OFICINA DE POSGRADOS

Tema:

METODOLOGIA PARA MITIGAR VULNERABILIDADES DE ALMACENAMIENTO MEDIANTE INTELIGENCIA DE FUENTES ABIERTAS(OSINT) EN LA EEASA.

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de Investigación:

Seguridad de la información

Autor:

Ing. Jorge Enrique Freire Silva

Director:

PhD. Gustavo David Salazar Chacón, Mg.

Ambato – Ecuador

Marzo 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

METODOLOGIA PARA MITIGAR VULNERABILIDADES DE ALMACENAMIENTO MEDIANTE INTELIGENCIA DE FUENTES ABIERTAS(OSINT) EN LA EEASA

Línea de Investigación:

Seguridad de la información

Autor: Ing. Jorge Enrique Freire Silva

Gustavo David Salazar Chacón, PhD. f._____

CALIFICADOR

Verónica Maribel Pailiacho Mena, Ing. Mg. f._____

CALIFICADOR

Darío Javier Robayo Jácome, Ing. Mg. f._____

CALIFICADOR

Juan Carlos Acosta Teneda, P. Mg. f._____

COORDINADOR DE LA OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villaroel, Dr. f._____

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Marzo 2022

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo: **JORGE ENRIQUE FREIRE SILVA**, con CC. **180473866-2** autor del trabajo de graduación intitulado: "**METODOLOGIA PARA MITIGAR VULNERABILIDADES DE ALMACENAMIENTO MEDIANTE INTELIGENCIA DE FUENTES ABIERTAS(OSINT) EN LA EEASA**", previa a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD**, en la OFICINA DE POSGRADOS.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, marzo 2022

Jorge Enrique Freire Silva
CC. 1804738662

AGRADECIMIENTO

A Dios, gracias a él escribo estas palabras.

DEDICATORIA

A mi amada esposa Rosana.

RESUMEN

Debido al constante uso de las nuevas tecnologías, las instituciones pertenecientes a sectores estratégicos se ven obligadas a salvaguardar la información para minimizar riesgos de ataques a los que, se encuentran latentes.

Para esto, en el contexto ético del hacking existe una serie de herramientas que ayudan a determinar el nivel de exposición de la información, lo cual, permite anticiparse ante la explotación vulnerabilidades. Con este antecedente, la presente investigación consiste en implementar una propuesta metodológica que permita mitigar los riesgos referentes a las vulnerabilidades de almacenamiento detectadas en el análisis de fuentes abiertas, esto es posible con la aplicación de Magerit y las matrices que provee para la gestión de riesgos. El proyecto tiene un enfoque cuantitativo tanto que usa listado de vulnerabilidades determinadas en OWASP e ISO27001; además, se hace uso de técnicas OSINT con un diseño preexperimental y el enfoque cualitativo para la valoración de Magerit. Los resultados obtenidos demuestran que la aplicación de la propuesta metodológica cumple con los parámetros necesarios para mitigar riesgos; por otra parte, permite anticiparse a posibles ataques informáticos que, se desencadenan diariamente en el Ecuador.

Palabras clave: OWASP, ISO27001, OSINT, MAGERIT, vulnerabilidad, explotación, hacking.

ABSTRACT

Due to the constant use of new technologies, institutions belonging to strategic sectors are forced to safeguard information in order to minimize the risk of latent attacks.

Under this background, among the ethical context of hacking, there is a series of tools that help determine the level of exposure of information, which allows to anticipate the exploitation of vulnerabilities. Due to this fact, the current research consists of implementing a methodological proposal that allows mitigating the risks related to storage vulnerabilities detected in the analysis of open sources, this is possible with the application of Magerit and the matrixes it provides for risk management.

The project has a quantitative approach that uses a list of vulnerabilities determined in OWASP and ISO27001; in addition, OSINT techniques are used with a pre-experimental design and the qualitative approach for the Magerit assessment. The results obtained show that the application of the methodological proposal complies with the necessary parameters to mitigate risks; on the other hand, it allows anticipating possible computer attacks that occur in Ecuadorian a daily basis.

Keywords: OWASP, ISO27001, OSINT, MAGERIT, vulnerability, exploitation, hacking.

ÍNDICE

PRELIMINARES

INDICE DE FIGURAS

INDICE DE CUADROS

INTRODUCCIÓN

La inteligencia de fuentes abiertas (*OSINT*) ha tomado el interés de los profesionales de la ciberseguridad debido a su accesibilidad y precisión. Según Alves F., (2020) TWITTER ha demostrado ser un centro de discusión sobre las últimas vulnerabilidades y *EXPLOITS*, pues en su estudio concluye que TWITTER proporciona alertas de seguridad más oportunas e impactantes debido a su análisis realizado cronológicamente a más de 9000 vulnerabilidades que fueron publicadas.

Según un informe de la empresa de ciberseguridad CONTINUITY SOFTWARE, los sistemas de almacenamiento tienen una postura de seguridad significativamente más débil que las otras dos capas de infraestructura de TI, a saber, equipos de TI (PC y servidores) y redes. El análisis de los datos de más de 400 dispositivos de almacenamiento empresarial reveló que, en promedio, cada dispositivo de seguridad empresarial estaba expuesto a 6.300 problemas de seguridad discretos relacionados con 15 vulnerabilidades. El análisis cubrió equipos de proveedores como BROCADE, CISCO, DELL EMC, IBM, HITACHI DATA SYSTEMS y NETAPP (*Storage Security Solution for Real Data Protection*, s. f.).

El desarrollo de metodologías para la mitigación de amenazas cibernéticas es un tema en el cual diversas entidades gubernamentales del Ecuador aún no la conocen, esto es notorio debido a los ataques informáticos que han sido denunciados a través de la Fiscalía General de Estado (Indio & Isidoro, s. f.), la falta de buenas prácticas y ausencia de *HARDENING* en los servidores al momento de la implementación de servicios en línea, es una de las causas que permite la existencia de un mercado apetecible por los *CIBERDELICUENTES* para aprovecharse y obtener información valiosa, esto genera a las empresas pérdidas económicas y daño reputacional.

OSINT, además de un complemento imprescindible para cualquier profesional, se ha convertido en una profesión, debido a que saber buscar datos e información sobre personas, hechos, empresas o instituciones es importante, pero saber encontrar la información que necesite o si la necesita, es imprescindible para tomar

buenas decisiones respecto a la prevención de ataques informáticos futuros (V et al., 2020).

Una correcta aplicación de *OSINT* permite anticiparse a los riesgos. Pese a que el aprovechamiento de las oportunidades es esencial para cualquier organización, en materia de seguridad cibernética, los riesgos acostumbran a ser más críticos que las oportunidades, porque condicionarían la propia existencia o incluso la supervivencia, ya sea con el análisis de riesgos personales, organizacionales e inclusive riesgos de país (Pastor-Galindo et al., 2020).

En un artículo relacionado menciona que la Inteligencia de fuentes abiertas (OSINT) es una rama de la ciber inteligencia usada para obtener y analizar información relacionada a posibles adversarios, para que sirva de apoyo a evaluaciones de riesgo y permita prevenir afectaciones contra activos críticos. En el artículo, se presenta una investigación acerca de diferentes tecnologías OSINT y como serían usadas para desarrollar tareas de ciber inteligencia de una nación. Un conjunto de transformadas apropiadas para un contexto colombiano son presentadas y contribuidas a la comunidad, permite a organismos de seguridad adelantar procesos de recolección de información de fuentes abiertas colombianas. Sin embargo, el verdadero aprovechamiento de la información recolectada, se da mediante la implementación de tres modelos de aprendizaje automático usados para desarrollar análisis de sentimientos sobre dicha información, con el fin de saber la posición del adversario respecto a determinados temas y así entender la motivación que tienen, lo cual permite definir estrategias de ciberdefensa apropiadas. Finalmente, algunos desafíos relacionados a la aplicación de técnicas OSINT también son identificados y descritos al respecto de su aplicación por agencias de seguridad del estado (Hernández et al., 2018).

Las sociedades publican mucha información en línea, parte de la cual es privada y propensa a ser explotada en la red mundial. Los hackers de sombrero negro explotan este tipo de información para una variedad de objetivos, como *SPEAR PHISHING* y fraudes en tarjetas de crédito. El punto clave a notar aquí es que tales investigaciones requieren una gran cantidad de tiempo y mano de obra. El trabajo

hace uso de *INTELLISPECT*, una herramienta *OSINT* que trabaja para reducir el tiempo total necesario para identificar y recopilar el objetivo de la información encontrada en la Web. *INTELLISPECT* presenta información relevante sobre el objetivo que, se investiga y produce resultados refinados y mucho más eficientes. Los investigadores dirigen las búsquedas de la forma que consideren adecuada, se utilizan varias funcionalidades disponibles en la herramienta (Chitkara et al., 2020).

Actualmente la Empresa Eléctrica Ambato Regional Centro Norte S.A. (EEASA) , es una entidad con 62 años de trayectoria y con una eficiente gestión en servicio eléctrico en la zona central del país, ha mantenido los mejores estándares calidad y continuidad de servicio a sus clientes dentro del área de concesión, gracias a la efectiva gestión de sus funcionarios y directivos. El trabajo veraz y puntual ha dado lugar a que la EEASA obtenga en el 2020 el premio categoría ORO entregado por la Comisión de Integración Energética Regional (CIER) referente a calidad de servicio. Por su eficiencia en la prestación de servicios, obtuvo la certificación ISO 9001:2015 en gestión de calidad, que constituye un privilegio, pero al mismo tiempo le compromete a una constante mejora. La empresa en este momento tiene la cobertura más grande del país, que incluye las provincias de Tungurahua, Pastaza, Napo y Morona Santiago. Es así como la EEASA cuenta con aproximadamente 285.00 clientes. En este escenario y en búsqueda dela eficiencia en la atención de las necesidades de sus clientes, busca garantizar constantemente la continuidad del servicio eléctrico y entre aspectos importantes de mejora está la protección de la información a través de metodologías que garantice la disponibilidad de acceso al servicio público en la sociedad.

El uso de plataformas web y servicios en línea dentro de la EEASA generan una serie de problemas como: Violación de datos, pérdida de datos, secuestro de cuenta o servicio, Interfaces y APIS de gestión inseguras, personal interno malicioso, software vulnerable, robo o pérdida de dispositivos. Con estos antecedentes el problema planteado como pregunta es: ¿Hay una forma adecuada de gestionar las vulnerabilidades de las fuentes de información pública de la EEASA?

Con base en lo expuesto la hipótesis de trabajo que, se plantea en la presente investigación es: El diseño de una metodología basada en Inteligencia de fuentes abiertas OSINT mitiga las vulnerabilidades de almacenamiento de la información de la EEASA.

En el contexto de lo citado, la investigación tiene como objetivo diseñar una metodología de mitigación de vulnerabilidades de almacenamiento mediante inteligencia de fuentes abiertas (OSINT) en la EEASA.

Por otra parte, los objetivos específicos aplicados son los siguientes:

1. Analizar el uso de métodos y técnicas de OSINT, basado en la investigación del estado del arte referenciado.
1. Establecer la situación actual del riesgo de almacenamiento de la información relacionada al uso de OSINT.
2. Diseñar una propuesta metodológica para emplear de manera ética los métodos y técnicas de OSINT.
3. Comprobar la mitigación de vulnerabilidades a través de la matriz de riesgos.

El presente proyecto trabaja con varias metodologías que, se menciona a continuación: para la investigación, se aplica mediante investigación cuantitativa y diseño PRE-EXPERIMENTAL con la aplicación técnicas OSINT de manera ética para la EEASA, para el desarrollo del trabajo, se utiliza la metodología SCRUM en el contexto de obtener en menor tiempo los resultados propuestos en línea de tiempo óptima, la aplicación de metodología Magerit, se utiliza para gestionar los riesgos detectados en la investigación de fuentes abiertas. Finalmente, el desarrollo de la presente investigación ayuda a gestionar riesgos ante la exposición de información que vive el día a día las empresas ecuatorianas, pues los datos detectados en el estudio de OSINT permite descubrir brechas de seguridad que son analizadas y corregidas antes de que, se desencadene una explotación masiva que provocan perdida de información temporal o definitiva.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Estado del Arte

El presente capítulo tiene como finalidad, proporcionar información sobre estudios preliminares que aporten como base de conocimiento, así como la definición preliminar de conceptos claves para un mejor entendimiento.

En estudios revisados con la aplicación de *OSINT*, se encuentra el trabajo presentado con tema *Using Twitter to generate alerts for Cybersecurity Threats and Vulnerabilities* (Uso de Twitter para generar alertas sobre amenazas y vulnerabilidades de ciberseguridad) trabajo que aplica inteligencia sobre amenazas de ciberseguridad y vulnerabilidades publicadas en la red Social *TWITER*. La inteligencia sobre estas amenazas está generalmente disponible en fuentes tanto abiertas como encubiertas como las alertas del *CERT*, publicaciones en blogs, redes sociales y recursos de la web oscura. Las actualizaciones de inteligencia sobre ciberseguridad son vistos como eventos temporales que un analista de seguridad debe realizar con el fin de asegurar un sistema informático. En el estudio presentado, se analiza las actualizaciones de información en tiempo real, en forma de tweets, para extraer información sobre diversas amenazas posibles. Mediante el uso de *RDF* de Web Semántica para representar la inteligencia recopilada y Reglas *SWRL* para razonar sobre la inteligencia extraída para emitir alertas para analistas de seguridad (Yeboah-Ofori, 2018)

La literatura del proyecto titulado “Inteligencia de fuentes abierta (OSINT) para operaciones de ciberseguridad”, concluye lo siguiente: La información que reposa en páginas web, redes sociales, foros e incluso los conjuntos de datos gratuitos, se convierten en fuentes de información, a la que, se accede para recopilar datos para utilizados en labores de inteligencia cibernética. La privacidad de los datos es un asunto muy serio, por lo que es imprescindible conocer y reconocer la diferencia entre violar la privacidad y recopilar información debido a la protección de activos críticos.

La identificación de posibles adversarios sirve para diseñar e implementar una estrategia de defensa que previene futuros ataques ciberseguridad. Una de las habilidades más valiosas para la inteligencia cibernética es saber buscar y encontrar información sobre un objetivo. Las organizaciones de inteligencia valoran esta habilidad porque representa una ventaja frente a los adversarios debido a que resulta útil para manejar incidentes de seguridad nacional. Una sugerencia final para organizaciones o individuos es estar al tanto de toda la información que, se comparte o publica en las redes sociales o en cualquier Página web (Hernández et al., 2018).

1.2. OSINT

En solo 17 años, Internet ha transformado prácticamente todas las facetas de la vida moderna. El lanzamiento de *MOSAIC*, el primer navegador web en 1993, fue el catalizador de una revolución de la comunicación, cuyas implicaciones aún, se investiga. La Web siempre tuvo la intención de ser un sistema de publicación multiusuario bidireccional que socavara la radiodifusión unidireccional controlada por el Estado. Dar rienda suelta a una red de comunicación mundial masiva para millones de personas ha traído enormes beneficios, pero también algunos peligros. La lucha contra las nuevas amenazas de la actividad maliciosa, criminal y terrorista son riesgos de seguridad difíciles de controlar y monitorear sin afectar la libertad personal. Asegurar las redes, rastrear los ataques y contrarrestar el extremismo ha impulsado el desarrollo de herramientas y técnicas *OSINT* (Best, 2012).

OSINT significa *OPEN SOURCE INTELLIGENCE* (en español Inteligencia de Fuentes Abiertas), se trata de un conjunto de técnicas y herramientas para recopilar información pública, correlacionar los datos y procesarlos.

Al igual que otras metodologías, cuando, se trabaja con *OSINT* se tiene diferentes fases o etapas a saber: Planificación, Selección de Fuentes, Obtención de Datos, Procesamiento, Análisis y Reporte. Todas ellas son importantes para avanzar con datos claros y no perderse entre la gran cantidad de información que existe en Internet. Sin embargo, para aquellos que recién se inician en estas técnicas, es algo problemático, por lo que una buena forma de empezar a familiarizarse con la metodología son las Guías de Flujos de Trabajo de *CIBERPATRULLA*.

Estas guías son muy útiles para ordenar la información y aprender a correlacionar los datos. Sin embargo, es necesario definir previamente los selectores y las palabras claves que se va a buscar.

OSINT funciona correctamente en todos los niveles de actividades de inteligencia en cada área de estudio, por lo que hay muchos actores que lo utilizan no solo para fines militares, sino también en el sector privado. La recuperación eficaz de información mediante OSINT ha encontrado su aplicación a nivel estratégico, operativo y táctico. En la era del desarrollo tecnológico, el uso de la "inteligencia blanca" OSINT ofrece muchas oportunidades nuevas para servicios especiales. (Ziółkowska, 2018)

En el sector de tecnologías de la información y la comunicación, se hace referencia a los sistemas que manipulan conjuntos de datos con el objeto de realizar predicciones valiosas con datos públicos que, se encuentra en el océano de internet, es así que la automatización de algoritmos permite generar conocimiento valioso de manera constante y en tiempo real, es aquí que un nuevo término denominado BIG DATA juega un rol importante.

La información resultante de las fases de OSINT es estandarizada y gestionada con el análisis de BIG DATA en el establecimiento y composición de predicciones útiles para tomar decisiones oportunas. (*Millan Lopez, Juan Antonio.pdf*, s. f.)

Los usos y aplicaciones de OSINT, se determinan a continuación:

- Identificación y prevención de posibles amenazas en el ámbito militar o de la seguridad nacional,
- Búsqueda y seguimiento de personas,
- Conocer la reputación online de un usuario o empresa,
- Realizar estudios sociológicos, psicológicos, lingüísticos, entre otros.,
- Auditorías de empresas y diferentes organismos, con el fin de evaluar el nivel de privacidad y seguridad,
- Evaluar tendencias de mercados,
- Documentación periodística,

- Análisis de mercado para lanzamiento de campaña de marketing,
- Estos son los usos más habituales de las técnicas de investigación OSINT.

(【*OSINT* 】*¿Qué Es?*, 2020)

Ventajas de OSINT

- Implica menos riesgos: recopilan información desde un despacho, la oficina o casa. No es necesario de hacer trabajo de campo ni que te desplazamiento a ningún lugar,
- Es más rentable: porque que en la mayoría de los casos es posible obtener la información de forma gratuita,
- Facilidad de acceso: se trata de fuentes abiertas a las que cualquiera accede,
- Actualización constante de la información: Cuando se usa éste sistema nunca, se topa con información obsoleta,
- Muy útil para cualquier tipo de investigación: cualquiera que sea el objetivo, ese sistema acelera el proceso de investigación,
- Ayuda a los profesionales de la seguridad: debido a que permite anticiparse a conflictos y sucesos, y así diseñar un plan de acción ajustado a las necesidades de la situación.

Desventajas de OSINT

- Exceso de información poco clara: la cantidad de información que hay en Internet es extensa. Tanto que uno de los principales problemas que tiene cualquier persona para aprender OSINT es que se ve incapaz de filtrar o jerarquizar,
- Fuentes poco fiables: las fuentes abiertas también acumulan una cantidad de información errónea o poco veraz, por lo que hay que aprender a discernir lo verídico de lo falso.

(【 *OSINT* 】*¿Qué Es?*, 2020)

Al igual que en otras metodologías, si se trabaja con OSINT, se aplica diferentes fases o etapas que se referencia en la Figura 1.

Figura 1. Fases de OSINT

Fuente: (CiberPatrulla - OSINT, s. f.)

1.3. Vulnerabilidades de Almacenamiento

1.3.1. OWASP

Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que un software sea inseguro, en su listado referente a vulnerabilidades de almacenamiento menciona algunos ejemplos:

En investigaciones realizadas, se hace mención a la utilización de guías de pruebas de penetración realizadas con OWASP es así que en un estudio realizado, se recopila información de robots, crawles y arañas , se hace referencia a OWASP-IG-001, motores de búsqueda descubrimiento, reconocimiento con (OWASP-IG-002), se identifica puntos de entrada en la aplicación (OWASP-IG-003). (Gómez Enciso, 2016)

Por otra parte, dentro del ámbito de la presente investigación, se aplica motores de búsqueda avanzados para la fase de reconocimiento y la verificación de vulnerabilidades que, se mencionan más adelante.

- Almacenamiento de credenciales y contraseñas en ficheros de configuración,
- Codificación de contraseñas de forma estática en el código de la aplicación,
- No borrado de datos no necesarios para la aplicación,
- Utilización de librerías criptográficas débiles.

Por otra parte, explica la forma correcta de prevención de estas vulnerabilidades de la siguiente forma:

- Evitar el almacenamiento de datos en lugares compartidos del sistema. En caso de que sea necesario, utilizar un esquema de cifrado fuerte,
- Deshabilitar la posibilidad de copiar la aplicación a la tarjeta *SD* del dispositivo,
- No crear ficheros dentro de la *SANDBOX* con permisos de lectura para otras aplicaciones,
- Utilizar siempre que sea necesario las *API* ofrecidas por los sistemas operativos para añadir una capa de cifrado adicional a los ficheros.

1.3.2. ISO 27001

Por otra parte, las vulnerabilidades informáticas son tratadas en el acápite 8 de la norma ISO 27001. Su correcta identificación es un aspecto clave de un sistema de seguridad de la información dentro del proceso de evaluación de riesgos.

Un punto de conexión a internet es siempre un posible punto de vulnerabilidad y, por lo tanto, un área donde, se requiere controles. En este sentido, la selección del control depende de la evaluación de la organización sobre la probabilidad y el impacto potencial de amenazas específicas y debe centrarse en tratar de reducir el nivel de amenaza o menorar el alcance de la vulnerabilidad.(Salazar Chacón, 2021)

De hecho, la mayoría de los incidentes de seguridad de la información, se originan dentro del perímetro de la organización.

El rango de vulnerabilidades en ISO 27001 es muy amplio. Por ello, se presenta un listado de vulnerabilidades, como una forma de apoyo para los profesionales que trabajan hoy en la implementación del sistema de gestión de seguridad de la información en esta tarea de identificación.(Gordón & Salazar-Chacón, 2020)

Listado vulnerabilidades en ISO 27001

- Interfaz de usuario complicada,
- Contraseñas predeterminadas no modificadas,
- Eliminación de medios de almacenamiento sin eliminar datos,
- Sensibilidad del equipo a los cambios de voltaje,
- Sensibilidad del equipo a la humedad, temperatura o contaminantes,
- Inadecuada seguridad del cableado,
- Inadecuada gestión de capacidad del sistema,
- Gestión inadecuada del cambio,
- Clasificación inadecuada de la información,
- Control inadecuado del acceso físico,

- Mantenimiento inadecuado,
- Inadecuada gestión de red,
- Respaldo inapropiado o irregular,
- Inadecuada gestión y protección de contraseñas,
- Protección física no apropiada,
- Reemplazo inadecuado de equipos viejos,
- Falta de formación y conciencia sobre seguridad,
- Inadecuada segregación de funciones,
- Mala segregación de las instalaciones operativas y de prueba,
- Insuficiente supervisión de los empleados y vendedores,
- Especificación incompleta para el desarrollo de software,
- Pruebas de software insuficientes,
- Falta de política de acceso o política de acceso remoto,
- Ausencia de política de escritorio limpio y pantalla clara,
- Falta de control sobre los datos de entrada y salida,
- Falta de documentación interna,
- Carencia o mala implementación de la auditoría interna,
- Falta de políticas para el uso de la criptografía,
- Falta de procedimientos para eliminar los derechos de acceso a la terminación del empleo,
- Desprotección en equipos móviles,
- Falta de redundancia, copia única,
- Ausencia de sistemas de identificación y autenticación,
- No validación de los datos procesados,
- Ubicación vulnerable a inundaciones,
- Mala selección de datos de prueba,
- Copia no controlada de datos,
- Descarga no controlada de Internet,
- Uso incontrolado de sistemas de información,
- Software no documentado,

- Empleados desmotivados,
- Conexiones a red pública desprotegidas,
- Los derechos del usuario no se revisan regularmente.

1.4. Metodologías para mitigar riesgos

Hoy día la mayoría de las compañías a nivel mundial se enfocan en manejar y cuidar a cabalidad su más valioso activo, en este caso, se determina dos tipos de activos: los primarios que incluyen la información y los secundarios o de apoyo, que incluyen Hardware, Software, Red, Usuarios y Estructura. Compañías que dedican 100% de sus operaciones a proteger y resguardar millones de datos organizados que contienen material confidencial y de la cual dependen cada una de ellas. Por tal razón, cualquier incidente o amenaza contra esta, ocasiona impactos adversos en los objetivos de la compañía.

A la existencia de estos riesgos, ya sea internos como fallas ocasionadas por el personal, mala administración de equipos y de información, operacionales, presupuestales, entre otros; y externos como los ambientales, entorno político, económico y legal; que de materializarse afectarían la continuidad de las operaciones, el cumplimiento de objetivos y metas, compromete el patrimonio de la empresa, es lo que a la mayoría de empresas les ha llevado a invertir millones de dólares para determinar y contrarrestar esas vulnerabilidades, físicas y lógicas. (Kluppelberg & Straub, 2014)

Para hablar de gestión de riesgo, se define inicialmente qué es el riesgo, el cual es como una probabilidad que ocurra un evento para que el mismo sea previsto y evitado, las amenazas y las vulnerabilidades por separadas no llegan a presentar un daño de grandes magnitudes, en cambio, si se mezclan la probabilidad de daño es mucho más grande.

En el siguiente apartado, se da a conocer sobre dos metodologías que permiten gestionar el riesgo como son:

- OCTAVE,
- MAGERIT.

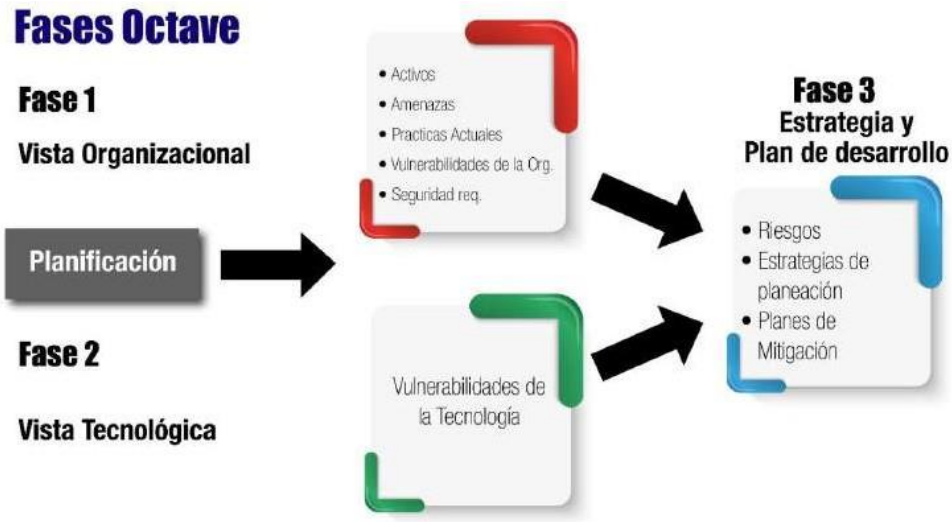
1.4.1. Metodología OCTAVE

OCTAVE (*OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION*), es una técnica de evaluación de riesgos desarrollada por el SEI (*SOFTWARE ENGINEERING INSTITUTE)* en Estados Unidos. Es reconocida a nivel mundial y ha tenido excelente adaptación. Las fases que la componen la catalogan como más complicada que las demás metodologías. La misma está enfocada en el riesgo y no en la tecnología como las demás, si se usa este tipo de metodología personal de varios departamentos como el operativo, el de tecnología, entre otros; trabajan en conjunto proyectados a la necesidad de seguridad, apoyados por un especialista.(Devia & Calvache, 2014)

Es necesario considerar, que esta metodología fue desarrollada para ser implementada en organizaciones de más de 300 empleados y se encuentra dividido en tres etapas:

- La fase 1 *BUILD ASSET-BASED THREAT PROFILES*, desarrollar perfiles de amenazas basados en los activos, en la cual, se identifican los bienes, las amenazas, prácticas actuales, vulnerabilidades y los recursos de seguridad de la compañía,
- La fase 2, *IDENTIFY INFRASTRUCTURE VULNERABILITIES*, identificar las vulnerabilidades de la infraestructura, se basa en los componentes clave y sus correspondientes vulnerabilidades técnicas,
- Por último, en la fase 3 *DEVELOP SECURITY STRATEGY AND PLANS*, desarrollar estrategias y planes de seguridad, con base a los riesgos, la estrategia de protección y los planes de mitigación.

Figura 2. Fases OCTAVE



Fuente: (ENISA, s. f.)

1.4.2. Metodología MAGERIT

Acrónimo de Metodología de Análisis y Gestión de Riesgo de Sistemas de la Información, el Consejo Superior de Administración Electrónica de España (CSAE), considera que la sociedad depende mucho de las tecnologías de la información y las comunicaciones para la consecución de los objetivos. El uso de las mismas proporciona una variedad de beneficios y de igual manera abre una brecha para el surgimiento de riesgos que deben ser neutralizados con las medidas de seguridad que promuevan la confianza de los usuarios que manejen la estructura.

