ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

DIRECCIÓN DE POSGRADO Y EDUCACIÓN CONTINUA

INFORME DE TRABAJO DE TITULACIÓN

PREVIA LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES Y SISTEMAS DISTRIBUIDOS

MODALIDAD:

PROYECTO DE INVESTIGACIÓN Y DESARROLLO

TEMA:

ANÁLISIS DE VULNERABILIDAD UTILIZANDO HERRAMIENTAS DE INTELIGENCIA DE CÓDIGO ABIERTO (OSINT). CASO DE ESTUDIO SISTEMAS DE INFORMACIÓN ESPAM MFL

AUTORES:

KEVIN DANIEL CUSME ZAMBRANO

LEYDI TALIA ZAMBRANO MENDOZA

TUTORA:

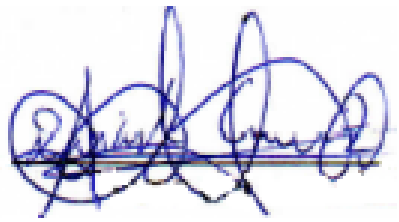
ING. JESSICA JOHANA MORALES CARRILLO, MGS.

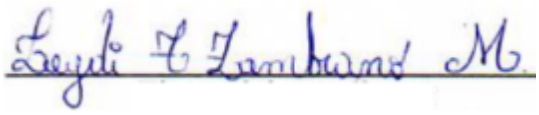
CALCETA, FEBRERO DE 2022

DERECHOS DE AUTORÍA

Kevin Daniel Cusme Zambrano y Leydi Talia Zambrano Mendoza, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, que se han respetado los derechos de autor de terceros, por lo que asumimos la responsabilidad sobre el contenido del mismo, así como ante la reclamación de terceros, conforme a los artículos 4, 5 y 6 de la Ley de Propiedad Intelectual.

A través de la presente declaración cedemos los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido en el artículo 46 de la Ley de Propiedad Intelectual y su Reglamento.





ING. KEVIN D. CUSME ZAMBRANO **ING. LEYDI T. ZAMBRANO MENDOZA**

CERTIFICACIÓN DE TUTORA

M.Sc. JESSICA JOHANA MORALES CARRILLO, certifica haber tutelado el trabajo de titulación **ANÁLISIS DE VULNERABILIDAD UTILIZANDO HERRAMIENTAS DE INTELIGENCIA DE CÓDIGO ABIERTO (OSINT). CASO DE ESTUDIO SISTEMAS DE INFORMACIÓN ESPAM MFL**, que ha sido desarrollado por **KEVIN DANIEL CUSME ZAMBRANO Y LEYDI TALIA ZAMBRANO MENDOZA**, previo a la obtención del título de Magister en Tecnologías de la Información mención Redes y Sistemas Distribuidos, de acuerdo al Reglamento de la unidad de Titulación de Posgrado de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

Firmado electrónicamente por:
JESSICA JOHANNA
MORALES CARRILLO

ING. JESSICA JOHANA MORALES CARRILLO, MGS.

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaramos que hemos **APROBADO** el trabajo de titulación **ANÁLISIS DE VULNERABILIDAD UTILIZANDO HERRAMIENTAS DE INTELIGENCIA DE CÓDIGO ABIERTO (OSINT). CASO DE ESTUDIO SISTEMAS DE INFORMACIÓN ESPAM MFL**, que ha sido propuesto, desarrollado y sustentado por **KEVIN DANIEL CUSME ZAMBRANO y LEYDI TALIA ZAMBRANO MENDOZA**, previa la obtención del título de Magister en Tecnologías de la Información mención Redes y Sistemas Distribuidos, de acuerdo al Reglamento de la unidad de titulación de los programas de Posgrado de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

GUSTAVO GABRIEL MOLINA GARZON

CN=GUSTAVO GABRIEL MOLINA GARZON, SERIALNUMBER=270421194455, OU=ENTIDAD DE CERTIFICACION DE INFORMACION, O=SECURITY DATA S.A. 2, C=EC

ING. GUSTAVO G. MOLINA GARZÓN, MGS.
MIEMBRO

Firmado electrónicamente por:
RAMON AGUSTIN VARELA MUNOZ

ING. RAMÓN A. VARELA MUÑOZ, MGS.
MIEMBRO

Firmado electrónicamente por:
RAMON JOFFRE MOREIRA PICO

ING. JOFFRE RAMÓN MOREIRA PICO, MGS.
PRESIDENTE

AGRADECIMIENTO

A Dios por la salud de la que gozamos, por guiarnos por el buen camino, por iluminar nuestros días y llenar nuestra mente de sabiduría para alcanzar nuestro objetivo.

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, quien nos abrió las puertas de sus aulas para forjar nuestros conocimientos profesionales y concebir nuestros ideales a través de una educación de calidad.

A los docentes encargados de nuestra formación, por capacitarnos y enriquecernos de grandes enseñanzas y experiencias que estamos seguros nos servirán en el ámbito laboral, de manera especial a nuestra tutora Ing. Jessica Morales Carrillo quien con sus conocimientos y paciencia guio nuestras ideas de la mejor manera no solo para concluir exitosamente con el desarrollo del trabajo de titulación, sino también en nuestra formación como investigadores.

Y, por supuesto, el agradecimiento más profundo y sentido va para nuestros padres y familia por su continua dedicación en nuestra formación, con todo el esfuerzo que esto conlleva y su apoyo incondicional en todas las acciones que hemos emprendido a lo largo de nuestra vida. El mérito también es gran parte de ellos.

LOS AUTORES

DEDICATORIA

A dios por la bendición de la vida, del estar día a día, por la fortaleza de nunca decaer y de saber que nunca me puedo rendir, de siempre ir por más cosechar más éxitos en este caminar.

A mi madre, una guerrera incansable que con su ayuda y por siempre estar conmigo me ha brindado la fortaleza y la decisión de seguir adelante, para poderle devolver todo lo que ella hace por mí.

A mi papá y a mi hermano por brindarme su apoyo incondicional en los tiempos más difíciles, por darme aliento de no decaer y dar lo mejor de mí.

A mi abuela Juana que siempre con sus consejos y sus deseos de verme superar siente el orgullo de tenerme como su nieto, de contagiarme de felicidad con su sonrisa, sus consejos y enseñanzas.

A mi compañera de vida, quien me ha acompañado en este caminar, alguien que no ha desmayado, ni me ha dejado decaer y que juntos hemos alcanzado esta meta propuesta.

KEVIN D. CUSME ZAMBRANO

DEDICATORIA

A Dios por estar presente en mi vida, por guiarme y darme la fortaleza necesaria para siempre avanzar y nunca desmayar; su amor y fidelidad me acompañan día a día.

A mis padres por su amor, apoyo y dedicación, gracias por inculcar en mí el ejemplo de esfuerzo y valentía. A mi hermano por ser parte de mi motivación en este proceso y por aquellos momentos de risas que me llenan el alma.

A mi madre de corazón, Annabel Zambrano por compartir momentos significativos conmigo y estar siempre a mi lado. Gracias por inculcarme valores, principios y por impulsarme cada día a ser mejor humana y profesional.

A mis abuelitos por sus incansables oraciones, por sus consejos, por su ejemplo y palabras de aliento que me inspiran a seguir con más fuerza y dedicación. Gracias por ser luz en mi vida y por regalarme su amor y comprensión.

A mi enamorado, mi compañero de tesis y cómplice de este sueño que juntos hemos logrado, gracias por la paciencia y dedicación conmigo.

LEYDI T. ZAMBRANO MENDOZA

CONTENIDO GENERAL

CONTENIDOS DE TABLAS, ILUSTRACIONES, FIGURAS Y ANEXOS

CONTENIDO DE TABLAS

CONTENIDO DE ILUSTRACIONES.

CONTENIDO DE FIGURAS

CONTENIDO DE ANEXOS

RESUMEN

El presente trabajo de titulación tuvo como principal objetivo ejecutar un análisis de vulnerabilidades orientado hacia los sistemas de información de la ESPAM MFL apoyado con herramientas de inteligencia de código abierto. Para su ejecución se cumplieron cuatro objetivos específicos; en el primer objetivo mediante la técnica de revisión bibliográfica se realizó una búsqueda exhaustiva de las herramientas OSINT y su aplicación en el área de Ciberseguridad a través de metabuscadores; en el segundo objetivo se aplicó una entrevista virtual a los miembros de la Unidad de Tecnología, con el fin de conocer el estado en que se encontraban los sistemas de información y las metodologías implementadas para mitigar posibles vulnerabilidades, posteriormente se definieron las herramientas OSINT a emplear, las cuales fueron Hunter, Spyse, Shodan, Siteliner, Crt.Sh, Website Informer, Zoom Eyes, Whois y Domain Dossier; en el tercer objetivo se ejecutó el escaneo de vulnerabilidades en los sistemas de información, mostrando reportes de riesgos en los activos de la institución; y en el último objetivo como medida de solución se presentó un propuesta de políticas de seguridad que permitirá a los interesados tomar acciones para salvaguardar la integridad de su información. Cabe mencionar también que la investigación estuvo basada en la metodología por objetivos (APO), la cual tiene como finalidad determinar objetivos conjuntos y proporcionar retroalimentación sobre los resultados. factor

PALABRAS CLAVE

OSINT, Ciberseguridad, Internet, Sistemas de Información

ABSTRACT

The objective of this investigation was to perform a vulnerability analysis oriented towards the information systems at ESPAM MFL, supported by open-source intelligence tools. For its execution, four specific objectives were met; in the first objective, through the bibliographic review technique, an exhaustive search of the OSINT tools and their application in the area of Cybersecurity was carried out through metasearch engines; in the second objective, a virtual interview was applied to the members of the Technology Unit, in order to know the state of the information systems and the methodologies implemented to mitigate possible vulnerabilities, later the OSINT tools to be used were defined, which were Hunter, Spyse, Shodan, Siteliner, Crt.sh, Website informer, Zoom Eyes, WhoIs and Domain dossier; in the third objective, the scanning of vulnerabilities in the information systems was carried out, showing risk reports in the assets of the institution; and in the last objective, as a solution measure, a proposal for security policies was presented, which will allow the interested parties to take actions to safeguard the integrity of their information. It is also worth mentioning that the research was based on the methodology by objectives (APO), which aims to determine joint objectives and provide feedback on the results.

KEYWORS

OSINT, Cybersecurity, Internet, information systems.

CAPÍTULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

En los últimos años la interconexión de sistemas computacionales ha crecido de forma vertiginosa, abriendo un espacio en la red de Internet para que millones de personas en todo el mundo se comuniquen e intercambien datos a través de lo que ahora se conoce como la era digital (Millán, 2019). De tal manera el mundo actual se encuentra en medio de una explosión de la información, donde la mayor parte de la inteligencia predictiva se puede obtener de fuentes públicas, volviendo vulnerable la información que se encuentra situada en internet.

Pintado y Hurtado (2015), manifiestan que la seguridad de la información es un punto clave de estudio y análisis tanto en instituciones públicas y privadas, debido a la cantidad de información importante que manejan en sus bases de datos, conllevando a crear mecanismos de seguridad que permitan salvaguardar la integridad de los datos, los cuales juegan un papel importante en el desarrollo de un proceso conocido en el mundo de la seguridad de la información como inteligencia en fuentes abiertas u OSINT (Cuesta, 2019).

Diversos casos reportados en los últimos años muestran la magnitud global que este tema ha tomado en la sociedad debido a la proliferación del uso del internet y redes sociales. Un caso clave fue en el año 2016 cuando, en nombre de Anonymous, los ciberactivistas revelaron información de gran importancia de Donald Trump, quedando al descubierto el supuesto número de teléfono, su número de la seguridad social, así como las direcciones personales y otros datos íntimos de sus más allegados, además los datos revelados incluyen otras cuestiones referidas a la infraestructura web de Donald Trump y animaba a más hackers a tomar medidas contra él gracias a esta información (Becares, 2021).

Según Raudales (2018), los ataques cibernéticos no sólo ocurren en países avanzados o con tecnologías de primer nivel. Latinoamérica, también ha sido víctimas en muchas ocasiones de delitos cibernéticos, entre los que se mencionan a Colombia, donde se han reportado constantes ataques a la página de la

Presidencia de la República y Ministerio de Defensa Nacional dejando inactivos durante varias horas a dichos portales. En el 2009, se originaron desfalcos a cuentas bancarias por un monto superior a los 50 millones de dólares, mientras que en el 2012 se pudo capturar a Jorge Maximiliano Pachón, un delincuente cibernético, que tenía en su poder más de 8000 tarjetas de crédito clonadas y más de 92 millones de dólares divididos entre 5 países de América Latina en los que operaba (Izaguirre & León, 2018).

Uno de los más recientes casos de delitos cibernéticos que ha afectado a todo América Latina es la famosa aplicación Pokemon GO, donde miles de usuarios se unieron al desafío del juego, sin tener en cuenta si descargaban la aplicación oficial u otras versiones que no contaban con la seguridad adecuada, llevando a generar un alto índice de ataques a la información de las cuentas registradas. Sin embargo, este no fue el único delito que los delincuentes aprovecharon con el juego. Pokemon GO permitía interactuar entre el mundo real y el mundo virtual en lo que se conoce como realidad aumentada, por lo que debía jugarse con el móvil al aire libre, lo que ocasionó que se generaran falsos reportes de puntos o Pokémon en zonas poco transitadas donde delincuentes robaban teléfonos a los usuarios (Guzmán, 2017).

En Ecuador, como un acto de repudio en contra de la censura a la libertad de expresión, Anonymous escogió el 10 de agosto del 2011 para atacar la web de la Presidencia impidiendo a los usuarios ingresar a la página electrónica (El Comercio, 2012). Un año después, en agosto de 2012, la asociación de hackers realizó ataques a las páginas de organismos públicos de Ecuador, entre ellos, los municipios de Manabí y Esmeraldas en rechazo a un artículo mediante el cual se podría solicitar a los proveedores de servicio de Internet las direcciones IP de los usuarios. La Presidencia, el Ministerio de Telecomunicaciones y la Asamblea Nacional también sufrieron la suspensión temporal de sus páginas, al igual que empresas particulares como Hunter y Quiport (El Comercio, 2014).

La compañía de seguridad informática vPnMentor en 2019, aseguró en un informe que una empresa hizo la utilización de un servidor dedicado al análisis de datos

donde este contenía millones de logs de información personal de personas ecuatorianas, los cuales, no se regían bajo ningún protocolo de protección de la información necesarios. Gracias a esta mala práctica de protección de la información casi cualquier persona podía acceder a ellos. Portales como los del Servicio de Rentas Internas (SRI), Ministerio de Relaciones Exteriores, Consejo Nacional Electoral (CNE), Gobiernos Autónomos Descentralizados, Ministerio de Turismo, entre otros, resultaron afectados, advirtiendo que el principal ataque cibernético consiste en lo que se conoce como “denegación de servicio”. El viceministro de telecomunicaciones que estaba al cargo en ese entonces afirmó que en Ecuador se suscitaron más de 40 millones de ataques cibernéticos desde Francia, Austria, Holanda, Alemania, Reino Unido, Estados Unidos, Brasil y Ecuador. Ecuador pasó del puesto 51 al 31 a escala mundial en el volumen de ataques cibernéticos, según las autoridades del Mintel (El Telégrafo, 2019).

Como caso de estudio sobre detección de vulnerabilidades aplicado en la ESPAM MFL, se encuentra “Ciberseguridad y su Aplicación en las Instituciones de Educación Superior Públicas de Manabí” efectuado en el 2019 donde se obtuvo como resultado que la ESPAM MFL tiene el mayor riesgo en seguridad de la información con respecto a las otras IES alcanzando el 50% del nivel crítico y un promedio de vulnerabilidades encontradas de 29% en los diferentes dominios de seguridad (Avellán & Zambrano, 2019).

Por las circunstancias presentadas los autores del presente trabajo de titulación se plantean la siguiente interrogante:

¿Cómo determinar vulnerabilidades en los sistemas de información de la ESPAM MFL, mediante herramientas de inteligencia de código abierto (OSINT)?

1.2. JUSTIFICACIÓN

Los grandes avances generados en el mundo entero, debido al constante desarrollo tecnológico, los problemas de seguridad ligados a la gran accesibilidad de información, el aumento de vulnerabilidades y el amplio campo de las amenazas imponen nuevos retos y técnicas en la práctica de análisis de vulnerabilidades en empresas y organizaciones, en particular en las instituciones de educación superior por ser entidades que guardan gran cantidad de información sensible y confiable de los procesos académicos, personal docente, administrativos y estudiantes.

Los ataques informáticos surgen cada vez más sofisticados y con más impulso para lograr su objetivo y junto a ello crece la importancia de implementar medidas de prevención y respuesta a amenazas de terceros frente a los diferentes sistemas de información, donde es fundamental tener en cuenta el análisis de vulnerabilidades y herramientas, que permitan reducir significativamente el riesgo existente en este tipo de entorno, contribuyendo a que la información se encuentre segura e integra (Arévalo et al., 2020).

Desde una perspectiva social, se puede identificar que se vive en una época donde no hay esfera de la sociedad en la que no se empleen en mayor o menor grado las tecnologías de la informática y las comunicaciones; al escuchar que la información es poder, lo que se pretende decir es que el hecho de conocer determinada información facilita que se puedan tomar decisiones que conllevan un beneficio para el poseedor de dicha información.

Mientras que la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), en el artículo 1 indica que “el acceso a la información pública es un derecho de las personas. Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado, en cualquiera de sus modalidades, conforme lo dispone están sometidas al principio de publicidad” (LOTAIP, 2004). De acuerdo con el artículo de esta ley citada, se puede observar que existe información denominada de carácter pública a la cual se puede acceder, pero a su vez existe información que es confidencial

como los datos de carácter personales, que no deben ser visible y que podrían ser una vulnerabilidad al ser expuestos en dominios no gubernamentales. Por esta razón se ve la necesidad de elaborar un análisis de vulnerabilidades apoyados con herramientas OSINT, y los ataques relacionados, para proponer políticas de distribución y difusión de la información.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Realizar un análisis de vulnerabilidades en los sistemas de información de la ESPAM MFL utilizando herramientas de inteligencia de código abierto (OSINT), para proponer políticas en la distribución y difusión de la información.

1.3.2. OBJETIVOS ESPECÍFICOS

- Obtener información sobre los sistemas de información a partir de metabuscadores.
- Definir las herramientas de OSINT a emplear en las pruebas dentro de los sistemas de información.
- Ejecutar un experimento con herramientas y/o técnicas de OSINT, aplicado a la vulnerabilidad de los sistemas de información.
- Presentar la propuesta de políticas en la distribución y difusión de la información en los dominios no gubernamentales del Ecuador, a la Unidad de Tecnología de la ESPAM MFL, de acuerdo con los resultados obtenidos en el experimento.

1.4. HIPÓTESIS, PREMISAS Y/O IDEAS A DEFENDER

Mediante un análisis de vulnerabilidades apoyado con herramientas de inteligencia de código abierto (OSINT), se pueden proponer políticas de distribución y difusión de la información en la ESPAM MFL.

CAPÍTULO II. REVISIÓN BIBLIOGRÁFICA

2.1. CONTRAMEDIDAS Y PLANES DE ACCIÓN PARA FORTALECER LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.

Partiendo de la interpretación de la información sobre los diversos artículos científicos y ahondando en temas referentes al tema de estudio se pone como punto de partida saber sobre las contramedidas y los planes de acción que son técnicas o herramientas que permiten fortalecer sistemas de seguridad de la información. Son maneras de contrarrestar los ciberataques sabiendo a que se va a enfrentar y teniendo las armas para emplear una eficiente respuesta. Las contramedidas son pruebas de seguridad para los sistemas de información que servirán para la protección de sus datos (Industrial, 2016). Los planes de acción son una estrategia de evaluación, sirven para poder ver cómo está nuestra infraestructura y como están esquematizados los sistemas de información para evitar los posibles ataques.

2.2. PREVENCIÓN DE FUGA DE INFORMACIÓN Y CONTROL DE ACCESO.

La prevención, parte desde saber la sensibilidad que tiene los datos, la accesibilidad a ellos y la fuga de datos, con el tiempo el índice de pérdida de información ha incrementado por ataques informáticos, los cuales, hacen vulnerables los sistemas de información que tienen como origen defectos de diseño e implementación de las aplicaciones, malos usos de los protocolos de una buena programación, escasa medidas de control sobre los accesos en su implementación o la nula validación y perfección de las entradas de datos; “la prevención de fuga de información (Data Loss Prevention – DLP), hace referencia a las actividades y mecanismos empleados para prevenir el uso no autorizado de información sensible de una organización” (Dávila & Pacheco, 2017).

Según Torres (2015), define a “la prevención de fuga de información - Data Loss Prevention (DLP) como un término de seguridad informática que comprende un

conjunto de herramientas destinadas a evitar el envío de información sensible, confidencial o crítica, fuera del entorno de la organización", se debe considerar que para los DLP es fundamental la clasificación acertada de la información, siendo la construcción de patrones para la detección la principal función para el análisis de sus contenidos. Para garantizar el cumplimiento de las necesidades de las organizaciones en el control de acceso, se deben definir claramente los roles y responsabilidades para los usuarios ya que son quienes cuentan con la autorización de manipular la información sensible para las organizaciones y/o instituciones.

2.3. DETECCIÓN, AMENAZAS Y RIESGOS.

Para Industrial (2016), "Las amenazas informáticas están relacionadas con la posibilidad de que algún tipo de evento se pueda presentar en cualquier instante de tiempo, en el cual existe un daño material o inmaterial sobre los activos informáticos y los sistemas de información". La ciberseguridad es un punto crítico para la prosperidad y seguridad. Las actividades cibernéticas maliciosas no tan sólo amenazan la economía mundial, sino, también el funcionamiento mismo de nuestros sistemas de información (Schwartz, 2020). La seguridad del futuro depende de que se pueda transformar la capacidad para protegernos contra las amenazas cibernéticas que dependen de sistemas digitales seguros (Balcázar, 2020).

El crecimiento de los niveles de penetración de los sistemas digitales en el mundo y en la región, surgen de las cambiantes transformaciones de los procesos sobre la información que las potencias mundiales están implementando; los cuales, en conjunto con la directa dependencia que brindan las tecnologías en general, son elementos primordiales y que han incidido directamente con las detecciones, amenazas y riesgos sobre el sistema de gestión de la seguridad de la información que el mundo y los países de la región enfrentan: "Los riesgos informáticos son problemas potenciales, que pueden afectar a los sistemas de información o a los equipos de cómputo" (Balcázar, 2020).

2.4. RESPUESTA – EVIDENCIAS DIGITALES Y SISTEMAS DE RECUPERACIÓN.

Partiendo desde un esquema estructurado de adquisición de información, las evidencias digitales sirven como sustento informático para aumentar la eficiencia los procesos de los procesos descritos (Fennema *et al.,* 2017). Dada su naturaleza las evidencias digitales, acarrean una fácil modificación y pueden llegar a ser muy volátiles, el recabar evidencias digitales es un proceso deben contar con protocolos que aseguren y mantengan la veracidad, fiabilidad e integridad de la información y los datos. La presentación de las evidencias digitales se puede dar en forma sistemáticamente programada que permite ver los cambios que se le hace a la información que se encuentran contenida dentro de un sistema de información y la segunda es generada por una persona y parte del almacenamiento en dispositivos digitales, para esto es importante que se planteen estandarizar mecanismos que abarquen la adquisición y procesamiento de evidencias digitales de una manera correcta (Prieto, 2018).

El proceso de adquisición de evidencias digitales también debe estar apoyado en métodos científicos que sustente su ejecución o apoyen a su desarrollo en todas las etapas, contar con una buena sostenibilidad en los procedimientos con claridad permitirá que la calidad de las evidencias digitales sea mejor. “Por evidencia digital entendemos cualquier documento, fichero, registro o dato contenido en un soporte informático, susceptible de tratamiento digital y que puede ser utilizado como prueba en un proceso legal” (Industrial, 2016).

De acuerdo con Industrial (2016), y utilizando la revisión bibliográfica de artículos referentes a los sistemas de recuperación se pueden definir “a los sistemas de recuperación como una función que permite al usuario devolver el estado de su equipo y las aplicaciones al punto de partida anterior a que se haya producido un problema y así solucionarlo”. Además, los sistemas de recuperación no requieren estar en un entorno de lenguaje controlado, permiten resolver contradicciones de tal manera como la indización automática, son reforzados por rangos o booleanos que son sistemas de recuperación suficientemente eficaces. Evaluar el

aprovechamiento que los usuarios hacen de estos sistemas de recuperación, se convierte en una obligación detectar sus defectos y mejorarlos para aquellos archivos que pretendan ofrecer un buen servicio.

2.5. IMPACTO DE VULNERABILIDADES INFORMÁTICAS EN LATINOAMÉRICA.

Hoy en día, las continuas intrusiones en redes de datos y aplicaciones informáticas por parte de ciberdelincuentes a nivel mundial han llevado al sector académico y empresarial a la búsqueda de nuevas soluciones que permitan detener o disminuir estos hechos (Dadkhah *et al.,* 2018). Sin embargo, “la presencia de vulnerabilidades en sistemas informáticos aumenta continuamente, no solo en número sino también en el impacto de su explotación individual" (Huang *et al.*, 2017). En otras palabras, es un evento que se encuentra en constante evolución, donde se muestran diversas formas de ataques, que violan la confidencialidad e integridad de la información registrada en las diferentes bases de datos y sistemas de empresas, gobiernos e instituciones.

La compañía ESET (2018), “mediante un estudio a 2.500 empresas y más de 4.500 participantes en Latinoamérica, dio a conocer que Venezuela y Ecuador”, estaban dentro de los países con más afectaciones a mano de los malwares, específicamente por un malware que su principal función era el secuestro de información malware conocido como ransomware. Por otro lado, la misma compañía en su informe ESET Security Report, afirma que los códigos maliciosos son la principal preocupación (64%) en el segundo y tercer puesto en el orden de las preocupaciones en el robo de la información (60%) y el mal uso de los controles de acceso a los sistemas (56%). En este sentido y de acuerdo con la telemetría de ESET, las empresas en Brasil (19%) fueron las más afectadas por el malware según el total de las detecciones en Latinoamérica durante 2020, seguidas por las de México (17,5%) y Argentina (13,3%) (ESET, 2021).

