar FOCA, el primer paso consiste en crear un nuevo proyecto, donde se define el dominio que será objeto de análisis. El proyecto actúa como contenedor de todas las consultas y resultados que genera la herramienta, lo cual facilita la organización del trabajo y la documentación de los hallazgos.

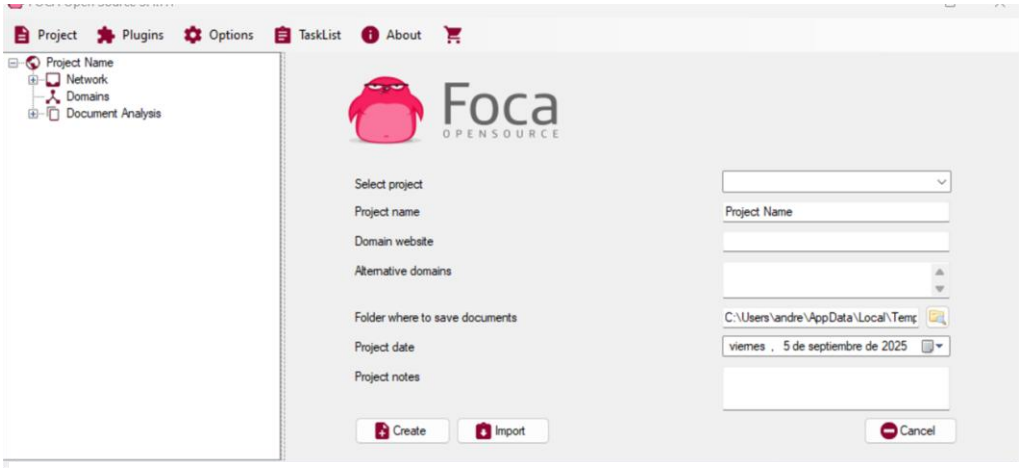


Figura 63: Interfaz de la herramienta de OSINT FOCA

Introducir el dominio de la entidad pública. En este punto se introdujo en la herramienta el dominio institucional de la entidad pública (por ejemplo, dominio.gob.ec). FOCA utiliza este dato como referencia principal para localizar y descargar documentos publicados en línea que estén asociados al dominio ingresado, permitiendo así la recolección de información accesible públicamente.

Figura 64: Creación de Proyecto en FOCA Open Source.

Permitir que FOCA descargue automáticamente documentos asociados al dominio. Una de las funcionalidades más relevantes de FOCA es su capacidad para rastrear y descargar de manera automatizada documentos vinculados al dominio ingresado. Estos documentos suelen estar alojados en servidores institucionales y haber sido expuestos públicamente de forma involuntaria. Cabe señalar que en el momento del análisis algunos archivos estaban disponibles públicamente, aunque posteriormente fueron retirados.