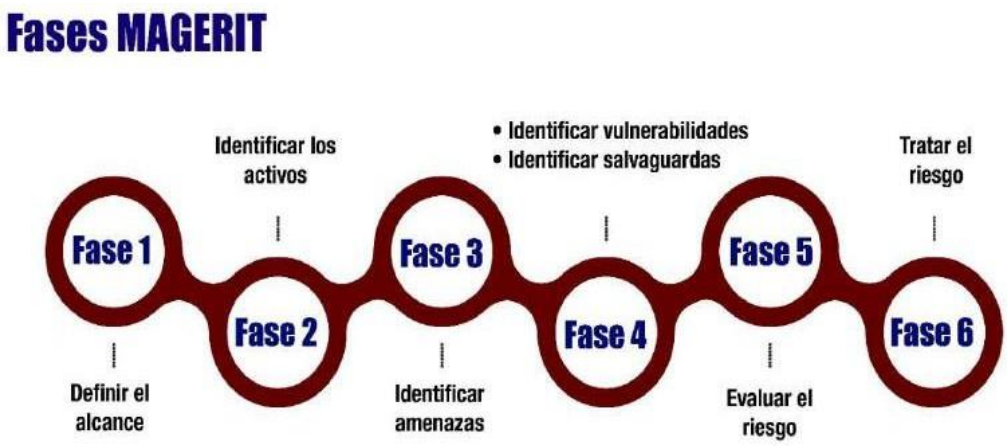
MAGERIT fue creada en el año de 1997 y actualmente, se encuentra en su tercera versión, esta metodología trabaja con términos como:

- Activos,
- Amenazas,
- Vulnerabilidades,
- Impacto,
- Riesgos,

- Contingencia.

La cuáles son ramales fundamentales en el análisis y gestión del riesgo. Si bien, el avance de la tecnología ha permitido el crecimiento exponencial de los beneficios de la misma, de igual manera, las vulnerabilidades cada día son más y los invasores incrementan el interés de ese llamado juego para romper las barreras y acceder a la información, por tal razón, MAGERIT ha parametrizado el método de trabajo actualizado en cada uno de sus componentes, se renueva cada programa obsoleto y se crea nuevos sistemas de información a la vanguardia de la tecnología.

Figura 3. Fases MAGERIT



Fuente:(PAe - Inicio, s. f.)

Cuadro 1 Comparativo entre la metodología MAGERIT y OCTAVE

METODOLOGIAS	OCTAVE	Pts.	MAGERIT	Pts.
Características Principales	• Construcciones de los perfiles de amenazas basados en activos. • Identificación de la infraestructura de vulnerabilidad. • Desarrollo de planes y estrategias de seguridad.	**5**	• Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarles. • Ofrecer un método sistemático para analizar los riesgos derivados del uso de las tecnologías de la información y comunicaciones. • Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control indirecto. • Preparar a la Organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.	**5**
Ámbito de aplicación	• Octave usa como herramientas de apoyo o aplicación a Octave Automated Tool. • Aplica a PYME (Pequeña y mediana empresa)	**4**	• Gobierno, organismos, compañías grandes, PYME, compañías comerciales y no comerciales. • Magerit ofrece una aplicación para el análisis y gestión de riesgos de un sistema de información denominado PILAR (Proceso Informatico lógico para el análisis de gestión de riesgos) Esta herramienta es de uso gratuito para la administración española y de uso comercial para las organizaciones privadas.	**5**

Ventajas	• Cualquier metodología que aplica los criterios (principio, atributos y resultados) es considerados compatible con la metodología octave • Involucra todo el personal de la entidad • Es la mas completa, involucra como elementos de su modelo de análisis: procesos, activos y dependencias, recursos, vulnerabilidades, amenazas y salvaguardas.	**4**	• Es metódica por lo que, se hace fácil su comprensión. • Los activos, se identifican, tipifican y buscan sus dependencias se valoran en cuanto a: disponibilidad, confidencialidad, autenticidad, integridad y trazabilidad. • Comprende los procesos de análisis y gestión de riesgos. • Usa un modelo de análisis de riesgos cualitativo y cuantitativo. • Soporta herramientas comerciales EAR y NO comerciales PILAR, así como las normas ISO/IEC 27001:2005, ISO/IEC 15408:2005, ISO/IEC 17799:2005	**5**
Desventajas	• Aplicable solo en PYME (Pequeña y mediana empresa). • No tiene compatibilidad con estándares.	**3**	• No toma en cuenta el principio de no repudio de la información como objetivo de seguridad. • No toma en cuenta un análisis de vulnerabilidad. • La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión y evaluación. • Comprende como elementos del modelo de análisis solo: activos y dependencias, vulnerabilidades y amenazas. • La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos.	**5**
Total	OCTAVE	**16**	MAGERIT	**20**

Fuente: Elaboración Propia

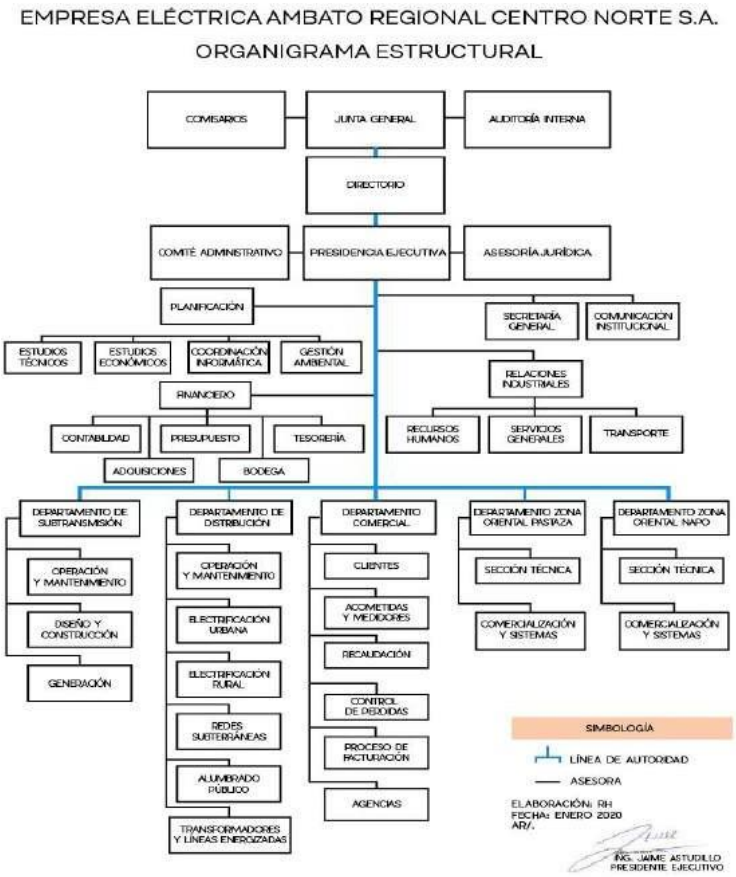
El cuadro 1 muestra que la aplicación de Magerit es más adecuado para la presente investigación y de la información que se dispone luego del estudio de OSINT.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la Institución

Empresa Eléctrica Ambato Regional Centro Norte S.A. (EEASA) es una institución dedicada a la distribución de energía eléctrica en la zona central del país. Su actividad económica está comprometida con el desarrollo de los sectores urbanos y rurales de su área de concesión, y en su misión está claramente definido el compromiso con la calidad y continuidad del servicio eléctrico. Como es normal en las organizaciones y sucede también con los seres vivos, la incidencia de factores internos y externos promueve la rápida adaptación con el medio, a fin de garantizar su supervivencia y fortalecimiento en el tiempo. Para la EEASA, el caso más palpable es su transformación de empresa netamente privada a empresa pública, lo cual ha desencadenado una serie de retos por enfrentar en el corto y mediano plazo. La empresa hace lo más adecuado cuando arremeten los desafíos: enfrentarlos. En la delicada tarea de manejar recursos públicos, la Administración de la empresa pone todo su empeño para cumplir la misión institucional; sin embargo, también es consciente que toda tarea, por bien hecha que se encuentre, es susceptible de mejora. Uno de los aspectos a mejorar es la gestión de la seguridad de la información, que constituyen uno de sus activos más importantes. El presente trabajo de investigación aporta alternativas de mejora mediante la implementación de una metodología para mitigar vulnerabilidades de almacenamiento con la aplicación de inteligencia de fuentes abiertas. Dentro de las respuestas al riesgo, se incluye un método utilizado para identificar, evaluar y mitigar la información confidencial que se encuentra en fuentes abiertas, lo cual genera disponibilidad en los servicios de manera ininterrumpida la cual aporta a una buena imagen nacional e internacional en la calidad del servicio.

Figura 4. Organigrama funcional EEASA



Fuente: EEASA (2021)

2.2. Metodología de investigación

El enfoque de investigación utilizado para el desarrollo del presente proyecto es el cuantitativo y diseño preexperimental, por cuanto preliminarmente, se utiliza fuentes abiertas de varias herramientas; para luego clasificarlas y pormenorizarlas para análisis de las vulnerabilidades de almacenamiento encontradas.

2.2.1. Enfoque de investigación

Diseño Pre-Experimental

Según Fidias Arias “Como su nombre lo indica, este diseño es una especie de prueba o ensayo que, se realiza antes del experimento verdadero. Su principal limitación es el escaso control sobre el proceso, por lo que su valor científico es muy cuestionable y rebatible”.

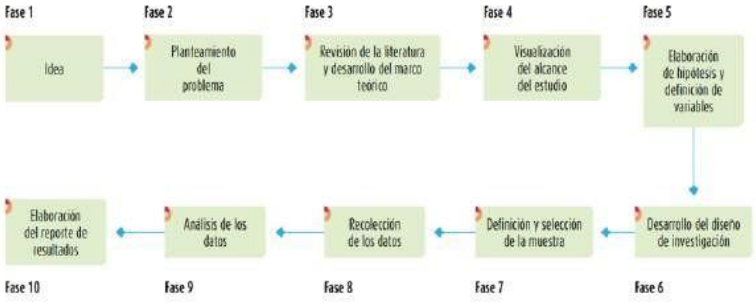
Según Sampieri “Diseño de un solo grupo cuyo grado de control es mínimo. Generalmente es útil como un primer acercamiento al problema de investigación en la realidad”.

2.2.2. Tipo de Investigación

Cuantitativa

El enfoque cuantitativo es secuencial y probatorio. Cada etapa precede a la siguiente y no “brinca” o elude pasos. El orden es riguroso, aunque desde luego, se redefine alguna fase. Parte de una idea que se acota y, una vez delimitada, se derivan objetivos y preguntas de investigación, se revisa la literatura y, se construye un marco o una perspectiva teórica. De las preguntas, se establecen hipótesis y determinan variables; se traza un plan para probarlas (diseño); se miden las variables en un determinado contexto; se analizan las mediciones obtenidas con métodos estadísticos, y se extrae una serie de conclusiones respecto de la o las hipótesis. Este proceso se representa en la figura 5.

Figura 5. Fases Método Cuantitativo



Fuente: Sampieri (2019)

2.2.3. Técnicas e instrumentos

Planteamiento del problema

El problema planteado como pregunta es: ¿Hay una forma adecuada de gestionar las vulnerabilidades de las fuentes de información pública de la EEASA?

Planteamiento de hipótesis

El diseño de una metodología mitiga las vulnerabilidades de almacenamiento detectadas mediante la aplicación de OSINT de manera ética para la EEASA.

Definición de variables

Variables Dependientes

- OSINT
- OWASP
- ISO27001

Variable independiente

- Metodología

Operacionalización de variables

Cuadro 2. Operacionalización de variable dependiente

TIPO	VARIABLE	DESCRIPCIÓN	INDICADOR	TÉCNICAS	INSTRUMENTOS
DEPENDIENTE	OSINT	No. entero de puertos abiertos, correos, dns, subdominios	Cantidad de información disponible en fuentes abiertas	observación directa	Software
	OWASP	No. entero vulnerabilidades almacenamiento	Cantidad de vulnerabilidades	observación directa	Listas
	ISO27001	No. entero vulnerabilidades almacenamiento	Cantidad de vulnerabilidades	observación directa	Listas

Fuente: elaboración propia

Cuadro 3. Operacionalización de variable independiente

TIPO	VARIABLE	DESCRIPCIÓN	TÉCNICAS	INSTRUMENTOS
INDEPENDIENTE	Metodología	Diseño de metodología para mitigar vulnerabilidades	SCRUM	MAGERIT

Fuente: elaboración propia

Procedimiento y recolección de datos

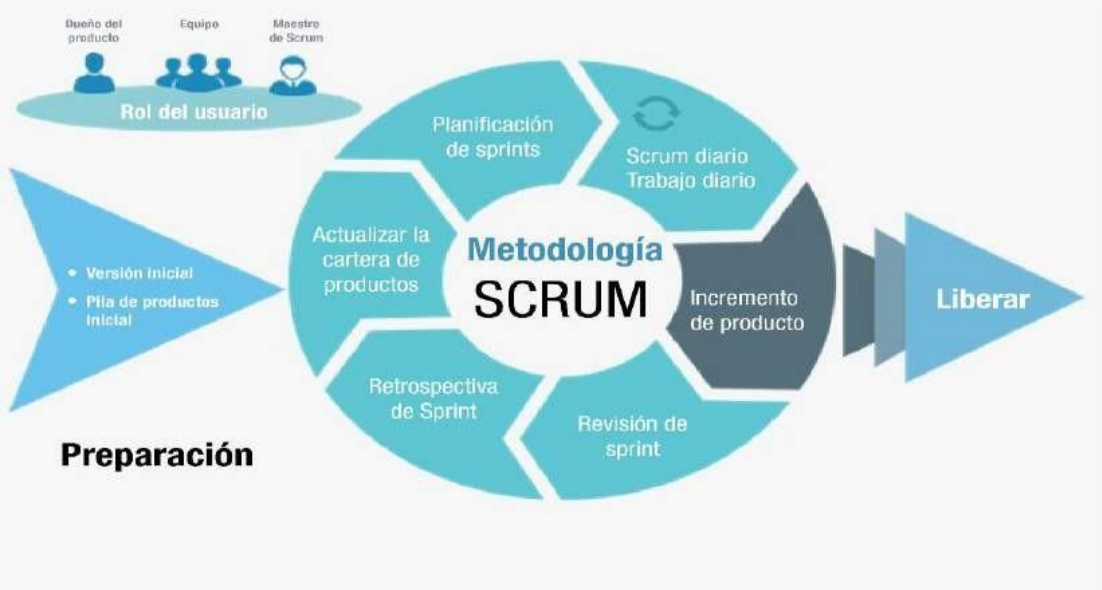
Se utilizó la técnica de observación y búsqueda de información bibliográfica en sitios web sobre la solución propuesta, se consideró artículos científicos de alto nivel en su mayoría de la IEEE, los cuales permiten organizar la información para detectar vulnerabilidades informáticas.

Finalmente, para la verificación de la hipótesis, se utilizó el software R como herramienta de análisis estadístico.

2.3. Metodología de desarrollo

La metodología aplicada al presente trabajo es SCRUM por su importante aporte en la gestión de los flujos de trabajo y mejoramiento continuo de la productividad como, se aprecia en la figura 6. Permite probar los productos sin tener que pasar por todo el ciclo de producción.

Figura 6. Fases SCRUM



Fuente: Inicio | Scrum.org, s. f. (2021)

Un equipo Scrum está compuesto por el equipo (Investigador), el Maestro Scrum (director de Tesis) y el dueño del producto (Investigador), en el cuadro 3, se define a cada uno de sus integrantes con su respectivo rol.

Cuadro 4 Roles SCRUM

Rol	Cargo	Actividades
Dueño del producto	**Investigador**	Es el dueño del producto. Realiza la lista de prioridades, donde, él es el encargado de ver que el producto cumpla su propósito, también, es responsable de las ganancias o pérdidas del producto trabajado con el Equipo, es importante indicar que únicamente existe un dueño del producto.
Maestro Scrum	**Director de Tesis**	Es el líder del equipo Scrum, donde, pone en práctica SCRUM, sus reglas y valores. Realiza el Daily Scrum, donde, informa del progreso del producto. También, es el responsable de que exista un buen ambiente entre el equipo. Debe estar presente en todas las etapas del Sprint de SCRUM.
Equipo	**Investigador**	Grupo de profesionales con los conocimientos técnicos necesarios y que desarrollan el proyecto de manera conjunta la cual lleva a cabo las historias a las que comprometen al inicio de cada sprint.

Fuente: elaboración propia

Los artefactos Scrum que, se aplican al proyecto son: pila del producto, pila de sprint, Producto incremental, en razón de lo expuesto en el cuadro 4 se explica cada uno de los productos del trabajo a obtener:

Cuadro 5 Artefactos SCRUM

Artefacto	**Descripción**	**Entregable**
Pila del Producto	Lista ordenada en cualquier formato que contiene todos los requerimientos a implementar en el producto. Debe de estar gestionado por el dueño del producto y la única condicionante es que esté priorizado con aquellos temas que tengan más valor en ese momento	Listado ordenado y priorizado de los requisitos necesarios para la implementación de un proyecto
Pila de sprint	Plan detallado para el desarrollo del próximo sprint y está gestionado por el equipo quien, se encarga de mantenerlo actualizado durante la ejecución.	Lista de tareas identificadas por el equipo de desarrollo.
Producto incremental	Resultado requerido de cada Sprint. Es una versión integrada del producto, mantenida con una calidad lo suficientemente alta como para ponerse en producción si el dueño del producto lo deseara.	Tabla del trabajo pendiente, en progreso y concluido.

Fuente: elaboración propia

La planificación, se la desarrolla con la siguiente estructura de sprints:

Sprint 1 - Inicio. - en esta etapa, se recolecta todos los requisitos y variables de aplicación directa al tema de investigación pues, se establece una forma sistemática de OSINT, MAGERIT y de las vulnerabilidades establecidas en la ISO 270001 y OWASP.

Producto Incremental:

Listado de fases de metodologías y vulnerabilidades aplicadas a la investigación.

Sprint 2- Planificación y estimación. – En esta etapa, se viabiliza la recolección de información desde fuentes abiertas y una aplicabilidad de MAGERIT en lo referente a las vulnerabilidades de almacenamiento.

Producto Incremental:

Aplicación de las fases que contiene cada metodología aplicada en la investigación.

Sprint 3- Implementación. - En esta etapa, se gestiona de riesgos descubiertos en el caso de estudio.

Producto incremental:

Listado de recomendaciones que permite gestionar el riesgo descubierto en la investigación.

Sprint 4- Revisión y retrospectiva. - En esta etapa, se evalúa la propuesta metodológica.

Producto incremental

Evaluación del planteamiento de la propuesta metodológica realizado por un experto.

Sprint 5-Lanzamiento. - Finalmente, se redacta de manera formal la metodología del proyecto como un documento.

Producto incremental:

Propuesta metodológica aceptada por parte del dueño del producto.

La actividad para cada sprint, se desarrolla en tiempos específicos y su ejecución, se establece de la siguiente forma:(Rivas & Salazar, 2019, pp. 800-834)

Figura 7. Estructura Sprints

Fuente: elaboración propia

2.3.1. Sprint 1 – Inicio

El sprint inicial tiene como objetivo conocer y definir las fases que dispone los métodos *OSINT* y *MAGERIT* para mitigar las vulnerabilidades de almacenamiento identificadas en OWASP e ISO 27001 como, se observa en el cuadro 5, esto permite fijar y establecer los entregables en corto tiempo de manera ordenada y concreta.

Cuadro 6. Definición de fases de los modelos aplicados y listado de vulnerabilidades objeto de estudio

Fases OSINT	Fases *MAGERIT*	Vulnerabilidades de Almacenamiento
1. Requisitos, 2. Fuentes, 3. Adquisición, 4. Procesamiento, 5. Análisis, 6. Presentación.	1. Caracterización de activos, 2. Caracterización de amenazas, 3. Caracterización de salvaguardas, 4. Estimación del estado del riesgo.	1. Listas OWASP 2. Listas ISO 27001

Fuente: elaboración propia

2.3.2. Sprint 2 - Planificación y estimación

Para el cumplimento de este sprint, se aplica las fases de OSINT y MAGERIT, se delimita el objeto de estudio a las vulnerabilidades de almacenamiento definidas por OWASP e ISO27001, esto permite tanto al maestro de scrum y al equipo validar la pila del producto y planificar la pila de sprint.

FASES OSINT – Pila de sprint

La presente pila de sprint tiene como objetivo detallar el plan para el desarrollo del próximo sprint esto es gestionado por el equipo quien, se encarga de actualizar el porcentaje de avance durante la ejecución de cada uno de los requisitos.

Fase 1.- Requisitos

En esta fase, se establece el objetivo de búsqueda para determinar la utilidad de la información y formatos de los informes obtenidos. En virtud de aquello, se da a conocer los siguientes pasos a través de la Figura 8.

Figura 8. Pasos para recolección de requisitos

Fuente: elaboración propia

Fase 2.- Fuentes

En este epígrafe, se identifica las fuentes relevantes para cumplir el objetivo de la fase 1 y, para elaborar esta tarea, se utiliza herramientas *Open Source* propias del sistema operativo *KALI,* pues es importante destacar 2 actividades previas que, se mencionan a continuación.

Identificación de escenario de ejecución técnicas OSINT

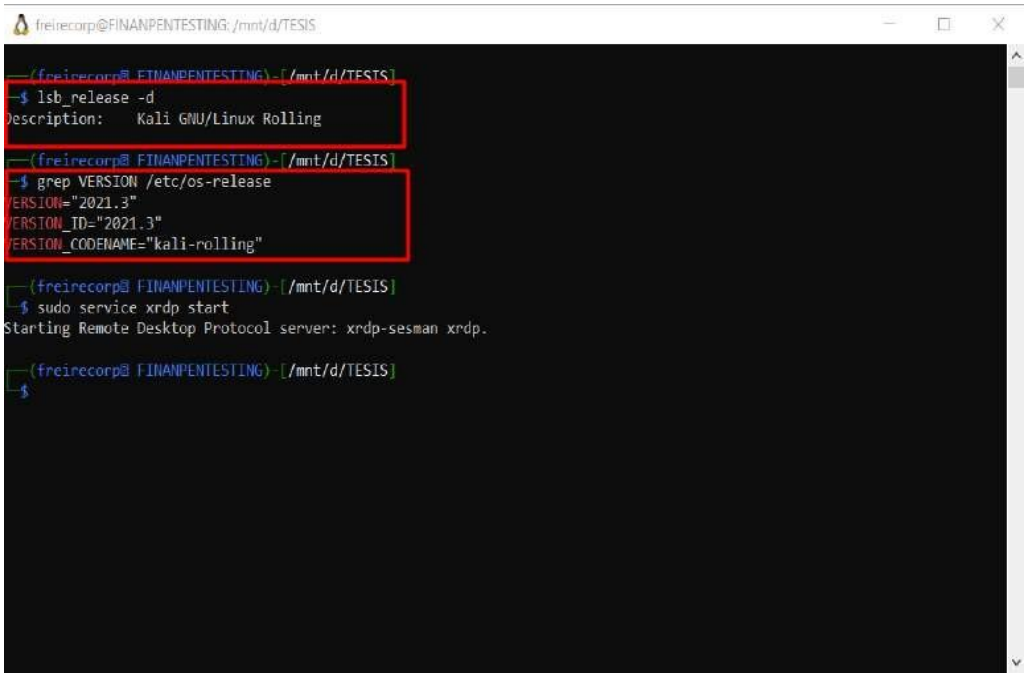
Para la recolección de información mediante OSINT, se utiliza subsistema de Windows para Linux, el cual es una característica introducida en Windows 10 que permite instalar un *KERNEL* Linux directamente sobre el sistema operativo de Microsoft. Esto gracias a la virtualización de *HYPER-V,* para una mejor compresión sobre la configuración de esta utilidad, se establece en el Anexo 1 el modo de instalación y configuración de WSL 2, XCFE y XRDP.

A continuación, se muestra las versiones utilizadas tanto de Windows como sistema base y KALI como subsistema:

Figura 9.Sistema Operativo Base

Fuente: elaboración propia

Figura 10.Subsistema de Windows para Linux



Fuente: elaboración propia

Identificación palabras de búsqueda

Se utiliza navegador Microsoft Edge Versión 96.0.1054.43 con el un motor de búsqueda https://www.google.com/ para digitar el nombre de la empresa y conocer el dominio.

Finalmente, en el cuadro 6, se da a conocer las fuentes que se utilizan para enumerar los activos de la empresa.

Cuadro 7 Fuentes para enumeración de activos

Item	**Fuente**	**Entrada**	**Salida**
1	*Fast-Google-Dorks-Scan*	Dominio de la empresa	Archivo Plano
2	*Dmitry*	Dominio de la empresa	Archivo Plano
3	*Nexfil*	Nombre de la empresa	Archivo Plano
4	*Theharvester*	Dominio de la empresa	Archivo Plano
5	*Maltego*	Dominio de la empresa	Hoja de Calculo
6	*Iky*	Correos	Hoja de Calculo

Fuente: elaboración propia

Fase 3.- Adquisición

Para la obtención de la información, se selecciona datos de interés a través de las fuentes abiertas como por ejemplo ip, páginas web y archivos multimedia. En esta sección, se realiza la ejecución de herramientas identificadas referirse al Anexo 2 para conocer los resultados del estudio OSINT , obtiene los resultados tabulados a continuación:

Dorks

Para la ejecución automática de DORKS de Google, se utiliza un DOCKER denominado "*FAST-GOOGLE-DORKS-SCAN*" creado por la empresa RECONSHELL ON SECURITY que fue fundada en septiembre de 2020, por profesionales de la seguridad cibernética. La herramienta fue publicada el 6 de noviembre del 2021 a través de GIT (Sebastian, s. f.).

Cuadro 8. Resultados de FAST-GOOGLE-DORKS-SCAN -OSINT

Dominio analizado	**"eeasa.com.ec"**
CHECK LOGIN	La herramienta detecta 3 sitios que contiene la palabra "LOGIN", se menciona 3: https://sig.eeasa.com.ec/arcgis/sharing/login https://sigsrv.eeasa.com.ec/arcgis/login/ https://sigsrv.eeasa.com.ec/arcgis/rest/services/Utilities/OfflinePackaging/GPServer
CHECK PORTAL	La herramienta detecta 7 sitios que contienen la palabra "PORTAL", se menciona 3: https://sig.eeasa.com.ec/arcgis/portalhelp/en/portal/latest/use/embedded-content.htm https://www.eeasa.com.ec/content/uploads/2021/12/Logotipo-Ministerio-Sponsor_MERNNR-1.png https://www.eeasa.com.ec/portal-web-mi-eeasa/
CHECK AUTH	La herramienta detecta 2 sitios que contienen la palabra "AUTH" , se menciona 2: https://proveedores.eeasa.com.ec/auth/forgot-password https://proveedores.eeasa.com.ec/auth/register
CHECK FILES	La herramienta detecta 4 archivos ofimáticos y 64 PDF, se mencionan 1 de cada tipo: DOC https://www.eeasa.com.ec/content/uploads/2020/09/Formulario_21_dc.doc DOCX https://www.eeasa.com.ec/content/uploads/2021/01/invitacion.docx XLS https://www.eeasa.com.ec/content/uploads/2020/12/A2-OCTUBRE.xls XLSX https://www.eeasa.com.ec/content/uploads/2020/11/A3-NORMATIVA.xlsx PDF https://www.eeasa.com.ec/content/uploads/2021/09/Instructivo_SISSOL_WEB.pdf
NO DETECTA	FILES PPT, PPTX, MDB, SQL, TXT, RTF, CSV, XML, CONF, DAT, INI ,LOG ,ID_RSA. PATH TRAVERSAL "INDEX OF" "PARENT DIRECTORY" ,"INDEX OF" "DCIM" ,"INDEX OF" "FTP" ,"INDEX OF" "BACKUP" "INDEX OF" "MAIL","INDEX OF" "PASSWORD", "INDEX OF" "PUB"

Fuente: elaboración propia

Dmitry

Revela toda la información disponible sobre un host. Se utiliza para realizar búsquedas de Internet, número whois, recuperar la hora del sistema y los datos del servidor. La capacidad de realizar búsquedas de subdominios en un objetivo. también realiza la exploración de los puertos TCP.

Cuadro 9. Resultados de DMITRY-OSINT

Dominio analizado	***"eeasa.com.ec"***
Subdominios	*La herramienta detecta 5 subdominios:* *www.eeasa.com.ec* *servicios.eeasa.com.ec* *www2.eeasa.com.ec* *zimbra.eeasa.com.ec* *proveedores.eeasa.com.ec*
IP ADDRESS	*La herramienta detecta 4 direcciones IP* *186.42.191.28* *190.95.194.68* *190.95.194.89* *190.95.194.70*
Puertos	*Análisis de IP 190.95.194.70* *Port State* *25/TCP filtered* *80/TCP open* *Segmentation fault*

Fuente: elaboración propia

Nexfil

Herramienta OSINT escrita en Python permite buscar perfiles por nombre de usuario. Los nombres de usuario se verifican en más de 350 sitios web en pocos segundos. El objetivo de esta herramienta es obtener resultados rápidamente mientras se mantienen bajas cantidades de falsos positivos.