Según Schwartz (2020), en un estudio realizado por el Banco Interamericano de desarrollo y la Organización de los Estados Americanos, indica la importancia de

implementar políticas y medidas de ciberseguridad que brinden a los ciudadanos un espacio digital abierto y seguro para todos. Por ejemplo, en el artículo publicado por Hernandez *et al.,* (2018), se analiza una serie de tecnologías OSINT para las actividades de ciberinteligencia de la nación, adaptando varias transformaciones al contexto colombiano.

2.6. ESTUDIOS BASADOS EN ATAQUES INFORMÁTICOS EN ECUADOR.

Según Zuña *et al.,* (2019), en su estudio menciona que “los ataques cibernéticos como phishing o malware son el pan de cada día para los hackers, aprovechándose de la mínima vulnerabilidad, no solo en el Ecuador sino en países con grandes sistemas empresariales”. Tal es el caso del malware y phishing, que han utilizado el tema del COVID-19 para sus campañas, así como las noticias falsas que circulan por las diferentes plataformas y las estafas que a diario se distribuyen mediante correo electrónico, redes sociales o aplicaciones de mensajería.

De acuerdo con Tates y Recalde (2019), en su investigación señalan que el CERT (Equipos de Respuesta ante Emergencias Informáticas) de Ecuador (EcuCERT), inició sus actividades en noviembre de 2013, cuyo alcance se enmarca en el ámbito de la aplicación de la Ley Orgánica de Telecomunicaciones (LOT), muestra objetiva de ello es que, para mediados del 2020, CERT habría trabajado sobre doscientos sesenta y dos incidentes vulnerables reportados sobre los activos críticos del país, apoyando de esta forma a las organizaciones afectadas.

De acuerdo con el artículo “Análisis de ataques cibernéticos hacia el ecuador ” en el 2017, “Ecuador quedó en tercer lugar de afectación en América Latina por el virus Wannacry”, y en 2019 quedó al descubierto la información de los más de 17 millones de ecuatorianos hecho realizado por hackers, por el caso del asilo político al representante de wikileaks, Julián Assange ocurrido el 11 de abril del 2019, lo cual provocó que se desarrollaran ciberataques, 40 millones exactamente ataques dirigidos directamente a sitios web gubernamentales como el “Banco Central, la Presidencia, la Cancillería, el Consejo de la Judicatura, el Ministerio del Interior, el

SRI, la Corte Constitucional del Ecuador", GAD cantonales y provinciales, etc. Siendo la más grande filtración de seguridad en América Latina (Alvarado, 2020).

En consecuencia, tras la revisión bibliográfica realizada en diferentes fuentes de datos, los autores destacan la importancia de tener en cuenta las posibles amenazas y vulnerabilidades en los sistemas de información tanto en las instituciones públicas o privadas de Ecuador, para garantizar la confidencialidad, integridad y disponibilidad permanentes a las diferentes infraestructuras tecnológicas. Dado que con el caso Julian Assange se demostró que el país no estaba preparado para mitigar las amenazas que se presentan, aunque sí existe una tenue legislación, las entidades no están debidamente coordinadas, hasta la fecha se desconocen los objetivos de control para las entidades comprometidas con ataques informáticos a nivel nacional, tampoco se han identificado cuáles son las entidades públicas gubernamentales que se encuentran en un nivel crítico y cómo podrían afrontar los riesgos y daños en caso de un ciberataque. De esta forma surge la necesidad de fomentar la implementación de políticas y estrategias de protección de la información.

2.7. COMPARATIVA ENTRE HERRAMIENTAS Y TÉCNICAS OSINT.

Un correcto uso de técnicas disponibles en la red para controlar la información proporcionada por los usuarios sería suficiente, sin embargo, el uso desmedido del internet en los últimos años ha provocado que estos métodos de seguridad no sean tan seguras y confiables. En este sentido, el potencial de OSINT propone utilizar tantas herramientas como sea posible para mejorar la protección de datos y privacidad de los internautas. No obstante, es necesario mencionar que el uso combinado de varias técnicas OSINT, no es recomendable debido a los extensos procesos de investigación (Pastorino, 2019).

Para ello, basados en estudios realizados por investigadores y desarrolladores, en la tabla 1 se enumeran las herramientas más precisas para aplicar técnicas de inteligencia en fuentes abiertas (OSINT), donde se presentan las características

principales, como el tipo de entradas y salidas, el tipo de interfaz de usuario y la plataforma de funcionamiento. Las cuales son las más usadas para recolectar información de calidad (Ángulo, 2020; Pastor et al., 2020).

Tabla 2.1. Tabla comparativa herramientas OSINT

Herramienta OSINT	Conjunto de datos de entrada	Interfaz	Plataforma	Resultado de salida
Maltego	Información personal, de empresa, dominio	Programa	Linux, Windows, MAC	Múltiple información
FOCA	Dominio, archivos	Programa	Linux, Windows	Metadatos
Recon-ng	Información personal, dominio	Línea de comandos	Linux	Múltiple información
Spiderfoot	Información personal, información de red, dominio	Interfaz Web	Linux, Window, Online	Múltiple información
The Harverster	Dominio	Línea de Comandos	Linux	Información de red. Contactos
Shodan	Ciudad, información de red	Interfaz Web	Online	Información de red
Osint Framework	Información personal, de empresa, de red, archivos	Interfaz Web	Online	Múltiple información

Fuente: Basado en (Pastor *et al*., 2020)

De acuerdo con lo expuesto, es importante mencionar que las herramientas utilizadas en OSINT van de acuerdo con la necesidad de cada usuario, dado que cada una se acopla a una tarea específica. Es decir, si lo que se desea es extraer información oculta de archivos, FOCA es la indicada para llevar a cabo el proceso, mientras que, si el objetivo es información de red, las opciones son shodan, Spiderfoot y The Harvester, las cuales incluyen información específica sobre servicios inteligentes. Finalmente, si el propósito de la búsqueda es recopilar la mayor cantidad de información posible, los recursos Recong-NG Y Maltego son los más apropiados y útiles.

2.8. LA EVOLUCIÓN DE LA INTELIGENCIA DE FUENTES ABIERTAS EN LA ACTUALIDAD.

En el mundo actual, internet ha revolucionado muchos ámbitos de manera radical, donde los sistemas de información, los datos contenidos en ellas y la información expuesta en las diferentes plataformas son los activos más importantes para las

organizaciones empresariales, gobiernos e instituciones, convirtiendo a Open Source Intelligence (OSINT) en la próxima mina de oro de Internet. De hecho, los recientes avances en tecnología están haciendo que OSINT evolucione a un ritmo vertiginoso, proporcionando aplicaciones innovadoras impulsadas por datos y basadas en inteligencia artificial que permitan ofrecer a la sociedad nuevas líneas de acción contra las ciberamenazas y el ciberdelito (Millán, 2019).

La revisión realizada sobre OSINT, muestra los grandes desafíos que están abiertos hoy en día, donde prevalecer la integridad de los datos es el principal reto. Aunque las técnicas OSINT ya son un gran paso para esta problemática, la mayoría de ellas todavía dependen en gran medida del usuario final por lo que se considera relevante incorporar técnicas más sofisticadas que permitan mejorar la exploración de OSINT en grandes volúmenes de datos abiertos. Así mismo Pastor *et al.*, (2020), señala que el OSINT del futuro debería poder proporcionar al internauta la información específica que está buscando, así como devolver respuestas convincentes en las investigaciones.

2.9. INTEGRACIÓN DE OSINT EN INVESTIGACIONES DE CIBERATAQUES.

En la actualidad, las empresas y organizaciones están más expuestas y junto con ellas lo está la información que estas manejan, para ello deben de implementar obligatoriamente mecanismos de detección y respuesta contra ciberataques. Ya que no tan solo, deben de estar regidos por soluciones técnicas como firewalls, sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS) o antivirus, etc, soluciones que se despliegan sirven solamente para evitar amenazas conocidas. OSINT en la ciberseguridad se centra en proponer mejoras defensivas ante amenazas. Por el contrario, muy pocas veces buscan la identificación de los ciberatacantes. “OSINT es una fuente de conocimiento que podría apoyar la investigación de un ciberataque”, yendo desde los detalles más pequeños de la acción maliciosa hasta la raíz del problema, además, OSINT permitirá saber la motivación del atacante, evaluar sus procedimientos y perfilar al responsable (Pastor et al., 2020).

CAPÍTULO III. DESARROLLO METODOLÓGICO

La presente investigación se desarrolló como caso de estudio en la Escuela Superior Politécnica Agropecuaria de Manabí “Manuel Félix López”, con la finalidad de detectar y analizar vulnerabilidades a las que se encuentran expuestos los sistemas de información de la institución, utilizando herramientas de inteligencia de código abierto. De acuerdo con lo descrito, para su ejecución se empleó la metodología APO, tomando como referencia los objetivos planteados en la propuesta.

La metodología de administración por objetivos (APO) se define como una estrategia empresarial, mediante el cual los superiores de una organización trabajan mancomunadamente para definir objetivos de desempeño y establecer metas específicas, revisando periódicamente el avance haciendo los objetivos. Hoy en día funciona como un enfoque amigable, participativo y democrático, dando paso a nuevos esquemas de evaluación del desempeño humano (ASTURIAS, 2017).

3.1. DESARROLLO DE FASE 1: RECOPILACIÓN DE INFORMACIÓN SOBRE LOS SISTEMAS DE INFORMACIÓN A PARTIR DE METABUSCADORES.

Para el desarrollo de esta primera fase, se utilizó la técnica de revisión bibliográfica, la cual tuvo como objetivo la búsqueda de información, para obtener una mejor comprensión de la evolución de OSINT, sus herramientas, técnicas y su papel en la ciberseguridad. De acuerdo con Hart (1998), una revisión bibliográfica es “La selección de documentos disponibles sobre un tema específico, que contienen información, datos y evidencias sobre un punto de vista en particular para cumplir ciertos objetivos o expresar determinadas opiniones” en otras palabras es un análisis de documentos que se utiliza para recopilar información y hacer uso del pensamiento crítico de esos estudios de una manera ordenada, precisa y analítica.

Para el respectivo desarrollo del objetivo, se estableció un protocolo de búsqueda donde se especificaron palabras claves como Cyberseguridad, Cyberattack, OSINT y Open Source Intelligence, con lo cual se encontró publicaciones en bases de datos para investigaciones con OSINT en inglés, así como publicaciones que contengan el acrónimo.

A continuación, se definieron las bases de publicación más relevantes que abordaban OSINT de las cuales se seleccionó: Biblioteca digital ACM, IeeeXplore, Dialnet, Applied Sciences , ResearchGate , Google Scholar y Science Direct, donde se empleó como filtros de búsqueda publicaciones de artículos científicos, libros, ponencias de especialistas y tesis de maestría o doctorado en un periodo comprendido entre el 2017 y 2021, todo esto coadyuvó a recabar información relevante acerca del tema de estudio, brindando una revisión metódica y logrando realizar una análisis y procesamiento de información de manera clara y organizada.

3.2. DESARROLLO DE FASE 2: DEFINIR LAS HERRAMIENTAS DE OSINT A EMPLEAR EN LAS PRUEBAS DENTRO DE LOS SISTEMAS DE INFORMACIÓN.

Dentro de esta etapa se usó la técnica de la entrevista no estructurada; según Trindade (2017), menciona que “es aquella que se realiza sin un guion previo adquiriendo las características de conversación y permitiendo la espontaneidad”. Por tanto, la entrevista se construye simultáneamente a partir de las respuestas de la persona entrevistada, la cual estuvo dirigida a los miembros de la Unidad de Tecnología de la ESPAM MFL, los Lic. Geovanny García, Ing. Néstor Mora. Siguiendo la secuencia, se realizó una visita técnica (reunión de manera virtual por la situación COVID-19 actual) a la ESPAM MFL, con la finalidad de verificar el estado en que se encuentren los sistemas de información de la institución antes mencionada y definir las herramientas OSINT que se utilizaron.

Según Espinoza (2018), la observación es uno de los procedimientos que permiten la recolección de datos sobre un individuo, fenómeno o situación particular y contemplar sistemática y detenidamente cómo se desarrolla la vida de un objeto

social. Por ello, mediante esta técnica se pudo obtener información sobre las herramientas utilizadas en el análisis de vulnerabilidades y el nivel con las que son presentadas en los sistemas de información de la ESPAM MFL. Donde en conjunto con los datos obtenidos y la información recopilada de la revisión bibliográfica se definieron las herramientas a usarse en el experimento propuesto, dado la necesidad del objeto de estudio y las herramientas más precisas para aplicar inteligencia de fuentes abiertas (OSINT). De la misma forma se estableció una metodología apropiada para el hallazgo de vulnerabilidades, basándose en estudios realizados. Mediante una comparativa de herramientas y/o técnicas de OSINT, se seleccionó las más apropiadas para realizar el objetivo de estudio y posteriormente se procedió a realizar el experimento del análisis de vulnerabilidades hacia los sistemas de información de la ESPAM MFL.

3.3. DESARROLLO DE FASE 3: EJECUTAR UN EXPERIMENTO CON HERRAMIENTAS Y/O TÉCNICAS DE OSINT, APLICADO A LA VULNERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN.

En la tercera fase se utilizaron las herramientas de OSINT hacia los sistemas de información objetivos del caso de estudio, para luego realizar un análisis, procesamiento de la información y validación de los resultados obtenidos. La utilización de OSINT permitió la recopilación de información de carácter pública en internet, con la utilización de un conjunto amplio de técnicas y/o herramientas. En el ciclo OSINT al igual que en otras metodologías se trabajó mediante diferentes fases o etapas, a lo largo del ciclo se van determinando ítems de evaluación y realización del análisis de vulnerabilidades para las herramientas de OSINT a utilizar, por lo cual se definió este ciclo como la metodología para la realización del experimento, fases que se detallan a continuación:

Ilustración 3.1 *Ciclo de OSINT.*
Fuente: (Cuesta, 2019).

En la primera fase se definieron los requerimientos necesarios que se deben cumplir, para conseguir el objetivo o resolver el problema planteado; en la segunda fase se establecieron las fuentes de información e interés, útiles del objetivo mediante herramientas de OSINT automatizadas o de trabajo manual, etc, recopiladas para posteriormente ser procesadas mediante la búsqueda de información obtenida a través de diferentes filtros; en la tercera fase se hizo la recopilación de datos obtenida en las diferentes fuentes. En la cuarta fase se procesó toda la información adquirida para posteriormente proceder al respectivo análisis; en la quinta fase se generó la inteligencia a partir de los datos recopilados y procesados; una vez ejecutado el experimento siguiendo el ciclo de OSINT y sus 5 primeras fases se hizo la validación de los resultados llevando una concordancia y correlación en cada una de las herramientas utilizadas.

El propósito de este trabajo de titulación es poder descubrir las relaciones constantes derivadas del fenómeno en estudio, el cual permitió identificar los factores positivos que generará el análisis de vulnerabilidades haciendo uso de herramientas de inteligencia de fuentes abiertas (OSINT) aplicados a los sistemas de información de la ESPAM MFL. Para posteriormente definir políticas de

distribución y difusión de la información de dicha institución en dominios no gubernamentales.

3.4. DESARROLLO DE FASE 4: PRESENTAR LA PROPUESTA DE POLÍTICAS DE DISTRIBUCIÓN Y DIFUSIÓN DE LA INFORMACIÓN EN LOS DOMINIOS NO GUBERNAMENTALES DEL ECUADOR, A LA UNIDAD DE TECNOLOGÍA DE LA ESPAM MFL, DE ACUERDO CON LOS RESULTADOS OBTENIDOS EN EL EXPERIMENTO.

Finalmente, para cumplir con el último objetivo se tomó en cuenta los resultados del objetivo 3 donde se definieron dos variables de estudio que fueron: Vulnerabilidades detectadas por cada herramienta y el nivel de afectación de las vulnerabilidades en la institución, el cual se midió mediante una matriz de vulnerabilidades que fueron aplicadas a los sistemas de información de la ESPAM MFL. De acuerdo con estos resultados, se elaboró una propuesta de políticas de distribución y difusión de información en los dominios no gubernamentales del Ecuador para posteriormente dar paso a la entrega de esta a la Unidad de Tecnología, con la finalidad de mitigar amenazas y riesgos a estos activos, la cual es fácilmente interpretable para futuras investigaciones o experimentos.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

En el presente apartado se muestran los resultados congruentes de la investigación realizada de acuerdo con la consecución de los objetivos específicos y basados en la metodología APO, los cuales permitieron llevar el desarrollo ordenado y satisfactorio del objetivo general.

4.1. FASE 1: RECOPILACIÓN DE INFORMACIÓN SOBRE LOS SISTEMAS DE INFORMACIÓN A PARTIR DE METABUSCADORES.

Basados en lo descrito en el capítulo 3 sección 3.1. Se presenta el desarrollo del primer objetivo siguiendo la primera fase, la misma que fue dividida en 4 pasos. El primer paso presenta el protocolo de búsqueda de los documentos; en el segundo paso se encuentra la aplicación del protocolo de la revisión bibliográfica; en el tercer paso se muestra la extracción de información con su respectiva categorización y finalmente en el cuarto paso se exponen los resultados de la información recopilada.

4.1.1. PROTOCOLO DE BÚSQUEDA BIBLIOGRÁFICA

En la tabla 4.2 se define el protocolo de búsqueda empleado en la respectiva recopilación de información y otros aspectos que se consideraron oportunos para obtener resultados favorables.

Tabla 4.2. Protocolo de Búsqueda

REVISIÓN BIBLIOGRÁFICA	
Palabras claves	Ciberseguridad, Cyberattack, OSINT y Open-Source Intelligence,
Base de datos consultadas	Biblioteca digital ACM, Applied Sciences, IeeeXplore, Dialnet, Google Scholar, ResearchGate y Science Direct
Cantidad de documentos recuperados	350
Filtro de búsqueda	Rango de fecha de la búsqueda entre los años 2017 al 2021
Fuentes de búsqueda	Documentos publicados en inglés y español. Revistas científicas, repositorios universitarios, libros, páginas web y conferencias.

Fuente: Los autores

4.1.2. APLICACIÓN DEL PROTOCOLO DE LA REVISIÓN BIBLIOGRÁFICA

Apoyados en los criterios de búsqueda definidos en el paso anterior se obtuvo como resultado el hallazgo de 350 publicaciones, de las cuales se seleccionaron 25 porque eran temas que se ajustaban a la temática de OSINT. La literatura preseleccionada se evaluó detalladamente leyendo en cada documento sus palabras claves, el resumen, los objetivos y los resultados pudiéndose constatar que en la mayoría de estos, se describe las técnicas, herramientas y metodologías más sofisticadas de hoy en día para investigaciones avanzadas con OSINT y la amplia gama de aplicaciones diarias en las que se utiliza, que incluyen evaluación de riesgos, análisis de sentimientos, campañas de marketing, análisis de redes sociales, periodismo de investigación y, lo que es más importante, ciberseguridad. En la figura 4.1 se muestra la clasificación de los documentos recuperados en las diferentes bases de datos.

Figura 4.1. Resultado de la búsqueda documental
Fuente: Los autores

Analizando los resultados del gráfico 3, se puede mencionar que las publicaciones con mayor concentración sobre OSINT están basadas en artículos de revistas científicas, representando el 72 % de los documentos (18), mientras que el 16% fueron seleccionados de repositorios universitarios correspondiendo a tesis de

maestrías o doctorales (4), el 8% de los documentos se seleccionaron de ponencias de expertos (2) y el menor porcentaje lo ocupa los libros con el 4% (1).

4.1.3. BÚSQUEDA Y EXTRACCIÓN DE INFORMACIÓN

En este apartado se presenta información relevante de cada uno de los documentos estudiados y analizados, de los cuales se extrajo el título, resumen, área de aplicación, base de datos consultada y el autor con el respectivo año de publicación. Las investigaciones se presentan en orden cronológico, del más reciente al más antiguo (Tabla 4.3, Anexo 1).

Tabla 4.3. Resumen de la revisión bibliográfica

N°	TÍTULO	RESUMEN	AREA DE APLICACIÓN	REFERENCIAS EDITORIALES	AUTOR (ES)
1	Coronavirus fake news detection via MedOSINT check in health care official bulletins with CBR explanation: The way to find the real information source through OSINT, the verifier tool for official journals	Esta investigación se basa en diseñar y prototipar una herramienta para realizar inteligencia en fuentes abiertas (OSINT), específicamente en boletines médicos oficiales para la detección de noticias falsas	Redes Sociales	Science Direct	(Martínez *et al.,* 2021)
2	OSINT-Based LPC-MTD and HS-Decoy for Organizational Defensive Deception	La investigación presenta una estrategia de señuelo de Ingeniería social basada en inteligencia de código abierto. Además, se propone una estrategia de defensa de objetivo móviles (MTD) basada en el control libremente proactivo que se basa en la exposición competitiva prevista de OSINT entre defensores y atacantes.	Ciberseguridad	Applied Sciences	(Seo & Kim, 2021)
3	OSINT Market & Technologies 2020-2026	La investigación pronostica que para 2026, la región de Asia y Pacífico tendrá el 35% del mercado global de inteligencia de código abierto. Además, se estima que una de las verticales de más rápido crecimiento es OSINT para la 5inteligencia cibernética, en el ámbito de la inteligencia sobre amenazas.	OSINT	Corporación de Investigación de Seguridad Nacional (HSRC)	(HSRC, 2021)
4	OSINT Techniques Integration with Risk Assessment ISO/IEC 27001	En este documento, se propone un proceso de integración entre las técnicas seleccionadas de OSINT (inteligencia de código abierto) y la norma ISO 27001 en algunos dominios relevantes para una seguridad adicional.	Gestión de riesgos	Biblioteca digital ACM	(Alkilani & Qusef, 2021)
5	Basic Study in Targeted E-mail Attack Method Using OSINT	En este documento, se formula un modelo de transición de estado que define el proceso mediante el cual los atacantes recopilan la información de un objetivo mediante el uso de herramientas OSINT.	Ciberseguridad	ResearchGate	(Uehara., 2020)
6	Análisis de ataques cibernéticos hacia el Ecuador.	La presente investigación se basa en un análisis sobre los ataques que han ocurrido en Ecuador en los últimos años, donde de acuerdo con el Ranking Nacional de Ciberseguridad (NCSI) se pudo constatar que Ecuador cuenta con 25 puntos de un total de 77 indicadores a evaluar, clasificándose de esta forma como un país con ciberseguridad deficiente.	Ciberseguridad	Revista Científica Aristas	(Alvarado, 2020)

Fuente: Los autores

4.1.4. ANÁLISIS DE LA INFORMACIÓN RECOLECTADA

Al estudiar cada uno de los artículos seleccionados se conoció la importancia que OSINT ha tomado desde su aparición, dado que en los inicios de su investigación incluso de la práctica, las publicaciones se enfocaban más en detectar y combatir el terrorismo. Actualmente, la investigación de OSINT está menos dirigida a la lucha contra el terrorismo y más centrada en las redes sociales y la seguridad de la información.

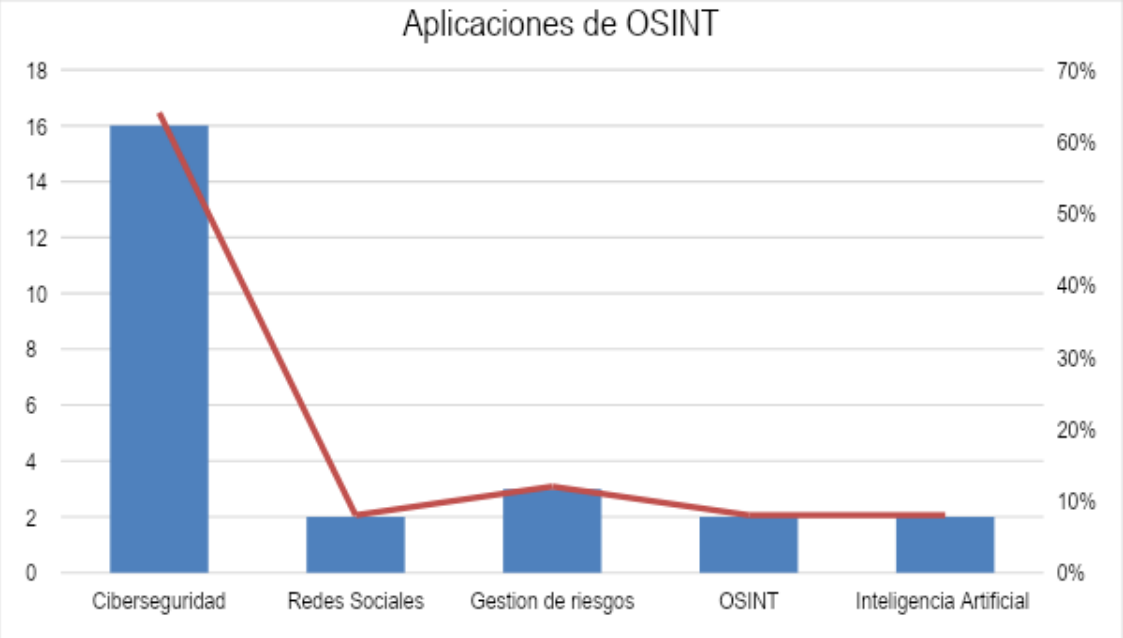


Figura 4.2. Áreas de aplicación de OSINT
Fuente: Revisión bibliográfica

Interpretando los datos de la figura 4.2, es posible identificar cuáles son las áreas donde OSINT se está aplicando más hoy en día. De las 25 publicaciones, dos son específicas del funcionamiento de OSINT, sus herramientas y metodología sin abordar otra área de manera objetiva. La mayor concentración se encuentra en el área de Ciberseguridad, con un total de 16 publicaciones, lo que representa el 64% del total de publicaciones. La segunda área de aplicación con la mayor concentración de publicaciones es gestión de riesgos con 12% y las áreas de redes sociales e inteligencia artificial aparecen juntas en tercer lugar, cada una con el 8% de publicaciones.

En contexto con lo mencionado, se puede observar que el área con mayores publicaciones realizadas entre los periodos 2017 a 2021 están enfocadas, en la búsqueda de información en el área de ciberseguridad, más específicamente sobre detección de vulnerabilidades, ciberataques y el uso de OSINT para obtener información como geolocalización, inteligencia de amenazas cibernéticas, seguridad inalámbrica y evidencia digital.