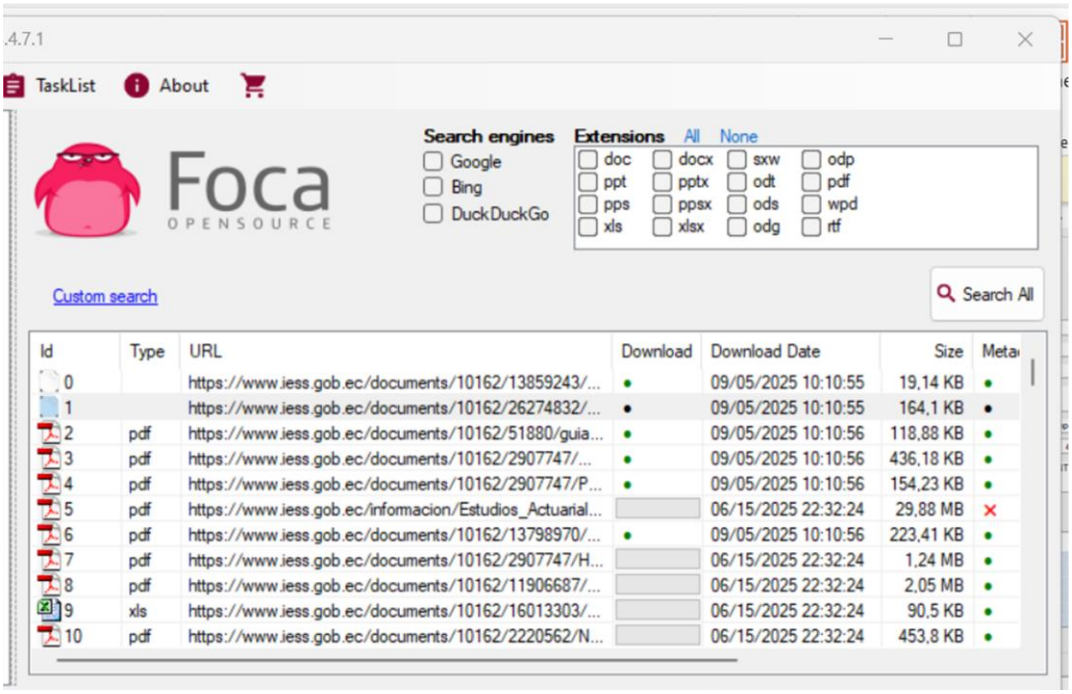


Figura 65: Descargando documentos para el análisis de metadatos con la herramienta FOCA.

Analizar los metadatos extraídos de los archivos. FOCA realiza automáticamente la extracción de metadatos presentes en documentos como PDF, DOC y XLS, permitiendo identificar información sensible que no siempre es visible en el contenido, pero que permanece registrada en la estructura interna del archivo. Estos datos pueden incluir nombres de usuarios, equipos de trabajo, fechas de creación, rutas internas o versiones de software utilizadas. El análisis de esta información constituye un paso crítico para detectar posibles vectores de exposición y entender mejor la configuración técnica del entorno institucional.

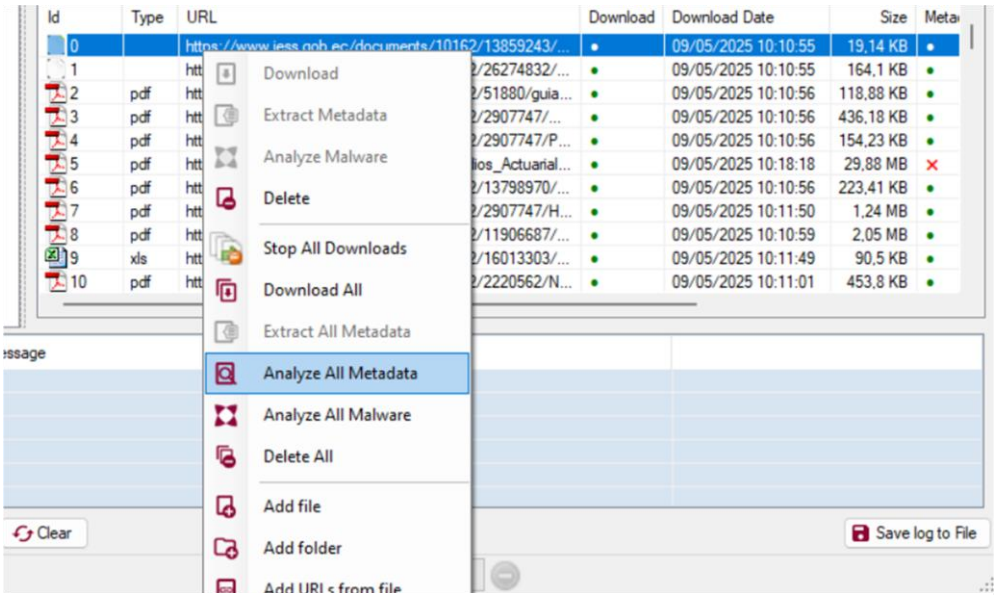


Figura 66: Análisis de metadatos en la interfaz de la herramienta FOCA.

Identificar información sensible en los metadatos. Dentro de los metadatos se identificaron elementos de alto valor para un posible atacante, como direcciones de correo electrónico, nombres de usuario, rutas de archivos internos, nombres de equipos, versiones de software utilizadas e incluso autores de los documentos como se muestra en la figura 67. Estos datos, aunque en su momento estuvieron accesibles públicamente, representan un riesgo significativo si son utilizados de manera maliciosa.