Cuadro 10.Resultados de NEXFIL – Palabra “EEASA”-OSINT

Perfil analizado:	“EEASA”
Perfiles detectados	http://en.gravatar.com/EEASA https://namemc.com/profile/EEASA https://eeasa.slack.com https://www.facebook.com/Eeasa https://www.clozemaster.com/dashboard https://issuu.com/EEASA https://forums.kali.org/member.php?username=EEASA https://quizlet.com/eeasa https://www.quora.com/profile/Eeasa https://ask.fm/EEASA https://www.reddit.com/user/EEASA https://scratch.mit.edu/users/EEASA/ https://eeasa.blogspot.com/ https://soundcloud.com/EEASA https://github.com/EEASA https://eeasa.newgrounds.com https://fortnitetracker.com/profile/all/EEASA

Fuente: elaboración propia

Cuadro 11. Resultados de NEXFIL - Palabra “EMPRESAELECTRICAAMBATO”-OSINT

Perfil analizado:	“EMPRESAELECTRICAAMBATO”
Perfiles detectados	https://namemc.com/profile/EmpresaElectricaAmbato https://www.facebook.com/EmpresaElectricaAmbato https://www.reddit.com/user/EmpresaElectricaAmbato https://issuu.com/EmpresaElectricaAmbato https://forums.kali.org/member.php?username=EmpresaElectricaAmbato https://www.clozemaster.com/dashboard https://blog.naver.com/EmpresaElectricaAmbato https://www.hackerearth.com/@EmpresaElectricaAmbato https://dlive.tv/EmpresaElectricaAmbato https://vote.casually.cat/u/EmpresaElectricaAmbato

Fuente: elaboración propia

Theharvester

Es una herramienta para conseguir información sobre emails, subdominios, hosts, nombres de empleados, puertos abiertos, banners, y demás, desde fuentes públicas como son los motores de búsqueda, servidores PGP, la red social LinkedIn y la base de datos de SHODAN (Buscador parecido a *GOOGLE* pero con la diferencia que no indexa contenido, si no que registra cualquier dispositivo conectado a Internet).

Cuadro 12. Resultados de THEHARVESTER-OSINT

Dominio analizado	"eeasa.com.ec"
Subdominios	La herramienta detecta 9 subdominios: app.eeasa.com.ec: dns1.eeasa.com.ec: dns2.eeasa.com.ec: mail.eeasa.com.ec: ntp.eeasa.com.ec: www.eeasa.com.ec: www1.eeasa.com.ec: www2.eeasa.com.ec: zimbra.eeasa.com.ec:
IP ADDRESS	La herramienta detecta 11 direcciones IP 186.42.191.28 186.42.191.4 190.95.194.67 190.95.194.68, 186.42.191.5 190.95.194.67 186.42.191.9 190.95.194.66, 186.42.191.6 186.42.191.5 186.42.191.7

Fuente: elaboración propia

Maltego

Herramienta para recopilar información en la web, y la potencia que posee, permite hallar perfiles en cualquier red social que levanten alguna sospecha de operaciones malintencionadas. La herramienta es capaz de hacer búsquedas de dominios, direcciones de correo electrónico, números telefónicos, entre otras utilidades.

Cuadro 13. Resultados de MALTEGO-OSINT

Dominio analizado	eeasa.com.ec
Correos Detectado	imorales@eeasa.com.ec ivargas@eeasa.com.ec jastudillo@eeasa.com.ec mbarrera@eeasa.com.ec mroldan@eeasa.com.ec mtorres@eeasa.com.ec presidencia@eeasa.com.ec
Web Archive	eeasa.com.ec,https://web.archive.org/web/20040609163853if_/http://www.eeasa.com.ec:80/ eeasa.com.ec,https://web.archive.org/web/20040728093409if_/http://www.eeasa.com.ec:80/ eeasa.com.ec,https://web.archive.org/web/20040831043701if_/http://www.eeasa.com.ec:80/ eeasa.com.ec,https://web.archive.org/web/20040928181229if_/http://www.eeasa.com.ec:80/ eeasa.com.ec,https://web.archive.org/web/20041206235546if_/http://www.eeasa.com.ec:80/ eeasa.com.ec,https://web.archive.org/web/20050130114926if_/http://eeasa.com.ec:80/ eeasa.com.ec,https://web.archive.org/web/20050210164728if_/http://www.eeasa.com.ec:80/ eeasa.com.ec,https://web.archive.org/web/20050309050216if_/http://www.eeasa.com.ec:80/ eeasa.com.ec,https://web.archive.org/web/20050408064826if_/http://www.eeasa.com.ec:80/ eeasa.com.ec,https://web.archive.org/web/20050903222902if_/http://www.eeasa.com.ec:80/ eeasa.com.ec,https://web.archive.org/web/20060414054632if_/http://eeasa.com.ec:80/ eeasa.com.ec,https://web.archive.org/web/20060420091828if_/http://eeasa.com.ec:80/ eeasa.com.ec,https://web.archive.org/web/20110208203455if_/http://www.eeasa.com.ec/ eeasa.com.ec,https://web.archive.org/web/20131221090844if_/http://www.eeasa.com.ec/ eeasa.com.ec,https://web.archive.org/web/20140517211037if_/http://www.eeasa.com.ec/ eeasa.com.ec,https://web.archive.org/web/20140526225612if_/http://www.eeasa.com.ec/
Sitios relacionados	eeasa.com.ec,_spf.google.com eeasa.com.ec,aortiz@eeasa.com.ec eeasa.com.ec,app.eeasa.com.ec eeasa.com.ec,consultasec.com eeasa.com.ec,csolis@eeasa.com.ec eeasa.com.ec,dns1.eeasa.com.ec eeasa.com.ec,dns1.eeasa.com.ec eeasa.com.ec,dns2.eeasa.com.ec eeasa.com.ec,dns2.eeasa.com.ec eeasa.com.ec,ec.todosnegocios.com eeasa.com.ec,ecuadorec.com eeasa.com.ec,eeasa.com eeasa.com.ec,eeasa.com.ec eeasa.com.ec,eeasa.org

Fuente: Elaboración propia

Iky

Es una herramienta que busca ser simple y visual, con la premisa de estar al alcance de cualquiera que la necesite.

Cuadro 14. Resultados de IKY – Correo cxxxxs@eeasa.com.ec- OSINT

Correo analizado	"cxxxxs@eeasa.com.ec"
vínculos Detectados	EMAILREP cxxxxs@eeasa.com.ec User 100 SUCCESS LEAKLOOKUP cxxxxs@eeasa.com.ec User 100 SUCCESS SEARCH cxxxxs IKY 1 PROCESS SHERLOCK cxxxxs IKY 1 SUCCESS HOLEHE csolis@eeasa.com.ec User 100 SUCCESS FULLCONTACT csolis@eeasa.com.ec User 100 SUCCESS PEOPLEDATALABS csolis@eeasa.com.ec User 100 PROCESS LEAKS csolis@eeasa.com.ec User 100 SUCCESS DARKPASS csolis@eeasa.com.ec User 100 SUCCESS SOCIALSCAN csolis@eeasa.com.ec User 100 SUCCESS

Fuente: elaboración propia

Cuadro 15. Resultados de IKY – Correo "jxxxxxxxxo@eeasa.com.ec"-OSINT

Correo analizado	"jxxxxxxxxo@eeasa.com.ec"
Vínculos Detectados	EMAILREP jxxxxxxxxo @eeasa.com.ec USER 100 SUCCESS LEAKLOOKUP jxxxxxxxxo @eeasa.com.ec USER 100 SUCCESS HOLEHE jxxxxxxxxo @eeasa.com.ec USER 100 SUCCESS FULLCONTACT jxxxxxxxxo @eeasa.com.ec USER 100 SUCCESS PEOPLEDATALABS jxxxxxxxxo @eeasa.com.ec USER 100 PROCESS LEAKS jxxxxxxxxo @eeasa.com.ec USER 100 SUCCESS DARKPASS jxxxxxxxxo @eeasa.com.ec User 100 SUCCESS SOCIALSCAN jxxxxxxxxo @eeasa.com.ec User 100 SUCCESS

Fuente: elaboración propia

Fase 4.- Procesamiento

En esta fase, se realizó un proceso de homologación de la información para establecer dimensiones dentro del ámbito de los activos detectados, se denota el siguiente resumen de herramientas *OSINT* con el número de coincidencias encontradas por cada palabra clave digitada.

Resultados OSINT

Cuadro 16. Resultados totalizados de manera general -OSINT

DESCRIPCIÓN – HERRAMIENTA	DORKS	DMITRY	NEXFIL		THEHARVESTER	IKY		MALTEGO
PALABRA CLAVE	eeasa.com.ec	eeasa.com.ec	EEASA	EMPRESAELECTRICAAMBATO	Eeasa.com.ec	jastudillo@eeasa.com.ec	csolis@eeasa.com.ec	Eeasa.com.ec
Web archivadas	-	-	-	-	-	-	-	24
Sitios Web activos	12	-	-	-	-	-	-	22
Puertos Abiertos	-	2	-	-	-	-	-	
Correos	-	-	-	-	-	-	-	13
Archivos multimedia	68	-	-	-	-	-	-	-
Subdominios	-	5	-	-	9	-	-	-
Direcciones IP	-	4	-	-	11	-	-	-
Perfiles Sociales	-		27	10	-	18	18	-
Total:	80	11	27	10	20	18	18	59

Fuente: Elaboración propia

Fase 5.- Análisis

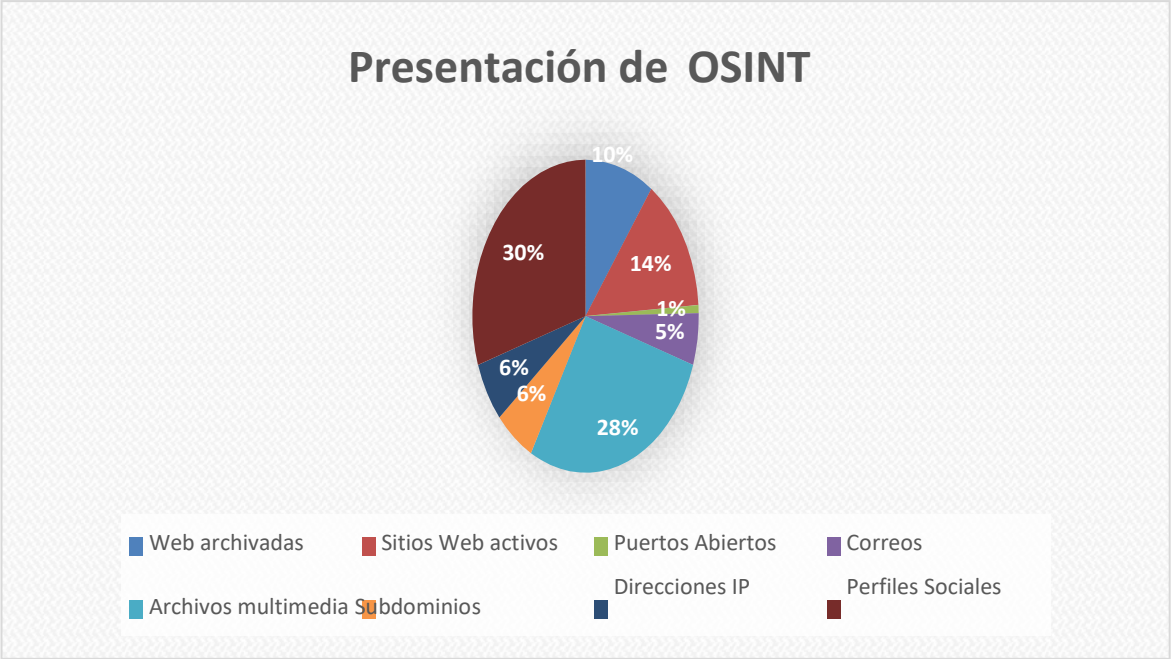
Luego de tabular la información encontrada en OSINT, se concluye lo siguiente:

- Con la ejecución de los Dorks de Google, se encontró sitios web archivados de páginas de contenido obsoletas de la EEASA y algunos archivos multimedia que contienen metadatos con el nombre del terminal y del usuario creador del contenido.
- La herramienta Dmitry reveló la información de puertos abiertos, subdominios y direcciones IP propias de la EEASA.
- La ejecución de Nexfil verificó perfiles en más de 350 sitios y, se detecta algunos usuarios en redes sociales, blogs y páginas de contenido.
- La utilidad TheHarvester arroja información de subdominios y direcciones con más resultados de las herramientas anteriormente mencionadas.
- Por otra parte, *Maltego* es la herramienta con más resultados encontrados y detecta correos que permite ejecutar el análisis con la utilidad de Iky.
- Finalmente, Iky detecta perfiles sociales de los correos detectados.

Fase 6. Presentación

La presentación de inteligencia son datos fácilmente interpretables y, se utilizan de forma práctica en la investigación, se da a conocer a través de la figura 11.

Figura 11. Presentación de resultados de OSINT



Fuente: elaboración propia

FASES MAGERIT – Pila de sprint

El presente script backlog tiene como objetivo la aplicación de MAGERIT en actividades definidas en el Método de Análisis de Riesgos (MAR) mismo es gestionado por el equipo quien, se encarga de actualizar el porcentaje de avance durante la ejecución de cada actividad completada.

Este conjunto de actividades tiene los siguientes objetivos:

- Levantar un modelo del valor del sistema, identifica y valora los activos relevantes.
- Levantar un mapa de riesgos del sistema, identifica y valora las amenazas sobre aquellos activos.
- Levantar un conocimiento de la situación actual de salvaguardas.
- Evaluar el impacto posible sobre el sistema en estudio, tanto el impacto potencial (sin salvaguardas), como el impacto residual (incluye el efecto de las salvaguardas desplegadas para proteger el sistema).

- Evaluar el riesgo del sistema en estudio, tanto el riesgo potencial (sin salvaguardas), como el riesgo residual (incluye el efecto de las salvaguardas desplegadas para proteger el sistema).
- Informar de las áreas del sistema con mayor impacto y/o riesgo a fin de que, se tome las decisiones de tratamiento con motivo justificado.

Cuadro 17. Método de análisis de riesgos

MAR – Método de Análisis de Riesgos
MAR.1 – Caracterización de los activos
MAR.11 – Identificación de los activos
MAR.12 – Dependencias entre activos
MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo
MAR.41 – Estimación del impacto
MAR.42 – Estimación del riesgo

Fuente: Libro I de MAGERIT v3 p.36

El análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

MAR 1. Caracterización de activos

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, y, se caracteriza por el tipo de activo, identifica las relaciones entre los diferentes activos, y determina en qué dimensiones de seguridad son necesarias y valora esta importancia.

El resultado de esta actividad es el informe denominado “modelo de valor”.

Subtareas:

- Tarea MAR.11: Identificación de los activos
- Tarea MAR.12: Dependencias entre activos
- Tarea MAR.13: Valoración de los activos

El objetivo de estas tareas es reconocer los activos que componen el sistema, definir las dependencias entre ellos, y determinar que parte del valor del sistema, se soporta en cada activo. Se resume en la expresión “conócete a ti mismo”.

MAR 1.1. Identificación de activos

Esta tarea es crítica. Una buena identificación es importante desde varios puntos de vista:

- Materializa con precisión el alcance del proyecto,
- Permite la interlocución con los grupos de usuarios: todos hablan el mismo lenguaje,
- Permite determinar las dependencias precisas entre activos,
- Permite valorar los activos con precisión,
- Permite identificar y valorar las amenazas con precisión,
- Permite determinar qué salvaguardas serán necesarias para proteger el sistema.

Caracterización de los activos

Para cada activo hay que determinar una serie de características que lo definen:

- Código, típicamente procedente del inventario
- Nombre (corto)
- Descripción (larga)
- Tipo (o tipos) que caracterizan el activo
- Unidad responsable. A veces hay más de una unidad. Por ejemplo, en el caso de aplicaciones cabe diferenciar entre la unidad que la mantiene y la que la explota.
- Persona responsable. Especialmente relevante en el caso de datos. A veces hay más de un responsable. Por ejemplo, en caso de datos de carácter personal cabe diferenciar entre el responsable del dato y el operador u operadores que lo manejan.
- Ubicación, técnica (en activos intangibles) o geográfica (en activos materiales)

- Cantidad, si procede como el caso de la informática personal (por ejemplo 350 equipos de sobremesa)
- Otras características específicas del tipo de activo

Cuadro 18. Proceso identificación de activos

Objetivo	Identificar los activos que componen el sistema, determina sus características, atributos y clasificación en los tipos determinados
Entradas	• Inventario de datos manejados por el sistema • Inventario de servicios prestados por el sistema • Procesos de negocio • Diagramas de uso • Diagramas de flujo de datos • Inventarios de equipamiento lógico • Inventarios de equipamiento físico • Locales y sedes de la Organización
Salidas	• Relación de activos a considerar • Caracterización de los activos: valor propio y acumulado • Relaciones entre activos
Técnicas, prácticas y pautas	• Ver “Libro II – Catálogo”. • Diagramas de flujo de datos • Diagramas de procesos • Entrevistas (ver "Guía de Técnicas") Reuniones

Fuente: MAGERIT v3

Para el caso de investigación de fuentes abiertas realizado en la EEASA, el descubrimiento de activos se realizó con herramientas OSINT y, en virtud de lo establecido se elabora la matriz donde se identifica y clasifica los activos de información con la descripción, se ofusca cierta información que es ocupada con fines maliciosos:

Cuadro 19. Identificación de Activos - MAGERIT

TIPO ACTIVO	NOMBRE ACTIVO	DESCRIPCIÓN
Servidor DNS	**Host:** xxx1.xxxsa.xxx.ec xxx2.xxxsa.xxx.ec	Es un sistema de nomenclatura jerárquico que se ocupa de la administración del espacio de nombres de dominio (*DOMAIN NAME SPACE*). Su labor primordial consiste en resolver las peticiones de asignación de nombres.
Servidor Correo	**Host:** xxxbra.xxxsa.xxx.ec xxxl.xxxsa.xxx.ec	Es el encargado de enviar y recibir mensajes de correo electrónico entre hosts, usuarios o servidores. Entre sus funciones, se incluyen el procesado de los mensajes, filtrado, almacenamiento, envío, recepción y reenvío de correos.
Servidor NTP	**Host:** xxx.xxxsa.xxx.ec	Es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usa el puerto 123.
Servidor Web	**Host**: xxx.xxxsa.xxx.ec xxxvicios.xxxsa.xxx.ec xxx2.xxxsa.xxx.ec xxxbra.xxxsa.xxx.ec xxxveedores.xxxsa.xxx.ec	Es una colección de contenido multimedia que, se encuentra relacionada y común a un dominio de internet o subdominio en la WORLD WIDE WEB dentro de Internet.

Fuente: elaboración propia

MAR.12: Dependencias entre activos

Para cada dependencia conviene registrar la siguiente información:

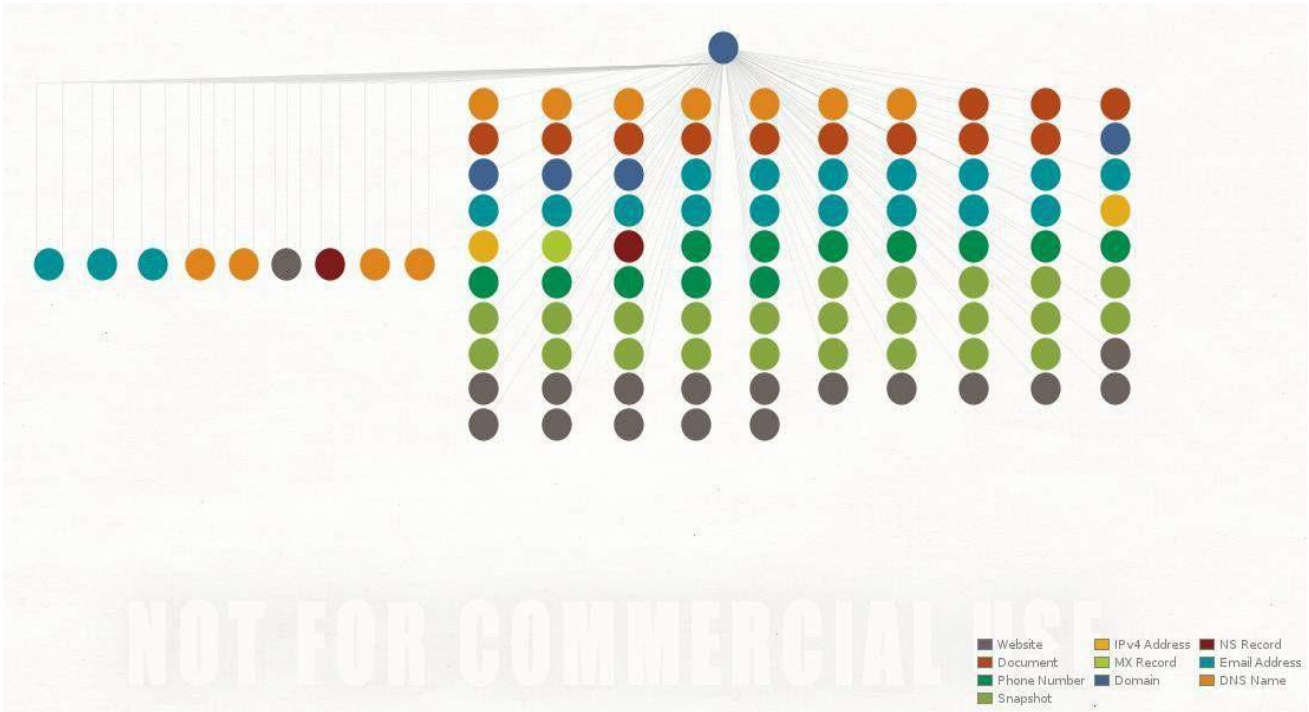
- Estimación del grado de dependencia: hasta un 100%
- Explicación de la valoración de la dependencia
- Entrevistas realizadas de las que, se ha deducido la anterior estimación

Cuadro 20. Proceso dependencia entre activos

Objetivo	Identificar y valorar las dependencias entre activos, es decir la medida en que un activo de orden superior, se ve perjudicado por una amenaza materializada sobre un activo de orden inferior
Entradas	• Resultados de la tarea MAR.11., Identificación • Procesos de negocio • Diagramas de flujo de datos • Diagramas de uso
Salida	• Diagrama de dependencias entre activos
Técnicas, prácticas y pautas	• Diagramas de flujo de datos • Diagramas de procesos • Entrevistas (ver "Guía de Técnicas") • Reuniones • Valoración Delphi (ver "Guía de Técnicas")

Fuente: MAGERIT v3

Figura 12. Dependencia de activos relacionados al dominio eeasa.com.ec



Fuente: MALTEGO

MAR.13: Valoración de los activos

Para la adquisición de este conocimiento es necesario entrevistar a diferentes colectivos dentro de la Organización:

- Dirección o gerencia, que conocen las consecuencias para la misión de la Organización,
- Responsables de los datos, que conocen las consecuencias de sus fallos de seguridad,
- Responsables de los servicios, que conocen las consecuencias de la no prestación del servicio o de su prestación degradada,
- Responsables de sistemas de información y responsables de operación, que conocen las consecuencias de un incidente.

En la investigación al ser un análisis de fuentes abiertas sin la intervención de funcionarios de la entidad de estudio, se valora en función de la criticidad de disponibilidad de servicio, para aquello, se crea el proyecto en pilar referirse al Anexo 3.

Para cada valoración conviene registrar la siguiente información:

- Dimensiones en las que el activo es relevante,
- Estimación de la valoración en cada dimensión,
- Explicación de la valoración,
- Entrevistas realizadas de las que, se han deducido las anteriores estimaciones.

Cuadro 21. Proceso valoración de activos

Objetivos	• Identificar en qué dimensión es valioso el activo, • Valorar el coste que para la Organización supondría la destrucción del activo.
Entradas	• Resultados de la tarea MAR.11, Identificación de los activos • Resultados de la tarea MAR.12, Dependencias entre activos
Salida	• Modelo de valor: informe de valor de los activos
Técnicas, prácticas y pautas	• Ver “Libro II – Catálogo”. • Entrevistas (ver "Guía de Técnicas") • Reuniones • Valoración Delphi (ver "Guía de Técnicas")

Fuente: MAGERIT v3

La valoración de los activos se cuantifica en función del nivel de servicio que proporciona cada servidor a la empresa por consecuente el siguiente cuadro, se establece matrices tanto de la dimensión como de los criterios de valoración para obtener una correcta tabulación, se utilizó el software PILAR.

- **Dimensiones**

Cuadro 22. Dimensiones

Dimensión	**Descripción**
[D]	Disponibilidad
[I]	Integridad de Datos
[C]	Confidencialidad de Datos
[A]	Autenticidad de los datos y de la información
[T]	Trazabilidad del servicio y de los datos
[V]	Valor
[DP]	Datos personales

Fuente: elaboración propia

- **Criterios de la valoración**

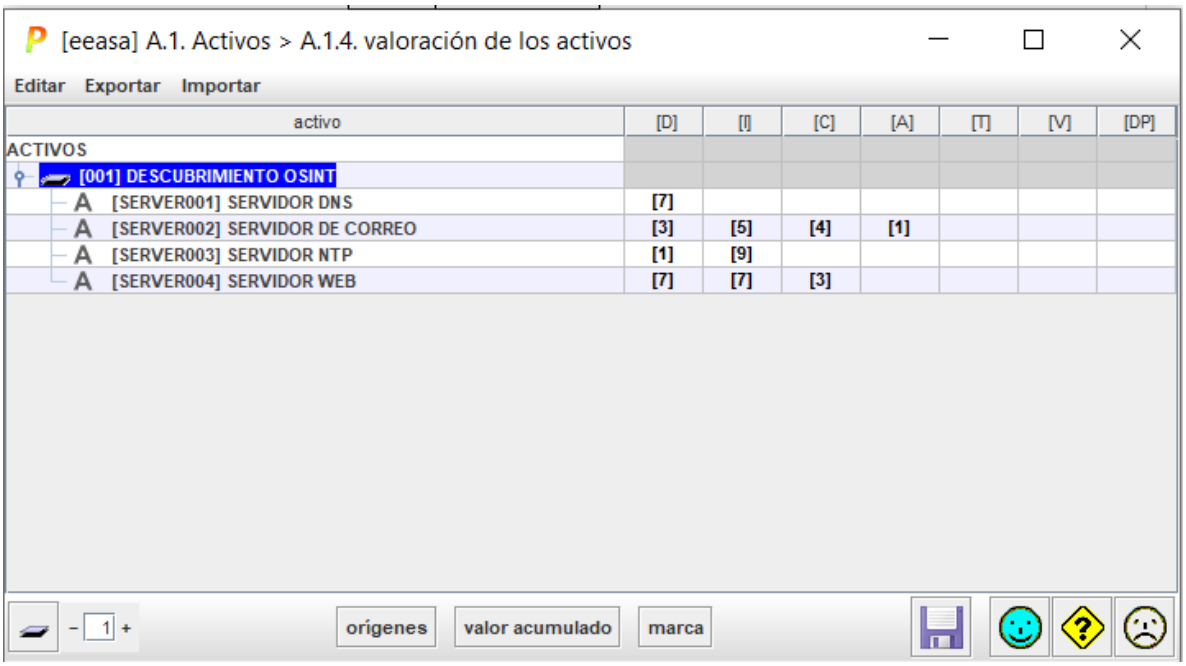
Cuadro 23. Criterios de valoración

Nivel	**Criterio**
10	Nivel 10
9	Nivel 9
8	Nivel 8 (+)
7	Alto
6	Alto (-)
5	Medio (+)
4	Medio
3	Medio (-)
2	Bajo (+)
1	Bajo
0	Depreciable

Fuente: Software PILAR RM (2021.1.3 – 12.2.2021)

Resultados

Cuadro 24. Valoración de activos



Fuente: Software PILAR RM (2021.1.3 – 12.2.2021)

MAR 2. Caracterización de amenazas

Esta actividad consta de dos subtareas:

- MAR.21: Identificación de las amenazas
- MAR.22: Valoración de las amenazas

El objetivo de estas tareas es caracterizar el entorno al que, se enfrenta el sistema, qué pasa, qué consecuencias, se derivarían y cómo de probable es que pase. Se resumirlo en la expresión “conoce a tu enemigo”.

MAR 21. Identificación de amenazas

En esta tarea, se identifican las amenazas significativas sobre los activos y toma en consideración lo siguiente:

- el tipo de activo
- las dimensiones en que el activo es valioso
- la experiencia de la Organización
- los defectos reportados por los fabricantes y organismos de respuesta a incidentes de seguridad (CERTS)

Para cada amenaza sobre cada activo conviene registrar la siguiente información:

- explicación del efecto de la amenaza
- entrevistas realizadas de las que, se ha deducido la anterior estimación
- antecedentes, si los hubiera, bien en la propia Organización, bien en otras organizaciones que, se haya considerado relevantes

Cuadro 25. Proceso identificación de amenazas

Objetivo	Identificar las amenazas relevantes sobre cada activo
Entrada	• Resultados de la actividad MAR.1, Caracterización de los activos • Informes relativos a defectos en los productos. Esto es, informes de vulnerabilidades.
Salida	• Relación de amenazas posibles
Técnicas, prácticas y pautas	• Catálogos de amenazas (ver "Catálogo de Elementos") • Árboles de ataque (ver "Guía de Técnicas") • Entrevistas (ver "Guía de Técnicas") • Reuniones • Valoración Delphi (ver "Guía de Técnicas")

Fuente: MAGERIT v3

Para la investigación, se estudia las amenazas del Catálogo de elementos de MAGERIT el apartado 5.4 [A] Ataques intencionados p40.

Catálogo de Amenazas – Ataques Intencionados -Fallos deliberados causados por las personas.

La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiere únicamente en el propósito del sujeto.