4.2. FASE 2: DEFINIR LAS HERRAMIENTAS DE OSINT A EMPLEAR EN LAS PRUEBAS DENTRO DE LOS SISTEMAS DE INFORMACIÓN

4.2.1. REALIZACIÓN DE VISITA TÉCNICA A LA UNIDAD DE TECNOLOGÍA DE LA ESPAM MFL PARA EVALUAR EL ESTADO DE LOS SISTEMAS DE INFORMACIÓN INSTITUCIONALES

Recabando información desde una entrevista como tipo encuesta no estructurada (reunión de manera virtual por la situación COVID-19 actual), que se les realizó a los miembros del departamento de tecnologías se obtuvo la información que será de ayuda para la ejecución del experimento utilizando herramientas y/o técnicas de OSINT, los autores pudieron recabar información sobre el estado de los servidores y la seguridad de los sistemas de información de la ESPAM MFL. El responsable a cargo de la instalación y mantenimiento de la seguridad de los servidores institucionales es el Mgs. Cesar Moreira Zambrano el cual mantiene segura la DMZ (Zona desmilitarizada), la actualización del software antivirus se lo realiza dependiendo de las notificaciones que el mismo sistema operativo notifica, también, se preguntó sobre si la institución cuenta con IDS, IPS y SOC. Además, se preguntó si la institución cuenta con un presupuesto para inversiones en ciberseguridad, de la cual se conoció que no cuenta con un presupuesto establecido o definido para ciberseguridad.

Se preguntó también, sobre cómo actúa o si el cuerpo docente y el personal de TI cuentan con la formación necesaria para prevenir errores de seguridad de la información y si son capaces de identificar un virus/malware; los cuales respondieron que no se tiene la formación necesaria para prevenir errores en la

seguridad de la información y que solamente el personal TI están en capacidad de identificar algún virus o malware. Así mismo se conoció investigo se acerca de la gestión de redes sociales dentro de la institución al cual se obtuvo como respuesta que se hace la utilización segura de las redes sociales en horario laboral.

Respecto con la gestión de contraseñas, correos institucionales y datos personales de los docentes y del personal del departamento de tecnologías, están apoyados en un modelo de sistema de gestión de la seguridad de la información (SGSI), ejecutado en la institución donde se definen los procedimientos de utilización de claves y mecanismos de utilización de cuentas de correo electrónicos institucionales, donde también dentro del modelo de SGSI está el plan de prevención de riesgos informáticos para los servidores y activos de la institución. (Anexo 2 y Anexo 3).

4.2.2. IDENTIFICAR UNA METODOLOGÍA PARA EL HALLAZGO DE VULNERABILIDADES PARA LAS INFRAESTRUCTURAS Y LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.

Para la identificación de una metodología acorde al caso que se estudió, los autores hicieron una exploración hacia el estado del arte escrito en este trabajo de titulación, para definir y determinar la metodología óptima para la ejecución del experimento. De la misma manera, se pudo identificar los factores positivos que generará el análisis de vulnerabilidades haciendo uso de herramientas de inteligencia de fuentes abiertas (OSINT) aplicados a los sistemas de información de la ESPAM MFL. La inteligencia de fuentes abiertas se considera como un proceso formado por una serie de fases previamente definidas en el capítulo III del desarrollo metodológico, mediante el ciclo de OSINT, donde estas fases permitieron una estructura de trabajo, de manera que sea ágil para la investigación.

4.2.3. SELECCIÓN DE LAS HERRAMIENTAS Y/O TÉCNICAS DE OSINT PARA EL ESCANEO DE VULNERABILIDADES.

Una vez que se escogió el ciclo de OSINT como la metodología a implementar, se definieron las herramientas de OSINT utilizadas dentro de la ejecución del experimento para el escaneo de vulnerabilidades:

Tabla 4.4. Herramientas OSINT a utilizar.

Herramienta OSINT	Conjunto de datos de entrada	Interfaz	Plataforma	Resultado de salida
Website Informer	Información personal, de empresa, dominio y evaluación de vulnerabilidades	Interfaz Web	Linux, Windows, Online	Múltiple información
WhoIs, DNS & Domain Info	Información personal, de empresa, dominio y evaluación de vulnerabilidades	Interfaz Web	Windows, Online	Múltiple información
Domain dossier	Información personal, de empresa, dominio	Interfaz Web	Windows, Online	Múltiple información
Siteliner	Información personal, de empresa, dominio y evaluación de vulnerabilidades	Interfaz Web	Windows, Online	Múltiple información
Hunter	Información personal, dominio	Interfaz Web	Linux, Windows, Online	Múltiple información
Crt.sh	Información sobre las certificaciones del dominio.	Interfaz Web	Windows, Online	Certificaciones SSH
Spyse	Información personal, información de red, dominio	Interfaz Web	Linux, Window, Online	Múltiple información
Zoom Eyes	Dominio	Interfaz Web	Linux, Window, Online	Información de red. Contactos
Shodan	Ciudad, información de red	Interfaz Web	Online	Información de red

Fuente: Los autores.

4.3. FASE 3: EJECUTAR UN EXPERIMENTO CON HERRAMIENTAS Y/O TÉCNICAS DE OSINT, APLICADO A LA VULNERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN.

4.3.1. IMPLEMENTACIÓN DEL CICLO DE OSINT PARA LA UTILIZACIÓN DE LAS HERRAMIENTAS Y/O TÉCNICAS PARA LA BÚSQUEDA DE VULNERABILIDADES.

Con OSINT al igual que en otras metodologías, se trabajó mediante fases o etapas, de donde se obtuvo los siguientes resultados por cada una de sus fases. En la primera fase del ciclo de OSINT, se diferenciaron y se obtuvieron los requerimientos necesarios, para comenzar a definir el objetivo de la información que se buscó y de qué tipo fue, en este caso la información que se buscó fueron referentes al dominio de la ESPAM MFL; en la segunda fase se identificaron las fuentes de información, especificadas a partir de los requerimientos iniciales establecidos, las fuentes de interés recopiladas, partiendo del volumen de información que se encuentra disponible en internet el cual fue infranqueable, por lo tanto fue imprescindible encontrar y seleccionar las fuentes informativas necesarias, para optimizar la adquisición de la información que siguió a continuación.

En la tercera fase se adquirió la información obtenida a partir de los datos obtenidos en los requerimientos iniciales y en las diferentes fuentes de orígenes indicados. En la cuarta fase se procesó toda la información adquirida de manera que se le dio formato para posteriormente ser analizada; en la quinta fase se procedió a generar la inteligencia a partir de los datos obtenidos y procesados, el objetivo de esta fase fue relacionar la información de los distintos orígenes buscando patrones que permitieron llegar a las conclusiones significativas.

4.3.2. EJECUCIÓN DEL EXPERIMENTO UTILIZADO HERRAMIENTAS OSINT, APLICADO A LAS VULNERABILIDADES DE LOS SISTEMAS DE INFORMACIÓN.

Definidas anteriormente las fases del ciclo de OSINT para la ejecución del experimento, los autores de este trabajo de titulación presentan los resultados de

la puesta en marcha de cada una de las herramientas que se utilizaron y los datos obtenidos en cada una de estas. Se hizo la validación de los resultados llevando una concordancia y correlación en cada una de las herramientas utilizadas para un mismo fin en el análisis y detección de vulnerabilidades aplicado a los sistemas de información, servidores, correos y dominios instituciones. Una vez que se ejecutó el experimento con cada una de las herramientas de OSINT utilizadas para el dominio institucional, se procedió a generar una tabla resumen de las herramientas utilizadas, los hallazgos y los riesgos encontrados, además, si se presentaron potenciales vulnerabilidades (Anexo 4, Anexo 5 y Anexo 6).

Tabla 4.4 Tabla resumen de las herramientas utilizadas, sus hallazgos y riesgos encontrados.

Herramientas utilizadas	Hallazgos encontrados	Riesgos encontrados	Vulnerabilidad encontrada.
La herramienta multiplataforma **hunter.io** sirve para encontrar y verificar direcciones de correo electrónico profesionales	Esta herramienta permitió obtener desde el dominio de la ESPAM MFL direcciones correos electrónicos institucionales que han sido utilizadas dentro de algunos de los subdominios de la institución.	Visualización de las direcciones correos electrónicos institucionales, posibles riesgos para phishing, spam, etc.	Exposición de correos (***Anexo 4***)
Domain Dossier: Esta herramienta permitió generar informes a partir de registros públicos sobre nombres de dominio y direcciones IP para ayudar a resolver problemas, investigar delitos cibernéticos o simplemente comprender mejor cómo se configuran los sistemas de información.	IP del dominio, quienes prestan los servicios de los servidores, direcciones donde se encuentra el proveedor del servicio, registros del DNS, tráfico de la red, puertos abiertos.	Puerto 80 abierto donde con la herramienta se pudo establecer conexión (***Anexo 4***)	S/V
Website informer permitió visualizar información detallada a partir del dominio.	Información referente a donde están alojados los servidores, quienes en la ESPAM MFL están considerados dentro del rol de administrador de los servidores y a nombre de quien se realiza la facturación.	Se muestra información personal como correo electrónico, nombres completos, la dirección donde se encuentra la ESPAM MFL y el número de convencional de la institución.	Datos personales, correos de administradores y de la persona a nombre de quien está registrado los servidores de la ESPAM MFL (***Anexo 4***).
Shodan es una herramienta multiplataforma, que permitió recabar información desde el dominio institucional.	Datos como la dirección IP, donde se alojan los servidores, los puertos que se encuentran abiertos y las tecnologías que dentro de la institución utilizaron para el desarrollo de la página web institucional y los servidores.	Puertos abiertos y las tecnologías que se utilizan (***Anexo 4***).	S/V

Spyse: Esta herramienta que partió desde el dominio de la institución permitió generar una evaluación diagnóstica del estado de toda la infraestructura de los sistemas de información de la ESPAM MFL.	Puesto en el que se encuentra rankeado el dominio dentro de Alexa Rank, los récords del DNS, si el sitio web cuenta con responsive, una calificación de la web en general, el nivel de riesgo potencial encontrado, las tecnologías utilizadas y los subdominios con sus respectivas puntuaciones del nivel de seguridad que emplean o tienen	Bajo nivel de seguridad en el dominio evaluaciondocente.espam.edu.ec (***Anexo 4***)	S/V
La herramienta **Siteliner** permitió hacer una evaluación de tipo scanner del sitio web de la institución, donde se muestra información de los problemas presentados dentro de los subdominios, enlaces todos y con dominios relacionados al sitio web.	Gráficos estadísticos del estado del sitio (porcentajes de errores, contenido duplicado, contenido común y contenido único) y la comparación con otros sitios web, en relación con el tamaño, tiempo de respuesta, número de palabras por página, porcentaje del contenido duplicado, común y único, los enlaces internos, externos y el total de los enlaces que contiene el sitio web institucional.	Dominios y subdominios institucionales, enlaces rotos (***Anexo 4*** y ***Anexo 5***).	S/V
Crt.sh es un verificador de certificaciones TLS/SSL para los dominios.	Permitió validar con fecha las certificaciones que el dominio www.espam.edu.ec ha generado los últimos 5 años (***Anexo 4***).	Sin riesgos, al ser solamente un verificador de certificados.	S/V
Zoom Eyes. Permitió ahondar con un análisis mucho más exhaustivo partiendo como base desde el dominio, en la búsqueda de vulnerabilidades más profundas para los sistemas de información evaluados en el caso de estudio.	Muestra una vista generalizada de la distribución global, regional, la distribución de los puertos y de los equipos que se utilizan (***Anexo 4***).	Vulnerabilidades presentadas en los servicios que utilizan dentro de los servidores.	(***Anexo 6***)

WhoIs, DNS & Domain Info.	Permitió encontrar información del dominio, la dirección IP, donde se encuentran alojados lógicamente los servidores, que sistema operativo utiliza ese servidor, el tipo de servidor que utiliza y un historial del mantenimiento del servidor web los últimos 9 años.	Información del dominio, donde se encuentran alojados los servidores para dicho dominio y las tecnologías que utilizan (***Anexo 4***).	S/V

Fuente: Los autores.

4.3.3. VALIDACIÓN DE LOS RESULTADOS DEL EXPERIMENTO

En la validación de los resultados del experimento efectuado, se pudo obtener un análisis y búsqueda de vulnerabilidades eficaz. Además, mediante una escala de valoración y semaforización para las variables y componentes de los factores de vulnerabilidades. Se procedió a determinar el nivel de riesgo que pueden llegar a determinar las vulnerabilidades encontradas con las herramientas de OSINT empleadas en el experimento.

Tabla 4.5 Escala de valoración y semaforización para las variables y componentes de los factores de vulnerabilidades.

Categoría	Valor	Semaforización
Informativo	0	
Bajo	1	
Medio	2 - 5	
Alto riesgo	6 - 10	

Fuente: Los autores.

Una vez establecida las escalas de valoración y semaforización de las vulnerabilidades encontradas, se realizó una matriz donde se encuentran detalladas varias vulnerabilidades relacionadas con el dominio www.espam.edu.ec (***Anexo 5***).

Tabla 4.6 Vulnerabilidades relacionadas utilizando herramientas de OSINT.

Vulnerabilidad relacionada	Categoría – Valoración	Semaforización
Apache	Alto riesgo - 10	
WordPress	Alto riesgo - 10	
Nginx	Alto riesgo - 9	
Gato apache	Alto riesgo - 9	
http	Alto riesgo - 10	
PhpMyAdmin	Alto riesgo - 10	
Microsoft es http	Alto riesgo - 10	
Placa de potencia invision	Alto riesgo - 7	

Fuente: Los autores.

Varias de las herramientas de OSINT y resultados de la ejecución de las herramientas con el escaneo de vulnerabilidades con la ayuda de la matriz de definición de las vulnerabilidades, permitieron determinar la elaboración de políticas de distribución y de difusión de la información dentro de la institución en los dominios de carácter no gubernamentales. Además, se pudo constatar que la página web institucional (www.espam.edu.ec) muestra altos niveles de seguridad

en su concesión y varias de las herramientas OSINT muestran este punto a favor pese a mostrar que esta no es una conexión segura, a lo que se muestra en cualquier navegador.

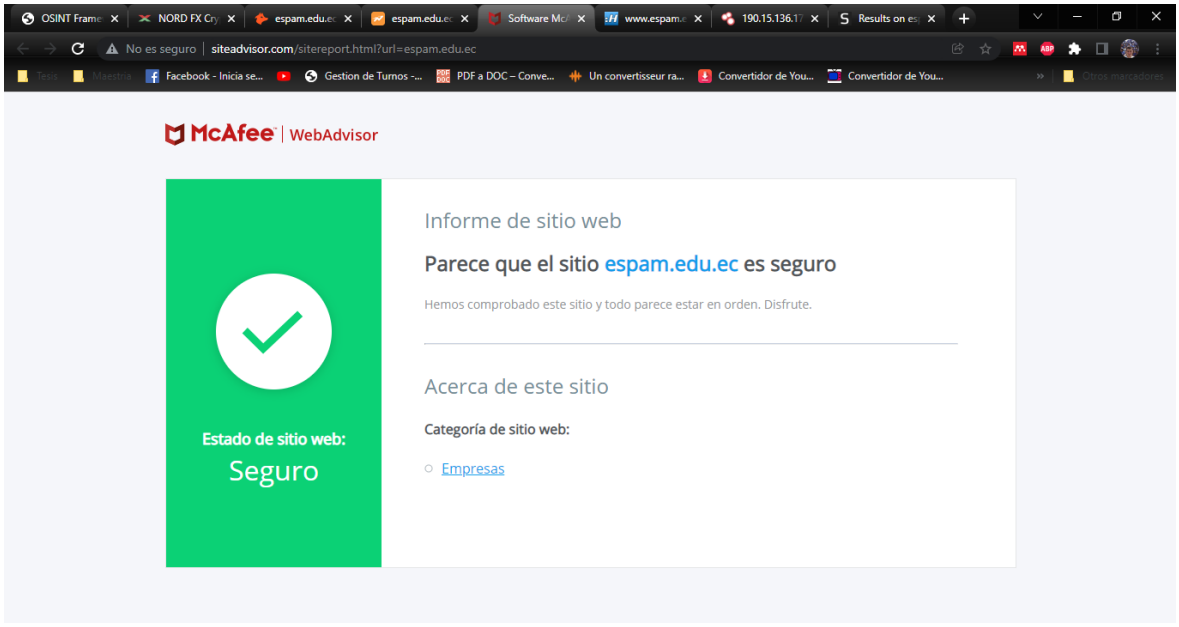


Figura 4.41. Verificación que el sitio web es seguro
Fuente: Los Autores

Figura 4.42. Nivel de riesgo de seguridad bajo
Fuente: Los Autores

4.4. FASE 4: PRESENTAR LA PROPUESTA DE POLÍTICAS DE DISTRIBUCIÓN Y DIFUSIÓN DE LA INFORMACIÓN EN LOS DOMINIOS NO GUBERNAMENTALES DEL ECUADOR, A LA UNIDAD DE TECNOLOGÍA DE LA ESPAM MFL, DE ACUERDO CON LOS RESULTADOS OBTENIDOS EN EL EXPERIMENTO.

Habiendo realizado el análisis de cada una de las herramientas y de acuerdo a los resultados obtenidos se propone la implementación de una propuesta de políticas de distribución y difusión de la información (**Anexo 7**), la cual es elaborada desde un marco estratégico, con la finalidad de proteger la información, contra la divulgación, modificación o destrucción de la misma en los dominios no gubernamentales del Ecuador, tomando como caso de estudio los sistemas de información de la ESPAM MFL, los cuales fueron analizados en forma de carácter académicos. Así mismo en la propuesta de las políticas se tomó como referencia la norma ISO/IEC 27002, la cual direcciona hacia las políticas y medidas de seguridad, que contribuyen a prevenir la fuga de información interna. Finalmente se procedió hacer la entrega a de la propuesta a la Unidad de Tecnología junto a una copia de la norma ISO en mención.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Diversos reportes encontrados y estudiados en el primer objetivo muestran la enorme importancia que las herramientas OSINT están tomando en la actualidad principalmente por la creciente proliferación del uso de internet y redes sociales, sin embargo, otros estudios revelan la diversidad de vulnerabilidades que los hackers aprovechan al exponer tanta información en la web, lo cual ha conllevado que los diferentes países destinen cada vez más recursos para implementar este tipo de herramientas dado que es innegable que puede aportar una mejor seguridad (***Anexo 1***).
- En el desarrollo del trabajo se presentaron diferentes técnicas y herramientas de fuentes abiertas que fueron utilizadas para la detección de vulnerabilidades y amenazas de los sistemas de información de la ESPAM MFL, y que fueron definidas luego de realizar una entrevista no estructurada a los encargados de la Unidad de Tecnología (***Anexo 2*** y ***Anexo 3***).
- Mediante la ejecución de las herramientas OSINT en el escaneo de vulnerabilidades, se pudo comprobar que los sistemas de información se encuentran expuestos a diversos ataques cibernéticos, dado que a través del test se pudo obtener información sensible y que no debería estar expuesta, lo cual fue ventajoso ya que gracias a las herramientas se pudo conocer los posibles factores de ataque y contrarrestar el riesgo (***Anexo 4***, ***Anexo 5*** y ***Anexo 6***).
- La propuesta de políticas para la distribución y difusión de información diseñada para la ESPAM MFL, proporcionará una guía a seguir para trabajar en los aspectos de seguridad de los sistemas de información y poder de esta forma afrontar las posibles amenazas. En el documento se establecen acciones concisas, con el fin de promover la ética y la concientización sobre los temas abordados (***Anexo 7***).

5.2. RECOMENDACIONES

- Las amenazas informáticas día a día aumentan vertiginosamente, condiciones que con la pandemia incrementaron el riesgo de sufrir un incidente de seguridad debido a una mayor dependencia de los recursos de Internet, por lo que es necesario que los países inicien una campaña de capacitación de seguridad de la información, que les permita a los usuarios tener a la mano herramientas para frenar amenazas y riesgos de los activos de su organización o institución.

- Como parte del buen desarrollo de la práctica se recomienda a la institución adoptar las herramientas de fuentes abiertas (OSINT) como parte de sus controles de seguridad, dado que permite identificar y prevenir posibles amenazas, además realizar auditorías con el fin de evaluar el nivel de privacidad y seguridad.

- Es fundamental seguir implementado metodologías para mitigar posibles vulnerabilidades, que permitan comprender las brechas de seguridad que pueden comprometer la integridad de la información, por lo que se exhorta a la Unidad de Tecnología realizar este tipo de análisis de forma periódica, de manera que los sistemas se encuentren preparados antes posibles ataques.

- Finalmente, se recomienda difundir las Políticas de Seguridad de la Información, proporcionada por las autoras a todos los miembros de la comunidad Universitaria, con el fin de preservar la información y los sistemas de la institución, garantizando la integridad, confidencialidad y disponibilidad de esta.

BIBLIOGRAFÍA

Alvarado, E. (2020). Análisis De Ataques Cibernéticos Hacia El Ecuador. *Revista Científica Aristas*, *2*(1), 18–27. https://revistacientificaistjba.edu.ec/images/home/documentos/Mayo_2020/2.pdf

Angulo, A. (2020). OSINT. Investigación, análisis y propuesta para su uso en instituciones educativas. In *UNIR*. https://reunir.unir.net/bitstream/handle/123456789/10652/Angulo Vidal%2C Alcides Augusto.pdf?sequence=1&isAllowed=y

ARCOTEL. (2018). *RESOLUCiÓN ARCOTEL-2018-0652*.

ASTURIAS. (2017). Administración por Objetivos (APO). *ASTURIAS - Corporación Universitaria*, *7*, 1–8.

Avellán, N., & Zambrano, M. (2019). *Informe de trabajo de titulación*. http://repositorio.espam.edu.ec/bitstream/42000/1032/1/TTMTI3.pdf

Balcázar, M. (2020). *Propuesta metodológica para mitigar el riesgo de seguridad informática con el uso de técnicas OSINT.*

Bausate, J. (2016). *Guía para la elaboración del Proyecto de tesis y del Informe final*.

Cuesta, C. (2019). *Fuentes de Información OSINT para la Clasificación y Selección de Perfiles sobre Repositorios*.

Dadkhah, M., Lagzian, M., & Borchardt, G. (2018). Academic Information Security Researchers: Hackers or Specialists? *Science and Engineering Ethics*, *24*(2), 785–790. https://doi.org/10.1007/s11948-017-9907-1

Dávila, L., & Pacheco, J. (2017). Evaluación de riesgos: Estudio de la fuga de datos en los sitios web del Ecuador. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, *1*(2), 15–20. https://doi.org/10.29018/issn.2588-1000vol1iss2.2017pp40-53

ESET. (2018). Eset Security Report Latinoamérica 2018. In *We Live Security*. https://www.welivesecurity.com/wp-

content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

ESET. (2021). Eset Security Report Latinoamérica 2021. In *We Live Security*. https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

Espinoza, F. (2018). Gestión del conocimiento mediado por tic en la Universidad Técnica de Machala. Management. *Scielo*, *16*, 199–219. http://www.scielo.org.bo/pdf/rfer/v16n16/v16n16_a11.pdf

Fennema, M. C., Figueroa, L. M., Viaña, G., Lesca, N., & Lara, C. (2017). Tratamiento de Evidencias Digitales Forenses en Dispositivos Móviles. *XIX Workshop de Investigadores En Ciencias de La Computación*, 648–652. http://sedici.unlp.edu.ar/handle/10915/62182

Guzmán, F. (2017). Impacto del cibercrimen: bajo la realidad aumentada. *ResearchGate*, 67–79. https://doi.org/10.22209/cice.n2a08

Hernandez, M., Pinzón, C., Díaz, D., Garcia, J., & Pinto, R. (2018). Open-source intelligence (OSINT) in a colombian context and sentiment analysis. *Revista Vínculos*, *15*(2), 195–214. https://doi.org/10.14483/2322939x.13504

Huang, H. C., Zhang, Z. K., Cheng, H. W., & Shieh, S. W. (2017). Web Application Security: Threats, Countermeasures, and Pitfalls. *Computer*, *50*(6), 81–85. https://doi.org/10.1109/MC.2017.183

IEDGE. (2022). *Políticas de Seguridad Informática 2022*.

Industrial, I. (2016). *Ciberseguridad, la protección de la información en un mundo digital*. https://upfinder.upf.edu/iii/encore/record/C__Rb1539055__S(seguretat digital) f:a b:fr__Ff:facetlocations:fr:fr:Poblenou::__Orightresult__U__X1?lang=cat

ISO. (2012). *Iso/iec 27032:2012 - Lineamientos para Ciberseguridad* (p. 27032).

ISO. (2013). *ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES 5.*

Izaguirre, J., & León, F. (2018). Análisis de los Ciberataques Realizados en América Latina. *INNOVA Research Journal*, *3*(9), 180–189. https://doi.org/10.33890/innova.v3.n9.2018.837

Millán, J. (2019). OSINT y big data: Monitorización y búsqueda en fuentes abiertas [UNIR]. In *Máster Universitario en Protección de Datos*. https://reunir.unir.net/bitstream/handle/123456789/9790/Millan Lopez%2C Juan Antonio.pdf?sequence=1&isAllowed=y

MINTEL. (2021). *ACUERDO MINISTERIAL 006-2021*.

Navarro, A. (2017). *Desarrollo de un modelo de Data Loss Prevention (DLP), en las instituciones de Educación superior (IES). Caso Universidad ECOTEC.*

Pastor, J., Nespoli, P., Gomez, F., & Martinez, G. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access*, *8*, 72–100. https://doi.org/10.1109/ACCESS.2020.2965257

Pastorino, C. (2019). *Técnicas y herramientas OSINT para la investigación en Internet*. Welivesecurity - ESET. https://www.welivesecurity.com/la-es/2019/10/07/tecnicas-herramientas-osint-investigacion-internet/

Prieto, B. (2018). El uso de los métodos deductivo e inductivo para aumentar la eficiencia del procesamiento de adquisición de evidencias digitales. *Scielo*, *18*(46). https://doi.org/10.11144/javeriana.cc18-46.umdi

Schwartz, M. (2020). CIBERSEGURIDAD, Riesgos, Avances y el camino a seguir en America Latina y El Caribe. *Bid- Oea*, *1*, 10–19. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Tates, C., & Recalde, L. (2019). La ciberseguridad en el ecuador, una propuesta de organización. *Revista de Ciencias de Seguridad y Defensa*, *4*(7), 156–169. http://geo1.espe.edu.ec/wp-content/uploads/2019/03/7art12.pdf

Torres Martínez, M. Á. (2015). *Dlp : Prevención De Fuga De Información (Data Loss Prevention)*. 1–6.