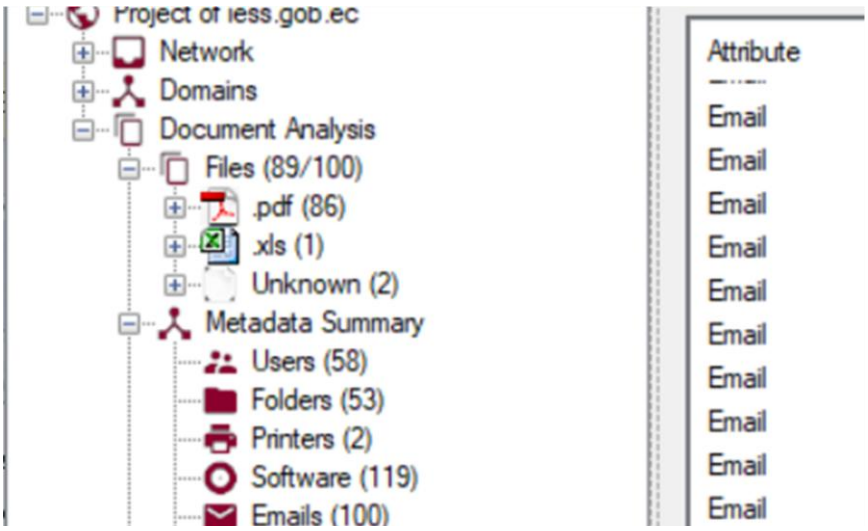


Figura 67: Resumen de metadatos, visualización de correos y usuarios extraídos con FOCA.

Documentar posibles riesgos de explotación. Finalmente, se documentaron los riesgos derivados de la información recolectada. Entre ellos se destacan la posibilidad de ataques de fuerza bruta sobre cuentas de correo, intentos de path traversal contra sistemas internos y campañas de ingeniería social dirigidas a usuarios específicos. Los hallazgos fueron registrados con evidencia visual y textual, resaltando que la información estuvo expuesta en el momento.

Prueba 3: Búsqueda avanzada en Google sobre el dominio

Abrir navegador web y acceder a Google.

La actividad comenzó mediante el uso de un navegador web con conexión a internet, accediendo directamente al buscador en https://www.google.com. Google fue elegido por su capacidad de indexar información expuesta públicamente en servidores institucionales, lo cual lo convierte en una herramienta esencial dentro de las metodologías OSINT aplicadas.

Ejecutar la consulta avanzada. En la barra de búsqueda se introdujo por ejemplo el siguiente dork: *site:dominio.ec filetype:pdf "telefono"*

Esta consulta avanzada permitió filtrar exclusivamente documentos PDF alojados en el dominio de la empresa que contuvieran la palabra clave "teléfono". El objetivo fue localizar listados institucionales que pudieran exponer datos de carácter personal.

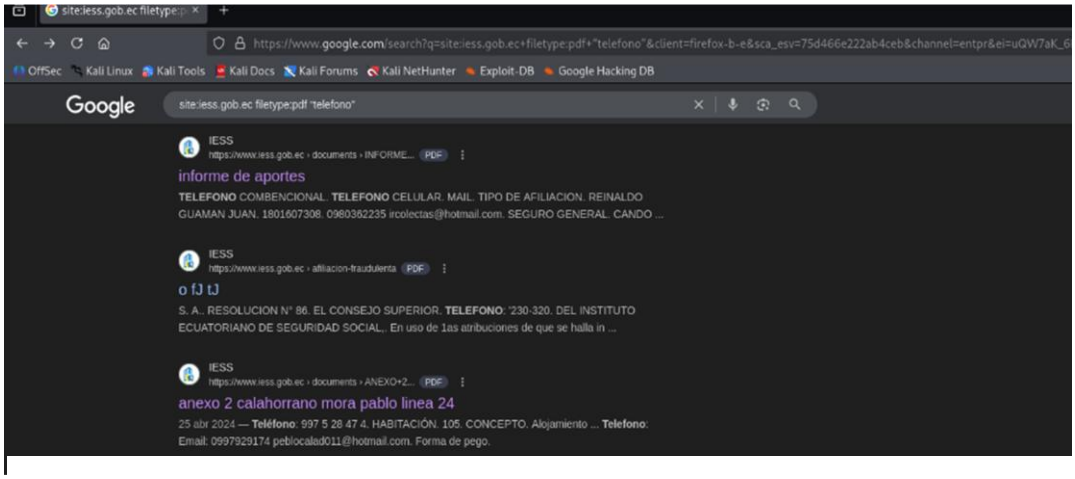


Figura 68: Búsqueda de información a través de Google Dorking.

Revisar los primeros resultados devueltos. El motor de búsqueda devolvió múltiples resultados en los que se encontraron documentos oficiales. Se realizó una revisión sistemática de los primeros enlaces, priorizando aquellos archivos que aparentaban contener listados administrativos. Es importante señalar que, en el momento del análisis, dichos documentos estaban accesibles públicamente, aunque algunos fueron retirados con posterioridad.