Origen:

Humano (deliberado)

Cuadro 26. Catálogo - Manipulación de registro de actividad

Manipulación de los registros de actividad (log)	
Tipos de activos: • [D.log] registros de actividad	Dimensiones: 1. [I] integridad (trazabilidad)
Descripción: Ver: EBIOS: no disponible	

Fuente: MAGERIT v3

Cuadro 27. Catálogo - Manipulación de configuración

Manipulación de la configuración	
Tipos de activos: • [D.log] registros de actividad	Dimensiones: 1. [I] integridad 2. [C] confidencialidad 3. [A] disponibilidad
Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, y de más controles. Ver: EBIOS: no disponible	

Fuente: MAGERIT v3

Cuadro 28. Catálogo – Suplantación de la identidad del usuario

Suplantación de la identidad del usuario	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	Dimensiones: 1. [C] confidencialidad 2. [A] autenticidad 3. [I] integridad
Descripción: Si un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza es perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. Ver: EBIOS: 40 - USURPACIÓN DE DERECHO	

Fuente: MAGERIT v3

Cuadro 29. Catálogo – Abuso de privilegios

Abuso de privilegios de acceso	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	Dimensiones: 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: cada usuario disfruta de un nivel de privilegios para un determinado propósito; si un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas. Ver: EBIOS: 39 - ABUSO DE DERECHO	

Fuente: MAGERIT v3

Cuadro 30. Catálogo – Difusión de software

Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	Dimensiones: 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, y demás software malicioso. Ver: EBIOS: no disponible	

Fuente: MAGERIT v3

Cuadro 31. Catálogo – [Re-]encaminamiento de mensajes

[Re-]encaminamiento de mensajes	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	Dimensiones: 1. [C] confidencialidad
Descripción: envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; se trata de mensajes entre personas, entre procesos o entre unos y otros. Un atacante fuerza un mensaje para circular a través de un nodo determinado de la red donde es interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, y la información termina en manos de quien no debe. Ver: EBIOS: no disponible	

Fuente: MAGERIT v3

Cuadro 32. Catálogo – Alteración de secuencia

Alteración de secuencia	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	Dimensiones: 1. [I] integridad
Descripción: alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, se perjudica a la integridad de los datos afectados. Ver: EBIOS: 36 - ALTERACIÓN DE DATOS	

Fuente: MAGERIT v3

Cuadro 33. Catálogo – Acceso no autorizado

Acceso no autorizado	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	Tipos de activos: 1. [C] confidencialidad 2. [I] integridad
Descripción: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente, se aprovecha un fallo del sistema de identificación y autorización. Ver: EBIOS: 33 - USO ILÍCITO DEL HARDWARE	

Fuente: MAGERIT v3

Cuadro 34. Catálogo – Interceptación de información

Interceptación de información (escucha)	
Tipos de activos: • [COM] redes de comunicaciones	Dimensiones: 1. [C] confidencialidad
Descripción: el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma, se vea alterada. Ver: EBIOS: 19 - ESCUCHA PASIVA	

Fuente: MAGERIT v3

Cuadro 35. Catálogo – Destrucción de información

Destrucción de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	Dimensiones: 1. [I] integridad
Descripción: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Ver: EBIOS: no disponible	

Fuente: MAGERIT v3

Cuadro 36. Catálogo – Denegación de servicio

Denegación de servicio	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	Dimensiones: 1. [D] disponibilidad
Descripción: la carencia de recursos suficientes provoca la caída del sistema si la carga de trabajo es desmesurada. Ver: EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	

Fuente: MAGERIT v3

Cuadro 37. Catálogo – Extorsión

Extorsión	
Tipos de activos: • [P] personal interno	Dimensiones: 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido. Ver: EBIOS: no disponible	

Fuente: MAGERIT v3

Cuadro 38. Catálogo – Ingeniería social

Ingeniería social (picaresca)	
Tipos de activos: • [P] personal interno	Dimensiones: 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. Ver: EBIOS: no disponible	

Fuente: MAGERIT v3

Una vez identificadas las amenazas intencionales cuyo contenido es el objeto de estudio, se establece una matriz de información donde se correlaciona con los activos identificados en MAR 11.

Cuadro 39. Activos expuestos ante posibles ataques

Activo	**Amenaza**	**Ataque**
Servidor DNS	• Manipulación de la configuración • Manipulación de los registros de actividad	• Phantom Domain • DNS domain lock-up • Floods

Servidor Correo	• Suplantación de la identidad del usuario • Acceso no autorizado • [Re-]encaminamiento de mensajes	• Brute force • Attachment-based • Email Spoofing • Open Relay • Homoglyphs
Servidor NTP	• Denegación de servicio • Ataque destructivo	• DoS • Buffer underflow/underrun
Páginas Web	• Interceptación de información (escucha) • Acceso no autorizado • Difusión de software dañino • Abuso de privilegios de acceso • Alteración de secuencia • Suplantación de la identidad del usuario • Extorsión • Ingeniería Social • Destrucción de información	• Inyección de backdoor • Defacement • Inyección de contenido SEO • Creación de páginas de spam • Mailers en PHP • Campañas de phishing • Redirección de usuarios a sitios maliciosos • Command & Control • Inyección de malware para minar criptomonedas

Fuente: elaboración propia

MAR 22. Valoración de amenazas

En esta tarea, se valoran las amenazas identificadas en la tarea anterior,la toma en consideración:

- La experiencia (historia) universal
- La experiencia (historia) del sector de actividad
- La experiencia (historia) del entorno en que, se ubican los sistemas
- La experiencia (historia) de la propia Organización
- Los informes anexos a los reportes de defectos proporcionados por los fabricantes y organismos de respuesta a incidentes de seguridad (CERTS)

Para cada amenaza sobre cada activo conviene registrar la siguiente información:

- Estimación de la frecuencia de la amenaza,
- Estimación del daño (degradación) que causaría su materialización,
- Explicación de las estimaciones de frecuencia y degradación,
- Entrevistas realizadas de las que, se han deducido las anteriores estimaciones.

Cuadro 40. Proceso frecuencia y degradación de amenazas

Objetivos	• Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo, • Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.
Entradas	• Resultados de la tarea MAR21, Identificación de las amenazas, • Series históricas de incidentes, • Informes de defectos en los productos, • Antecedentes: incidentes en la Organización.
Salida	• Mapa de riesgos: informe de amenazas posibles, caracterizadas por su frecuencia de ocurrencia y la degradación que causarían en los activos.
Técnicas, prácticas y pautas	• Árboles de ataque (ver "Guía de Técnicas"), • Entrevistas (ver "Guía de Técnicas"), • Reuniones, • Valoración Delphi (ver "Guía de Técnicas").

Fuente: MAGERIT v3

Una vez determinado que una amenaza perjudica a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

- degradación: cuán perjudicado resultaría el valor del activo
- probabilidad: cuán probable o improbable es que, se materialice la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera como, se aprecia en el cuadro 40.

Cuadro 41. Degradación del valor -MAGERIT

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Fuente: Libro I de MAGERIT v3 p.28

La degradación, se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo, se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”. Si la amenaza es intencional, no se piensa en proporcionalidad alguna, pues el atacante causa daño de forma selectiva, es por ello por lo que, se estima porcentajes altos de degradación para la presente investigación.

La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces, se modela cualitativamente por medio de alguna escala nominal: Cuadro 48.

Cuadro 42. Probabilidad de ocurrencia-MAGERIT

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Fuente: Libro I de MAGERIT v3 p.28

Por la naturaleza de la investigación los datos y registros, se los obtiene de fuentes públicas sin intervención de personal interno de la EEASA, en vista de aquello, se valora la ocurrencia de la presente investigación, se referencia a datos estadísticos de ataques informáticos publicados por la fiscalía general del Estado, para seguidamente contrastar con las amenazas identificadas en el MAR 21.

Cuadro 43. Ataques informáticos en Ecuador

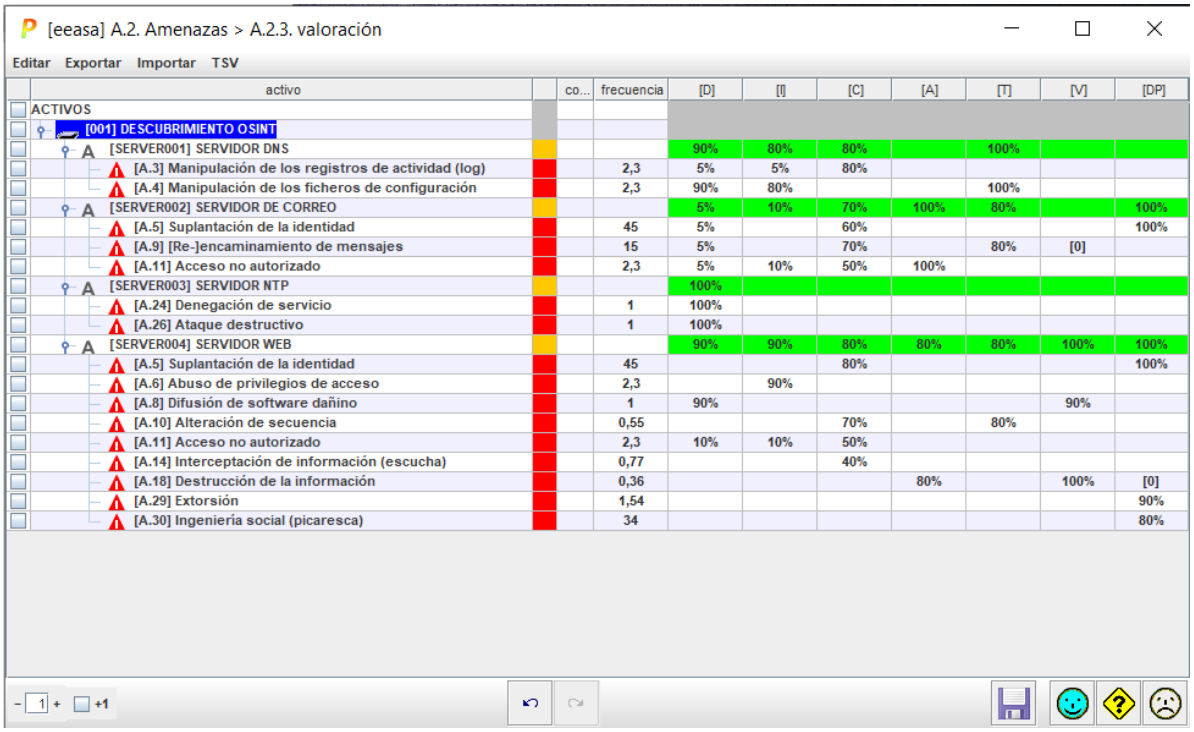
Tipo de delito	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**Total**	**%**
Suplantación de identidad	1355	3920	4152	3676	4180	4607	2162	24052	44,99%

Falsificación y uso de documento falso	1048	2594	3117	3183	3292	3231	1448	17913	33,51%
Apropiación fraudulenta por medios electrónicos	507	141	145	218	236	246	175	8022	15,00%
Acceso no consentido a un sistema informático telemático o de telecomunicaciones	54	141	145	218	236	246	175	1215	2,27%
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	21	80	108	159	202	166	85	821	1,54%
Ataque a la integridad de sistemas Informáticos	49	77	76	86	87	113	51	539	1,01%
Interceptación ilegal de datos	38	55	82	63	41	57	45	411	0,77%
Transferencia electrónica de activo patrimonial	17	59	47	54	38	49	31	295	0,55%
Revelación ilegal de base de datos	29	24	24	22	44	34	18	195	0,36%
Total	3118	8230	8796	8421	9571	10279	5048	53463	100%

Fuente: Diario el Universo (Los delitos informáticos crecen en Ecuador; cada clic en la web deja su rastro, 2020)

A continuación, se elabora un cuadro de amenazas en función de los datos anteriormente señalados con la valoración de ocurrencia y degradación.

Cuadro 44. Valoración de amenazas



activo		co...	frecuencia	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS										
[001] DESCUBRIMIENTO OSINT										
[SERVER001] SERVIDOR DNS				90%	80%	80%		100%		
[A.3] Manipulación de los registros de actividad (log)			2,3	5%	5%	80%				
[A.4] Manipulación de los ficheros de configuración			2,3	90%	80%			100%		
[SERVER002] SERVIDOR DE CORREO				5%	10%	70%	100%	80%		100%
[A.5] Suplantación de la identidad			45	5%		60%				100%
[A.9] [Re-]encaminamiento de mensajes			15	5%		70%		80%	[0]	
[A.11] Acceso no autorizado			2,3	5%	10%	50%	100%			
[SERVER003] SERVIDOR NTP				100%						
[A.24] Denegación de servicio			1	100%						
[A.26] Ataque destructivo			1	100%						
[SERVER004] SERVIDOR WEB				90%	90%	80%	80%	80%	100%	100%
[A.5] Suplantación de la identidad			45			80%				100%
[A.6] Abuso de privilegios de acceso			2,3		90%					
[A.8] Difusión de software dañino			1	90%					90%	
[A.10] Alteración de secuencia			0,55			70%		80%		
[A.11] Acceso no autorizado			2,3	10%	10%	50%				
[A.14] Interceptación de información (escucha)			0,77			40%				
[A.18] Destrucción de la información			0,36				80%		100%	[0]
[A.29] Extorsión			1,54							90%
[A.30] Ingeniería social (picaresca)			34							80%

Fuente: Software PILAR RM (2021.1.3 – 12.2.2021)

MAR 3. Caracterización de las salvaguardas

Esta actividad consta de dos subtareas:

MAR.31: Identificación de las salvaguardas pertinentes

MAR.32: Valoración de las salvaguardas

El objetivo de estas tareas es doble: saber qué necesitamos para proteger el sistema y saber si tenemos un sistema de protección a la altura de las necesidades.

MAR 31. Identificación de las salvaguardas pertinentes

Para cada salvaguarda conviene registrar la siguiente información:

- Descripción de la salvaguarda y su estado de implantación
- Descripción de las amenazas a las que pretende hacer frente
- Entrevistas realizadas de las que, se ha deducido la anterior información

Para determinar las salvaguardas pertinentes es frecuente recurrir a catálogos de salvaguardas o al consejo de personas expertas. De una u otra forma, se dispone de una colección de salvaguardas para elegir, de forma que el complejo problema de encontrar lo que necesitamos, se reduce al problema más sencillo de descartar lo que no necesitamos.

En el proceso de descarte hay varias razones para eliminar una salvaguarda propuesta:

- Porque no es apropiada para el activo que necesitamos defender,
- Porque no es apropiada para la dimensión de seguridad que necesitamos defender,
- Porque no es efectiva oponiéndose a la amenaza que necesitamos contrarrestar,
- Porque es excesiva para el valor que tenemos que proteger (desproporcionada),
- Porque disponemos de medidas alternativas.

Cuadro 45. Proceso identificación de salvaguardias

Objetivo	Identificar las salvaguardas convenientes para proteger el sistema.
Entradas	• Modelo de activos del sistema, • Modelo de amenazas del sistema, • Indicadores de impacto y riesgo residual, • Informes de productos y servicios en el mercado.
Salida	• Declaración de aplicabilidad: relación justificada de las salvaguardas necesarias, • Relación de salvaguardas desplegadas.
Técnicas, prácticas y pautas	• Catálogos de salvaguardas (ver "Catálogo de Elementos"), • Árboles de ataque (ver "Guía de Técnicas"), • Entrevistas (ver “Guía de Técnicas”), • Reuniones.

Fuente: MAGERIT v3

MAR 32. Valoración de las salvaguardas

En esta tarea, se valora la efectividad de las salvaguardas identificadas en la tarea anterior, se toma en consideración:

- La idoneidad de la salvaguarda para el fin perseguido,
- La calidad de la implantación,
- La formación de los responsables de su configuración y operación,
- La formación de los usuarios, si tienen un papel activo,
- La existencia de controles de medida de su efectividad,
- La existencia de procedimientos de revisión regular.

Para cada salvaguarda conviene registrar la siguiente información:

- Estimación de su eficacia para afrontar aquellas amenazas,
- Explicación de la estimación de eficacia,
- Entrevistas realizadas de las que, se ha deducido la anterior estimación.

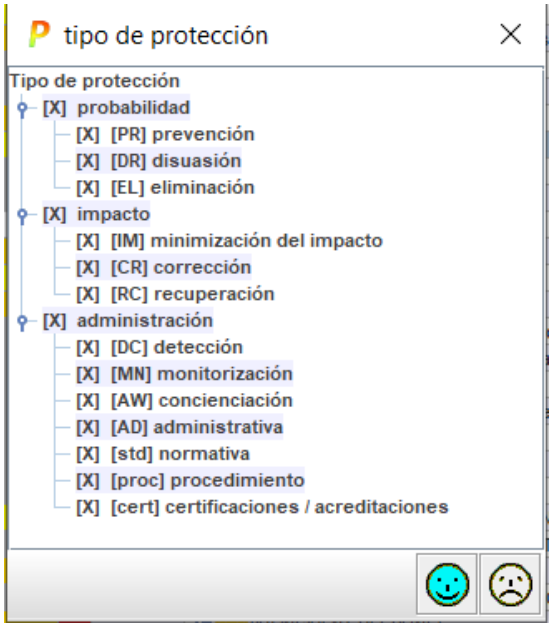
Cuadro 46. Proceso determinar la eficacia de las salvaguardias

Objetivo	Determinar la eficacia de las salvaguardas pertinentes.
Entrada	• Inventario de salvaguardas derivado de la tarea MAR.31.
Salidas	• Evaluación de salvaguardas: informe de salvaguardas desplegadas, caracterizadas por su grado de efectividad, • Informe de insuficiencias (o vulnerabilidades): relación de salvaguardas que estarían, pero no están desplegadas o están desplegadas de forma insuficiente.
Técnicas, prácticas y pautas	• Entrevistas (ver "Guía de Técnicas"), • Reuniones, • Valoración Delphi (ver “Guía de Técnicas”).

Fuente: MAGERIT v3

Para la selección de salvaguardias, se utiliza el software PILAR a través de su botón de recomendaciones por tal razón que se configura el tipo de protección en sus tres dimensiones que son: probabilidad, impacto y administración (Fig. 11) de modo tal que permita alcanzar el objetivo de la investigación.

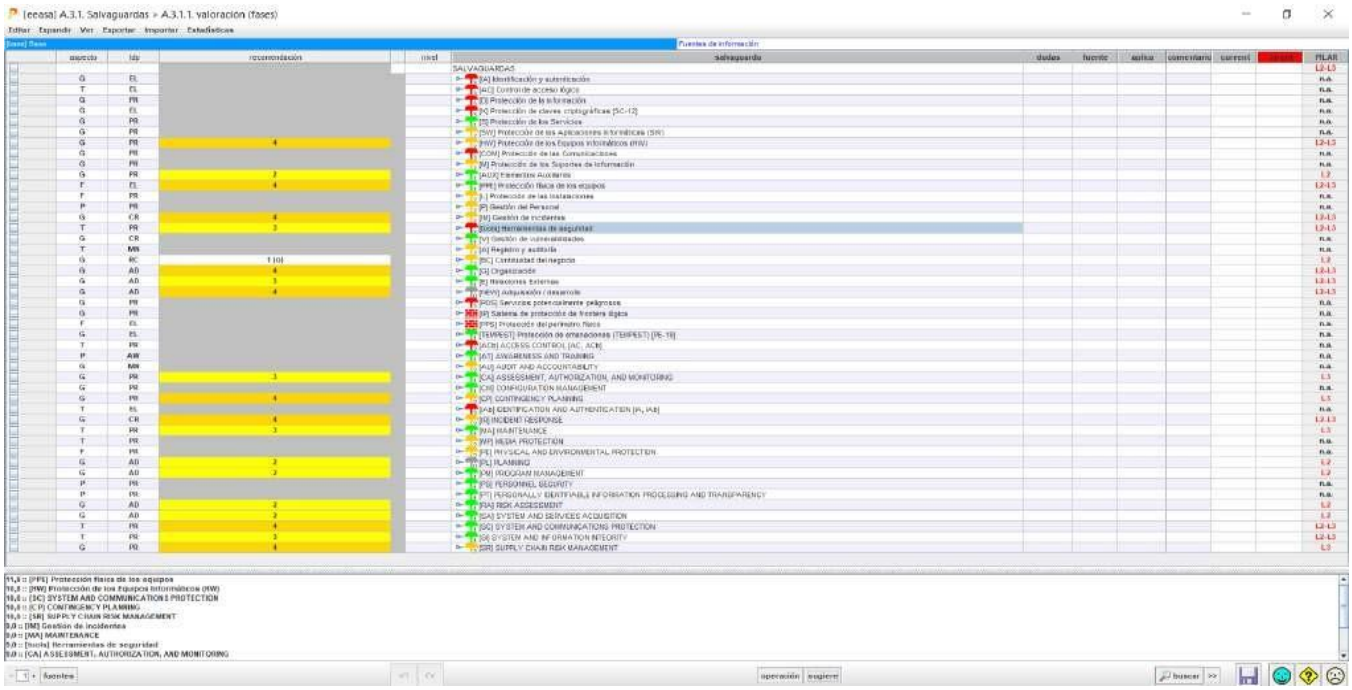
Figura 13. Tipo de protección de salvaguardias



Fuente: Software PILAR RM (2021.1.3 – 12.2.2021)

Finalmente, se obtiene la valoración de manera automática (Fig. 14) y permite continuar a la subsiguiente fase.

Figura 14. Salvaguardias



Fuente: Software PILAR RM (2021.1.3 – 12.2.2021)

MAR 4. Estimación del estado de riesgo

En esta tarea, se combinan los descubrimientos de las tareas anteriores (MAR.1, MAR.2 y MAR.3) para derivar estimaciones del estado de riesgo de la Organización.

Esta actividad consta de tres tareas:

MAR.41: Estimación del impacto

MAR.42: Estimación del riesgo

El objetivo de estas tareas es disponer de una estimación fundada de lo que ocurra (impacto) y de lo que probablemente ocurra (riesgo).

MAR 41. Estimación de impacto

En esta tarea, se estima el impacto al que están expuestos los activos del sistema:

- El impacto potencial, al que está expuesto el sistema tiene en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas,

- El impacto residual, al que está expuesto el sistema tiene en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.

Cuadro 47. Proceso impacto porcentual y residual

Objetivos	• Determinar el impacto potencial al que está sometido el sistema, • Determinar el impacto residual al que está sometido el sistema.
Entradas	• Resultados de la actividad MAR.1, Caracterización de los activos, • Resultados de la actividad MAR.2, Caracterización de las amenazas, • Resultados de la actividad MAR.3, Caracterización de las salvaguardas.
Salidas	• Informe de impacto (potencial) por activo, • Informe de impacto residual por activo.
Técnicas, prácticas y pautas	• Análisis mediante tablas (ver “Guía de Técnicas”), • Análisis algorítmico (ver “Guía de Técnicas”).

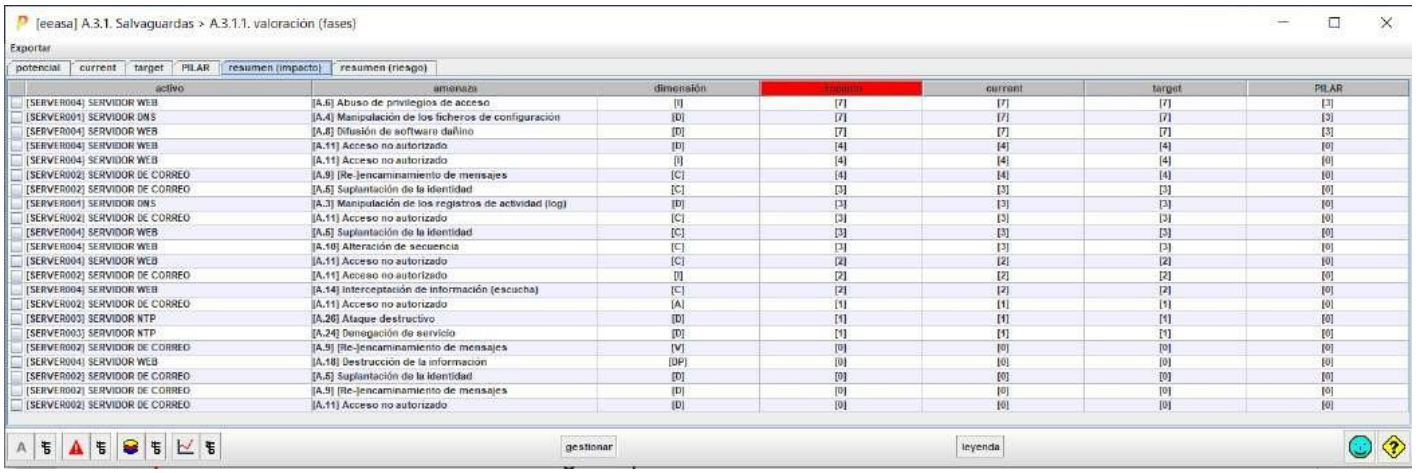
Fuente: MAGERIT v3

Figura 15. Análisis mediante tablas estimación de impacto

impacto		*degradación*		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: MAGERIT v3

Figura 16. Impacto potencial



Fuente: elaboración propia

MAR 42. Estimación del riesgo

En esta tarea, se estima el riesgo al que están sometidos los activos del sistema:

- El riesgo potencial, al que está sometido el sistema tiene en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas,
- El riesgo residual, al que está sometido el sistema tiene en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.

Cuadro 48. Proceso riesgo porcentual y residual

Objetivos	• Determinar el riesgo potencial al que está sometido el sistema, • Determinar el riesgo residual al que está sometido el sistema.
Entradas	• Resultados de la actividad MAR.1, Caracterización de los activos, • Resultados de la actividad MAR.2, Caracterización de las amenazas, • Resultados de la actividad MAR.3, Caracterización de las salvaguardas, • Resultados de la actividad MAR.4, Estimaciones de impacto.
Salidas	• Informe de riesgo (potencial) por activo, • Informe de riesgo residual por activo.
Técnicas, prácticas y pautas	• Análisis mediante tablas (ver "Guía de Técnicas"), • Análisis algorítmico (ver "Guía de Técnicas").

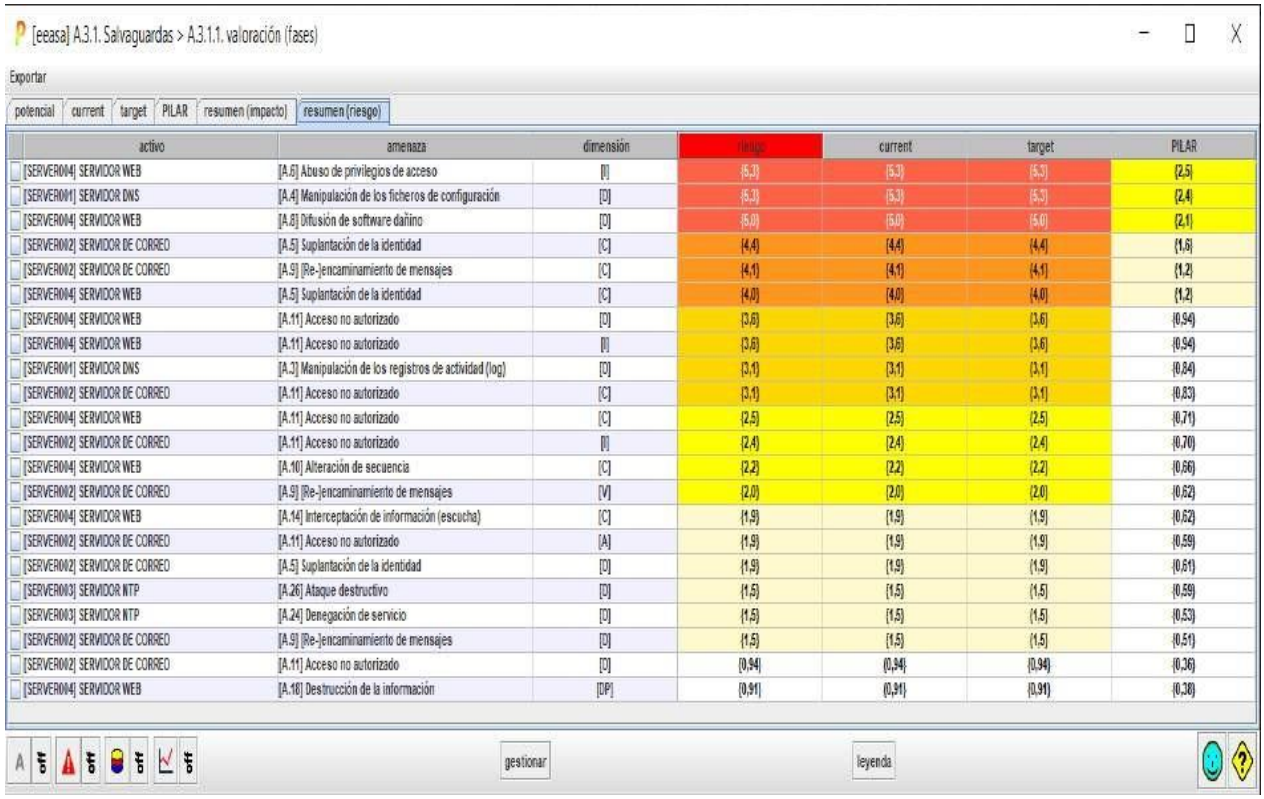
Fuente: MAGERIT v3

Figura 17. Análisis mediante tablas estimación de riesgos

riesgo		*probabilidad*				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: MAGERIT v3

Figura 18. Valoración del riesgo



Fuente: elaboración propia

2.3.3. Sprint 3 - Implementación

Proceso de gestión de riesgos

A la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones condicionadas por diversos factores:

- La gravedad del impacto y del riesgo
- Las obligaciones a las que por ley esté sometida la Organización
- Las obligaciones a las que por reglamentos sectoriales esté sometida la Organización
- Las obligaciones a las que por contrato esté sometida la Organización

Dentro del margen de maniobra que permita este marco, aparece consideraciones adicionales sobre la capacidad de la Organización para aceptar ciertos impactos de naturaleza intangible tales como:

- Imagen pública de cara a la Sociedad (aspectos reputacionales),
- Política interna: relaciones con los propios empleados, tales como capacidad de contratar al personal idóneo, capacidad de retener a los mejores, capacidad de soportar rotaciones de personas, capacidad de ofrecer una carrera profesional atractiva, y lo demás.,
- Relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, entre otras,
- Relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia,
- Relaciones con otras organizaciones, tales como capacidad de alcanzar acuerdos estratégicos, alianzas, y todo lo demás.,
- Nuevas oportunidades de negocio, tales como formas de recuperar la inversión en seguridad,
- Acceso a sellos o calificaciones reconocidas de seguridad.

Todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo, se determina si:

1. Es crítico en el sentido de que requiere atención urgente,
2. Es grave en el sentido de que requiere atención,
3. Es apreciable en el sentido de que es un objeto de estudio para su tratamiento,
4. Es asumible en el sentido de que no, se van a tomar acciones para atajarlo.

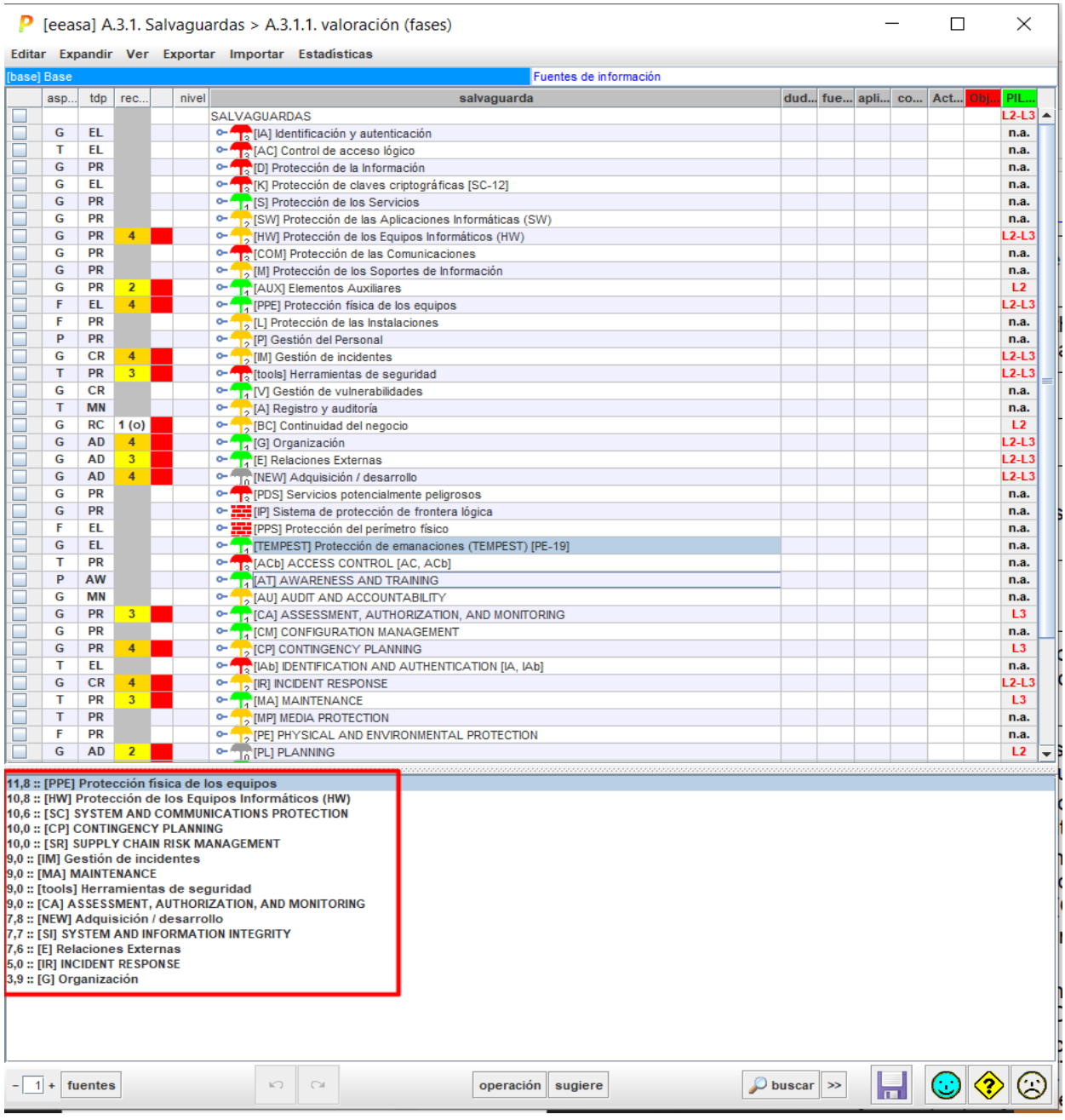
La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que llevan a esta aceptación son:

- Si el impacto residual es asumible,
- Si el riesgo residual es asumible,
- Si el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales.

La calificación de los riesgos tiene consecuencias en las tareas subsiguientes, y es un factor básico para establecer la prioridad relativa de las diferentes actuaciones.

Para gestionar el riesgo de los activos de la empresa, se establece la figura 19 en donde se identifican las salvaguardas correspondientes.

Figura 19. Identificación de salvaguardas



Fuente: elaboración propia

2.3.4. Sprint 4 - Revisión y retrospectiva

Por la estructura de la investigación, en este sprint, se realiza la evaluación de la propuesta metodológica la cual está documentada formalmente en el Capítulo 3 del documento.

2.3.5. Sprint 5 – Lanzamiento

Finalmente, en el presente sprint, se perfila a la redacción formal la metodología para mitigar riesgos y se detalla en el Capítulo 3 por la estructura propia de la investigación.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.1. Propuesta metodológica

Para cumplir con el objetivo de la investigación, se redacta el método que permite minimizar el riesgo, a través de 6 etapas definidas que, se detalla en el cuadro 48, ésta matriz es elaborada desde el punto de vista externo pues los activos que se protege son los resultantes del análisis de fuentes abiertas aplicado:

Cuadro 49. Propuesta para mitigar riesgos

Etapa 1	Informe de los servidores detectados éticamente.
Etapa 2	Informe de ataques informáticos más comunes a cada servidor.
Etapa 3	Planificación de estrategias, diseño y selección de planes de desarrollo.
Etapa 4	Análisis de vulnerabilidades con el uso técnicas de caja negra, gris y blanca.
Etapa 5	Priorización de riesgos, determinación de responsabilidades, establecimiento de protecciones.
Etapa 6	Informes y resultados.

Fuente: elaboración propia

Etapa 1 – Informe de los servidores detectados éticamente

El objetivo de la primera etapa es informar a la máxima autoridad y al responsable de la administración de la infraestructura tecnológica de la empresa, los activos descubiertos con la aplicación ética de OSINT. En este primer acercamiento, se establece prioridades en función de los intereses institucionales que, se desea proteger.

Acciones

Reunión de trabajo inicial.

Etapa 2 - Informe de ataques informáticos más comunes a cada servidor

El objetivo es socializar al administrador de la infraestructura tecnológica los ataques informáticos más comunes a los que verían comprometidos los activos enumerados en la etapa uno. En esta reunión, se determina la situación actual de cada servidor en el contexto propio de la EEASA.

Acciones

Reunión de trabajo con personal técnico.

Etapa 3 - Planificación de estrategias, diseño y selección de planes de desarrollo.

El objetivo es la revisión de la documentación existente como por ejemplo los siguientes documentos: plan informático institucional y plan de contingencia para continuidad de negocio. En esta etapa, se evalúa la situación actual y contrasta con los activos a proteger.

Acciones

Revisión de la documentación existente

Planificación de estrategias

Etapa 4 - Análisis de vulnerabilidades con el uso de técnicas de caja negra, gris y blanca.

En esta etapa, se realizan pruebas de penetración de los servidores con el objetivo de encontrar posibles vulnerabilidades. Se detalla el cuadro 50 con el enfoque de cada técnica aplicada por el pentester (Hacker ético).

Cuadro 50. Técnicas de Pentesting

Black Box	**White Box**	**Gray Box**
La prueba Black Box, o «Caja Negra», es casi como una prueba a ciegas, pues sigue la premisa de no poseer gran cantidad de información disponible sobre la corporación. Aunque sea dirigido, pues alcanza a la empresa contratante y descubre vulnerabilidades, el Pentest de Caja Negra es el más cercano a seguir las características de un ataque externo.	La prueba White Box, o de «Caja Blanca», es el Pentest más completo. Esto es porque parte de un análisis integral, que evalúa toda la infraestructura de red. En el caso de que, se produzca un error en el sistema, es posible que, al iniciar el Pentest, el hacker ético ya posee conocimiento de todas las informaciones esenciales de la empresa, como topografía, contraseñas, IPs, logins y todos los demás datos que, se refieren a la red, servidores, estructura, posibles medidas de seguridad, firewalls, entre otra información.	Definido como una mezcla de los dos tipos anteriores, el Gray Box – o «Caja Gris» – ya posee cierta información específica para realizar la prueba de intrusión. Sin embargo, esta cantidad de información es baja y no, se compara a la cantidad de datos disponibles en un Pentest de Caja Blanca.

Fuente: elaboración propia

Acciones

Generar un listado de vulnerabilidades

Etapa 5 - Priorización de riesgos, determinación de responsabilidades, establecimiento de protecciones.

Aquí establece un vínculo entre las salvaguardas que recomienda Magerit y un funcionario responsable. El cuadro 51, se detalla las salvaguardas resultantes del análisis cualitativo:

Cuadro 51. Codificación de salvaguardas

Código	**Salvaguarda**
PPE	Protección física de los equipos
HW	Protección de los Equipos Informáticos
SC	System And Communications protection
CP	Contingency Planning
SR	Supply Chain Risk Management
IM	Gestión de incidentes
MA	MAINTENANCE
Tools	Herramientas de seguridad
CA	Assessment, Authorization and monitoring
NEW	Adquisición y desarrollo
SI	System and Information integrity
E	Relaciones externas
IR	Incident Response
G	Organización

Fuente: elaboración propia

Acciones

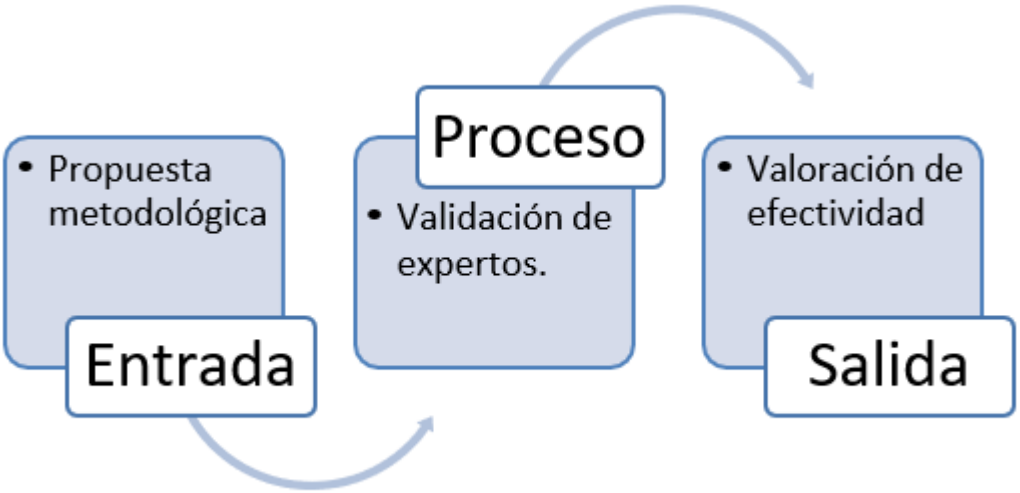
Actualización del plan informático existente con los roles, responsabilidades y frecuencia de aplicación.

Etapa 6 - Informes y resultados.

Elaboración de un acta de compromisos para la evaluación y valoración de efectividad de la aplicación de las salvaguardas.

3.2. Proceso de validación de la propuesta

Figura 20. Proceso validación de la propuesta



Fuente: Elaboración propia

El instrumento que, se usa para validar la efectividad de las 6 etapas de la propuesta metodológica es la encuesta

3.3. Evaluación de la propuesta

Para la valoración de la propuesta metodológica, se cuenta con el aporte de un experto en metodología Magerit y, se aplica un checklist como instrumento de evaluación, debido a que permite determinar la efectividad del trabajo realizado.

Cuadro 52. CheckList Validado por experto Magerit

Pregunta	SI	NO
¿En el contexto de Magerit, el descubrimiento de los activos con fuentes abiertas es claro?	X	
¿Considera adecuado socializar al grupo de tecnología los posibles ataques que experimenta un servidor?	X	
¿Es importarte conocer el plan informático institucional para mitigar los riesgos determinados por Magerit?	X	
¿Las pruebas de penetración ayudan positivamente a determinar exactamente cada vulnerabilidad de la propuesta metodológica?	X	
¿Considera adecuado la actualización del procedimiento, políticas, plan informático, contingencia, entre otros, para el seguimiento y control de cada actividad de la propuesta metodológica?	X	
¿La evaluación permanente de la propuesta metodológica permite optimizar en menor tiempo la gestión del riesgo?	X	

Fuente: Elaboración Propia

3.4. Validación de hipótesis

La propuesta metodológica permite mitigar los riesgos referentes a vulnerabilidades de almacenamiento de la información de la EEASA, pues, se enfoca en salvaguardar brechas que en cualquier momento son explotadas. El presente estudio, se aplicó la probabilidad de ocurrencia de los incidentes informáticos en Ecuador.

CONCLUSIONES

- El presente trabajo, se basa en la revisión del estado de arte referenciado, y concluye que los recursos materiales y humanos necesarios para realizar investigación en OSINT son menores respecto a otros métodos como HUMINT o IMINT, por lo que le convierte en un método útil para la realizar la investigación. En este sentido, con las técnicas de OSINT, se permite revelar los activos analizados en Magerit.

- El análisis de las vulnerabilidades de las Listas de OWASP e ISO27001, pone en manifiesto las brechas de seguridad en un sistema de información. Para determinar el nivel de riesgo en la empresa desde el punto de vista externo, se valora el nivel de ocurrencia de ataques en el Ecuador y concluye que existe un índice de probabilidad de ataque a los activos descubiertos con OSINT.

- Se diseñó una propuesta metodología estructurada por 6 etapas en las que, se establece una serie de mecanismos que permiten aplicabilidad a todas las empresas con similares características que aún no tienen definido un plan de acción debido a la falta de control de las fuentes públicas de información.

- Una vez culminado el trabajo, se llegó a la conclusión que la propuesta metodológica tiene efectividad para mitigar vulnerabilidades; sin embargo, ésta requiere ser socializada al equipo de tecnología para que, se tomen las medidas preventivas necesarias debido a que existe la posibilidad de ocurrencia en cualquier momento según la matriz de riesgo determinada.

RECOMENDACIONES

- Para el estudio de OSINT, se recomienda el uso de plugins que disponen las herramientas aplicadas utilizadas en la investigación, debido a que genera información complementaria de gran utilidad.

- Se recomienda para el análisis de ocurrencia de ataques informáticos, trabajar con estadísticas mundiales que manejan los equipos de respuesta ante emergencia informáticas (CERT) o el equipo de respuesta ante incidencias informáticas (CSIRT) para tener una mayor probabilidad previsora y afinar las salvaguardas de una manera estándar en el contexto de que la propuesta metodológica sea aplicable internacionalmente.

- Se recomienda la aplicación de BIGDATA y técnicas de MACHINE LEARNING, en el sentido de automatizar en tiempo real alertas que permitan establecer planes de acción en tiempos cortos, esto permite mitigar eventos antes de que, se susciten.

- Para futuras investigaciones, se recomienda realizar el estudio de vulnerabilidades en los sistemas SCADA, pues la protección de estos sistemas de gran escala tiene mayor beneficio en las empresas que lo dispongan, la cual gana mayor confidencialidad, integridad y disponibilidad de la información.

BIBLIOGRAFÍA

【 *OSINT* 】*¿Qué Es? + Ventajas y Desventajas ▷ 2022*. (2020, noviembre 25). Internet Paso a Paso. https://internetpasoapaso.com/osint/

Alves, F., Andongabo, A., Gashi, I., Ferreira, P. M., & Bessani, A. (2020). Follow the Blue Bird: A Study on Threat Data Published on Twitter. En L. Chen, N. Li, K. Liang, & S. Schneider (Eds.), *Computer Security – ESORICS 2020* (pp. 217-236). Springer International Publishing. https://doi.org/10.1007/978-3-030-58951-6_11

Chitkara, A., Singh, D., Gupta, A., & Varshney, G. (2020). IntelliSpect: Personal Information Search Tool. *2020 International Conference on Information Networking (ICOIN)*, 556-561. https://doi.org/10.1109/ICOIN48656.2020.9016488

CiberPatrulla - OSINT: Inteligencia en Fuentes Abiertas. (s. f.). Recuperado 28 de noviembre de 2021, de https://ciberpatrulla.com/

Devia, G., & Calvache, C. (2014). Mogrit: Towards a IT risks management model for MSME. *Sistemas y Telemática*, *12*, 35. https://doi.org/10.18046/syt.v12i30.1860

ENISA. (s. f.). Recuperado 5 de diciembre de 2021, de https://www.enisa.europa.eu/

Gordón, A., & Salazar-Chacón, G. (2020). DRP Analysis: Service Outage in Data Center due to Power Failures. *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 0182-0187. https://doi.org/10.1109/IEMCON51383.2020.9284920

Hernández, M., Hernández, C., Diaz-López, D., Garcia, J. C., & Pinto, R. A. (2018). Open source intelligence (OSINT) as Support of Cybersecurity Operations: Use of OSINT in a Colombian Context and Sentiment Analysis. *Revista Vínculos Ciencia, tecnología y sociedad*, *15*(2). https://revistas.udistrital.edu.co/index.php/vinculos/article/view/13504/14315

Indio, T., & Isidoro, Y. (s. f.). *Delitos informáticos frecuentes en el ecuador: Casos de estudio*. 12.

Inicio | *Scrum.org*. (s. f.). Recuperado 7 de diciembre de 2021, de https://www.scrum.org/

Kluppelberg, C., & Straub, D. (2014). *Risk. A multidisciplinary introduction*. https://doi.org/10.1007/978-3-319-04486-6

Los delitos informáticos crecen en Ecuador; cada clic en la web deja su rastro. (2020, septiembre 27). El Universo. https://www.eluniverso.com/noticias/2020/09/27/nota/7991905/delitos-informaticos-internet-casos-reales-redes-sociales-ecuador

Millan Lopez, Juan Antonio.pdf. (s. f.). Recuperado 5 de diciembre de 2021, de https://reunir.unir.net/bitstream/handle/123456789/9790/Millan%20Lopez%2C%20Juan%20Antonio.pdf?sequence=1&isAllowed=y

PAe—Inicio. (s. f.). Recuperado 5 de diciembre de 2021, de https://administracionelectronica.gob.es/pae_Home#.Ya0OFJGZNPY

Pastor-Galindo, J., Nespoli, P., Gómez Mármol, F., & Martínez Pérez, G. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access*, *8*, 10282-10304. https://doi.org/10.1109/ACCESS.2020.2965257

Rivas, K., & Salazar, G. (2019). Design of a Disaster Recovery Plan based on the NIST 800-34 standard and the PMBOK framework for an ecuadorian insurance company. *Latin American Journal of Computing*, *6*(2), 53-62.

Salazar Chacón, G. D. (2021). *Hybrid Networking SDN y SD-WAN: Interoperabilidad de arquitecturas de redes tradicionales y redes definidas por software en la era de la digitalización* [Tesis, Universidad Nacional de La Plata]. https://doi.org/10.35537/10915/129910

Sebastian, S. (s. f.). *Fast Google Dorks Scan—Herramientas de prueba de penetración, tutoriales de ML y Linux*. Recuperado 8 de diciembre de 2021, de https://reconshell.com/fast-google-dorks-scan/

Storage security solution for real data protection. (s. f.). Continuity™. Recuperado 5 de diciembre de 2021, de https://www.continuitysoftware.com/

V, A. A., A K, B., R, M., S, K., & Kumar Mohan, A. (2020). PeopleXploit: A hybrid tool to collect public data. *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, 1-6. https://doi.org/10.1109/ICCCSP49186.2020.9315266

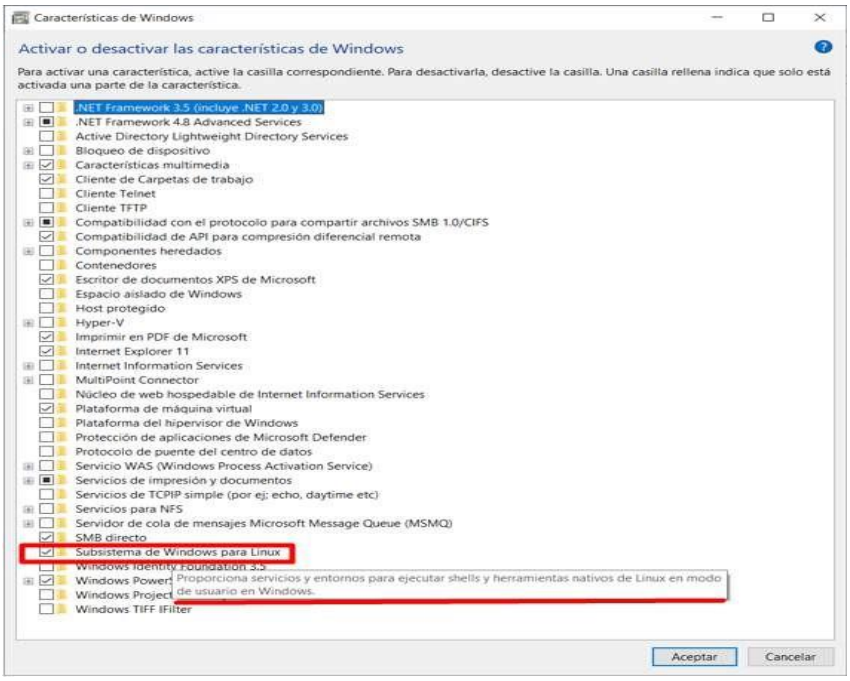
Yeboah-Ofori, A. (2018). Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media. *International Journal of Cyber-Security and Digital Forensics*, *7*, 87-98. https://doi.org/10.17781/P002378

Ziółkowska, A. (2018). Open source intelligence (OSINT) as an element of military recon. *Security and Defence Quarterly*, *19*(2), 65-77. https://doi.org/10.5604/01.3001.0012.1474

ANEXOS

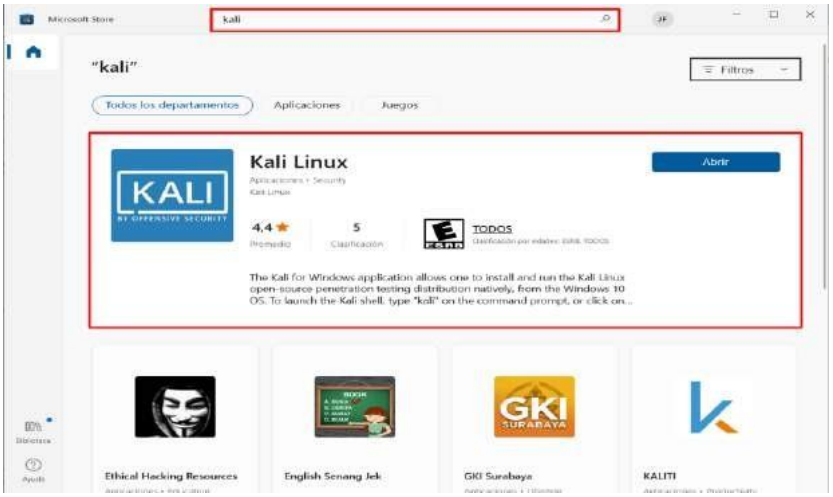
Anexo 1 Activar Kali Linux en Windows 10

Ilustración 1. Activar o desactivar características de *WINDOWS.*



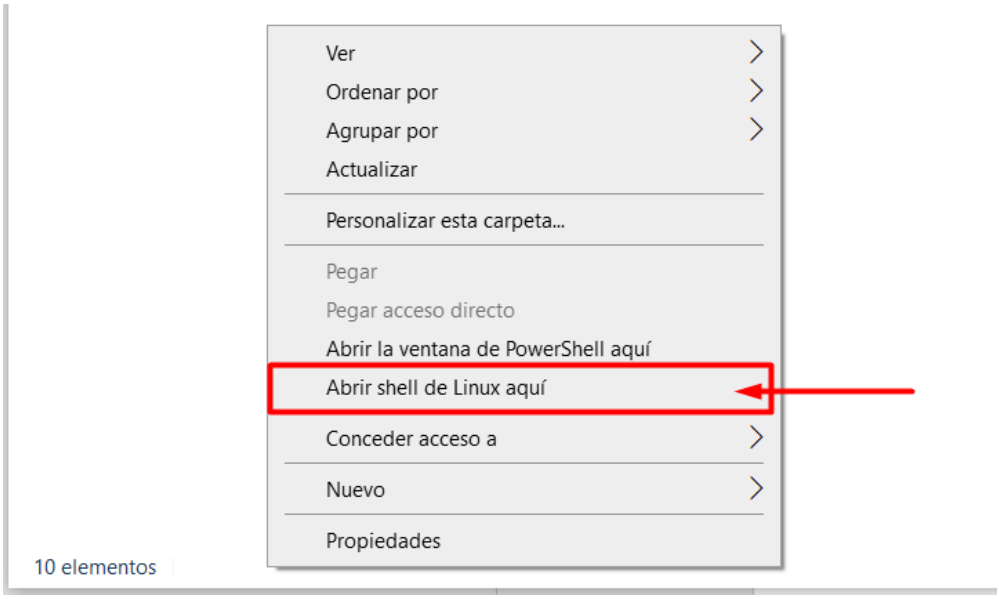
Fuente: elaboración propia

Ilustración 2. En Microsoft Store buscamos Kali e instalamos



Fuente: elaboración propia

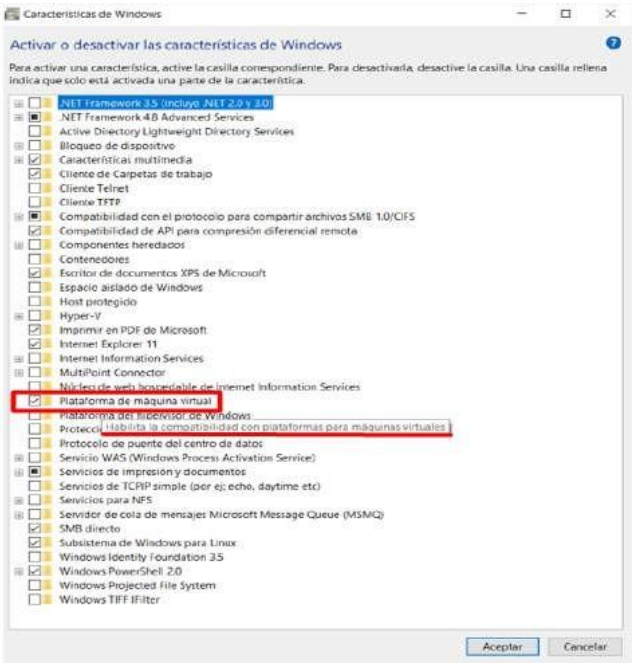
Ilustración 3. Para ejecutar una terminal, se presiona la tecla crtl + click derecho sobre cualquier directorio, seguidamente elegir la opción:



Fuente: elaboración propia

Instalación de entorno gráfico

Ilustración 4. Habilitar la opción plataforma de máquina virtual

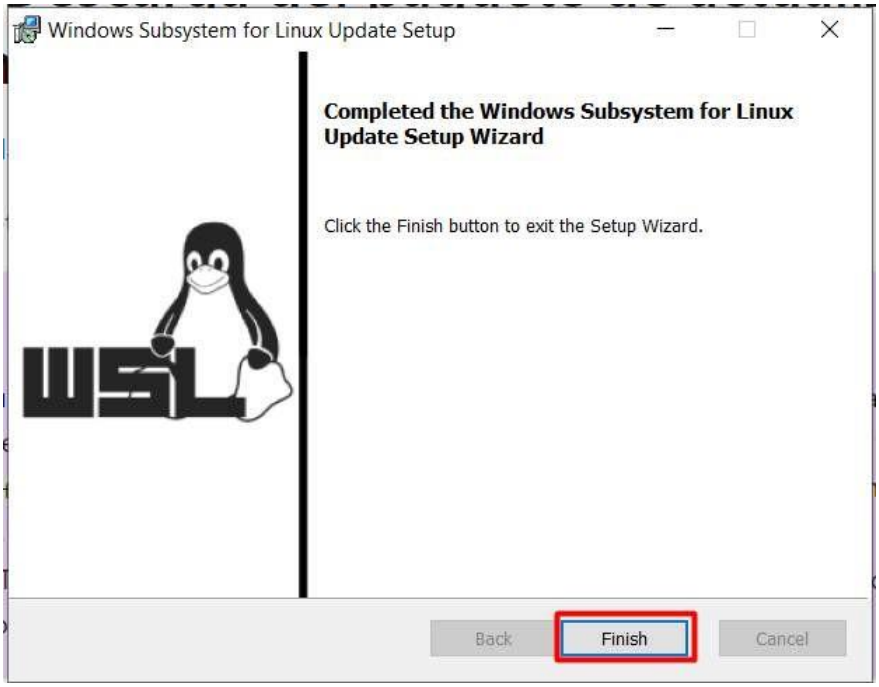


Fuente: elaboración propia

Ilustración 5. Descarga del paquete de actualización del kernel de Linux WSL 2 – Desde MICROSOFT