Trindade, V. (2017). La entrevista no estructurada en investigación cualitativa: una experiencia de campo. In *SEDICI*. http://sedici.unlp.edu.ar/handle/10915/64407

Zuña, E., Arce, A., Romero, W., & Soledispa, C. (2019). Análisis de la seguridad de la información en las PYMES de la ciudad de Milagro. *Universidad y*

Sociedad, *11*(4), 487–492. http://scielo.sld.cu/pdf/rus/v11n3/2218-3620-rus-11-03-186.pdf

ANEXOS

ANEXO 1. REVISIÓN BIBLIOGRÁFICA

N°	TÍTULO	RESUMEN	AREA DE APLICACIÓN	REFERENCIAS EDITORIALES	AUTOR (ES)
1	Coronavirus fake news detection via MedOSINT check in health care official bulletins with CBR explanation: The way to find the real information source through OSINT, the verifier tool for official journals	Esta investigación se basa en diseñar y prototipar una herramienta para realizar inteligencia en fuentes abiertas (OSINT), específicamente en boletines médicos oficiales para la detección de noticias falsas	Redes Sociales	Science Direct	(Martínez *et al.,* 2021)
2	OSINT-Based LPC-MTD and HS-Decoy for Organizational Defensive Deception	La investigación presenta una estrategia de señuelo de Ingeniería social basada en inteligencia de código abierto. Además, se propone una estrategia de defensa de objetivo móviles (MTD) basada en el control libremente proactivo que se basa en la exposición competitiva prevista de OSINT entre defensores y atacantes.	Ciberseguridad	Applied Sciences	(Seo & Kim, 2021)
3	OSINT Market & Technologies 2020-2026	La investigación pronostica que para 2026, la región de Asia y Pacífico tendrá el 35% del mercado global de inteligencia de código abierto. Además, se estima que una de las verticales de más rápido crecimiento es OSINT para la 5inteligencia cibernética, en el ámbito de la inteligencia sobre amenazas.	OSINT	Corporación de Investigación de Seguridad Nacional (HSRC)	(HSRC, 2021)
4	OSINT Techniques Integration with Risk Assessment ISO/IEC 27001	En este documento, se propone un proceso de integración entre las técnicas seleccionadas de OSINT (inteligencia de código abierto) y la norma ISO 27001 en algunos dominios relevantes para una seguridad adicional.	Gestión de riesgos	Biblioteca digital ACM	(Alkilani & Qusef, 2021)
5	Social media and open-source intelligence (OSINT) in Andalusian local governments: the cases of Instagram and Twitter	Esta investigación aborda un análisis cuantitativo y cualitativo centrado en Twitter e Instagram como plataformas ciudadanas para los municipios, contando con la recolección de información de la totalidad de sus publicaciones gracias a herramientas OSINT.	Redes Sociales	Arias Montano – Repositorio Institucional de la Universidad de Huelva	(Perea El Khalifi, 2021)
6	Análisis de ataques cibernéticos hacia el Ecuador.	La presente investigación se basa en un análisis sobre los ataques que han ocurrido en Ecuador en los últimos años, donde de acuerdo con el Ranking Nacional de Ciberseguridad (NCSI) se pudo constatar que Ecuador cuenta con 25 puntos de un total de 77 indicadores a evaluar, clasificándolo de esta forma como un país con ciberseguridad deficiente.	Ciberseguridad	Revista Científica Aristas	(Alvarado, 2020)

7	Basic Study on Targeted E-mail Attack Method Using OSINT	En este documento, se formula un modelo de transición de estado que define el proceso mediante el cual los atacantes recopilan la información de un objetivo mediante el uso de herramientas OSINT.	Ciberseguridad	ResearchGate	(Uehara ., 2020)
8	Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información	El presente artículo tiene como finalidad analizar los puntos vulnerables que existen en los sistemas de información, buscando, por lo consiguiente, sistemas o medidas de seguridad que se podrían tomar para evitar estos problemas debido a las fallas en los sistemas.	Ciberseguridad	Dialnet	(Arévalo *et al.,* 2020)
9	Open-Source Intelligence Educational Resources: A Visual Perspective Analysis	En este estudio se implementó un mapeo sistemático, donde se proyectó la inteligencia OSINT para el 2026 como uno de los mercados con mayor flujo de ingresos para su uso y estrategia de futuro, sin embargo, no refleja un alto grado de participación dentro de los repositorios y base de datos, siendo las fuentes de libre uso y sin ánimo de lucro las que tienen mayor presencia de recursos OSINT.	Ciberseguridad	IEEEXplore	(Herrera *et al.,* 2020)
10	Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies	Esta tesis propone una solución a las limitaciones relacionadas con la gestión del conocimiento de amenazas, habilitación tecnológica limitada en la clasificación de amenazas, alto volumen de información compartida sobre amenazas, calidad de los datos y capacidades limitadas de análisis avanzado y automatización de tareas mediante la información valiosa de fuentes OSINT.	Ciberseguridad	Repositorio de la Universidad de Lisboa	(Dinis, 2020)
11	The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends	Este trabajo se centra en la descripción del estado actual y futuro de OSINT, y de las diferentes técnicas y herramientas más sofisticadas hoy en día para investigaciones avanzadas. En otro contexto, se analizan los puntos fuertes de la metodología y como aplicarla y por el otro las limitaciones a la hora de implementarlo.	Ciberseguridad	IEEEXplore	(Pastor *et al.,* 2020)
12	A Threat Intelligence Tool for the Security Development Lifecycle.	El autor del artículo presenta una herramienta de minería inteligente para SDL, para automatizar el proceso de extracción de fuentes de información de amenazas de código abierto y entregar indicadores de amenazas específicos de productos diseñados.	Ciberseguridad	Biblioteca digital ACM	(Kannavara et al., 2019)
13	Análisis de la seguridad de la información en las Pymes de la Ciudad de Milagro	Este artículo basado en un análisis sobre el manejo y la protección de la información en las Pymes propone una perspectiva diferente para la detección de hishing o malware	Ciberseguridad	Revista “Universidad y Sociedad”	(Zuña *et al.,* 2019)

		que afectan a la Pymes, así mismo la aplicación de un plan de medidas preventivas que permiten mejorar la seguridad de la información.			
14	IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company)	El marco de pruebas de penetración que se utilizó en este estudio es la versión 4 de la guía de prueba OWASP, donde también fue importante trabajar con las herramientas basadas en OSINT para generar conocimientos de todas las fuentes de datos.	Gestión de riesgos	ResearchGate	(Wiradarma & Sasmita, 2019)
15	Open-Source Intelligence for Energy Sector Cyber attacks	El artículo presenta un amplio estudio sobre las fuentes de inteligencia que se pueden aprovechar para modelar un sistema de energía de gran escala, con lo cual se logró construir un gran sistema energético y procesarlo para identificar sus ubicaciones y críticas.	Ciberseguridad	ResearchGate	(Keliris *et al.,* 2019)
16	OSINT as a part of cyber defense system	El artículo presenta los resultados de la investigación sobre el desarrollo de principios fundamentales y aplicados para analizar los flujos de información en las redes informáticas globales mientras se realiza la inteligencia de código abierto (OSINT).	Ciberseguridad	Theoretical and Applied Cybersecurity scientific journal	(Lande & Shnurko, 2019)
17	OSINT y big data: Monitorización y búsqueda en fuentes abiertas	El autor en su artículo analiza los principales medios de búsquedas de información que las nuevas tecnologías han proporcionado y las implicaciones legales que el uso de esas tecnologías tiene sobre la privacidad de cada persona.	Inteligencia Artificial	Re- UNIR	(Millán, 2019)
18	SeedsMiner: Generación precisa de listas negras de URL basadas en la recolección eficiente de semillas OSINT	Proponen un método para recopilar URL candidatas maliciosas de manera eficiente a partir de información abierta (OSINT), con el cual se determinó que el 75% de la lista negra generada por el método propuesto fue desconocida para la Navegación segura de Google.	Ciberseguridad	Biblioteca digital ACM	(Tanaka & Kashima, 2019)
19	Análisis de los ciberataques realizados en América Latina.	Este artículo se basa en el análisis de los sucesos relevantes de ciberataques en varios países de América Latina. De acuerdo a los datos recabados por diferentes fuentes, se concretó que la mayoría de los países latinoamericanos tienen algún tipo de protección de datos y privacidad, sin embargo, no cuentan con los recursos necesarios para afrontar y evitar un ciberataque.	Ciberseguridad	INNOVA Research Journal	(Izaguirre & León, 2018)
20	Capacidades de las metodologías de pruebas de penetración para detectar	En este estudio se analizan las capacidades para la detección de vulnerabilidades en aplicaciones web que proponen las principales metodologías de pruebas de penetración como ISSAF, OWASP, PTES, entre otras. Los resultados alcanzados	Ciberseguridad	Revista Cubana de Ciencias Informáticas	(González & Montesino, 2018)

	vulnerabilidades frecuentes en aplicaciones web	demostraron que ninguna de las metodologías es capaz de brindar métodos, herramientas o pruebas de seguridad para detectar las vulnerabilidades actuales en su totalidad.			
21	Investigación del Cibercrimen y los Delitos Informáticos utilizando Inteligencia de Fuentes Abiertas de Información (OSINT)	El estudio comprende el problema de los ataques informáticos y el aumento considerable de estos en Colombia, partiendo de que se es más rentable la ciberdelincuencia que el narcotráfico según cifras examinadas en el artículo, además se contempla el concepto de OSINT y sus principales usos.	Ciberseguridad	ResearchGate	(Toro *et al.,* 2018)
22	Open-source intelligence (OSINT) as support of cybersecurity operations. "Use of OSINT in a colombian context and sentiment Analysis"	La presente investigación está basada en las diferentes tecnologías OSINT y el desarrollo de modelos automáticos utilizados para realizar análisis de sentimientos sobre datos recopilados. Las herramientas utilizadas en esta investigación fueron Maltego, Metagoof, Foca, Shodan, The Harvester, Recon-NG, Spiderfoot, Intel Techniques	Inteligencia Artificial	Revista Vínculos	(Hernández, *et al.,* 2018)
23	Open-Source Intelligence Methods and Tools	En este texto se incluyen recursos OSINT que pueden ser utilizados para identificar riesgos y recopilar inteligencia de fuentes públicas en línea. Además de aprender a utilizar los recursos de OSINT para realizar ataques de Ingeniería social.	OSINT	Libro	(Hassan & Hijazi, 2018)
24	Evaluación de riesgos: Estudio de la fuga de datos en los sitios web del Ecuador	En este trabajo se evaluó los riesgos que tiene la fuga de datos en los sitios web en Ecuador. Para el estudio se escogieron entidades como: La banca, administradores públicos, empresas y universidades, donde como resultados se pudo comprobar que existen altos niveles de fuga de datos de la información en las diferentes empresas públicas y privadas.	Gestión de riesgos	Revista de Producción, Ciencias e Investigación	(Dávila & Pacheco, 2017)
25	La brecha existente en la ciberseguridad en Honduras	Para el desarrollo de la investigación se hizo uso de tres reportes específicos sobre Ciberseguridad, donde el instrumento básico para medir el compromiso de los países con la seguridad cibernética fue el Global Cybersecurity Index. Los resultados demostraron que América Latina no cuenta con suficientes avances en la materia, por lo tanto, el índice es 0, ubicándose en los últimos lugares a nivel mundial.	Ciberseguridad	Revista Innovare – Ciencia y tecnología	(Raudales, 2017)

Anexo 1 Revisión bibliográfica.
Fuente: Los autores.

ANEXO 2. FORMATO DE LA ENTREVISTA REALIZADA A LA UNIDAD DE TECNOLOGÍA

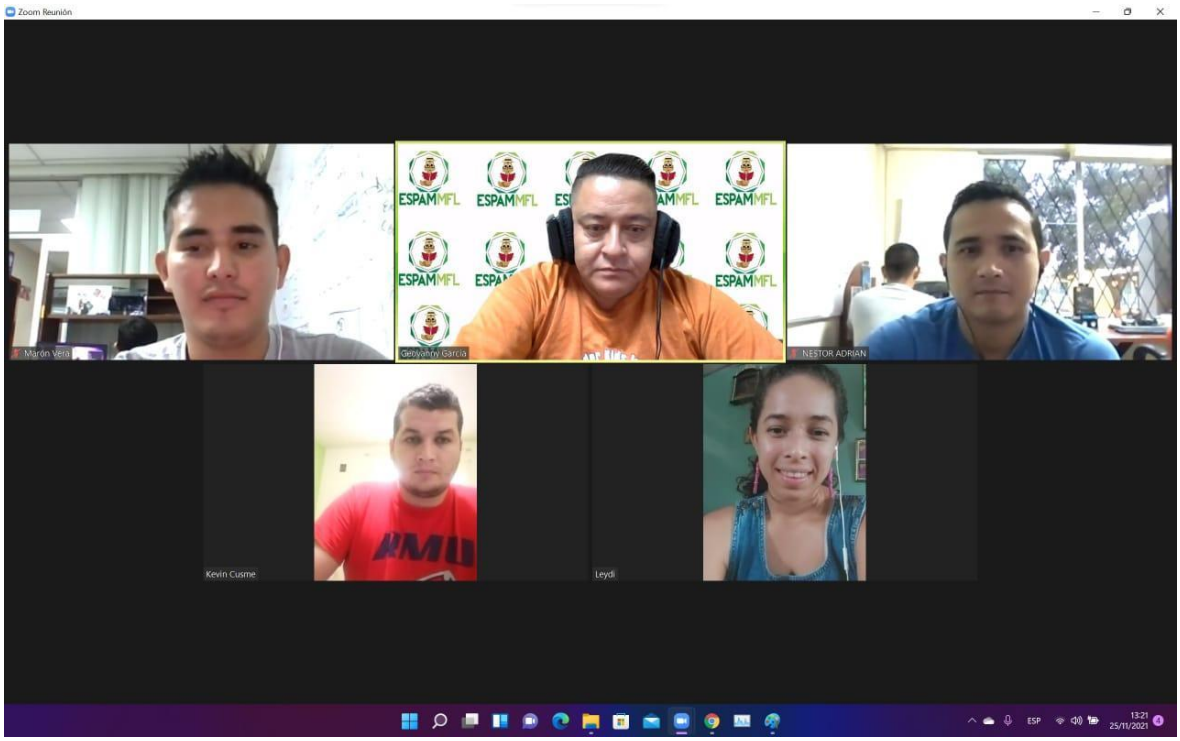
ESPAM MFL
ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ
Coordinación General de POSGRADO
MTI Maestría en Tecnologías de la Información

Entrevista dirigida a los miembros de la unidad de tecnología de la ESPAM MFL, con la finalidad de conocer el estado en que se encuentren los sistemas de información de la institución y los sistemas de seguridad empleados.

1. **¿Quién es responsable de instalar y mantener los sistemas de seguridad en los servidores/computadoras de la institución?**
   En los servidores área DMZ el responsable es Cesar Moreira Zambrano
2. **¿Con qué frecuencia se actualiza el software antivirus?**
   Dependiendo de la notificación del sistema operativo
3. **¿Cuenta la institución con IDS e IPS?**
   Si IDS-IPS y SOC
4. **¿La Institución invierte presupuesto en ciberseguridad?**
   No
5. **¿El cuerpo docente y el personal de TI tienen la formación que necesitan para prevenir errores de seguridad informática?**
   No
6. **¿El cuerpo docente y el personal de TI en general son capaces de identificar un virus/malware?**
   El personal de TI si está capacitado
7. **¿Se gestiona el uso seguro de redes sociales en horario laboral dentro de la institución?**
   Si
8. **¿Los docentes y el personal del departamento de TI hacen un uso adecuado de las contraseñas, correo institucional y datos personales?**
   Existe un modelo de SGSI donde se definen los procedimientos de utilización de claves y mecanismos de utilización de cuentas de correo electrónico institucional.
9. **¿Cuentan con un plan de prevención de riesgos informáticos?**
   No
   Si, está dentro del SGSI.
10. **¿Cuentan con políticas de distribución y difusión de la información dentro de la institución?**
    No

Anexo 2 Entrevista realizada a los miembros de la Unidad de Tecnología de la ESPAM MFL.
Fuente: Los autores.

ANEXO 3. APLICACIÓN DE LA ENTREVISTA



Anexo 3 Entrevista virtual con los miembros de la Unidad de Tecnología de la ESPAM MFL.
Fuente: Los autores.

ANEXO 4. INFORMES TÉCNICOS EXTRAÍDOS POR VARIAS HERRAMIENTAS UTILIZADAS

Hunter.io

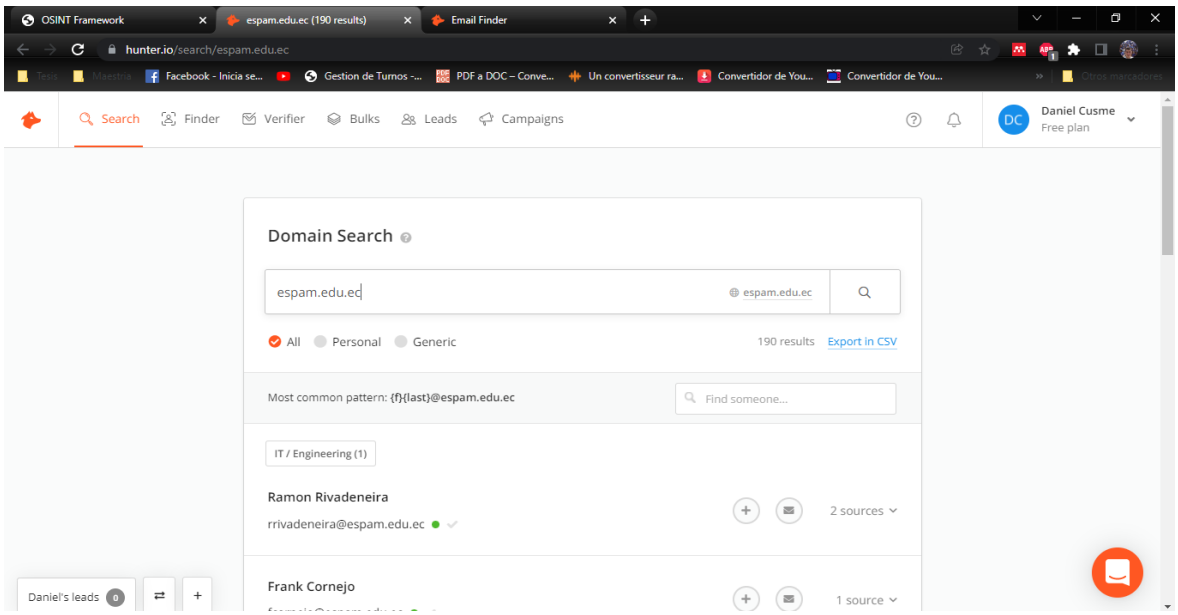


Figura 4.3. Ejecución de la herramienta Hunter.io bajo el dominio de la ESPAM MFL
Fuente: Los autores

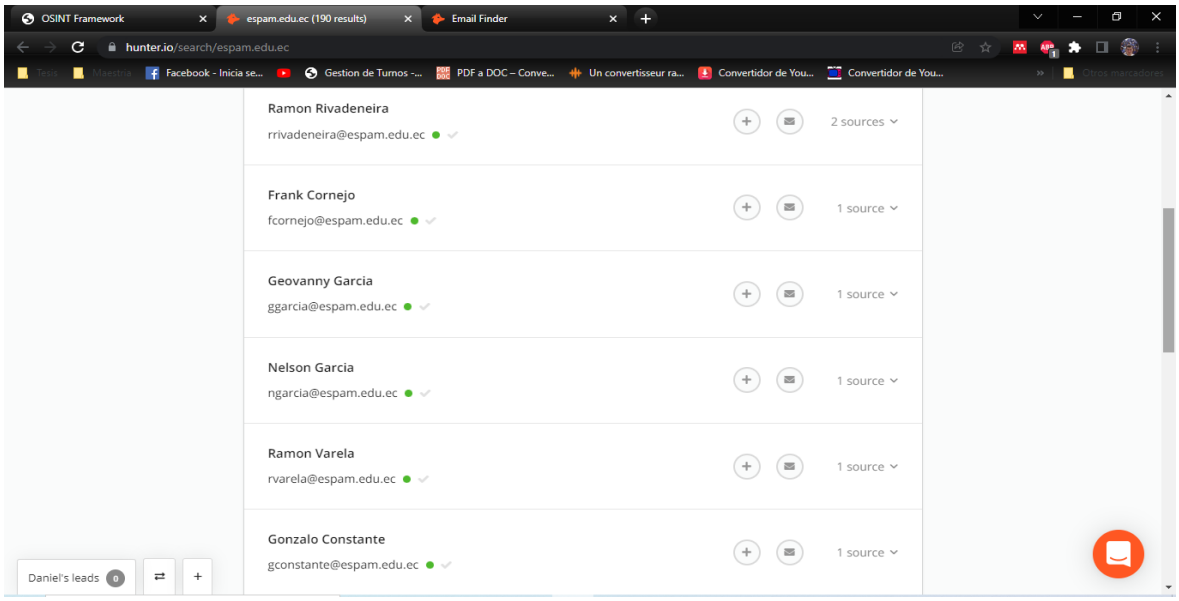


Figura 4.4. Verificación de correos electrónicos bajo el dominio de la ESPAM MFL
Fuente: Los Autores

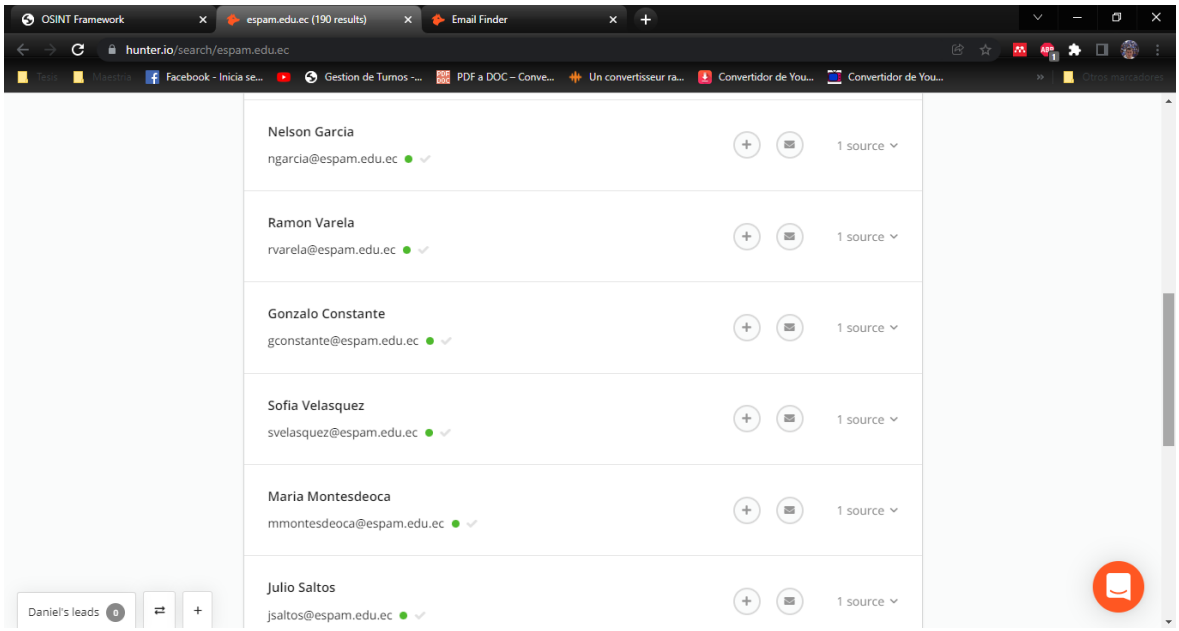


Figura 4.5. Verificación de correos electrónicos bajo el dominio de la ESPAM MFL
Fuente: Los Autores

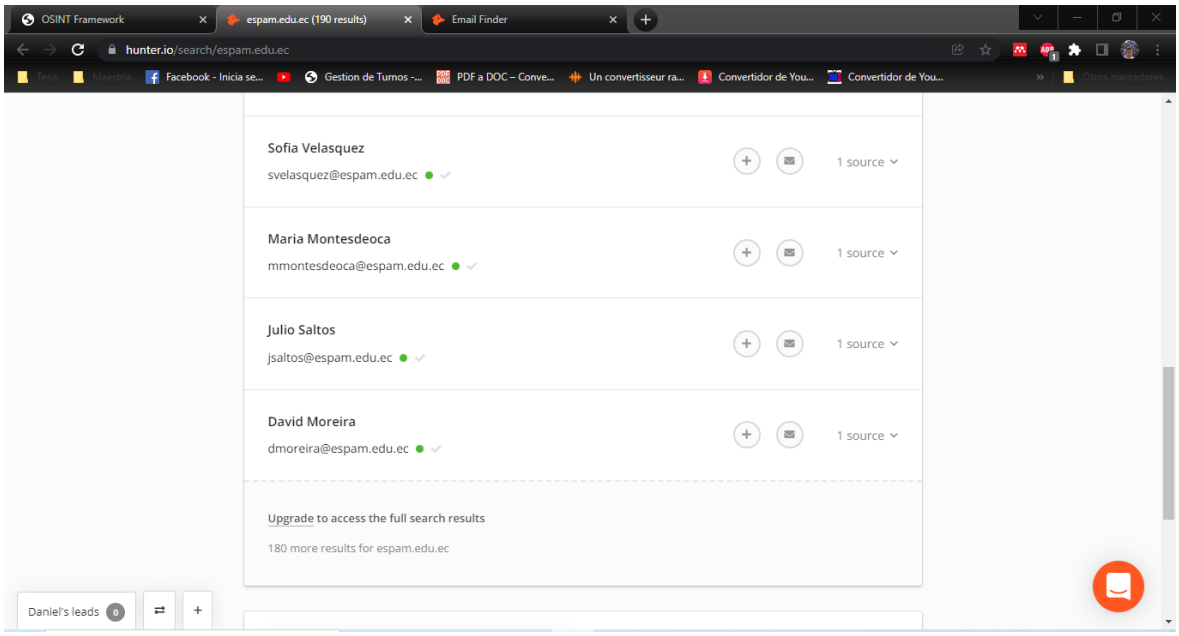


Figura 4.6. Verificación de correos electrónicos bajo el dominio de la ESPAM MFL
Fuente: Los Autores