Identificar la presencia de datos sensibles. Tras la revisión, se constató que los documentos contenían datos sensibles de carácter personal. Entre los registros se encontraron nombres completos, números de cédula, direcciones y teléfonos. Este tipo de información, aunque legítimamente recopilada por la institución, no debería haber estado disponible sin restricciones en un servidor público.

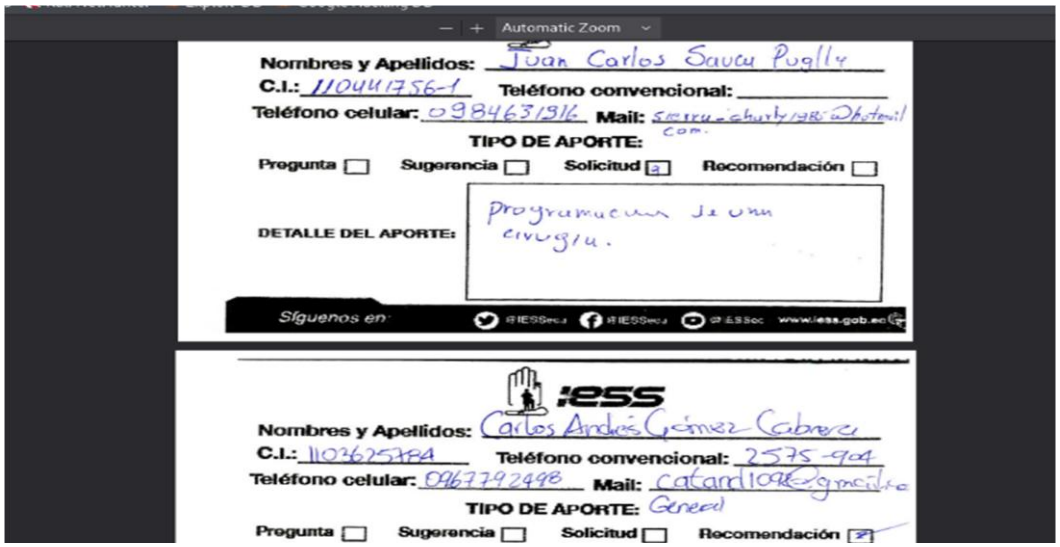


Figura 69: Formulario que contiene datos personales

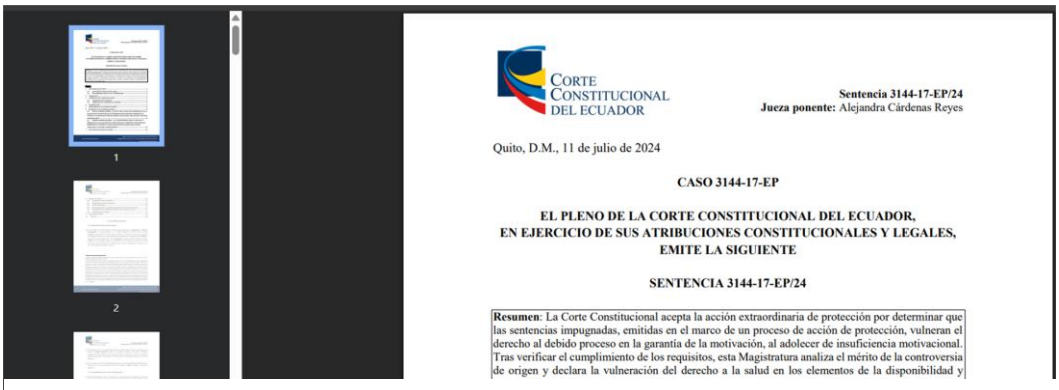


Figura 70: Exposición de información sensible en documentos públicos

En la figura 69 se observa un formulario institucional que muestra varios datos personales. El documento incluye información como nombres completos, números de identificación, direcciones y teléfonos. Estos elementos permiten identificar de forma directa a una persona, por lo que su presencia en un archivo accesible sin medidas de control representa un riesgo para la privacidad. El formulario evidencia cómo un contenido administrativo puede convertirse en una fuente de exposición no intencional.

En la figura 70 se aprecia una sentencia publicada por una entidad pública donde aparecen datos sensibles de varias personas. El documento muestra nombres completos, información sobre la edad, detalles de salud y fechas relacionadas con la atención médica. Al estar disponible sin controles adecuados, esta información puede ser obtenida mediante técnicas OSINT y usada con fines no deseados. La imagen refleja cómo un archivo oficial puede exponer datos que deberían mantenerse bajo mayor reserva para proteger la privacidad de los involucrados.