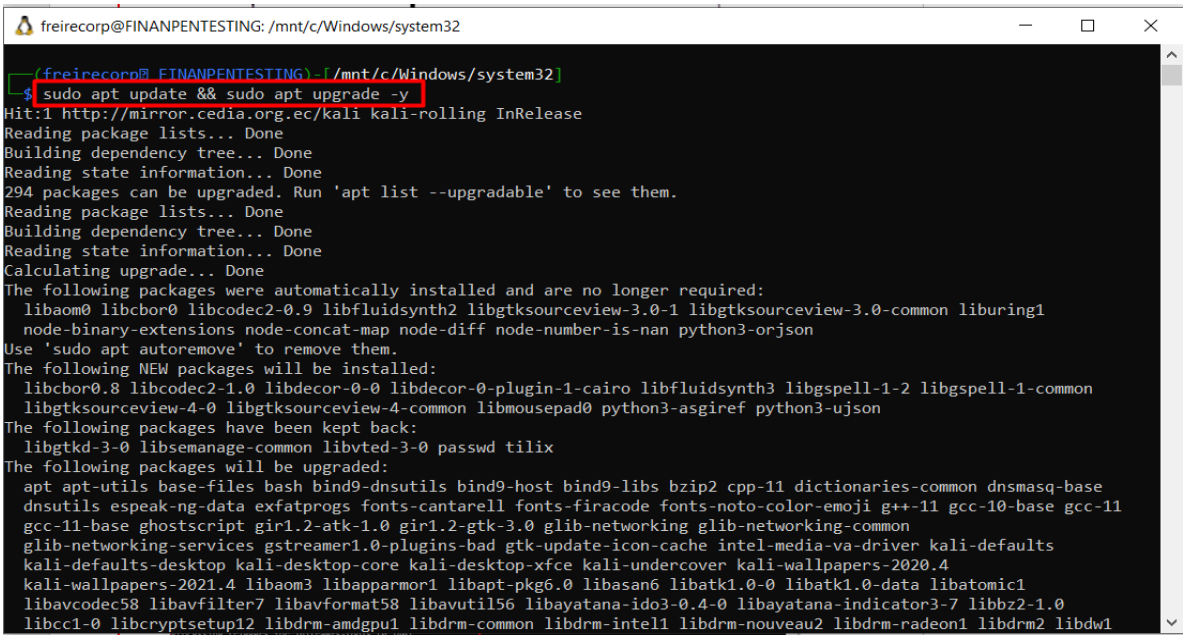
Fuente: elaboración propia

Ilustración 6. Ejecutar instalador y seguir el asistente de Windows hasta finalizar



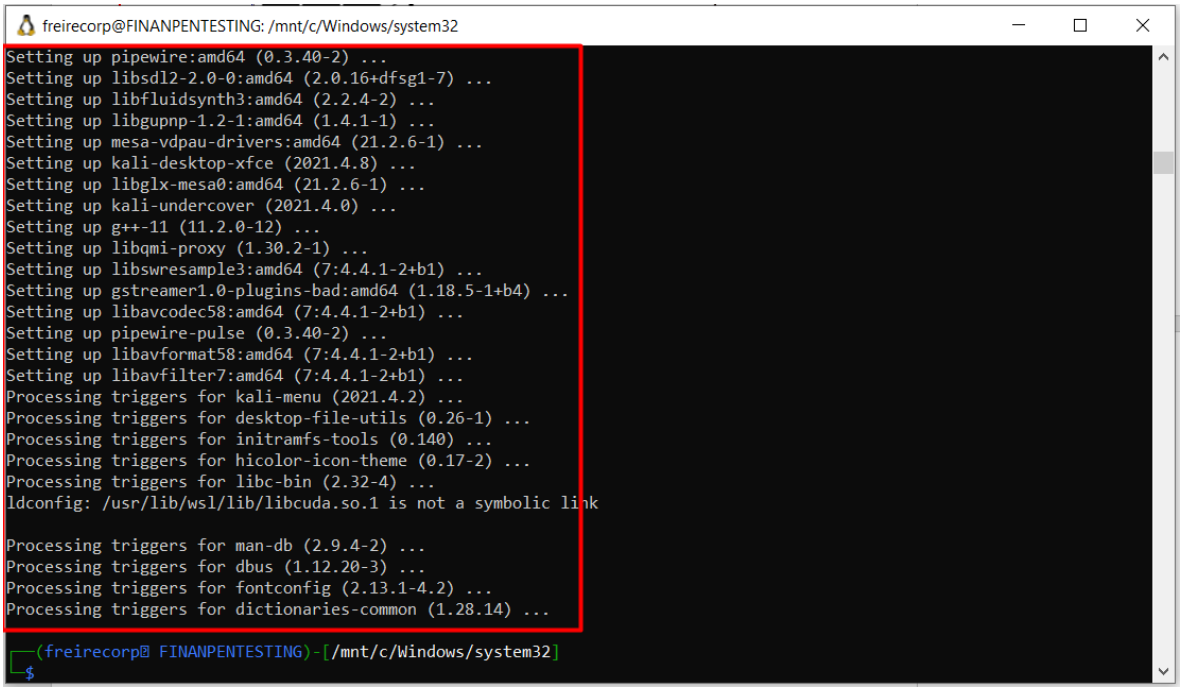
Fuente: elaboración propia

Ilustración 7. Actualizamos las librerías y sistema operativo con el comando update y upgrade



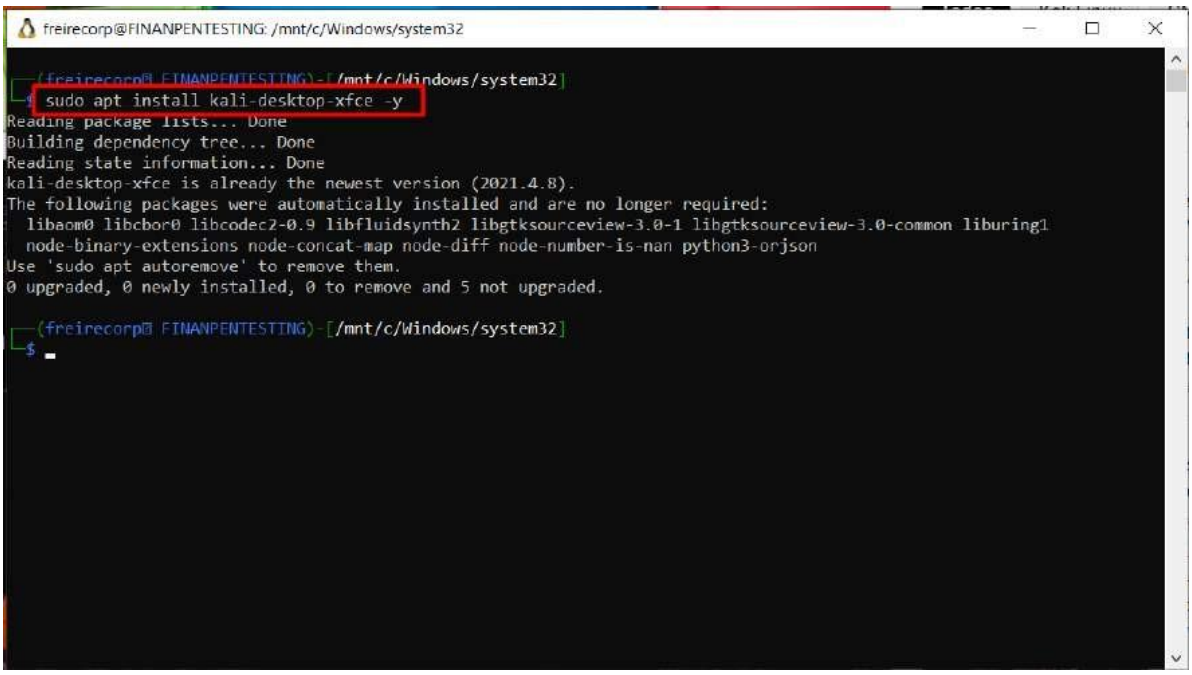
Fuente: elaboración propia

Ilustración 8. Finalización de comando update y upgrade



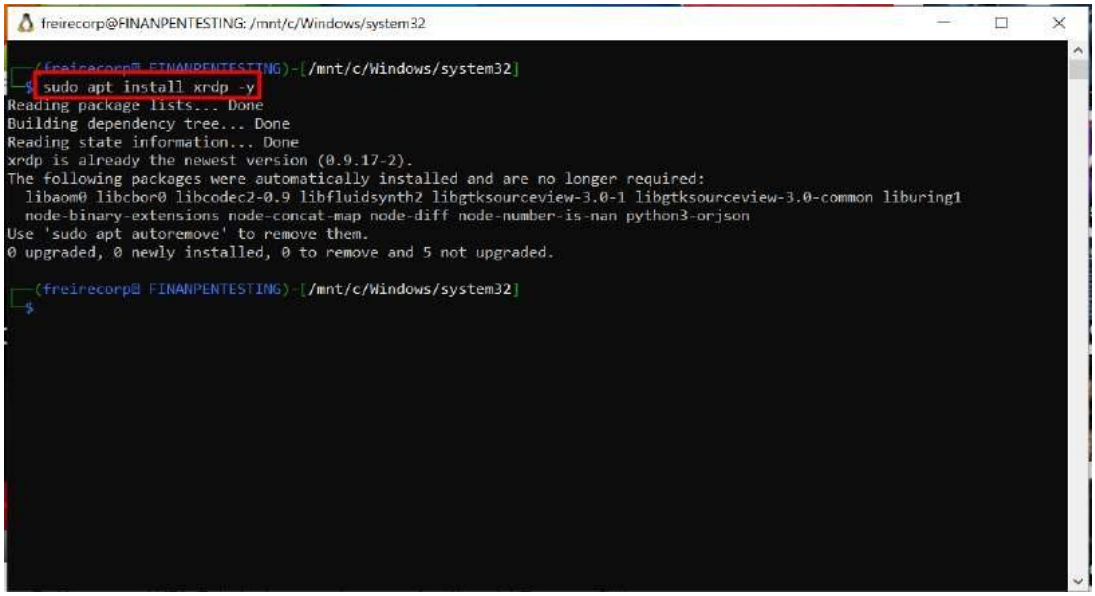
Fuente: elaboración propia

Ilustración 9. Instalación de entorno gráfico XFCE – Durante la Instalación pide seleccionar el idioma del teclado, elegir ingles.



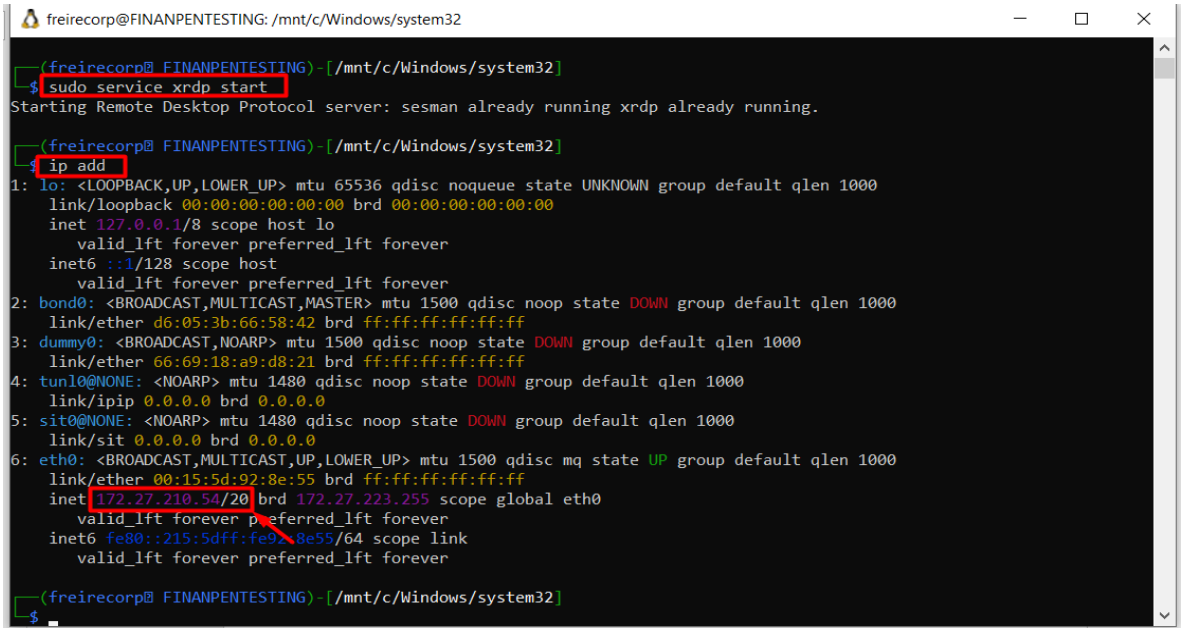
Fuente: elaboración propia

Ilustración 10. Instalación de XRDP, experiencia de escritorio remoto de WINDOWS



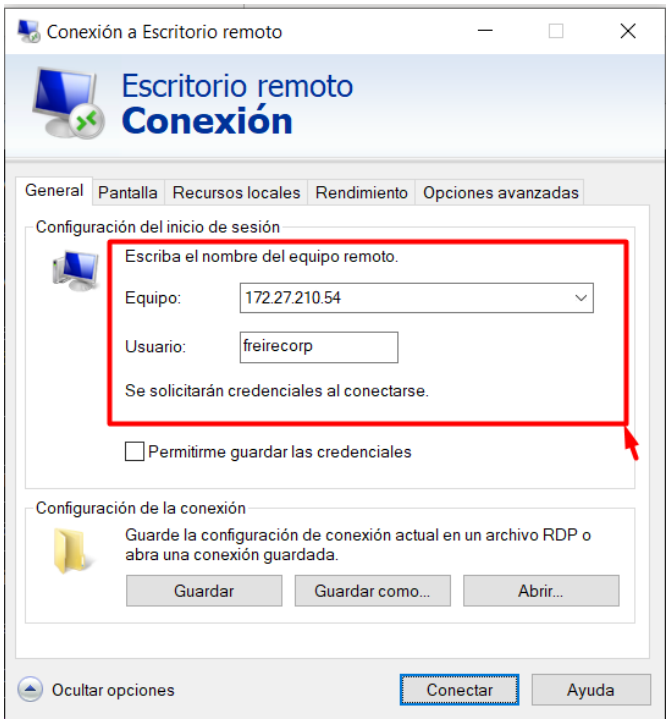
Fuente: elaboración propia

Ilustración 11. Ejecución de entorno gráfico y revisión de la ip virtual para conectarnos con Escritorio Remoto de Windows



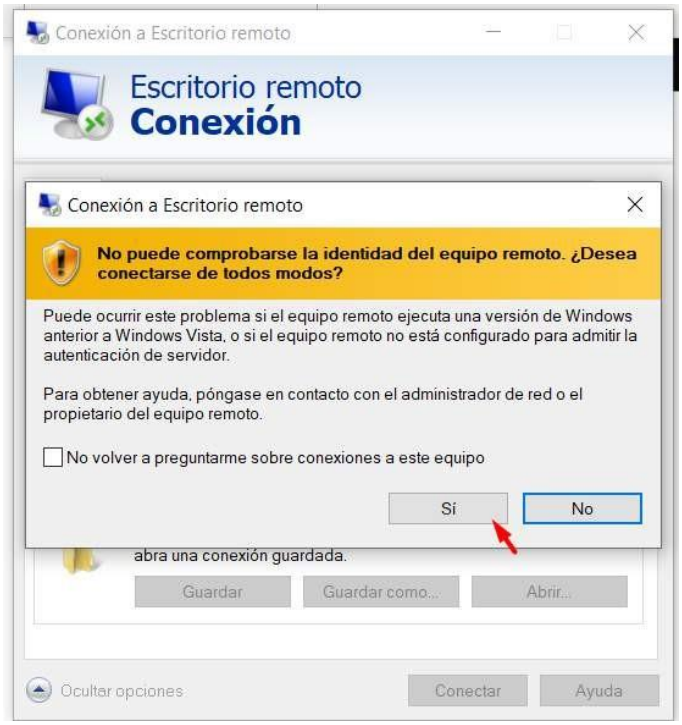
Fuente: Elaboración propia

Ilustración 12. Ejecución de escritorio remoto de Windows



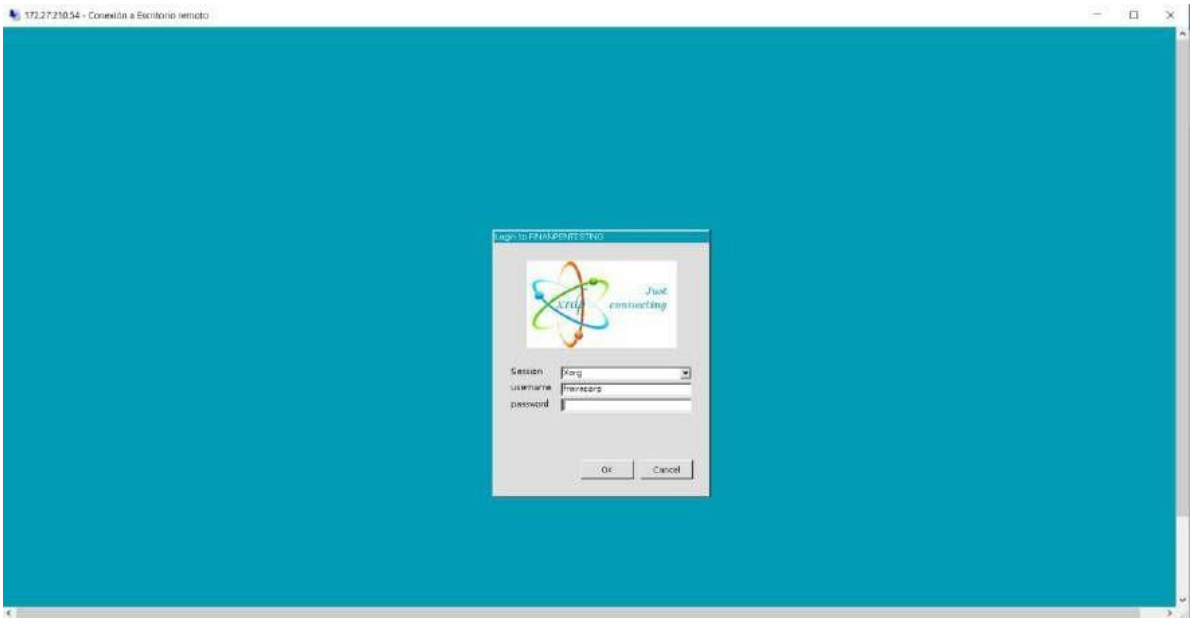
Fuente: elaboración propia

Ilustración 13. Aceptamos la comprobación de identidad de equipo remoto



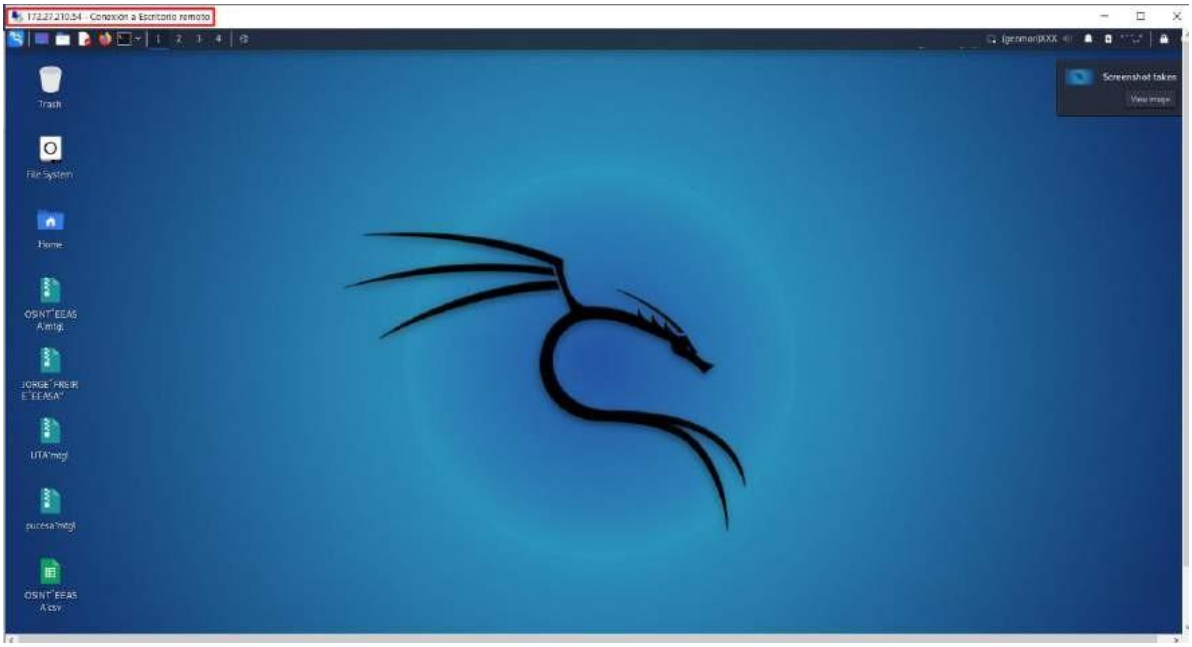
Fuente: elaboración propia

Ilustración 14. Colocar las credenciales configuradas en KALI de consola



Fuente: elaboración propia

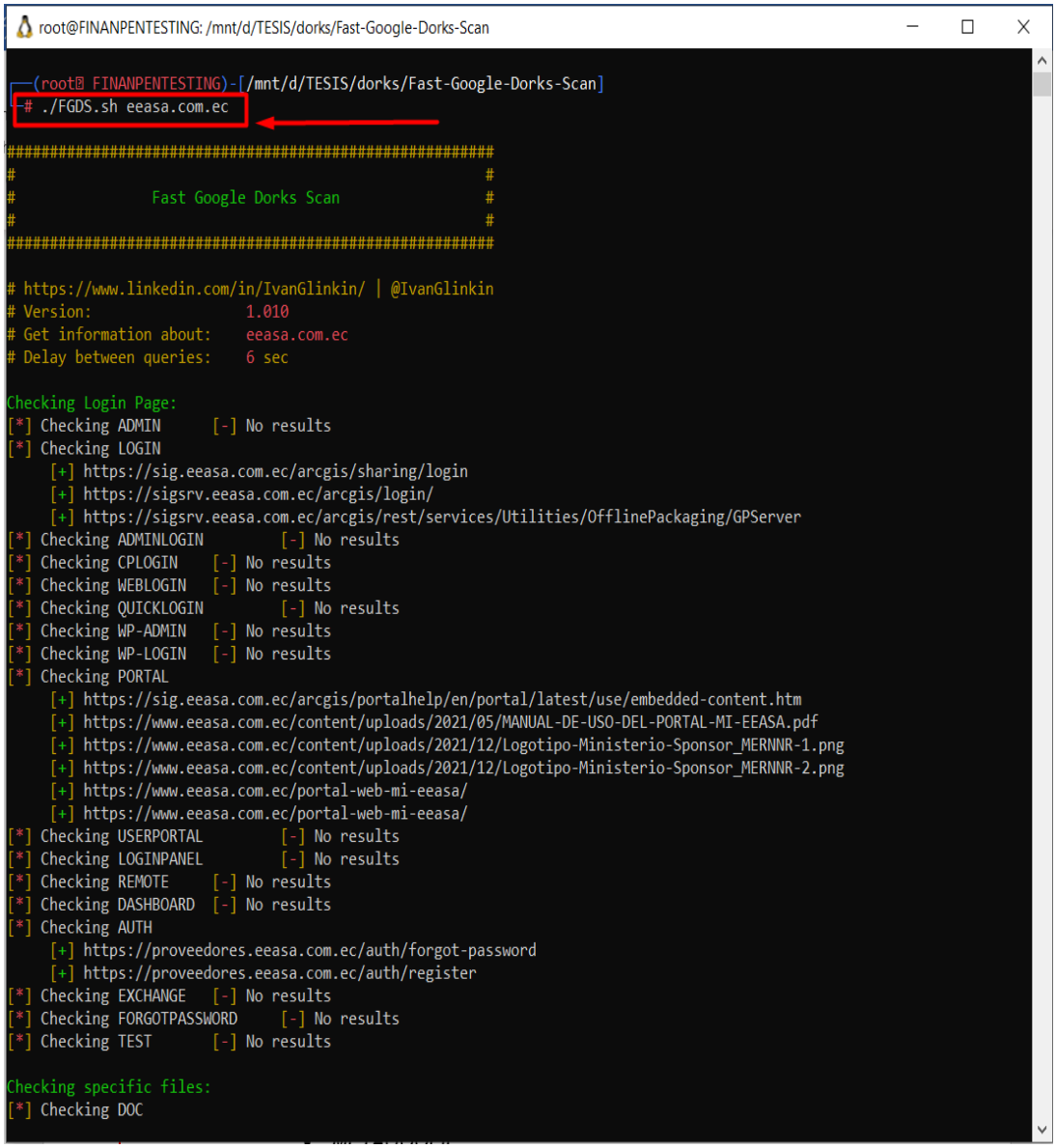
Ilustración 15. Entorno grafico de KALI, se ejecuta desde Windows 10



Fuente: elaboración propia

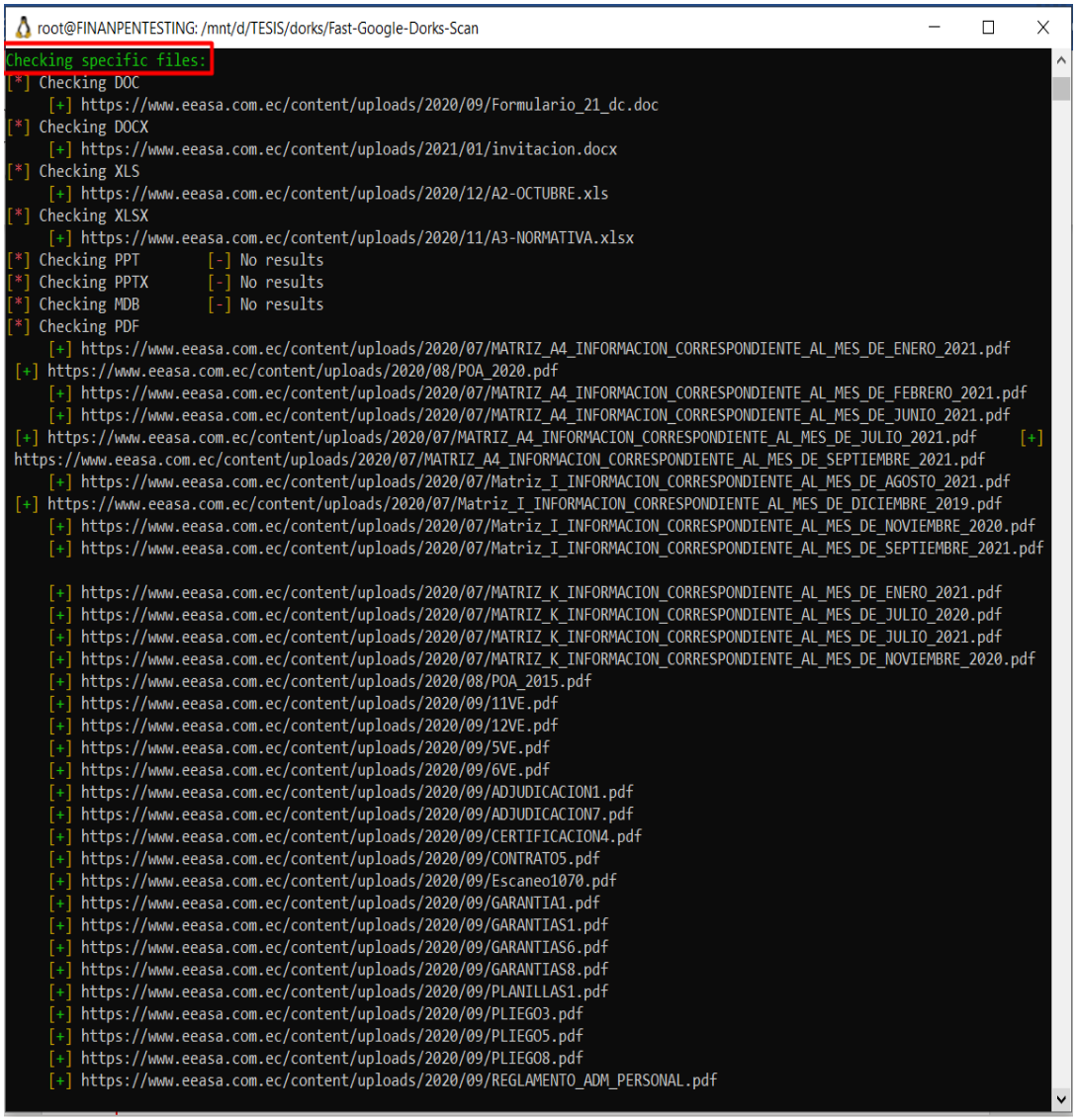
Anexo 2 Ejecución de herramientas aplicadas a la investigación.