Domain Dossier

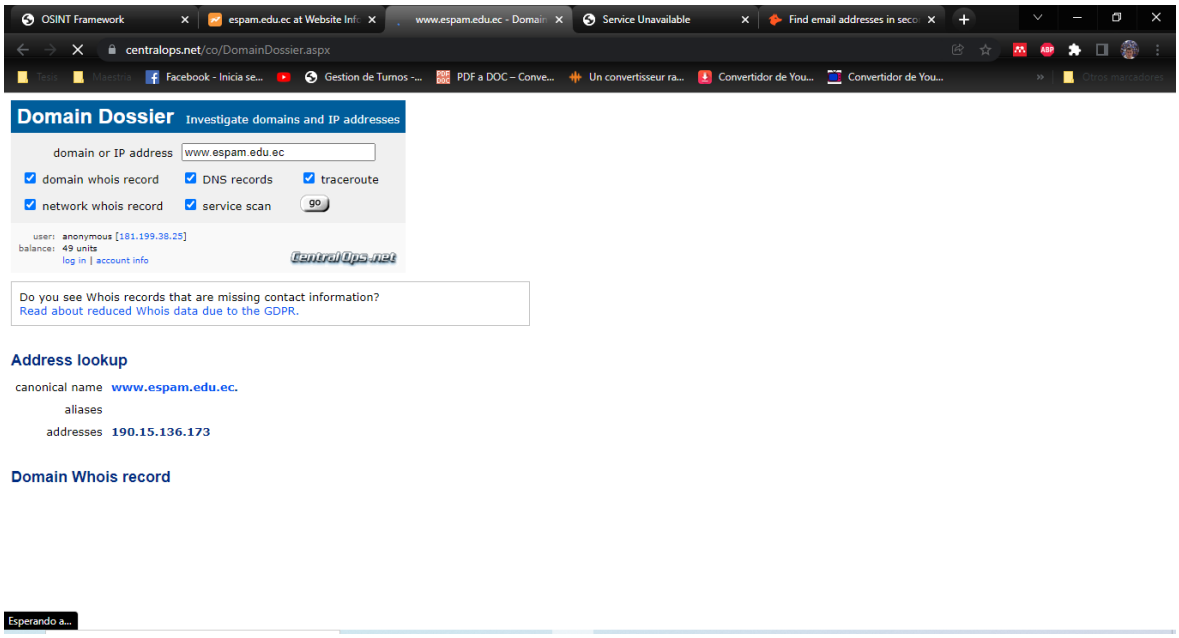


Figura 4.7. Ejecución de la herramienta Domain Dossier bajo el dominio de la ESPAM MFL
Fuente: Los Autores

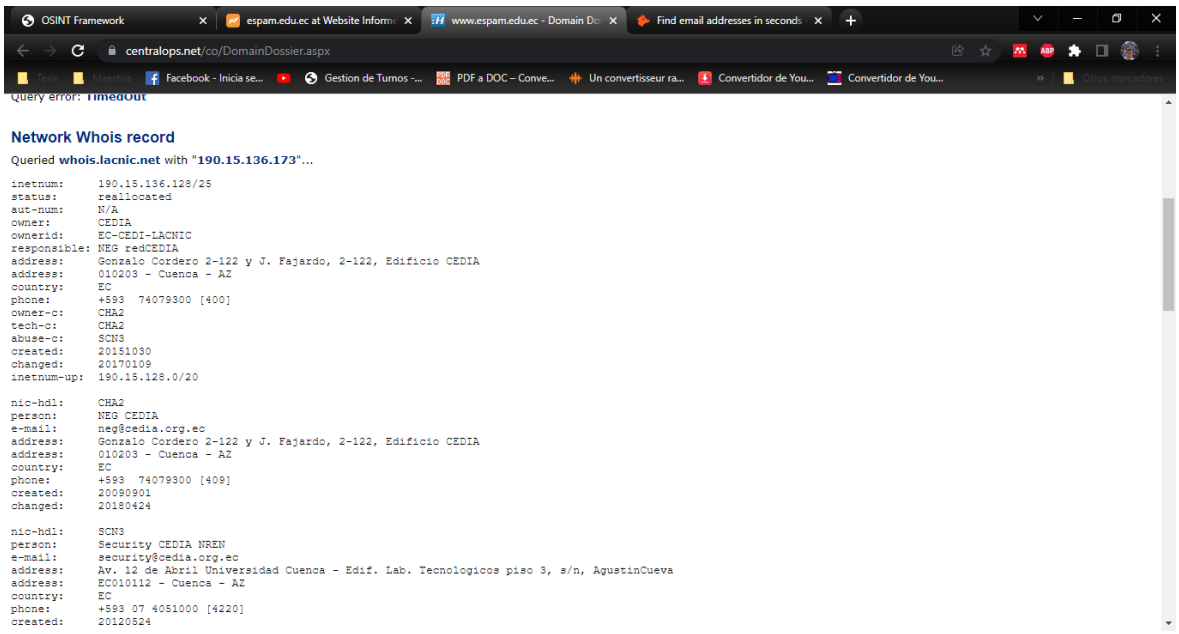


Figura 4.8. Datos del servidor de la ESPAM MFL escaneado por la herramienta Domain Dossier
Fuente: Los autores

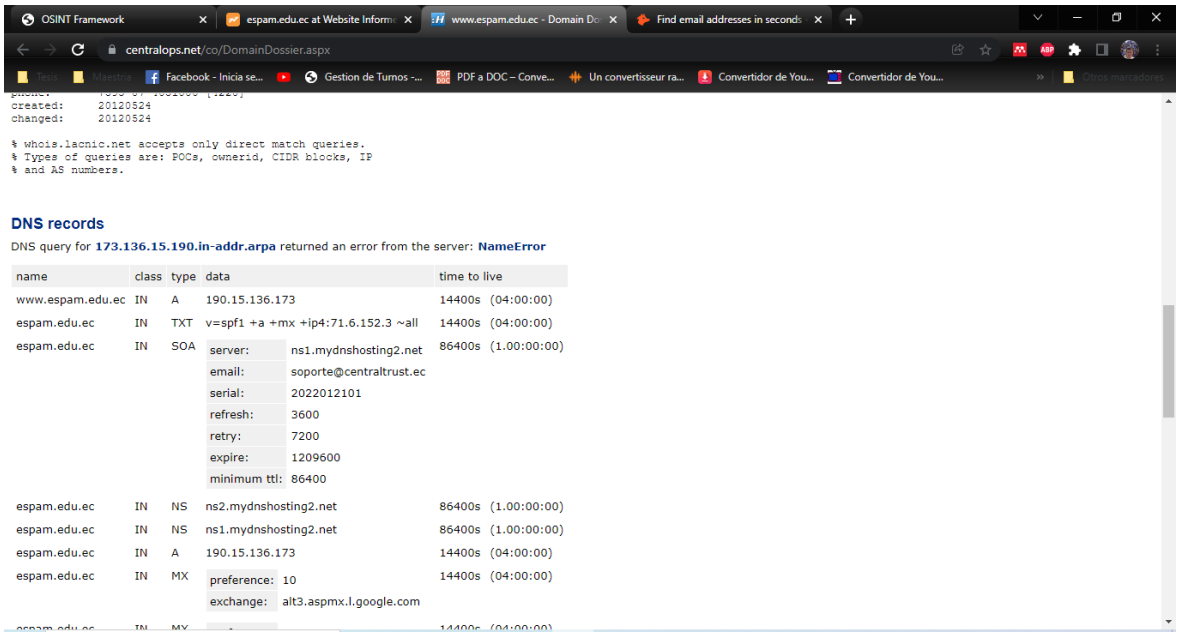


Figura 4.9. Escaeno del registro del DNS
Fuente: Los autores

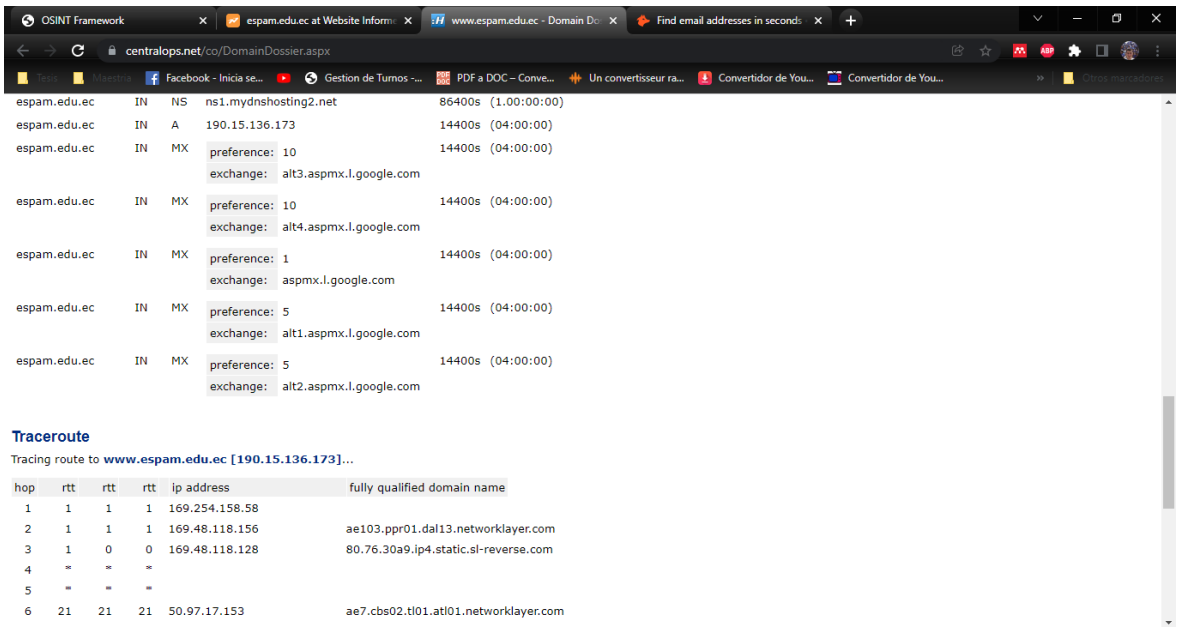


Figura 4.10. Escaneo del tráfico generado por la red
Fuente: Los autores

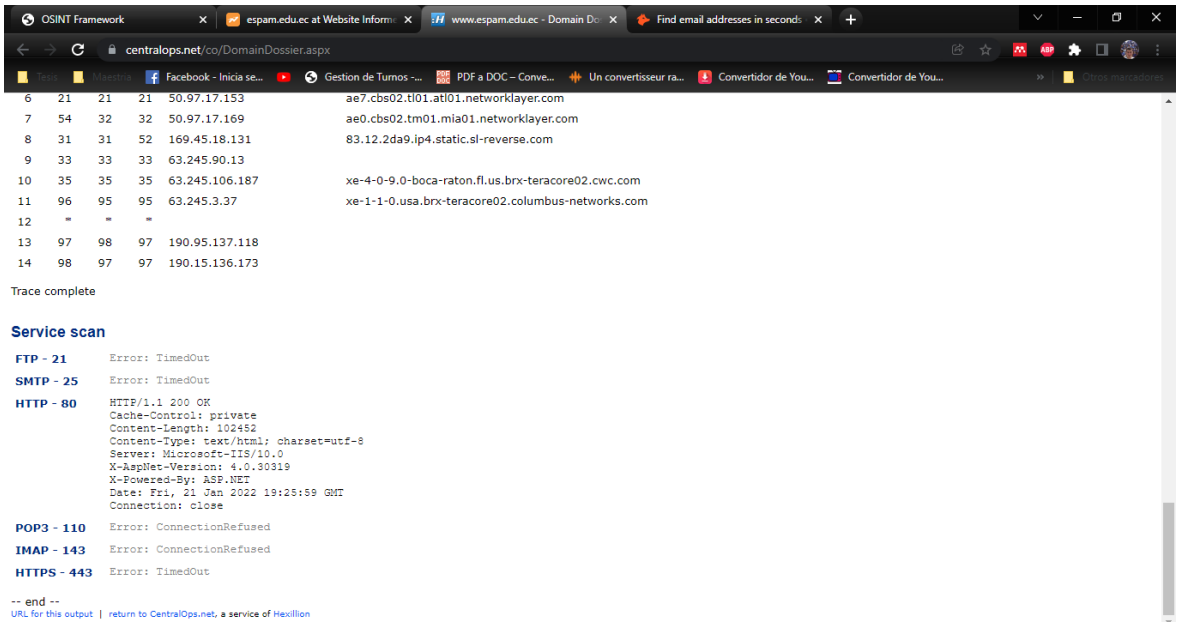


Figura 4.11. Escaneo de los puertos del servidor
Fuente: Los autores

Website Informer

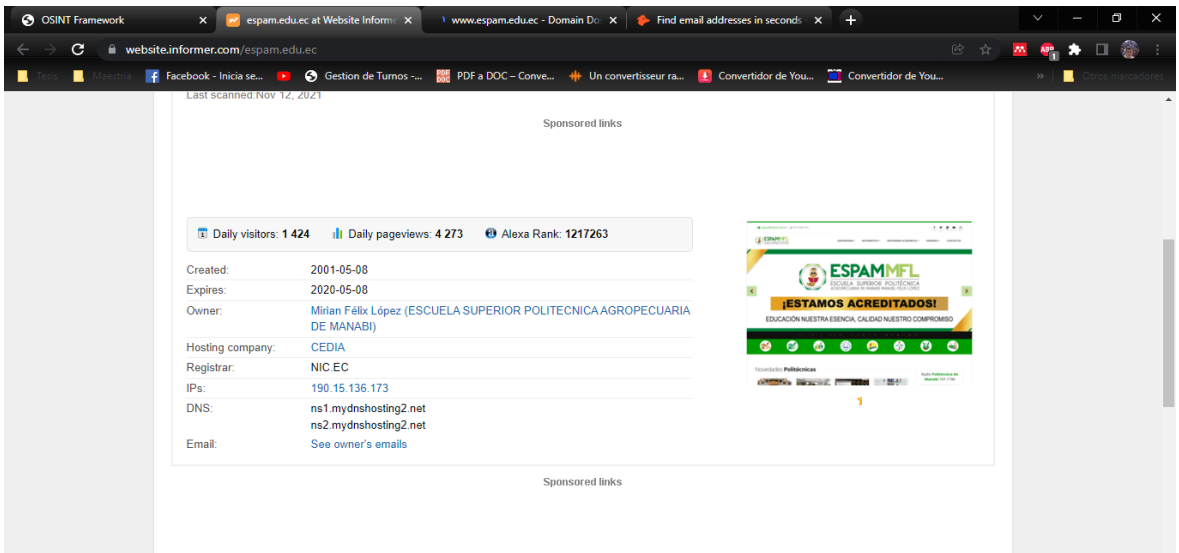


Figura 4.12. Ejecución de la herramienta Website informer bajo el dominio de la ESPAM MFL
Fuente: Los autores

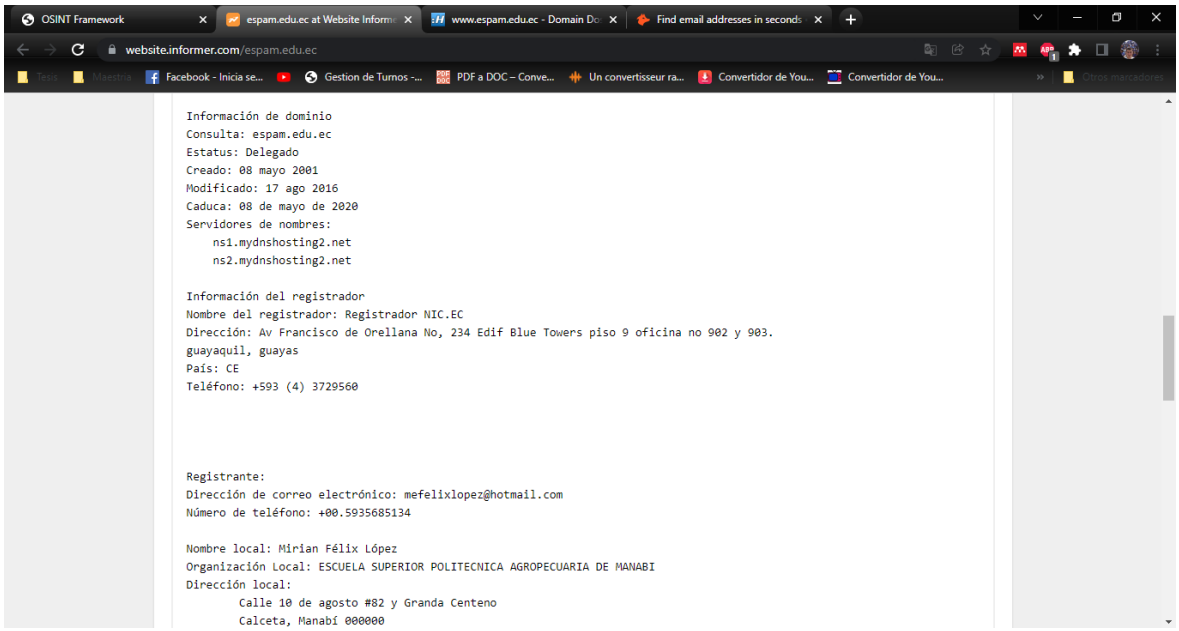


Figura 4.13. Resultados del escaneo de vulnerabilidades con la herramienta Website informer
Fuente: Los autores

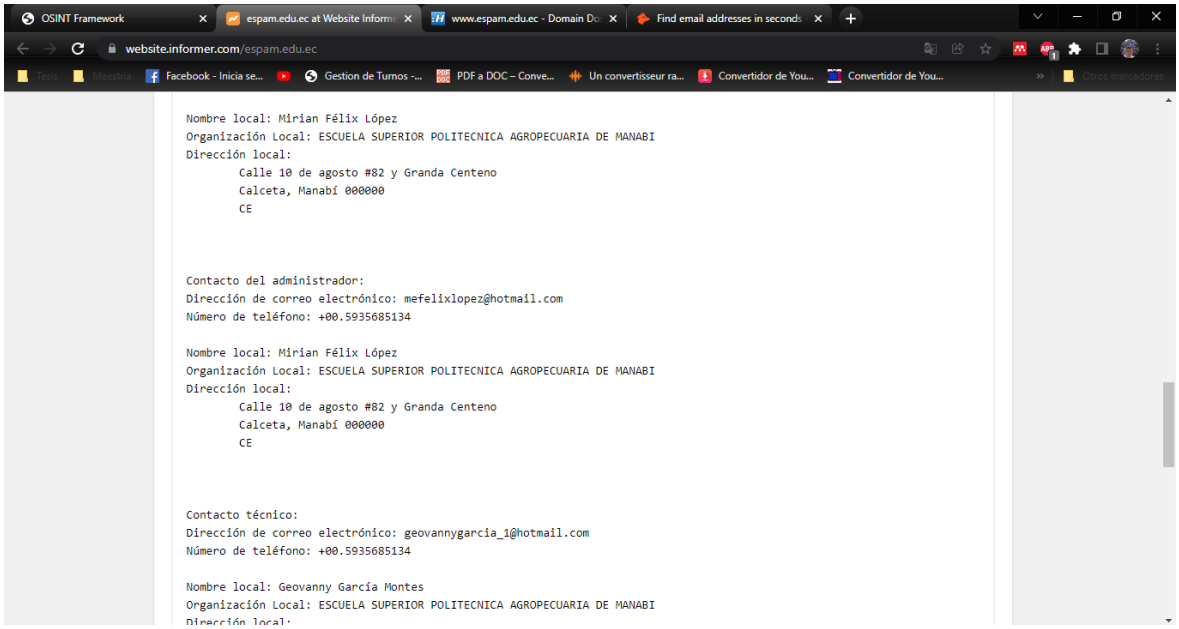


Figura 4.14. Resultados del escaneo de vulnerabilidades con la herramienta Website informer
Fuente: Los autores

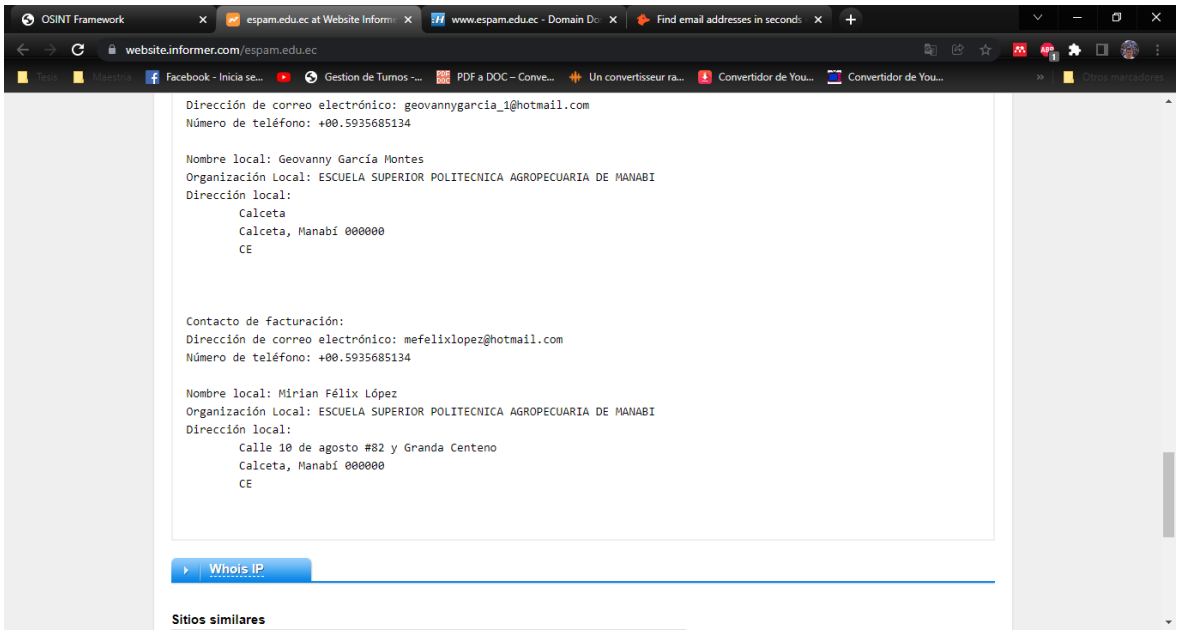


Figura 4.15. Resultados del escaneo de vulnerabilidades con la herramienta Website informer
Fuente: Los autores

Shodan.io

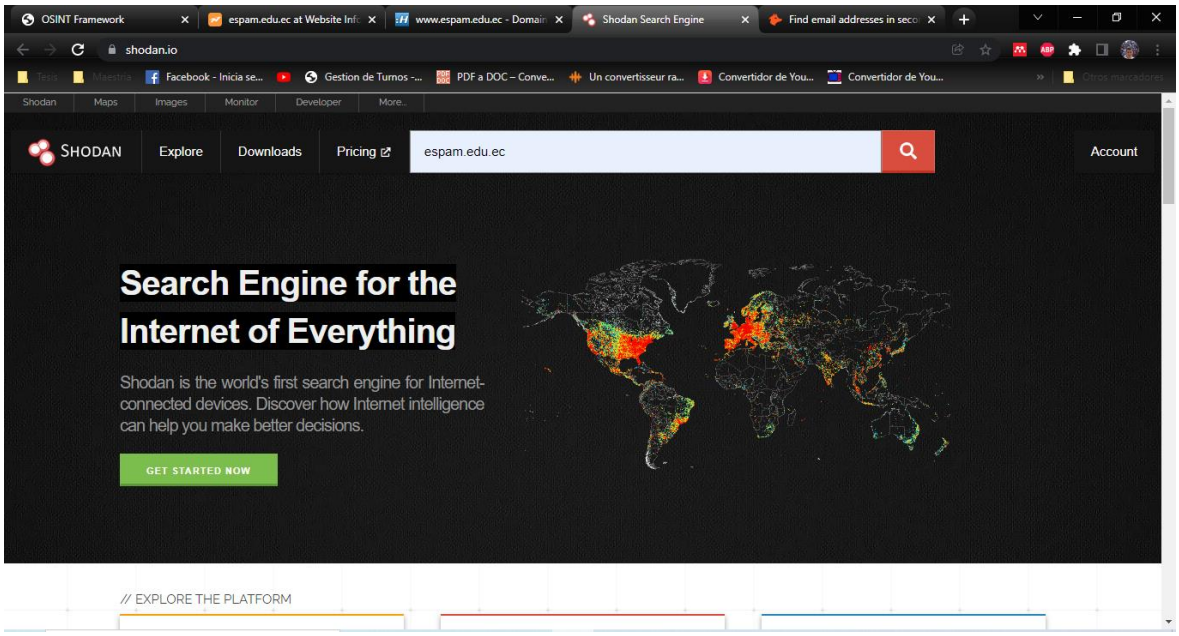


Figura 4.16. Ejecución de la herramienta Shodan bajo el dominio de la ESPAM MFL
Fuente: Los autores

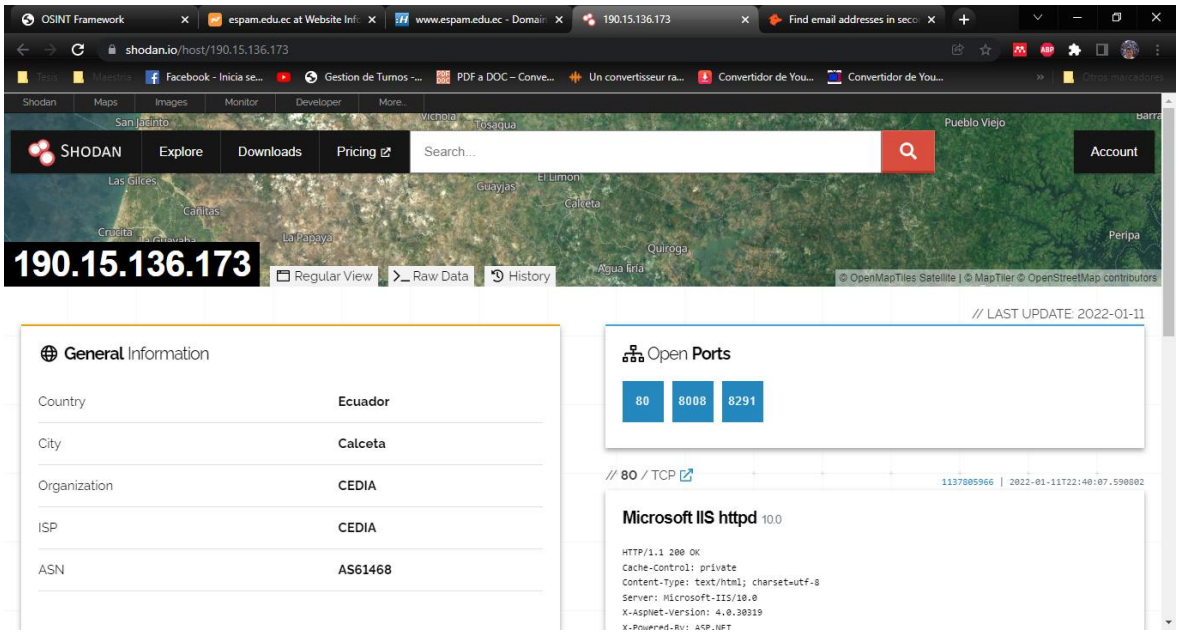


Figura 4.17. Resultados del escaneo de vulnerabilidades con la herramienta Shodan
Fuente: Los autores

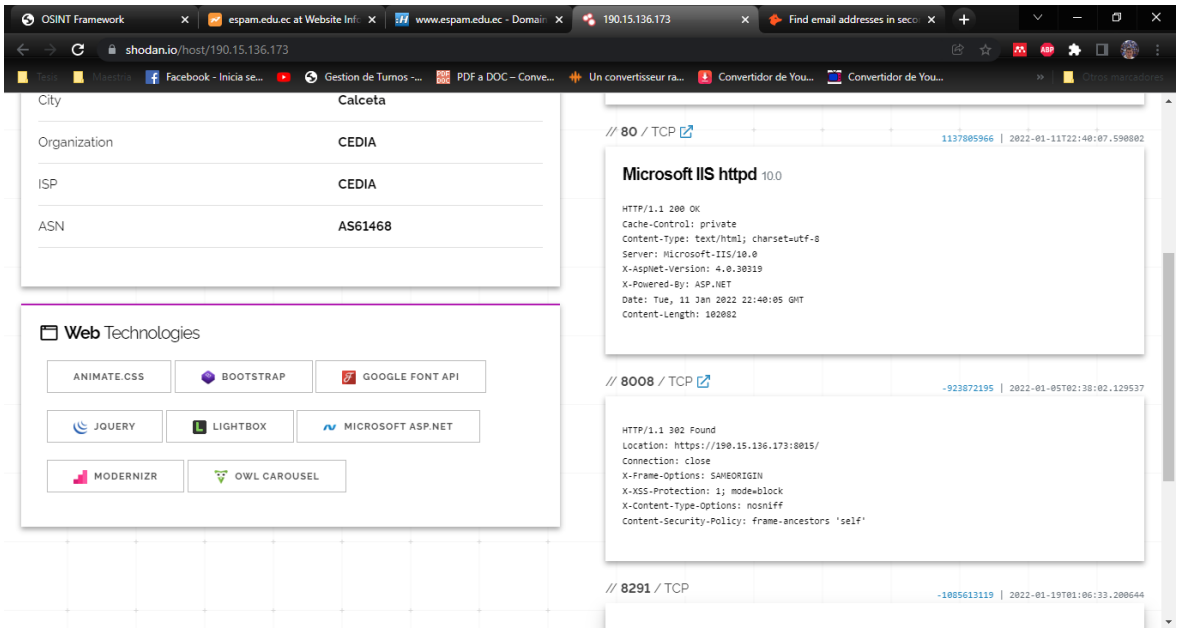


Figura 4.18. Resultados del escaneo de vulnerabilidades con la herramienta Shodan
Fuente: Los autores

Spyse

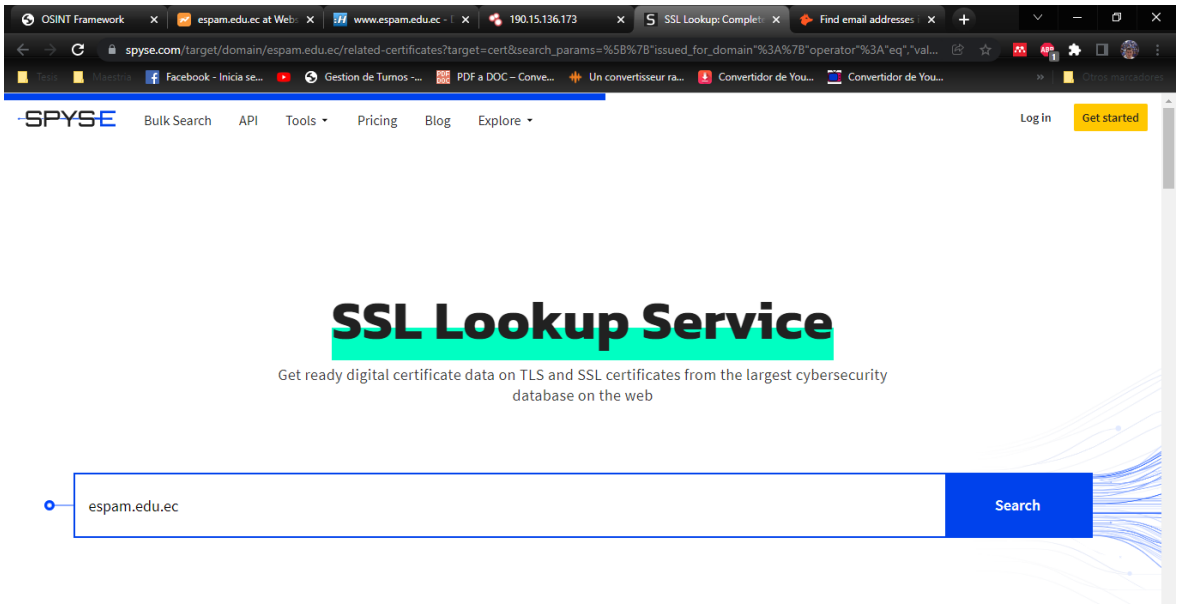


Figura 4.19. Ejecución de la herramienta Spyse bajo el dominio de la ESPAM MFL
Fuente: Los autores

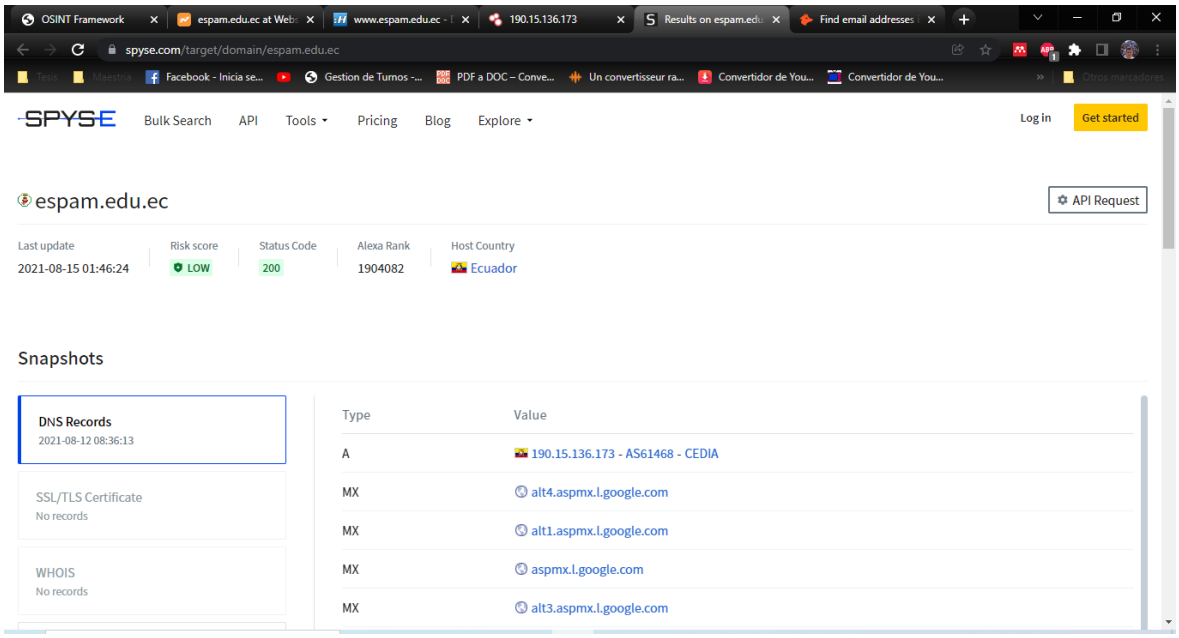


Figura 4.20. Resultados del escaneo de vulnerabilidades con la herramienta Spyse
Fuente: Los autores

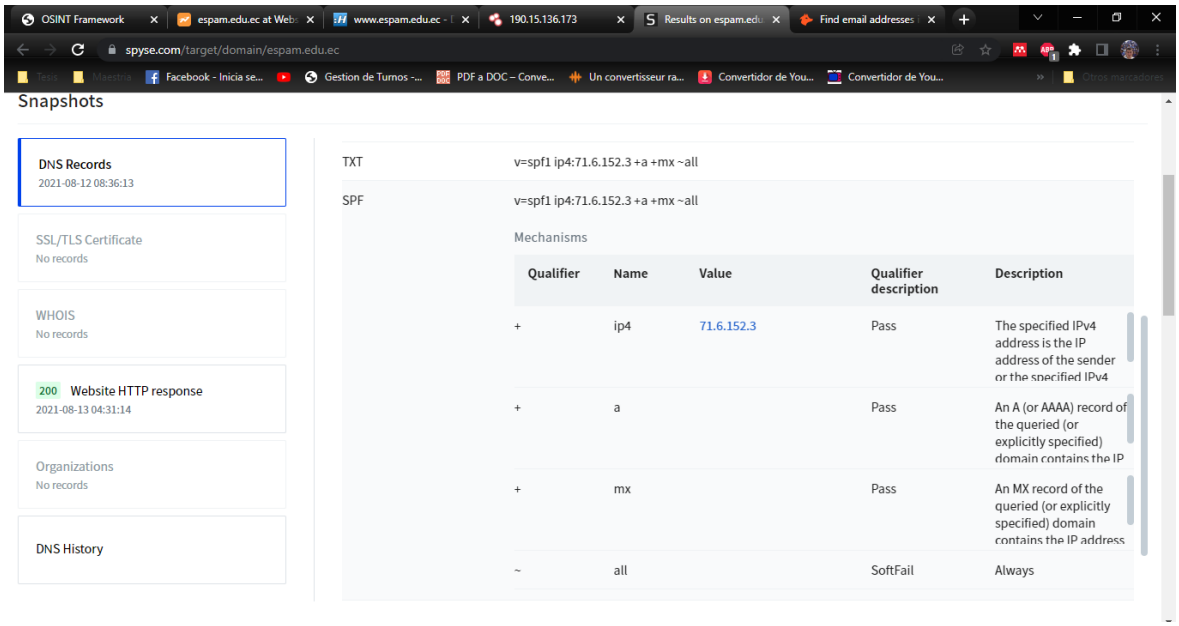


Figura 4.21. Resultados del escaneo de vulnerabilidades con la herramienta Spyse
Fuente: Los autores

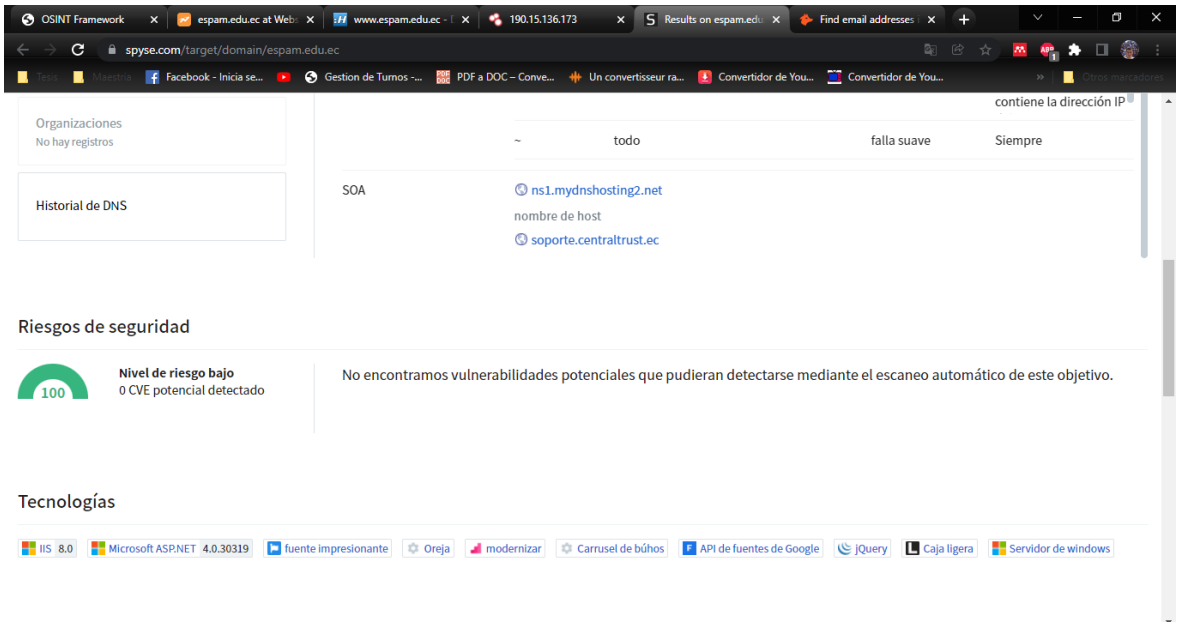


Figura 4.22. Resultados del escaneo de vulnerabilidades con la herramienta Spyse
Fuente: Los autores

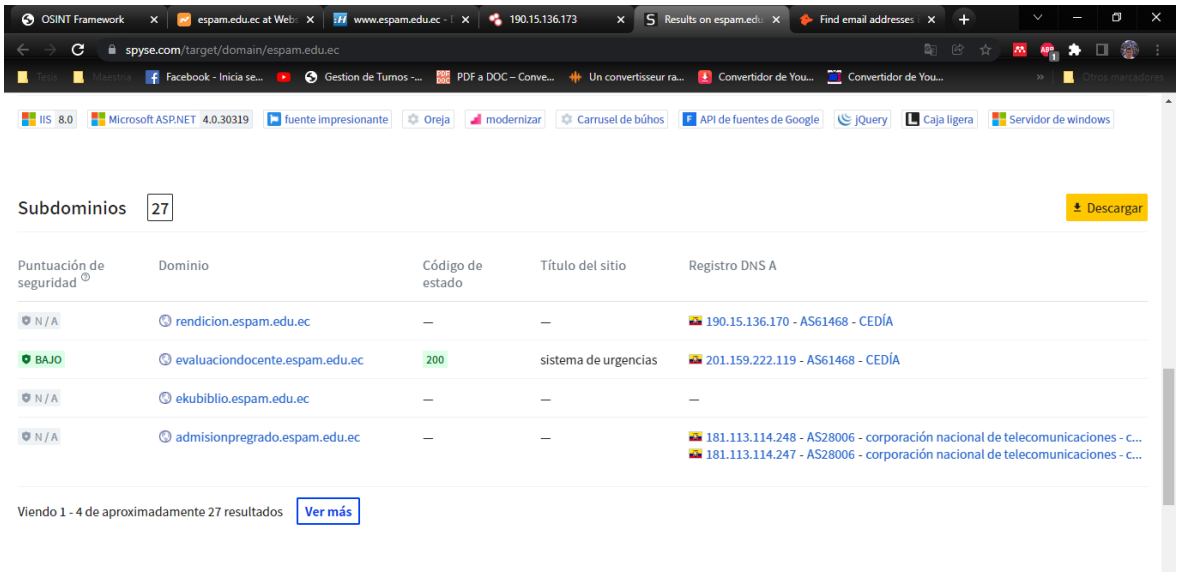


Figura 4.23. Resultados del escaneo de vulnerabilidades con la herramienta Spyse
Fuente: Los autores

Siteliner

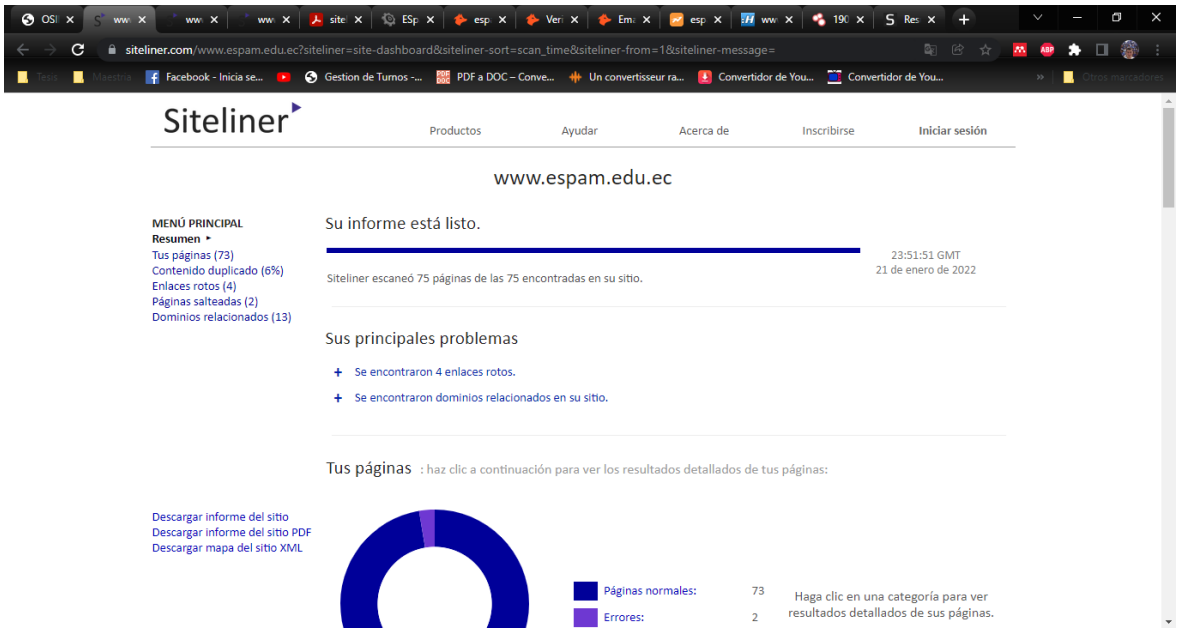


Figura 4.24. Ejecución de la herramienta Siteliner bajo el dominio de la ESPAM MFL
Fuente: Los autores

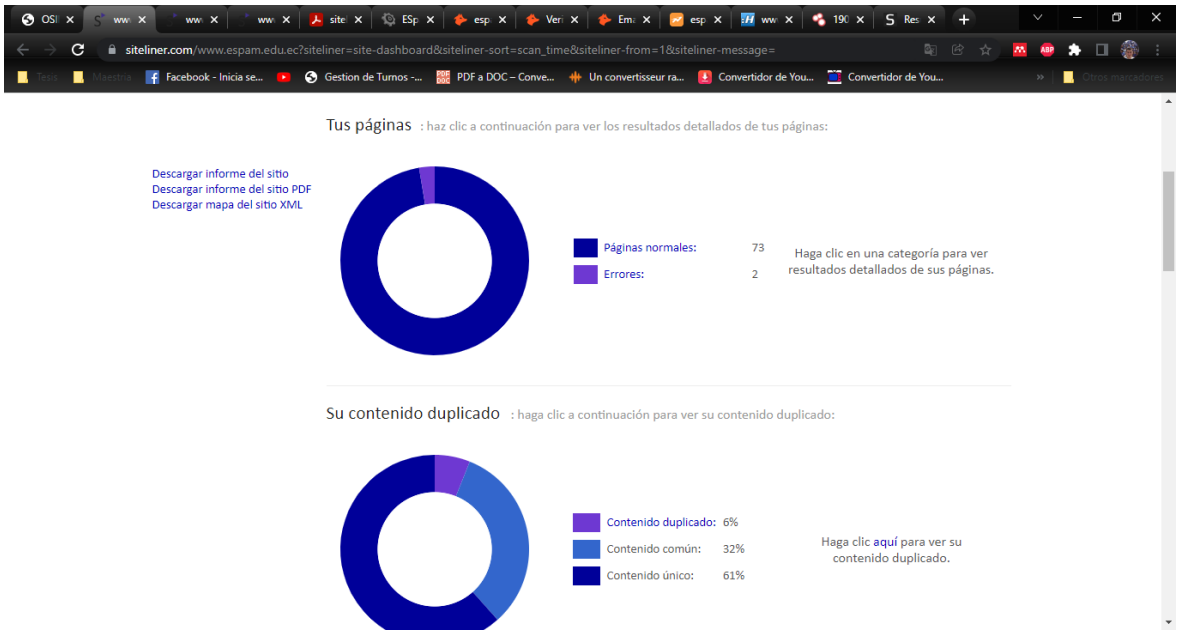


Figura 4.25. Resultados del escaneo de vulnerabilidades con la herramienta Siteliner
Fuente: Los autores

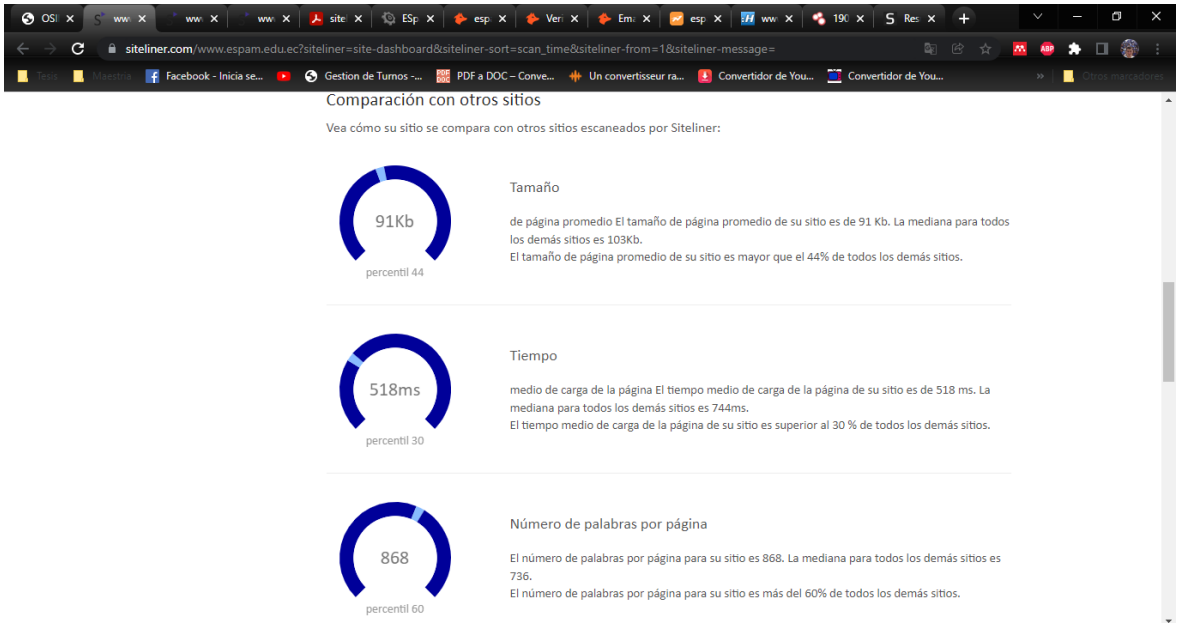


Figura 4.26 .Resultados del escaneo de vulnerabilidades con la herramienta Siteliner
Fuente: Los autores

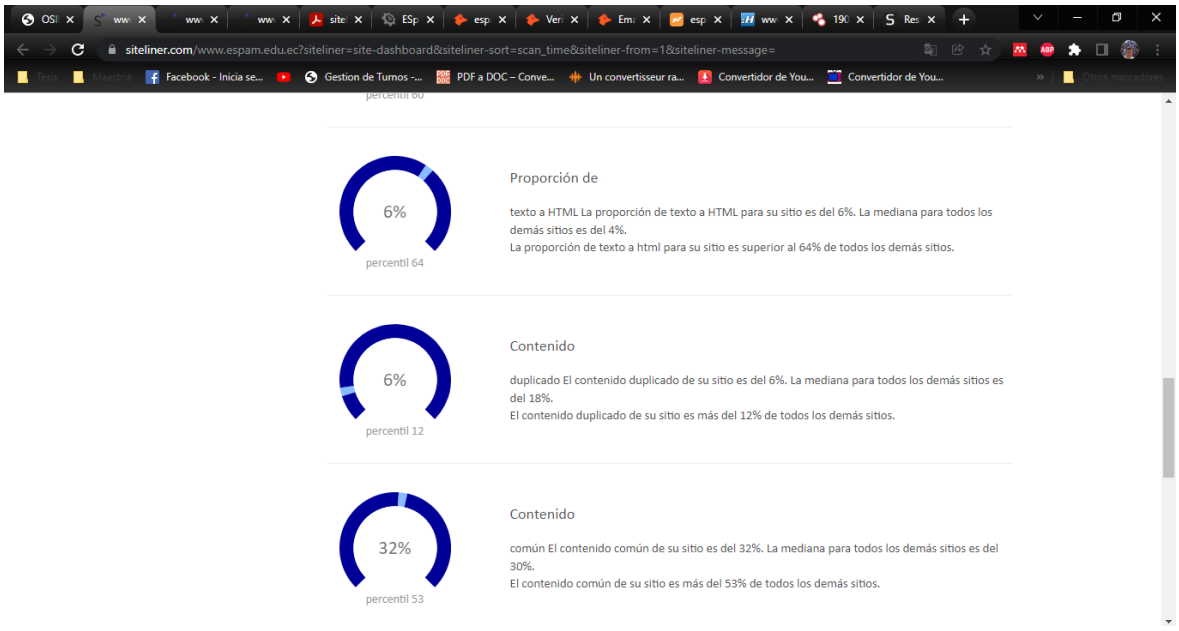


Figura 4.27. Resultados del escaneo de vulnerabilidades con la herramienta Siteliner
Fuente: Los autores