Ilustración 16. Búsqueda de dominio - Ejecución de *DORKS*



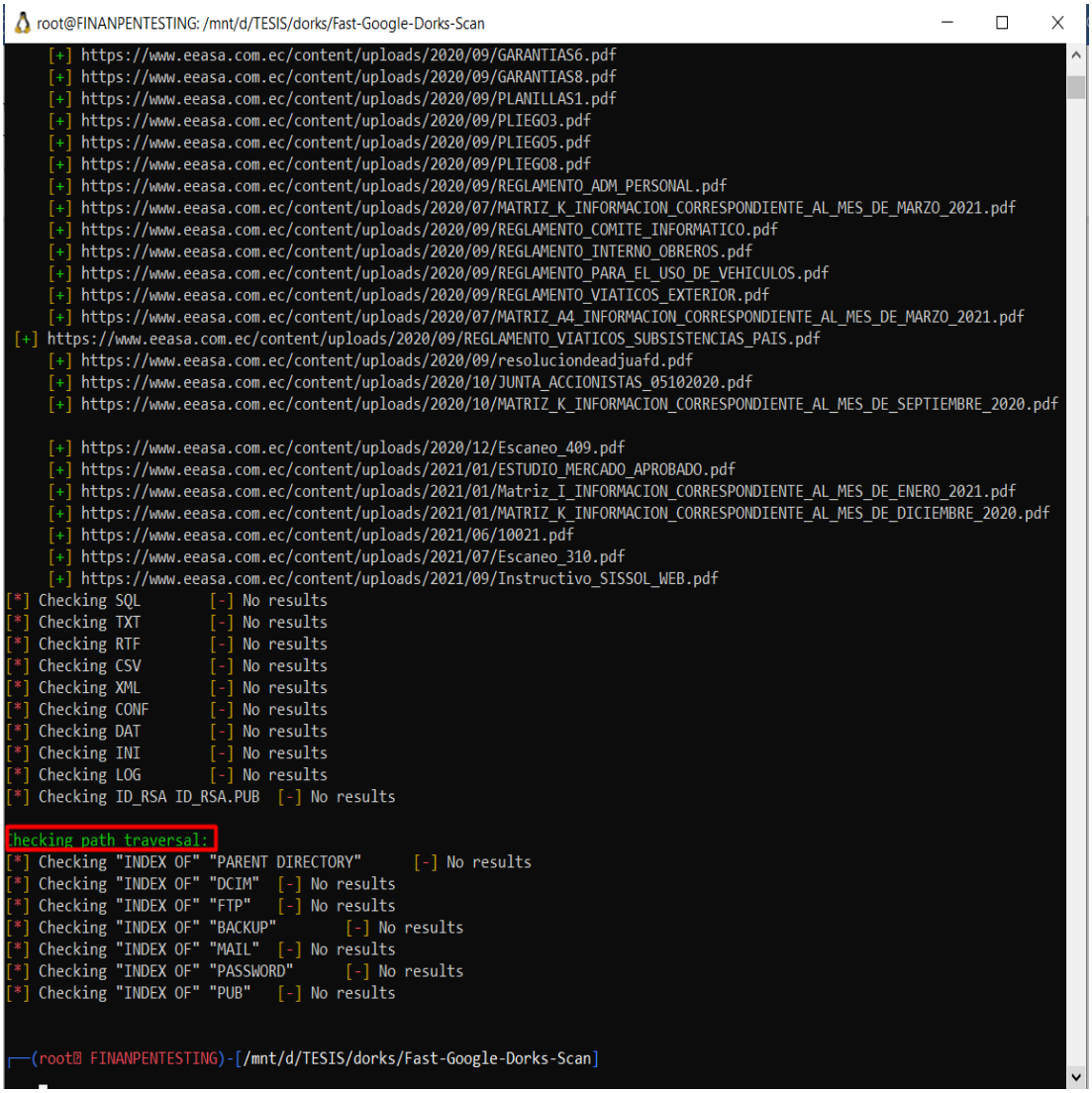
Fuente: elaboración propia

Ilustración 17. Archivos con formato específico – Ejecución de *DORKS*



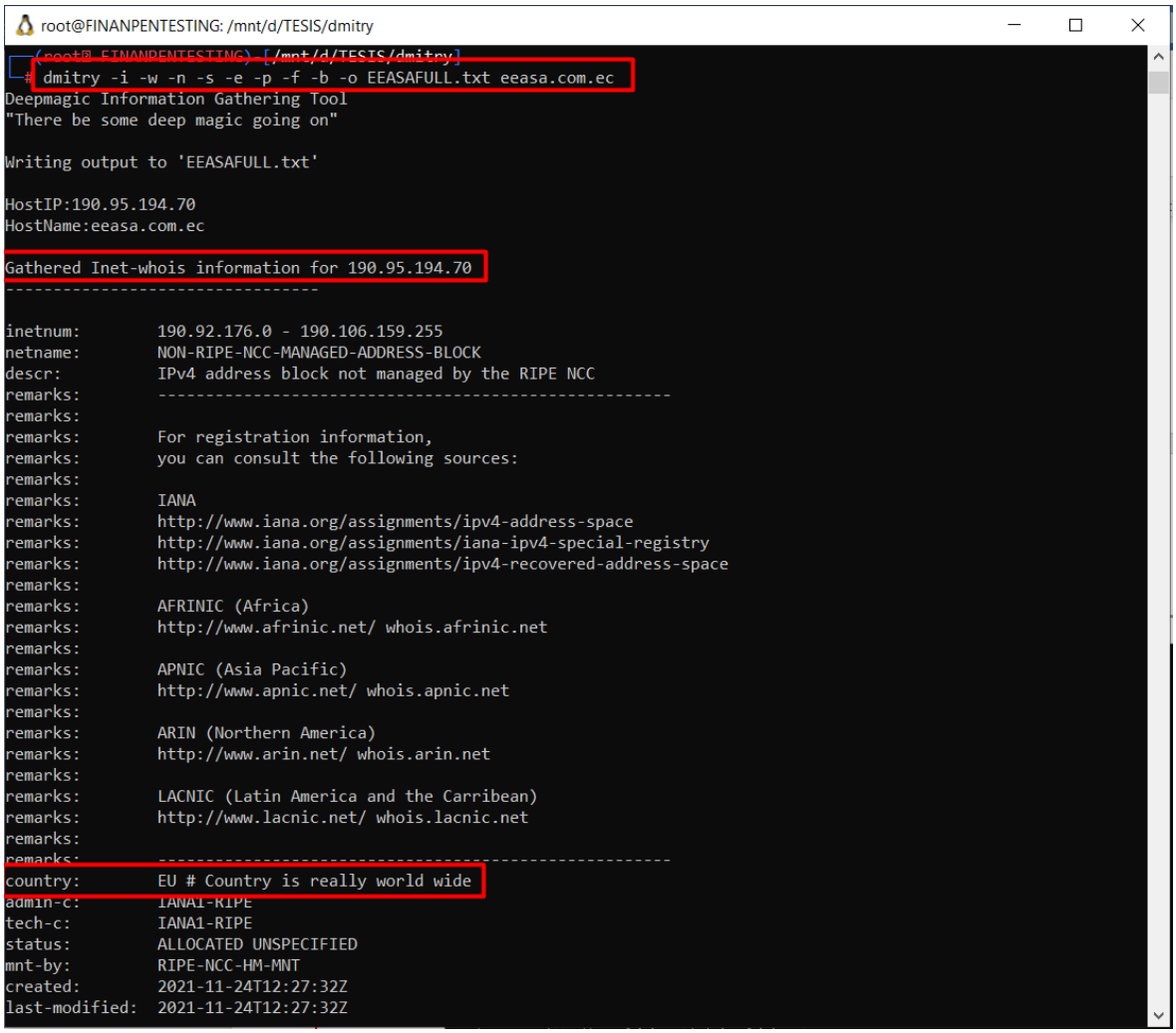
Fuente: elaboración propia

Ilustración 18. Verificación de path traversal – Ejecución de *DORKS*



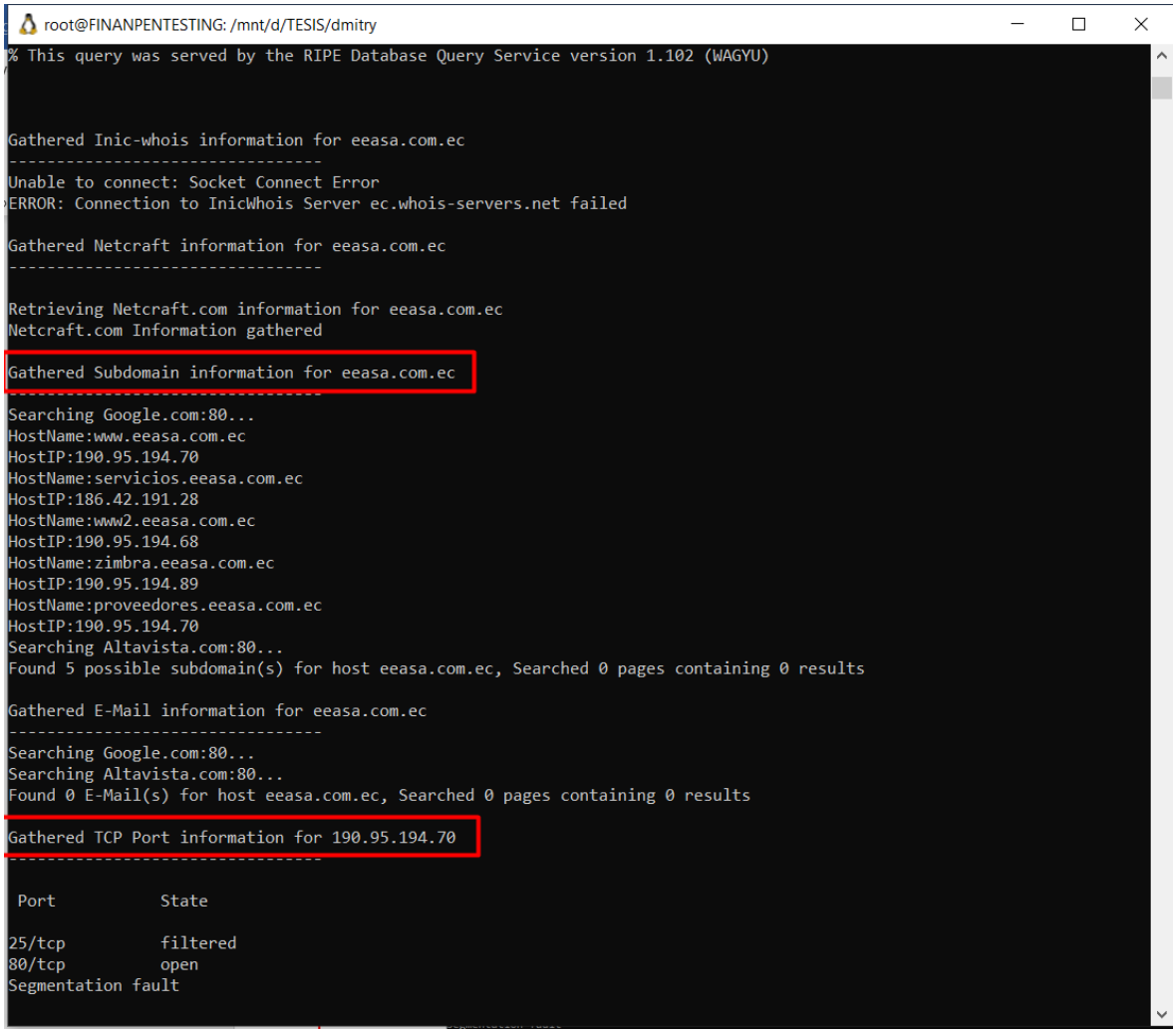
Fuente: elaboración propia

Ilustración 19. Búsqueda de dominio – Ejecución *DMITRY*



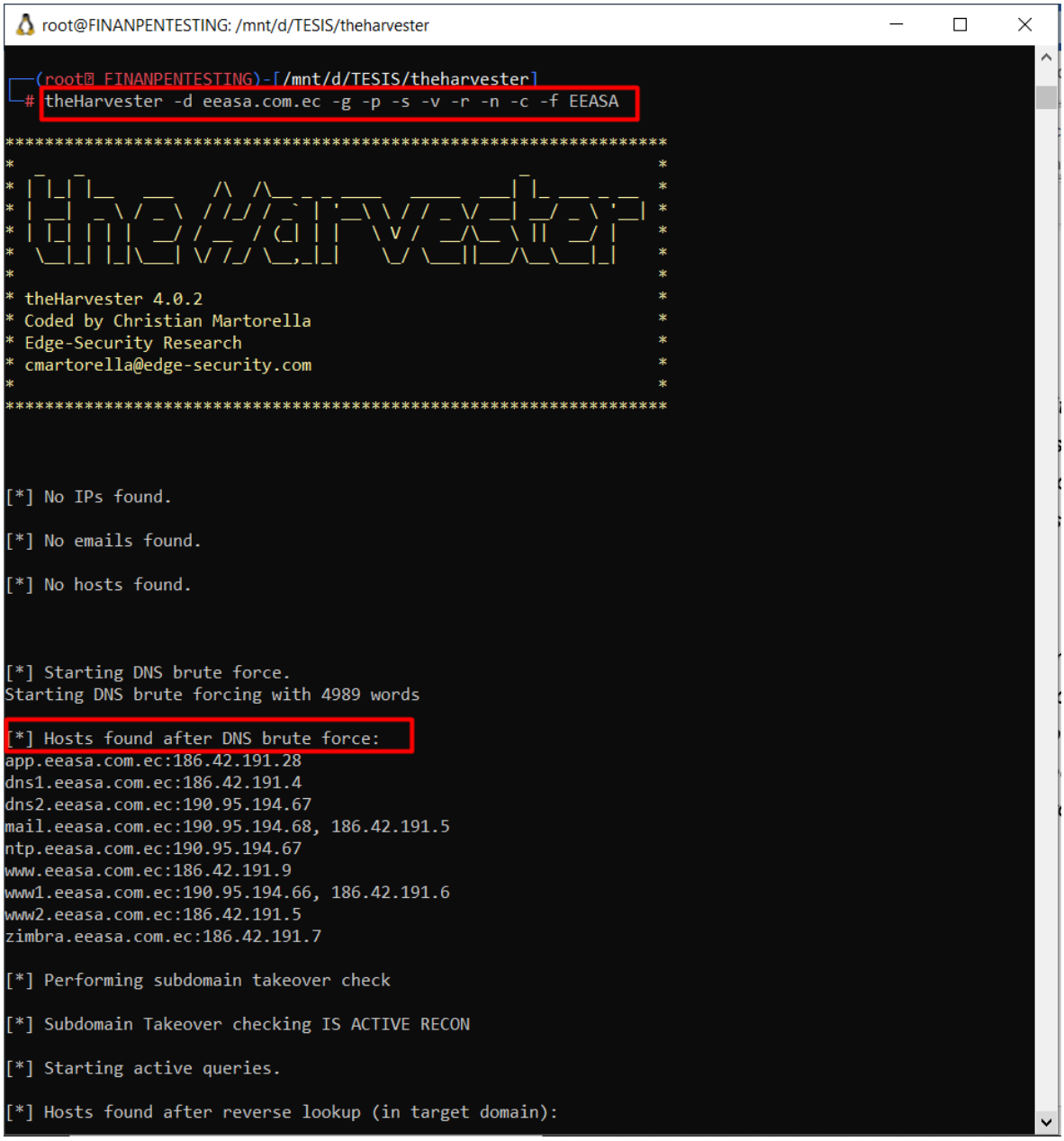
Fuente: elaboración propia

Ilustración 20. Subdominios – Ejecución Dmitry



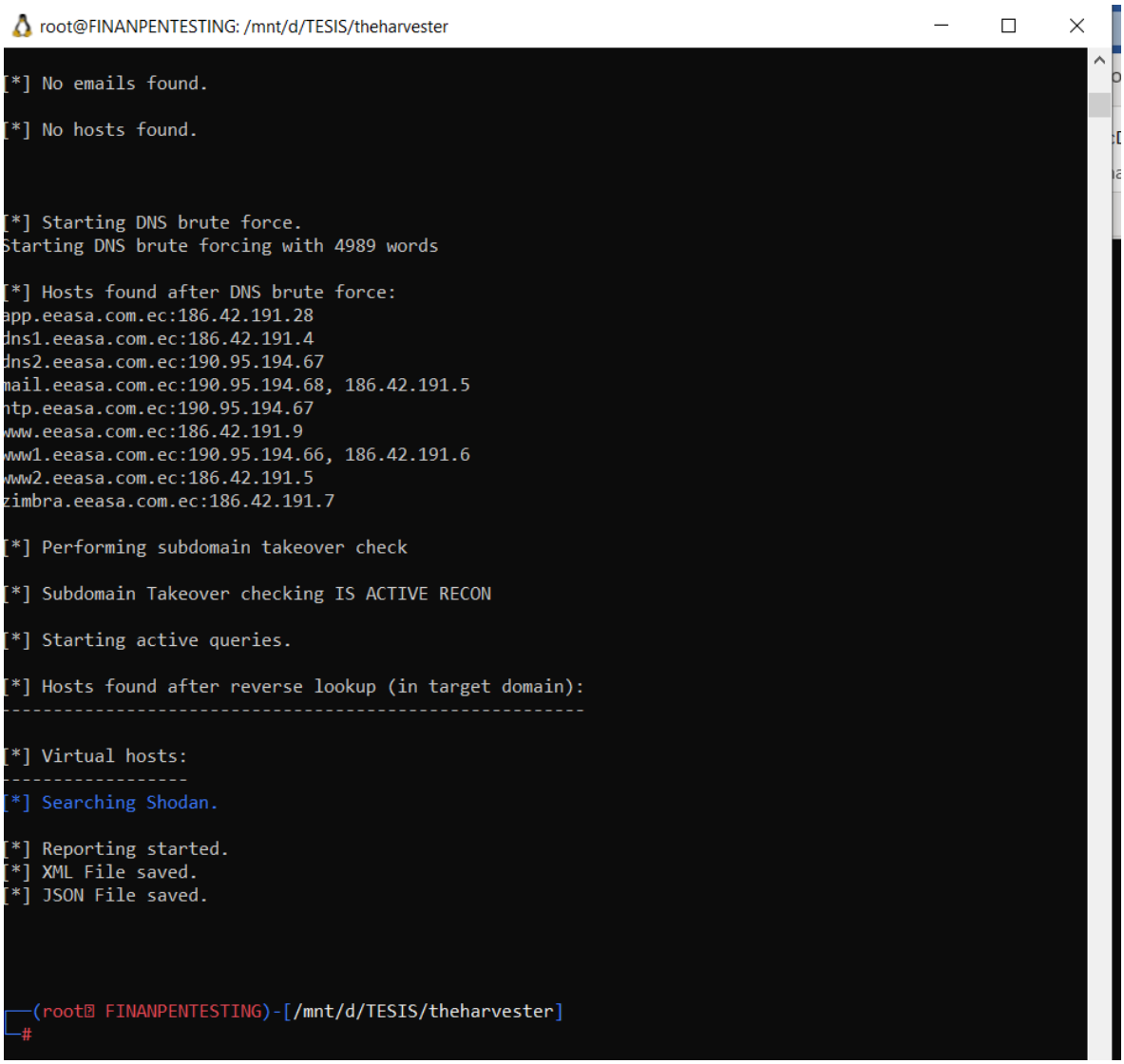
Fuente: elaboración propia

Ilustración 21. Host encontrados - The harvester



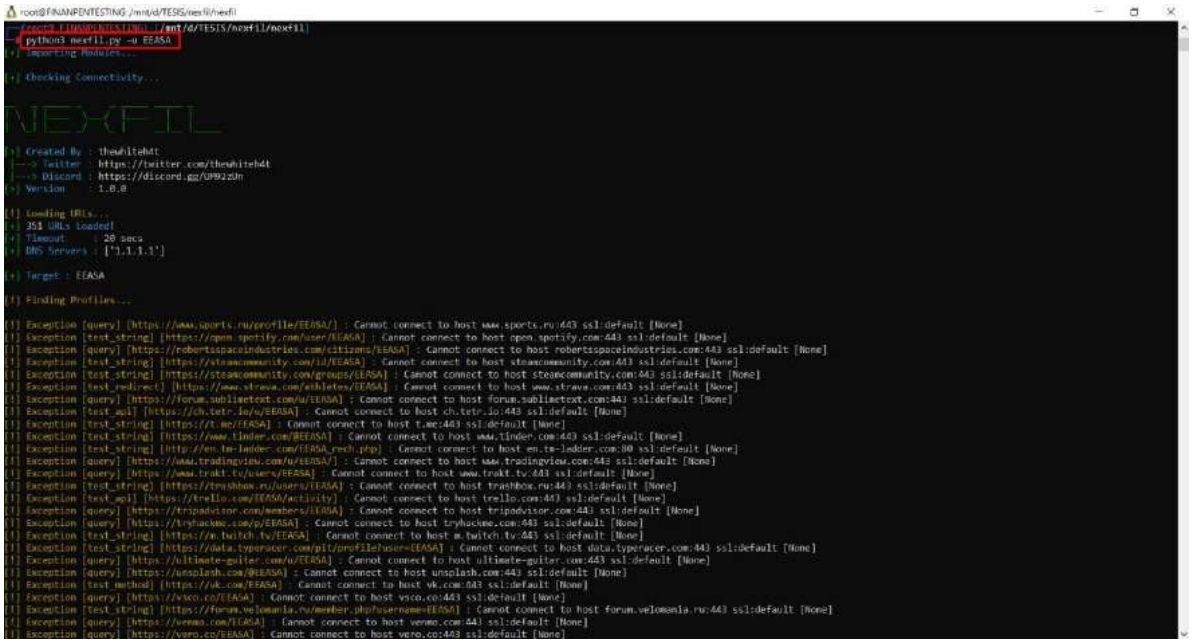
Fuente: elaboración propia

Ilustración 22. Los Dns serían explotados con brute force – The Harvester



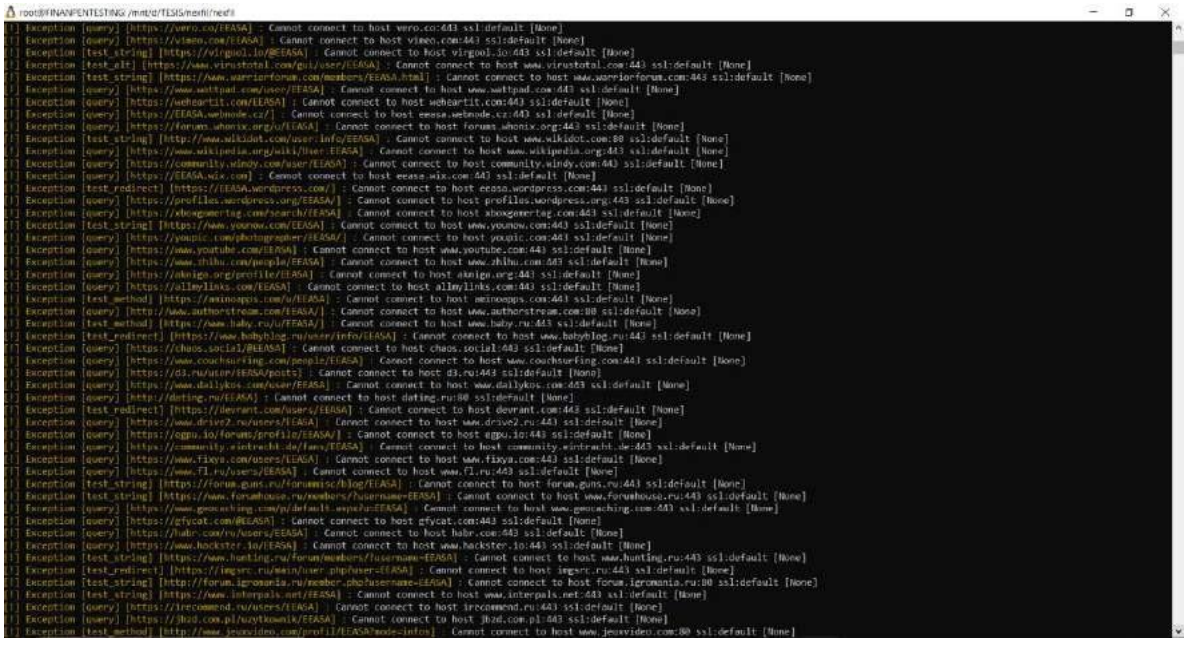
Fuente: elaboración propia

Ilustración 23. Perfiles sociales EEASA parte 1 – Nexfil



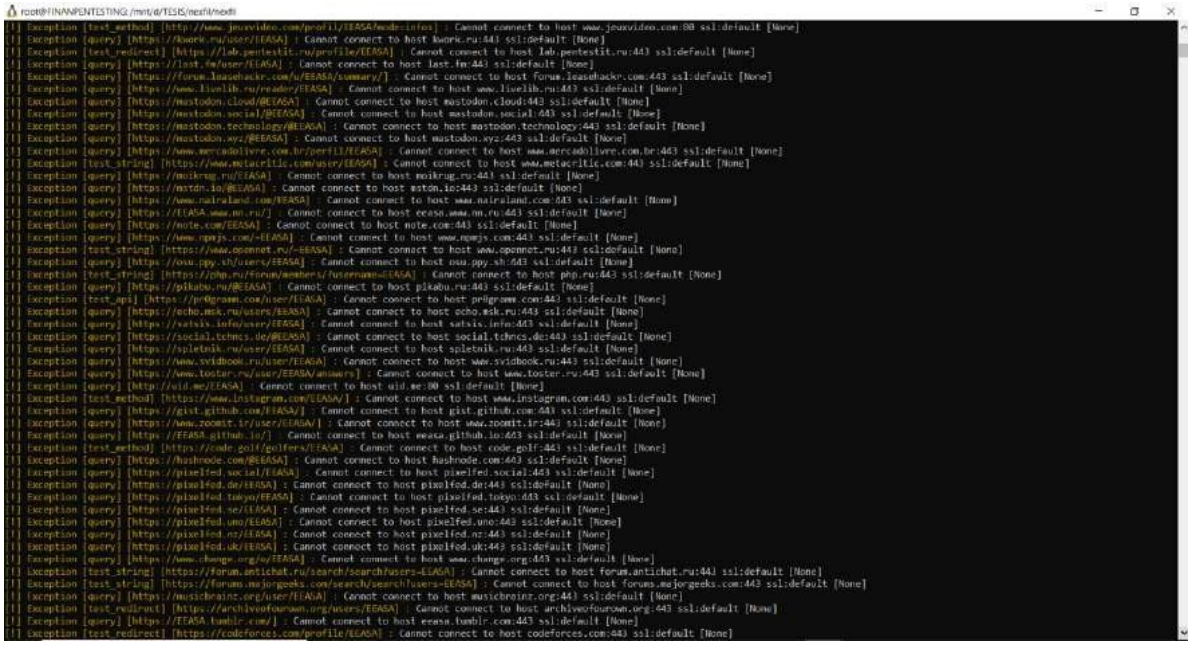
Fuente: elaboración propia

Ilustración 24. Perfiles sociales EEASA parte 2 – Nexfil



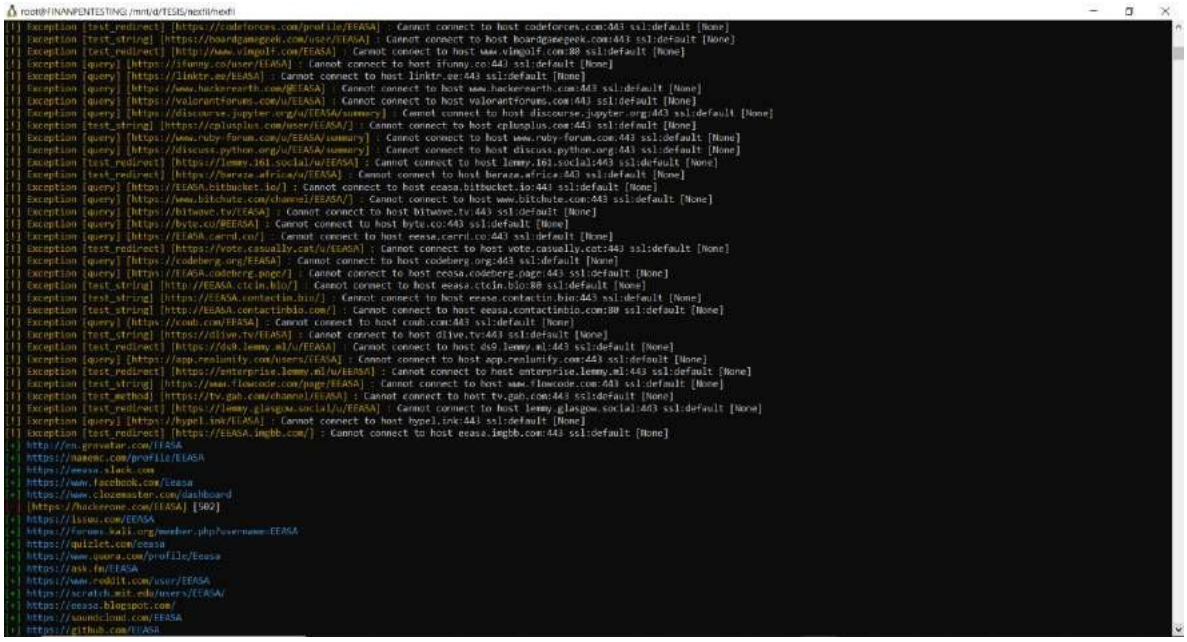
Fuente: elaboración propia

Ilustración 25 Perfiles sociales EEASA parte 4 – Nexfil



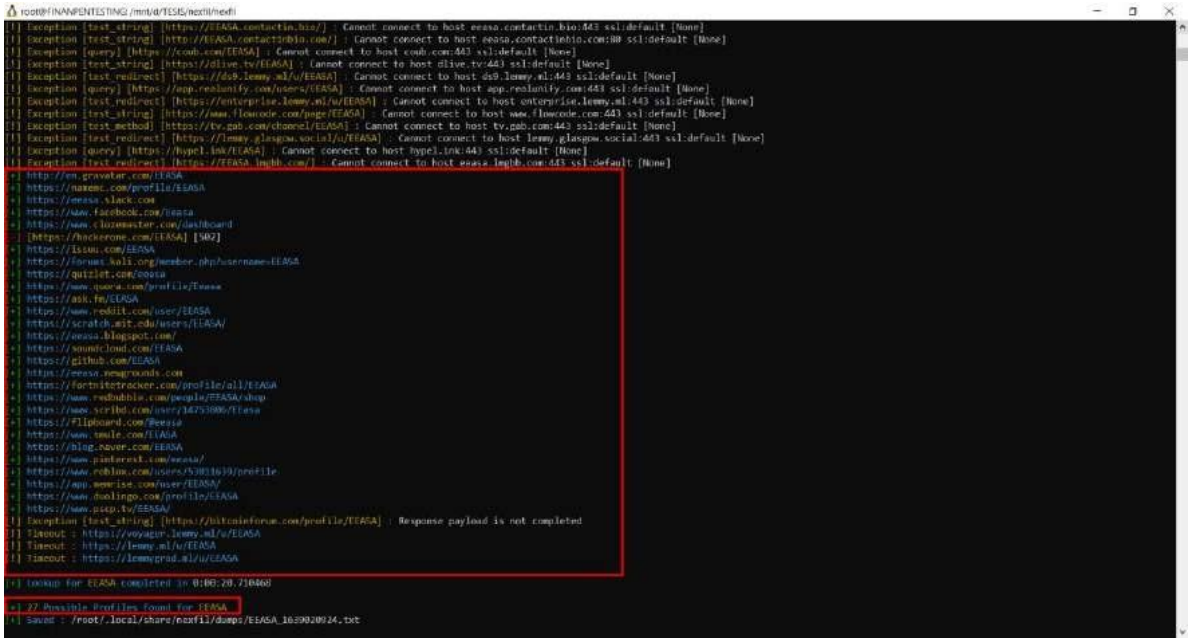
Fuente: elaboración propia

Ilustración 26. Perfiles sociales EEASA parte 5 – Nexfil



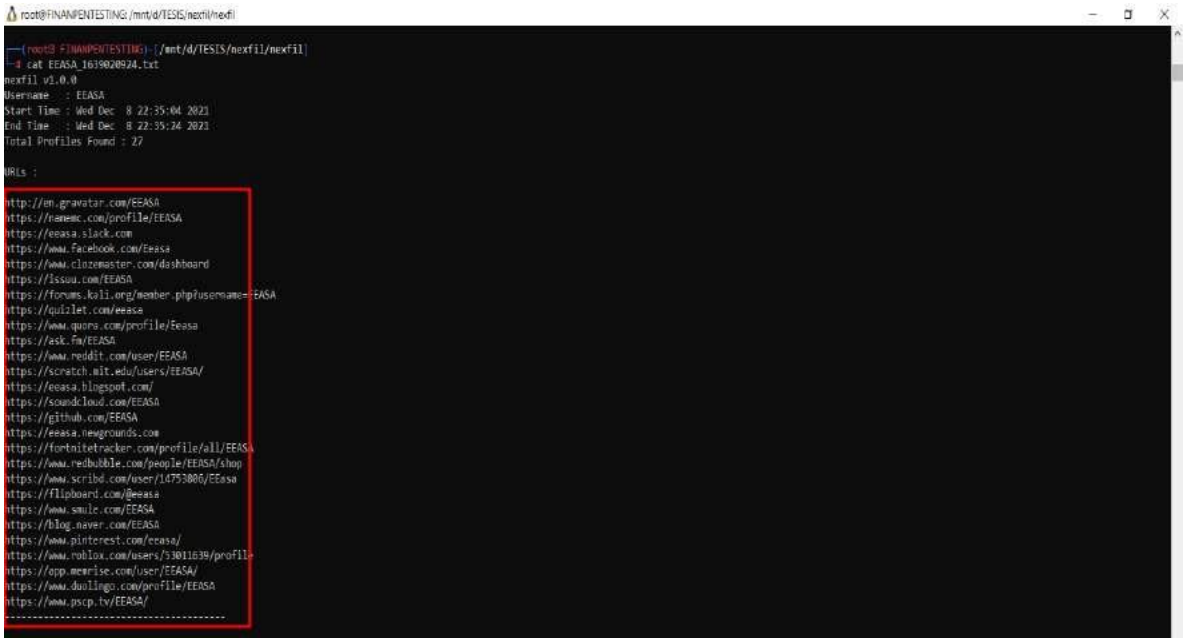
Fuente: elaboración propia

Ilustración 27. Perfiles sociales EEASA parte 6 – Nexfil