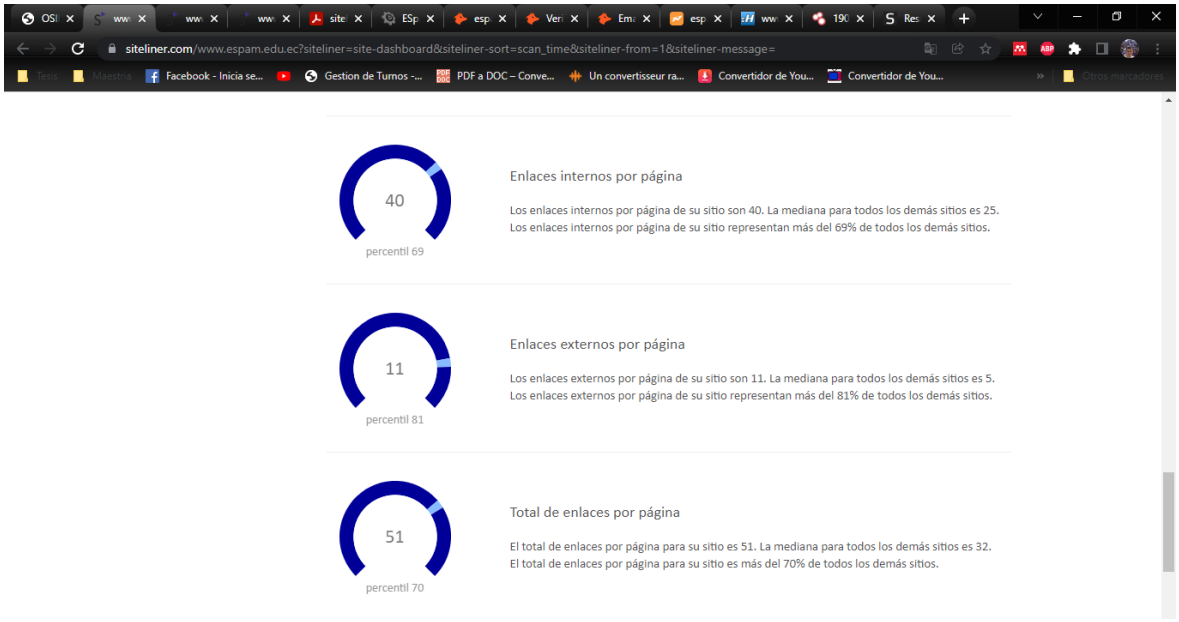


Figura 4.28. Resultados del escaneo de vulnerabilidades con la herramienta Siteliner
Fuente: Los autores

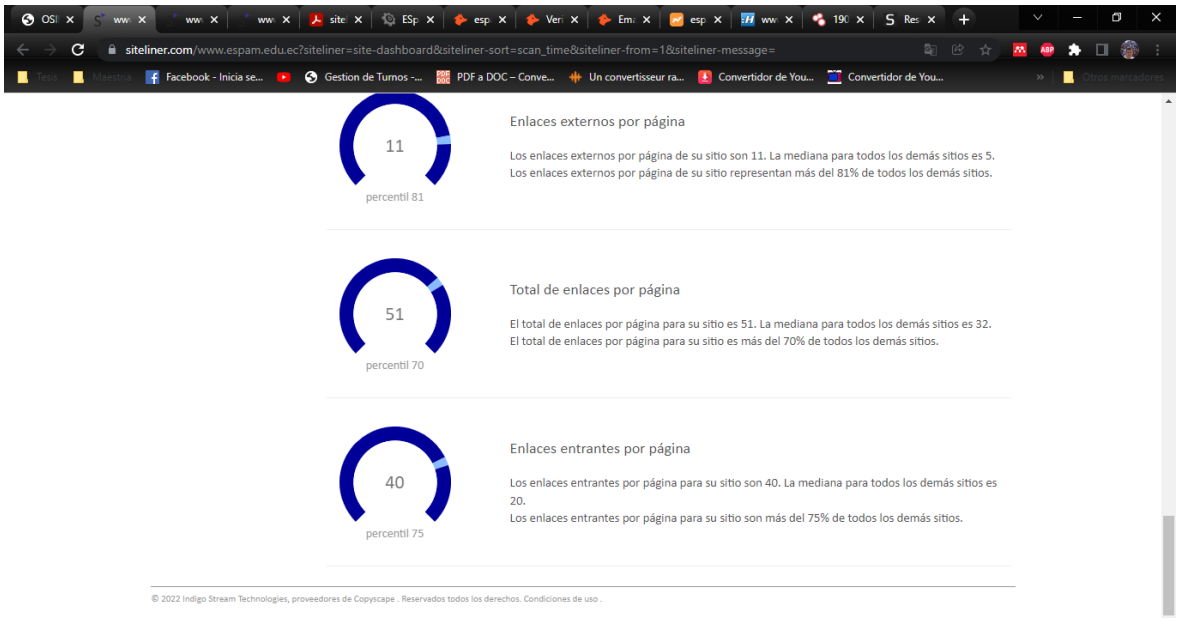
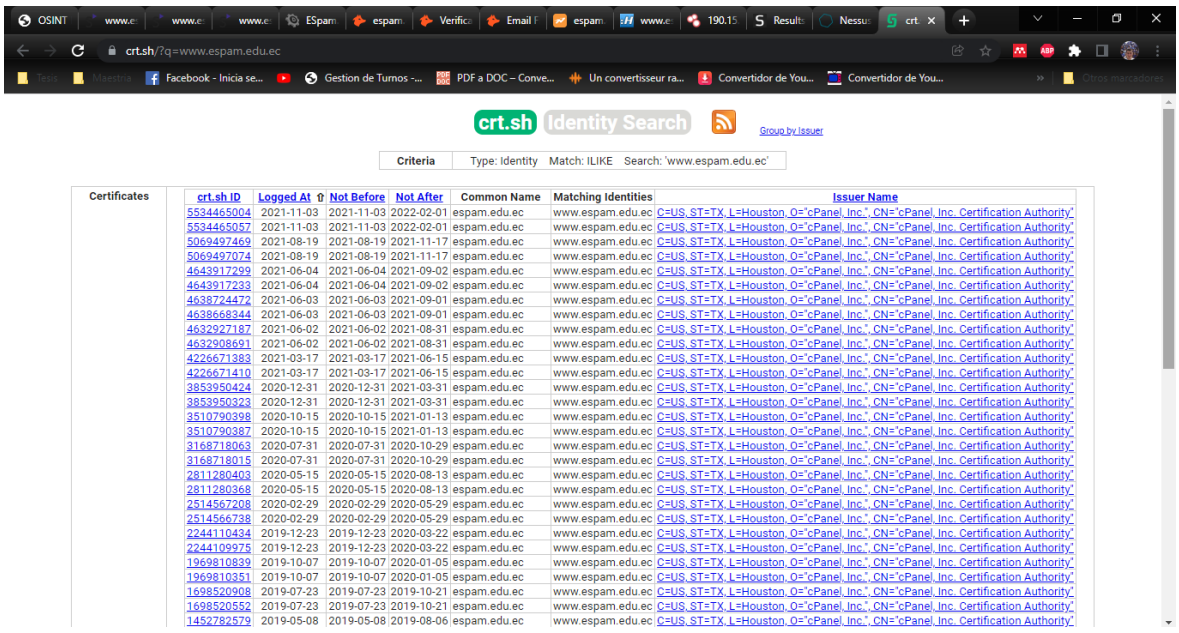


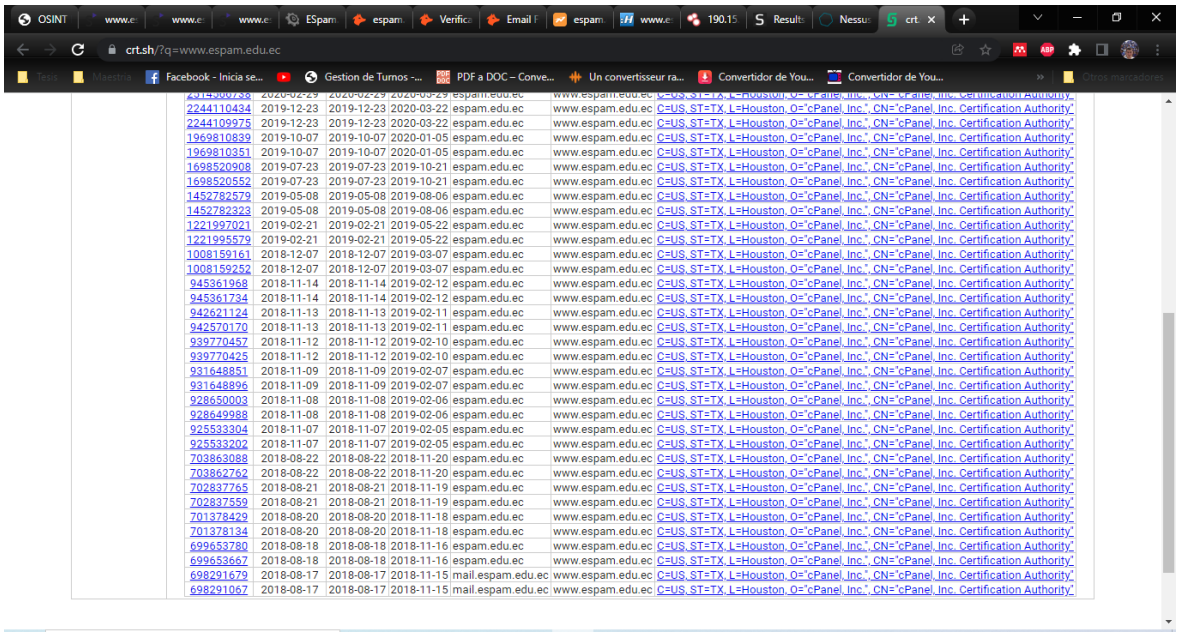
Figura 4.29. Resultados del escaneo de vulnerabilidades con la herramienta Siteliner
Fuente: Los autores

Crt.sh



crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
5534465004	2021-11-03	2021-11-03	2022-02-01	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
5534465057	2021-11-03	2021-11-03	2022-02-01	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
5069497469	2021-08-19	2021-08-19	2021-11-17	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
5069497074	2021-08-19	2021-08-19	2021-11-17	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
4643917299	2021-06-04	2021-06-04	2021-09-02	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
4643917233	2021-06-04	2021-06-04	2021-09-02	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
4638724472	2021-06-03	2021-06-03	2021-09-01	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
4638668344	2021-06-03	2021-06-03	2021-09-01	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
4632927187	2021-06-02	2021-06-02	2021-08-31	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
4632908691	2021-06-02	2021-06-02	2021-08-31	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
4226671383	2021-03-17	2021-03-17	2021-06-15	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
4226671410	2021-03-17	2021-03-17	2021-06-15	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
3853950424	2020-12-31	2020-12-31	2021-03-31	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
3853950323	2020-12-31	2020-12-31	2021-03-31	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
3510790398	2020-10-15	2020-10-15	2021-01-13	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
3510790387	2020-10-15	2020-10-15	2021-01-13	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
3168718063	2020-07-31	2020-07-31	2020-10-29	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
3168718015	2020-07-31	2020-07-31	2020-10-29	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2811280403	2020-05-15	2020-05-15	2020-08-13	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2811280368	2020-05-15	2020-05-15	2020-08-13	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2514567208	2020-02-29	2020-02-29	2020-05-29	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2514566738	2020-02-29	2020-02-29	2020-05-29	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2244110434	2019-12-23	2019-12-23	2020-03-22	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2244109975	2019-12-23	2019-12-23	2020-03-22	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1969810839	2019-10-07	2019-10-07	2020-01-05	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1969810351	2019-10-07	2019-10-07	2020-01-05	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1698520908	2019-07-23	2019-07-23	2019-10-21	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1698520552	2019-07-23	2019-07-23	2019-10-21	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1452782579	2019-05-08	2019-05-08	2019-08-06	espam.edu.ec	www.espam.edu.ec	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

Figura 4.30. Ejecución de la herramienta Crt.sh bajo el dominio de la ESPAM MFL
Fuente: Los autores



2244110434	2019-12-23	2019-12-23	2020-03-22	espam.edu.ec	www.espam.edu.ec
2244109975	2019-12-23	2019-12-23	2020-03-22	espam.edu.ec	www.espam.edu.ec
1969810839	2019-10-07	2019-10-07	2020-01-05	espam.edu.ec	www.espam.edu.ec
1969810351	2019-10-07	2019-10-07	2020-01-05	espam.edu.ec	www.espam.edu.ec
1698520908	2019-07-23	2019-07-23	2019-10-21	espam.edu.ec	www.espam.edu.ec
1698520552	2019-07-23	2019-07-23	2019-10-21	espam.edu.ec	www.espam.edu.ec
1452782579	2019-05-08	2019-05-08	2019-08-06	espam.edu.ec	www.espam.edu.ec
1452782323	2019-05-08	2019-05-08	2019-08-06	espam.edu.ec	www.espam.edu.ec
1221997021	2019-02-21	2019-02-21	2019-05-22	espam.edu.ec	www.espam.edu.ec
1221995579	2019-02-21	2019-02-21	2019-05-22	espam.edu.ec	www.espam.edu.ec
1008159161	2018-12-07	2018-12-07	2019-03-07	espam.edu.ec	www.espam.edu.ec
1008159252	2018-12-07	2018-12-07	2019-03-07	espam.edu.ec	www.espam.edu.ec
945361968	2018-11-14	2018-11-14	2019-02-12	espam.edu.ec	www.espam.edu.ec
945361734	2018-11-14	2018-11-14	2019-02-12	espam.edu.ec	www.espam.edu.ec
942621124	2018-11-13	2018-11-13	2019-02-11	espam.edu.ec	www.espam.edu.ec
942570170	2018-11-13	2018-11-13	2019-02-11	espam.edu.ec	www.espam.edu.ec
939770457	2018-11-12	2018-11-12	2019-02-10	espam.edu.ec	www.espam.edu.ec
939770425	2018-11-12	2018-11-12	2019-02-10	espam.edu.ec	www.espam.edu.ec
931648851	2018-11-09	2018-11-09	2019-02-07	espam.edu.ec	www.espam.edu.ec
931648896	2018-11-09	2018-11-09	2019-02-07	espam.edu.ec	www.espam.edu.ec
928650003	2018-11-08	2018-11-08	2019-02-06	espam.edu.ec	www.espam.edu.ec
928649988	2018-11-08	2018-11-08	2019-02-06	espam.edu.ec	www.espam.edu.ec
925533304	2018-11-07	2018-11-07	2019-02-05	espam.edu.ec	www.espam.edu.ec
925533202	2018-11-07	2018-11-07	2019-02-05	espam.edu.ec	www.espam.edu.ec
703863088	2018-08-22	2018-08-22	2018-11-20	espam.edu.ec	www.espam.edu.ec
703862762	2018-08-22	2018-08-22	2018-11-20	espam.edu.ec	www.espam.edu.ec
702837765	2018-08-21	2018-08-21	2018-11-19	espam.edu.ec	www.espam.edu.ec
702837559	2018-08-21	2018-08-21	2018-11-19	espam.edu.ec	www.espam.edu.ec
701378429	2018-08-20	2018-08-20	2018-11-18	espam.edu.ec	www.espam.edu.ec
701378134	2018-08-20	2018-08-20	2018-11-18	espam.edu.ec	www.espam.edu.ec
699653780	2018-08-18	2018-08-18	2018-11-16	espam.edu.ec	www.espam.edu.ec
699653667	2018-08-18	2018-08-18	2018-11-16	espam.edu.ec	www.espam.edu.ec
698291679	2018-08-17	2018-08-17	2018-11-15	mail.espam.edu.ec	www.espam.edu.ec
698291067	2018-08-17	2018-08-17	2018-11-15	mail.espam.edu.ec	www.espam.edu.ec

Figura 4.31. Resultados del escaneo de vulnerabilidades con la herramienta Crt.sh
Fuente: Los autores

Zoom Eyes.

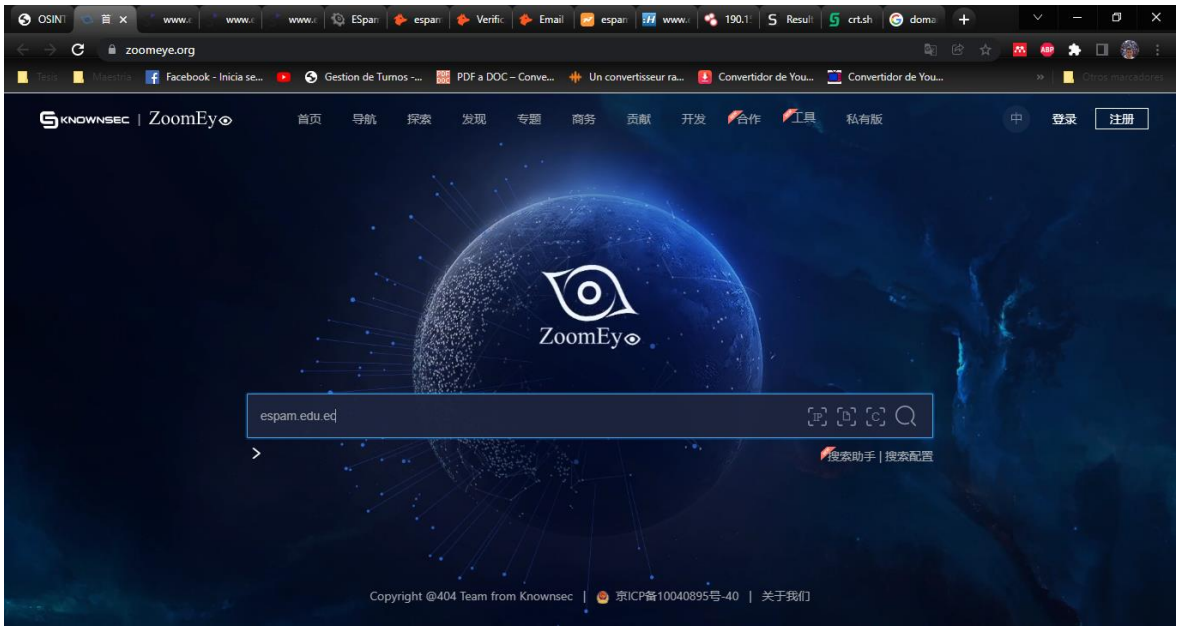


Figura 4.32. Ejecución de la herramienta Zoom Eyes bajo el dominio de la ESPAM MFL
Fuente: Los autores

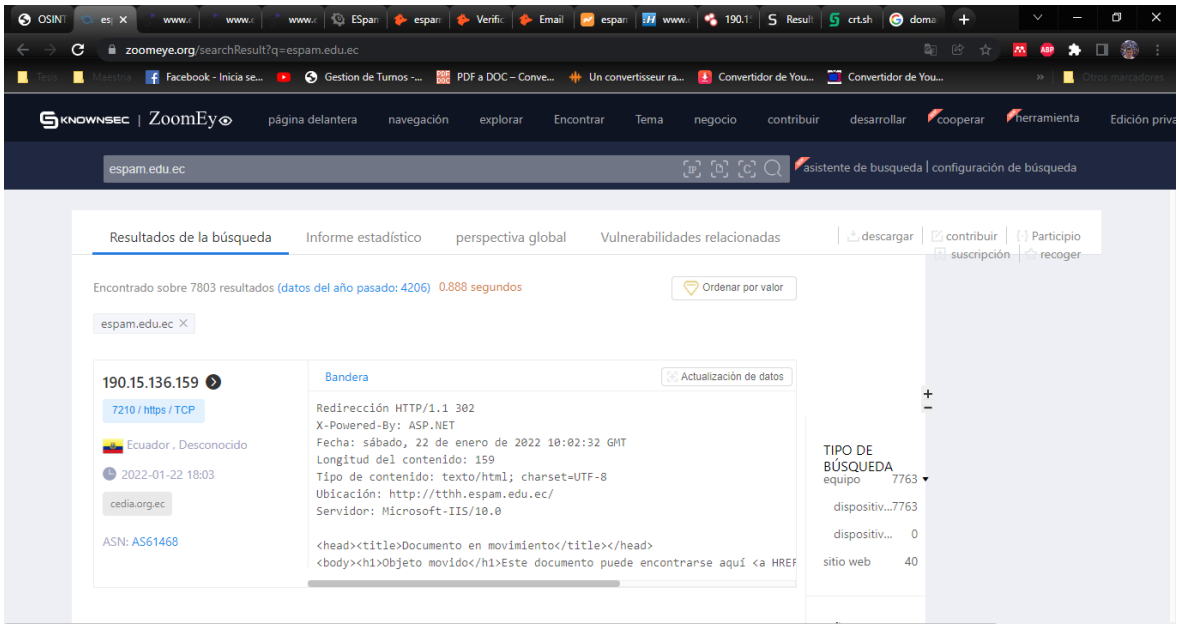


Figura 4.33. Resultados del escaneo de vulnerabilidades con la herramienta Zoom Eyes
Fuente: Los autores

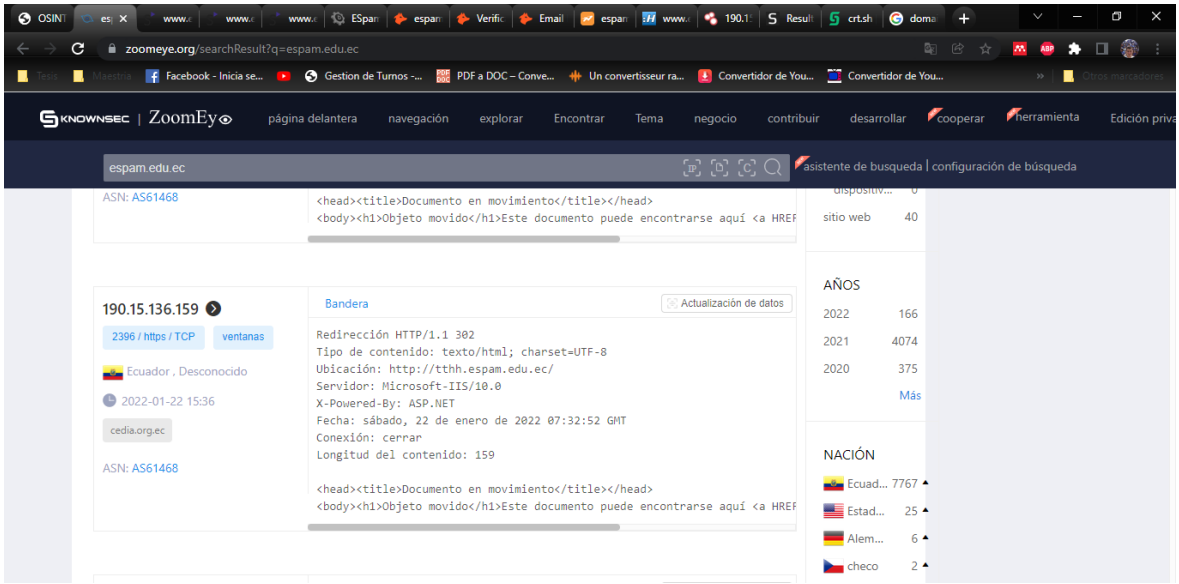


Figura 4.34. Resultados del escaneo de vulnerabilidades con la herramienta Zoom Eyes
Fuente: Los autores

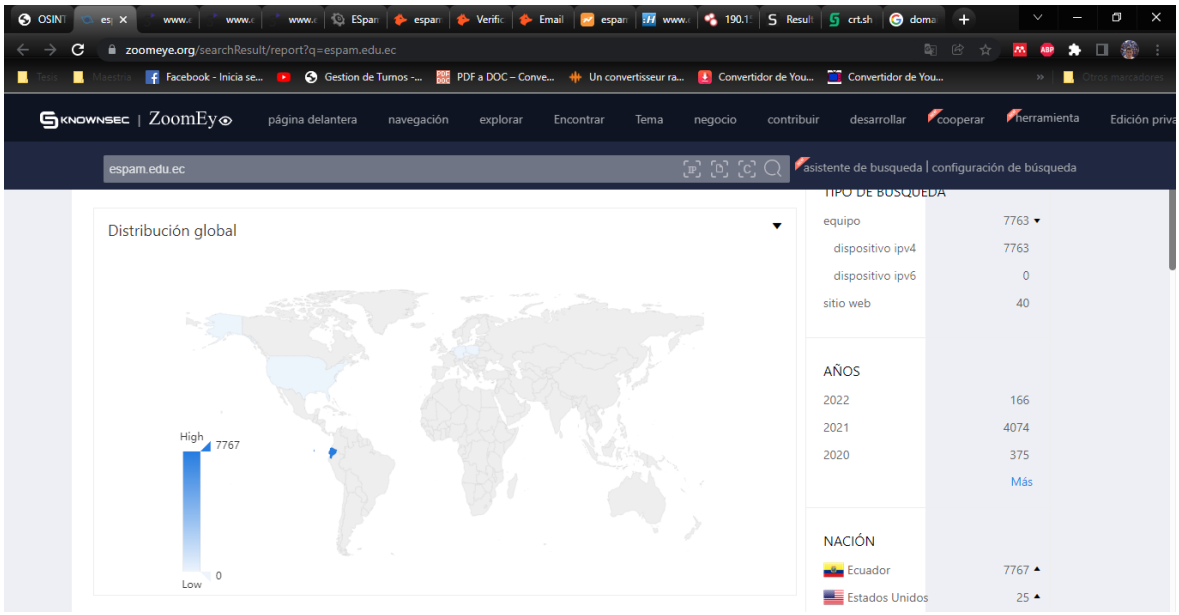


Figura 4.35. Resultados del escaneo de vulnerabilidades con la herramienta Zoom Eyes
Fuente: Los autores