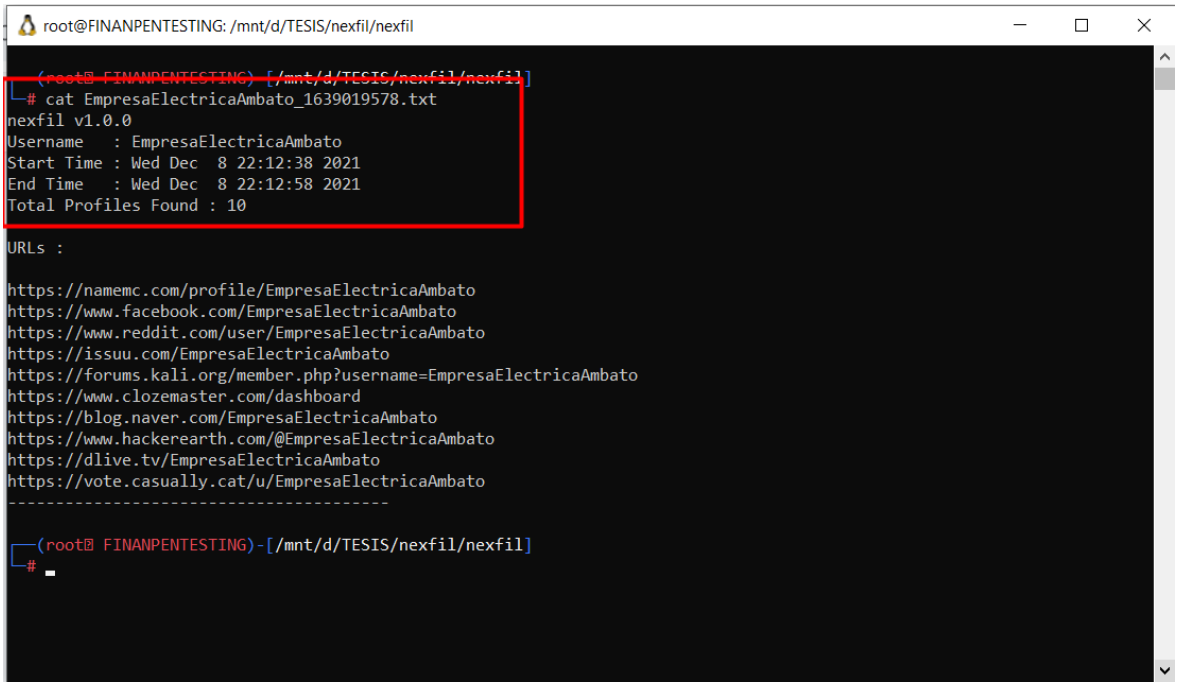
Fuente: elaboración propia

Ilustración 28. Perfiles sociales EEASA parte 7 – Nexfil



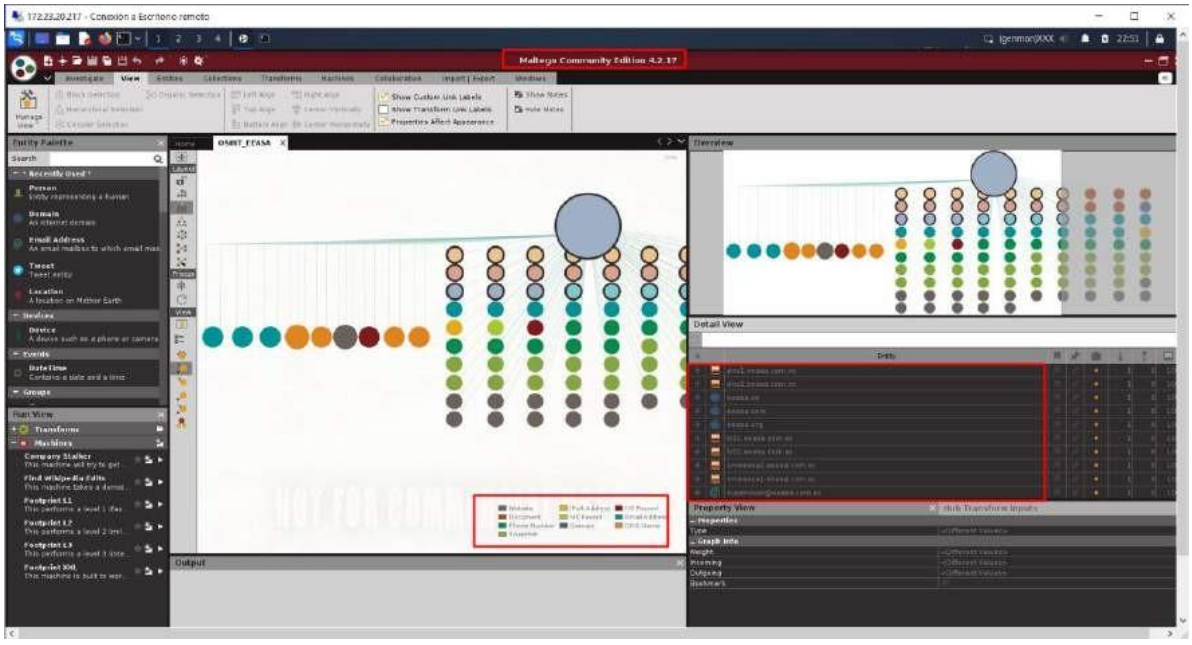
Fuente: elaboración propia

Ilustración 29. Perfiles sociales EEASA parte 8 – Nexfil



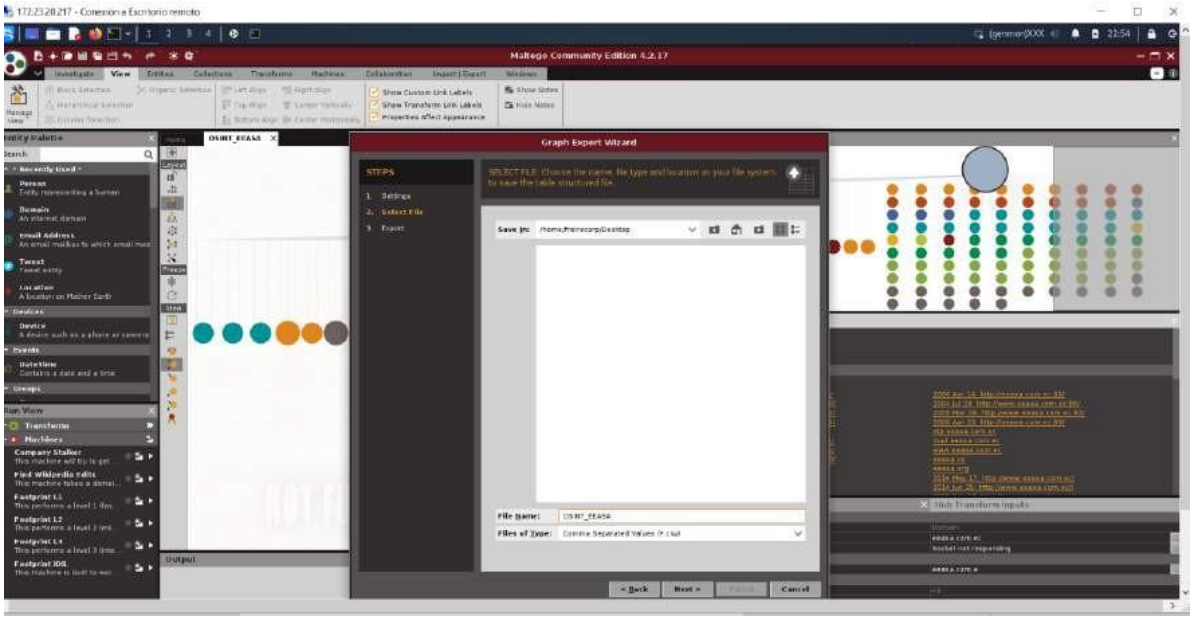
Fuente: elaboración propia

Ilustración 30. Descubrimiento del dominio EEASA – Maltego



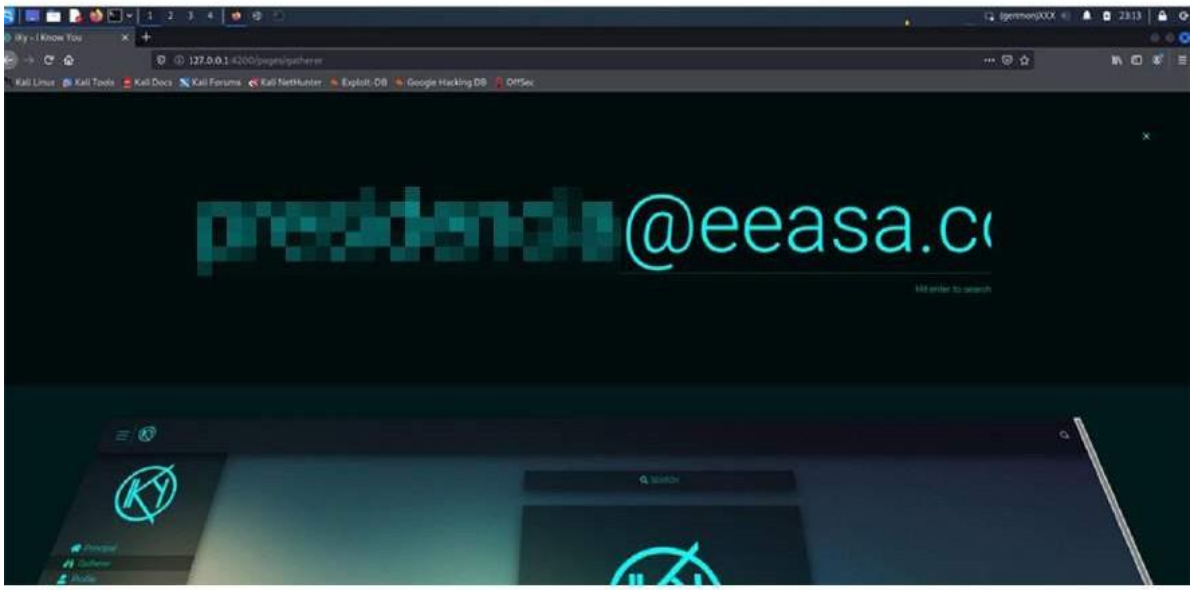
Fuente: elaboración propia

Ilustración 31. Descubrimiento del dominio EEASA formato xlsx – Maltego



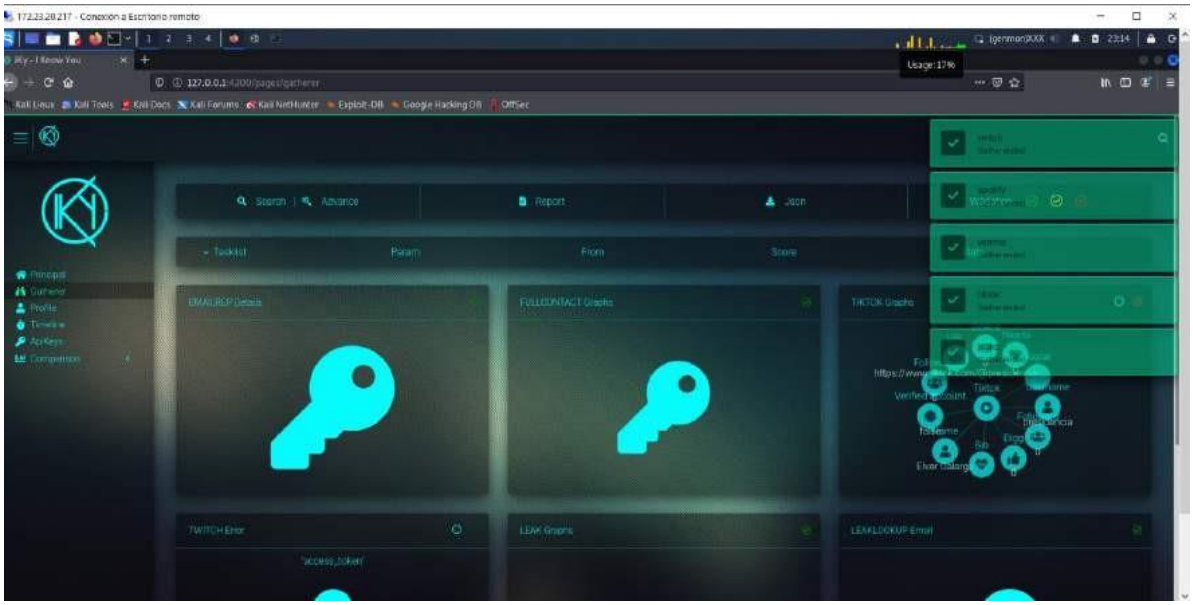
Fuente: elaboración propia

Ilustración 32. Búsqueda de información de correo 1– IKY



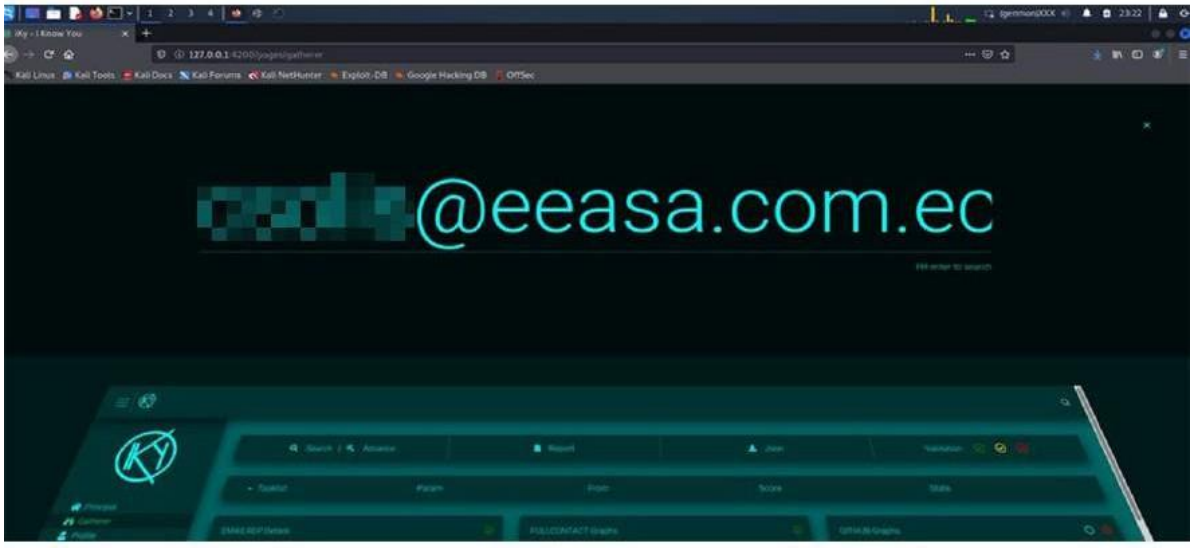
Fuente: elaboración propia

Ilustración 33. Descubrimiento de registros con el correo - IKY



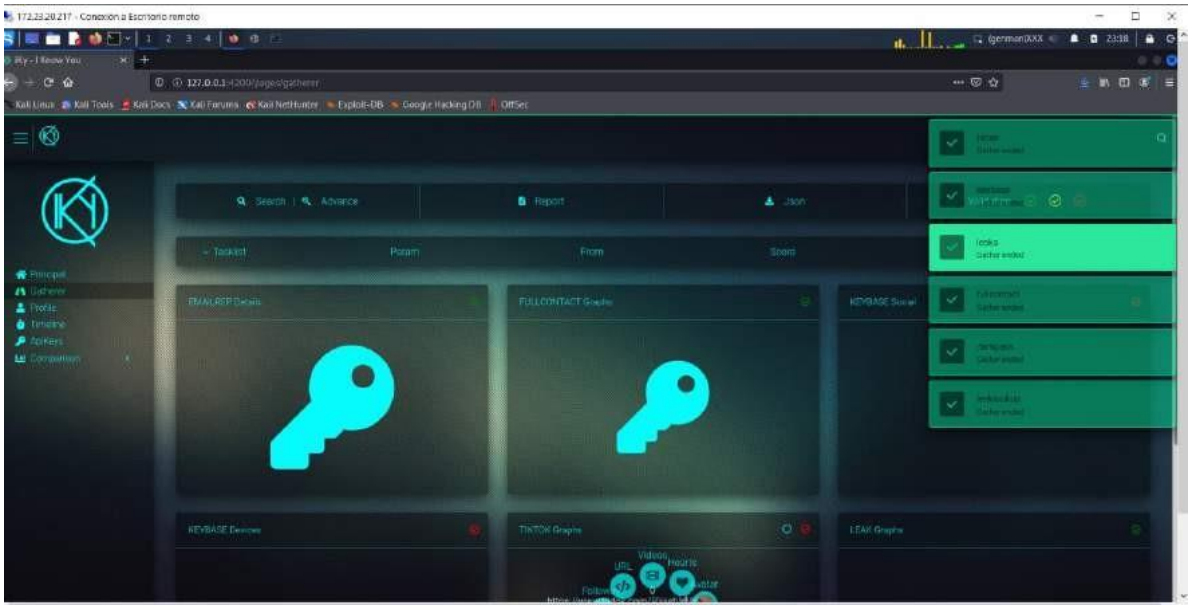
Fuente: elaboración propia

Ilustración 34. Búsqueda de información de correo 2– IKY



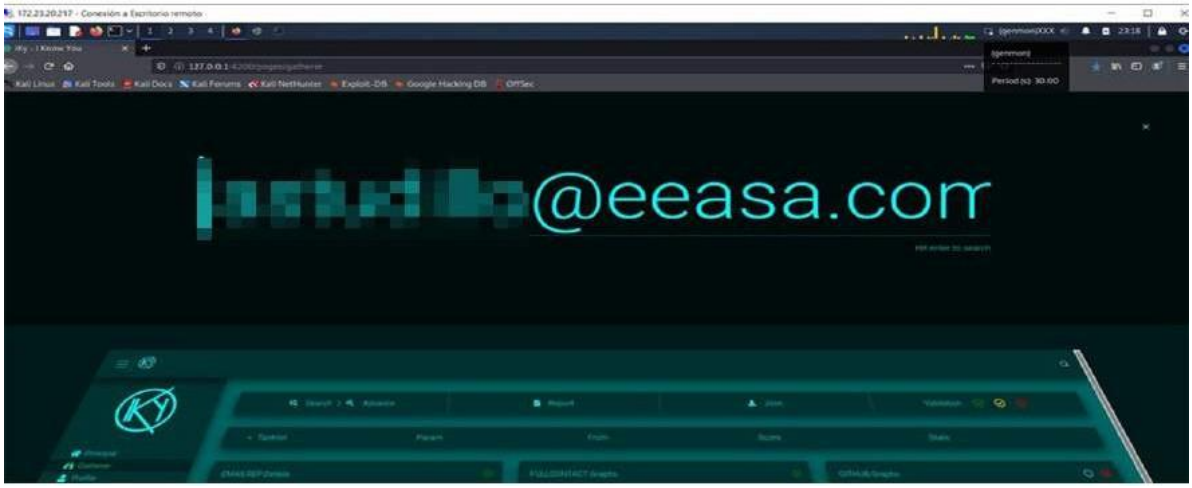
Fuente: elaboración propia

Ilustración 35. Descubrimiento de correos detectados parte 2 – IKY



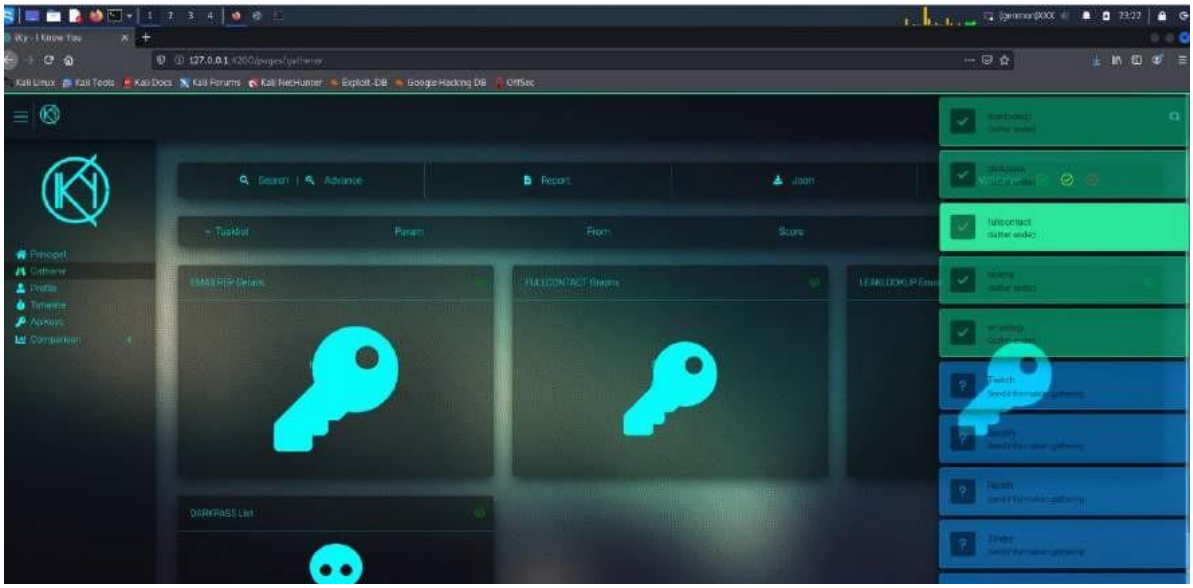
Fuente: elaboración propia

Ilustración 36. Búsqueda de información de correo 3- IKY



Fuente: elaboración propia

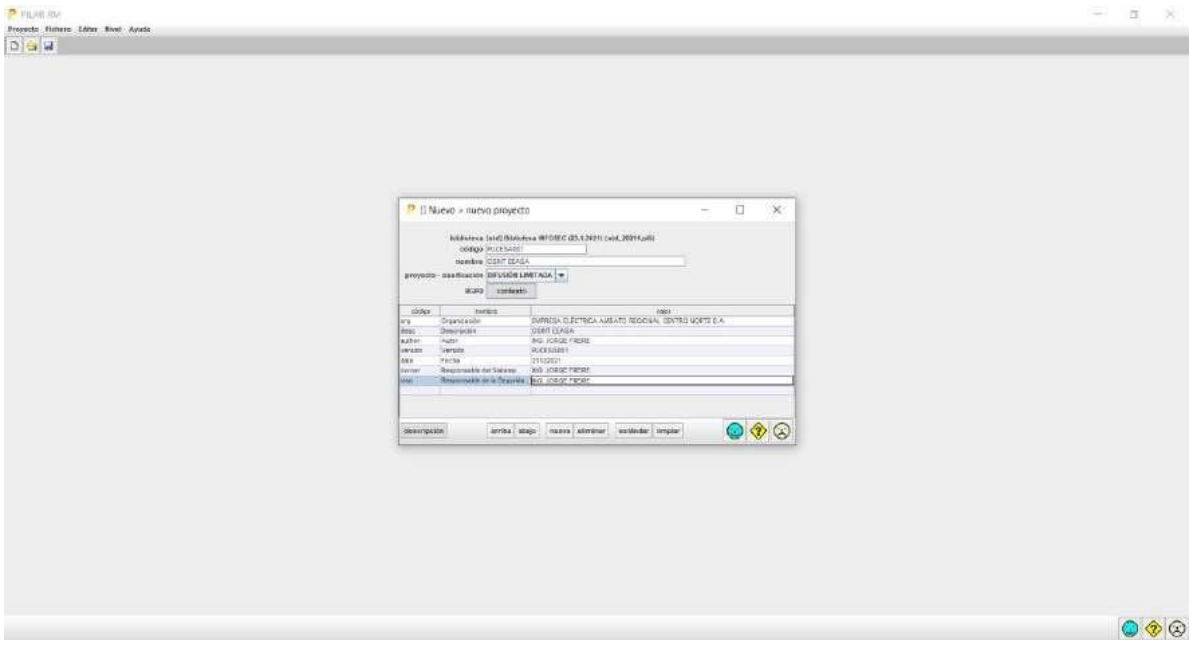
Ilustración 37. Descubrimiento de correos detectados parte 3 – IKY



Fuente: elaboración propia

Anexo 3 Creación del Proyecto en PILAR

Ilustración 38. Creación de proyecto en PILAR



Fuente: elaboración propia