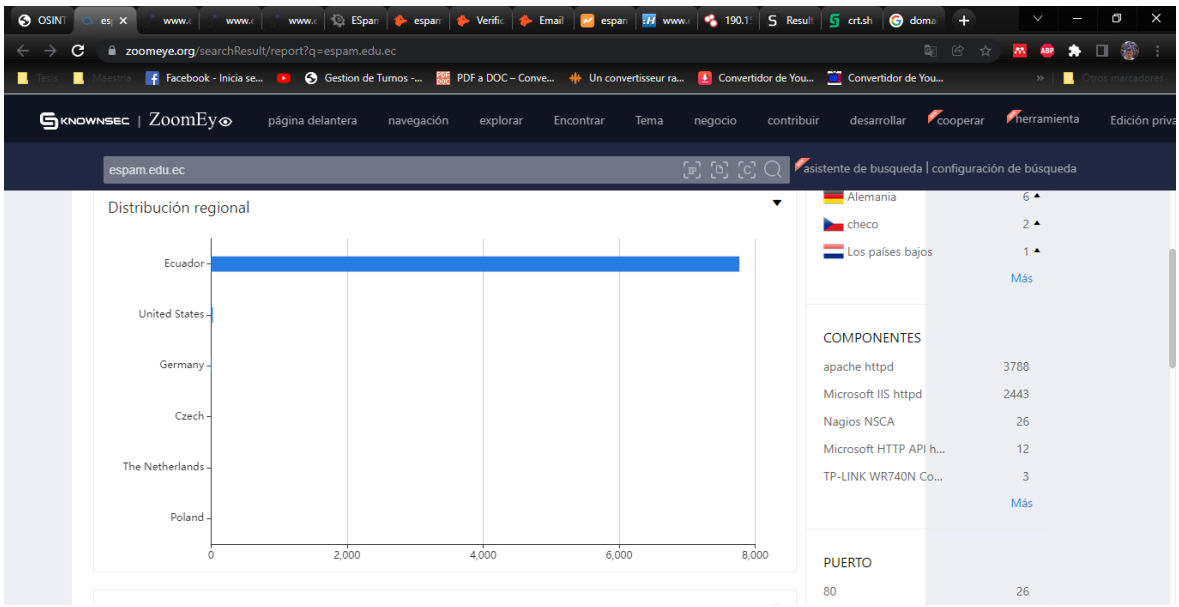


Figura 4.36. Resultados del escaneo de vulnerabilidades con la herramienta Zoom Eyes
Fuente: Los autores

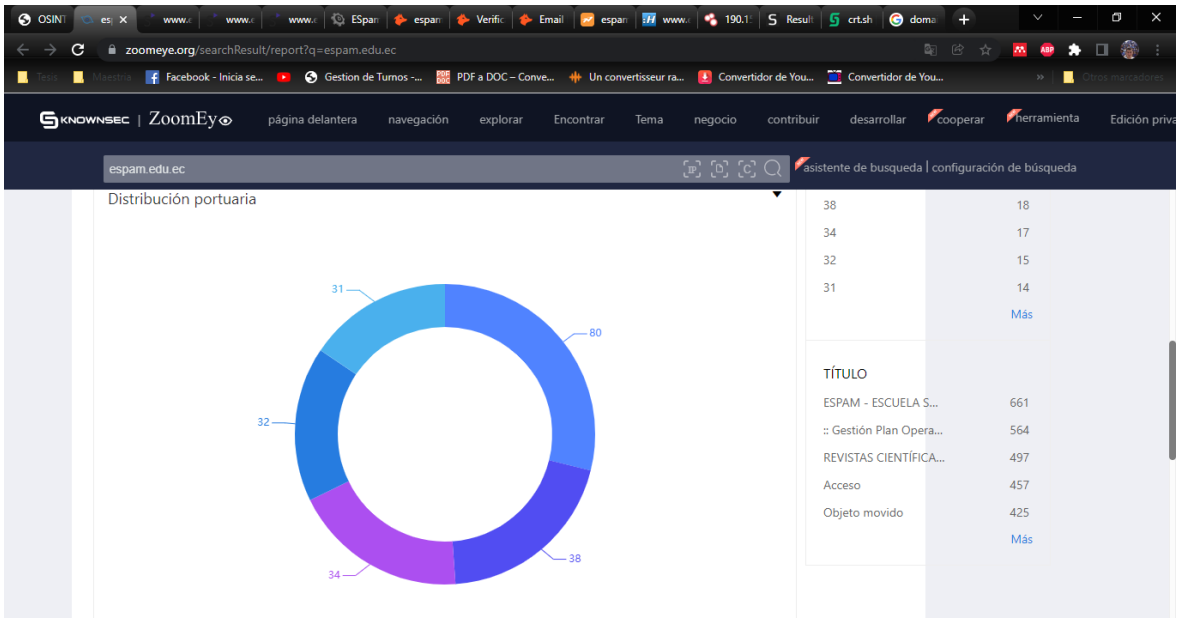


Figura 4.37. Resultados del escaneo de vulnerabilidades con la herramienta Zoom Eyes
Fuente: Los autores

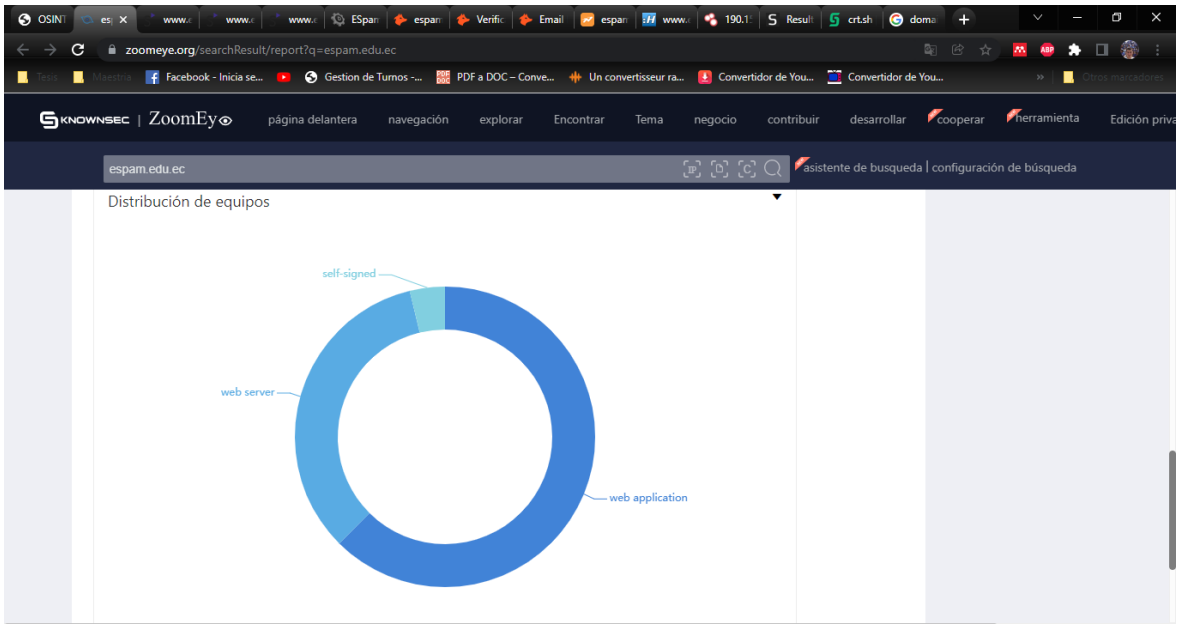


Figura 4.38. Resultados del escaneo de vulnerabilidades con la herramienta Zoom Eyes
Fuente: Los autores

WhoIs, DNS & Domain Info.

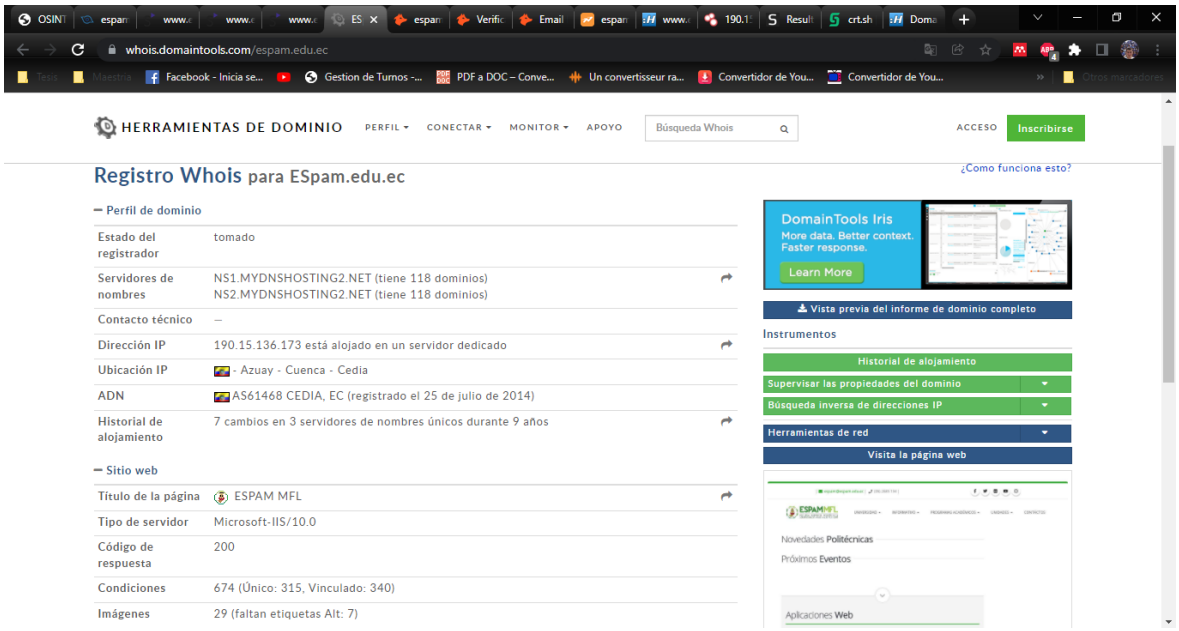


Figura 4.39. Ejecución de la herramienta Whols, DNS & Domain Info bajo el dominio de la ESPAM MFL
Fuente: Los autores

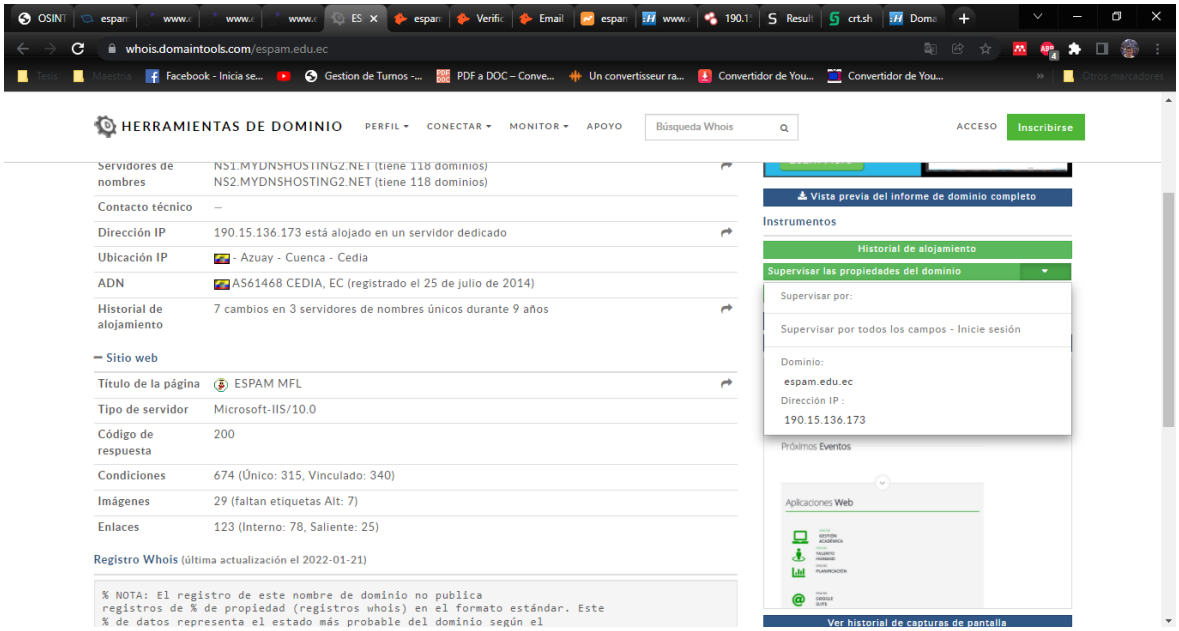


Figura 4.40. Resultados del escaneo de vulnerabilidades con la herramienta Whols, DNS & Domain Info
Fuente: Los autores

Anexo 4 Ejecución de las herramientas de OSINT bajo el dominio de la ESPAM MFL.

ANEXO 5. INFORMES TÉCNICOS EXTRAÍDOS POR VARIAS HERRAMIENTAS UTILIZADAS

Siteliner PREMIUM

Site Report for www.espam.edu.ec

Completed 11:51:51 pm GMT on Jan 21, 2022

Top Issues

4 broken links were found.

Related domains were found on your site.

Your Pages

75 pages scanned of 75 found.

Normal Pages: 73

Errors: 2

Duplicate Content

Duplicate Content: 6%

Common Content: 32%

Unique Content: 61%

Siteliner PREMIUM

URL	Title	Page Power	Size	Words	Modified	Match Words	Match %-age	Match Pages	Match Words (w cmn)	Match %-age (w cmn)	Match Pages (w cmn)	Broken Links Out	Links Out	Links In	Skip Reason	Redirected to
(home page)	ESPAM MFL	100	100 Kb	684	23:50, 21 Jan, 2022	407	60%	6	684	100%	22	0	52	71		
inicio.aspx	ESPAM MFL	100	100 Kb	684	23:51, 21 Jan, 2022	407	60%	4	684	100%	10	0	52	71		
web/universidad/historia.aspx	ESPAM MFL	99	49 Kb	282	23:51, 21 Jan, 2022	0	0%	0	280	99%	31	0	39	71		
web/universidad/autoridades.aspx	ESPAM MFL	99	51 Kb	574	23:51, 21 Jan, 2022	22	4%	1	309	54%	7	0	39	71		
web/universidad/filosofia.aspx	ESPAM MFL	99	47 Kb	315	23:51, 21 Jan, 2022	15	5%	1	295	94%	4	0	39	71		
web/universidad/organigrama.aspx	ESPAM MFL	99	46 Kb	282	23:51, 21 Jan, 2022	0	0%	0	280	99%	31	0	39	71		
web/universidad/calendario.aspx	ESPAM MFL	99	48 Kb	292	23:51, 21 Jan, 2022	0	0%	0	280	96%	30	0	39	71		
web/informativo/noticias.aspx	ESPAM MFL	100	130 Kb	1,173	23:51, 21 Jan, 2022	419	36%	9	760	65%	31	0	70	71		
web/informativo/eventos.aspx	ESPAM MFL	99	73 Kb	512	23:51, 21 Jan, 2022	17	3%	1	294	57%	9	0	40	71		
web/informativo/sigloxxi.aspx	ESPAM MFL	99	74 Kb	1,207	23:51, 21 Jan, 2022	79	7%	4	375	31%	20	0	39	71		
web/informativo/congresovinculacion.aspx	ESPAM MFL	99	60 Kb	813	23:51, 21 Jan, 2022	88	11%	3	365	45%	12	0	40	71		
web/informativo/	ESPAM MFL	99	1,284	16,886	23:51, 21	0	0%	0	280	2%	3	0	40	71		

lotaip.aspx			Kb		Jan, 2022											
web/informativo/rendicioncuentas.aspx	ESPAM MFL	99	102 Kb	463	23:51, 21 Jan, 2022	0	0%	0	280	60%	13	1	40	71		
web/informativo/procesos.aspx	ESPAM MFL	99	78 Kb	604	23:51, 21 Jan, 2022	0	0%	0	280	46%	13	0	39	71		
web/informativo/resoluciones.aspx	ESPAM MFL	99	266 Kb	3,442	23:51, 21 Jan, 2022	32	1%	1	324	9%	12	0	39	71		
web/informativo/planificacion.aspx	ESPAM MFL	99	98 Kb	688	23:51, 21 Jan, 2022	0	0%	0	286	42%	17	0	39	71		
web/informativo/financiero.aspx	ESPAM MFL	99	53 Kb	353	23:51, 21 Jan, 2022	0	0%	0	285	81%	19	0	39	71		

Siteliner PREMIUM

URL	Title	Page Power	Size	Words	Modified	Match Words	Match %-age	Match Pages	Match Words (w cmn)	Match %-age (w cmn)	Match Pages (w cmn)	Broken Links Out	Links Out	Links In	Skip Reason	Redirected to
web/informativo/reglamentacion.aspx	ESPAM MFL	99	203 Kb	2,423	23:51, 21 Jan, 2022	32	1%	1	352	15%	17	0	39	71		
web/oferta/grado/administracionempresas.aspx	ESPAM MFL	99	100 Kb	838	23:51, 21 Jan, 2022	97	12%	3	378	45%	13	0	39	71		
web/oferta/grado/administracionpublica.aspx	ESPAM MFL	99	103 Kb	794	23:51, 21 Jan, 2022	127	16%	3	404	51%	11	0	39	71		
web/oferta/grado/agroindustria.aspx	ESPAM MFL	99	100 Kb	929	23:51, 21 Jan, 2022	106	11%	4	390	42%	8	1	40	71		
web/oferta/grado/computacion.aspx	ESPAM MFL	99	90 Kb	806	23:51, 21 Jan, 2022	29	4%	1	306	38%	5	0	39	71		
web/oferta/grado/agricola.aspx	ESPAM MFL	99	94 Kb	857	23:51, 21 Jan, 2022	56	7%	2	333	39%	6	1	40	71		
web/oferta/grado/ambiente.aspx	ESPAM MFL	99	107 Kb	785	23:51, 21 Jan, 2022	94	12%	6	371	47%	23	1	40	71		
web/oferta/grado/medicinaveterinaria.aspx	ESPAM MFL	99	95 Kb	860	23:51, 21 Jan, 2022	38	4%	2	315	37%	27	0	39	71		
web/oferta/grado/turismo.aspx	ESPAM MFL	99	84 Kb	718	23:51, 21 Jan, 2022	29	4%	2	306	43%	9	0	39	71		
web/unidades/secretaria.aspx	ESPAM MFL	99	59 Kb	722	23:51, 21 Jan, 2022	0	0%	0	296	41%	5	0	39	71		
web/unidades/vicerrectorado.aspx	ESPAM MFL	99	60 Kb	928	23:51, 21 Jan, 2022	0	0%	0	280	30%	5	0	39	71		

web/unidades/academico.aspx	ESPAM MFL	99	56 Kb	402	23:51, 21 Jan, 2022	0	0%	0	293	73%	33	0	39	71		
web/unidades/investigacion.aspx	ESPAM MFL	99	57 Kb	786	23:51, 21 Jan, 2022	0	0%	0	288	37%	5	0	39	71		
web/unidades/biblioteca.aspx	ESPAM MFL	99	66 Kb	1,498	23:51, 21 Jan, 2022	0	0%	0	289	19%	4	0	39	71		
web/unidades/caai.aspx	ESPAM MFL	99	68 Kb	608	23:51, 21 Jan, 2022	0	0%	0	281	46%	5	0	39	71		
web/unidades/bienestar.aspx	ESPAM MFL	99	66 Kb	1,019	23:51, 21 Jan, 2022	0	0%	0	285	28%	4	0	39	71		

Siteliner PREMIUM

URL	Title	Page Power	Size	Words	Modified	Match Words	Match %-age	Match Pages	Match Words (w cmn)	Match %-age (w cmn)	Match Pages (w cmn)	Broken Links Out	Links Out	Links In	Skip Reason	Redirected to
web/unidades/vinculacion.aspx	ESPAM MFL	99	47 Kb	393	23:51, 21 Jan, 2022	0	0%	0	307	78%	31	0	39	71		
web/unidades/evaluacion.aspx	ESPAM MFL	99	120 Kb	611	23:51, 21 Jan, 2022	0	0%	0	280	46%	12	0	39	71		
web/unidades/planificacion.aspx	ESPAM MFL	99	63 Kb	441	23:51, 21 Jan, 2022	0	0%	0	301	68%	32	0	39	71		
web/unidades/financiero.aspx	ESPAM MFL	99	55 Kb	328	23:51, 21 Jan, 2022	0	0%	0	282	86%	32	0	39	71		
web/unidades/juridico.aspx	ESPAM MFL	99	52 Kb	481	23:51, 21 Jan, 2022	0	0%	0	286	59%	14	0	39	71		
web/unidades/tthh.aspx	ESPAM MFL	99	75 Kb	594	23:51, 21 Jan, 2022	0	0%	0	282	47%	12	0	39	71		
web/unidades/tecnologia.aspx	ESPAM MFL	99	70 Kb	508	23:51, 21 Jan, 2022	0	0%	0	299	59%	11	0	39	71		
web/informativo/merito.aspx	ESPAM MFL	24	56 Kb	554	23:51, 21 Jan, 2022	0	0%	0	291	53%	32	0	40	2		
web/informativo/noticia.aspx?key=10099	ESPAM MFL	25	56 Kb	408	23:51, 21 Jan, 2022	76	19%	11	353	87%	28	0	40	3		
web/informativo/noticia.aspx?key=10097	ESPAM MFL	25	54 Kb	450	23:51, 21 Jan, 2022	17	4%	1	306	68%	3	0	40	3		
web/informativo/noticia.aspx?key=10096	ESPAM MFL	25	55 Kb	458	23:51, 21 Jan, 2022	52	11%	8	329	72%	31	0	40	3		
web/informativo/noticia.aspx?key=10098	ESPAM MFL	25	56 Kb	524	23:51, 21 Jan, 2022	0	0%	0	297	57%	6	0	40	3		

web/informativo/noticia.aspx?key=9110	ESPAM MFL	25	59 Kb	476	23:51, 21 Jan, 2022	22	5%	1	333	70%	4	0	40	3		
web/informativo/noticia.aspx?key=9096	ESPAM MFL	25	58 Kb	384	23:51, 21 Jan, 2022	40	10%	4	321	84%	24	0	40	3		
web/informativo/noticia.aspx?key=9097	ESPAM MFL	25	54 Kb	409	23:51, 21 Jan, 2022	72	18%	3	364	89%	6	0	40	3		
web/informativo/noticia.aspx?key=9098	ESPAM MFL	25	59 Kb	396	23:51, 21 Jan, 2022	18	5%	1	313	79%	9	0	40	3		
web/informativo/noticia.aspx?key=9099	ESPAM MFL	25	59 Kb	441	23:51, 21 Jan, 2022	51	12%	2	354	80%	8	0	40	3		

Siteliner PREMIUM

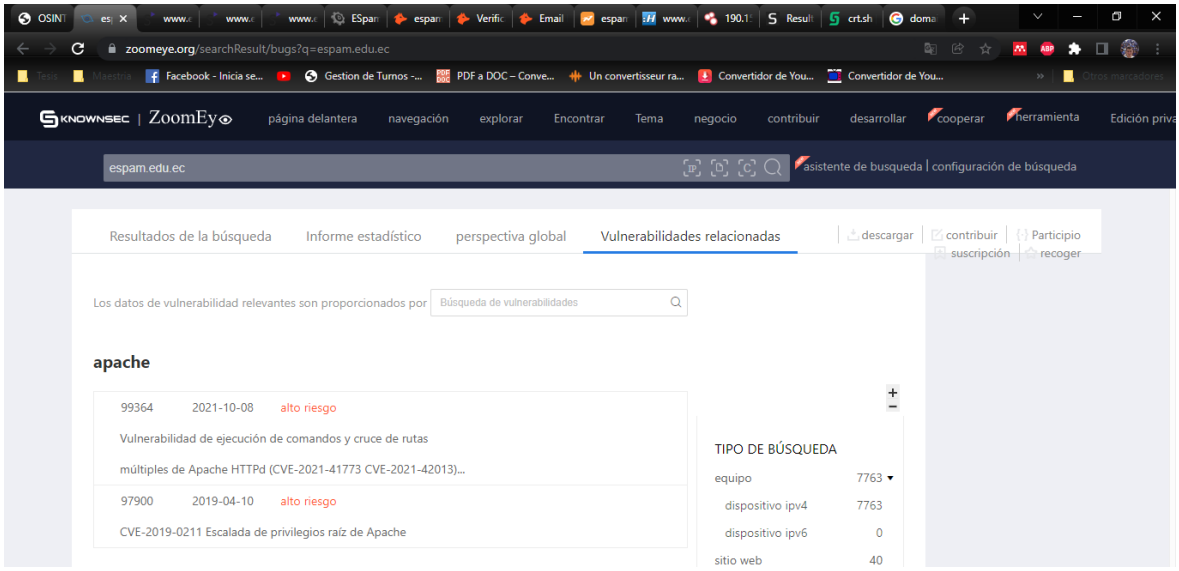
URL	Title	Page Power	Size	Words	Modified	Match Words	Match %-age	Match Pages	Match Words (w cmn)	Match %-age (w cmn)	Match Pages (w cmn)	Broken Links Out	Links Out	Links In	Skip Reason	Redirected to
web/informativo/noticia.aspx?key=9100	ESPAM MFL	25	59 Kb	477	23:51, 21 Jan, 2022	48	10%	2	360	75%	10	0	40	3		
web/informativo/noticia.aspx?key=9101	ESPAM MFL	25	57 Kb	408	23:51, 21 Jan, 2022	21	5%	1	320	78%	6	0	40	3		
web/informativo/noticia.aspx?key=9102	ESPAM MFL	25	58 Kb	432	23:51, 21 Jan, 2022	23	5%	2	349	81%	7	0	40	3		
web/oferta/grado/demo-business-consulting-team-detail.html		0	0 Kb	0	00:00, 1 Jan, 1970	0	0%	0	0	0%	0	0	0	3	Error 404 - Not Found	
recursos/sitio/informativo/archivos/rendicion/2016COMISION		0	0 Kb	0	00:00, 1 Jan, 1970	0	0%	0	0	0%	0	0	0	1	Error 404 - Not Found	
acceso/login.aspx	MICROSITIOS | ESPAM MFL	26	7 Kb	9	23:51, 21 Jan, 2022	0	0%	0	0	0%	0	0	0	3		
web/informativo/noticia.aspx?key=9103	ESPAM MFL	23	59 Kb	457	23:51, 21 Jan, 2022	77	17%	13	354	77%	31	0	40	1		
web/informativo/noticia.aspx?key=9104	ESPAM MFL	23	56 Kb	409	23:51, 21 Jan, 2022	0	0%	0	308	75%	4	0	40	1		
web/informativo/noticia.aspx?key=9105	ESPAM MFL	23	60 Kb	420	23:51, 21 Jan, 2022	32	8%	2	323	77%	4	0	40	1		
web/informativo/noticia.aspx?key=9106	ESPAM MFL	23	62 Kb	500	23:51, 21 Jan, 2022	159	32%	2	500	100%	5	0	40	1		
web/informativo/noticia.aspx?key=9107	ESPAM MFL	23	62 Kb	500	23:51, 21 Jan, 2022	500	100%	1	500	100%	1	0	40	1		

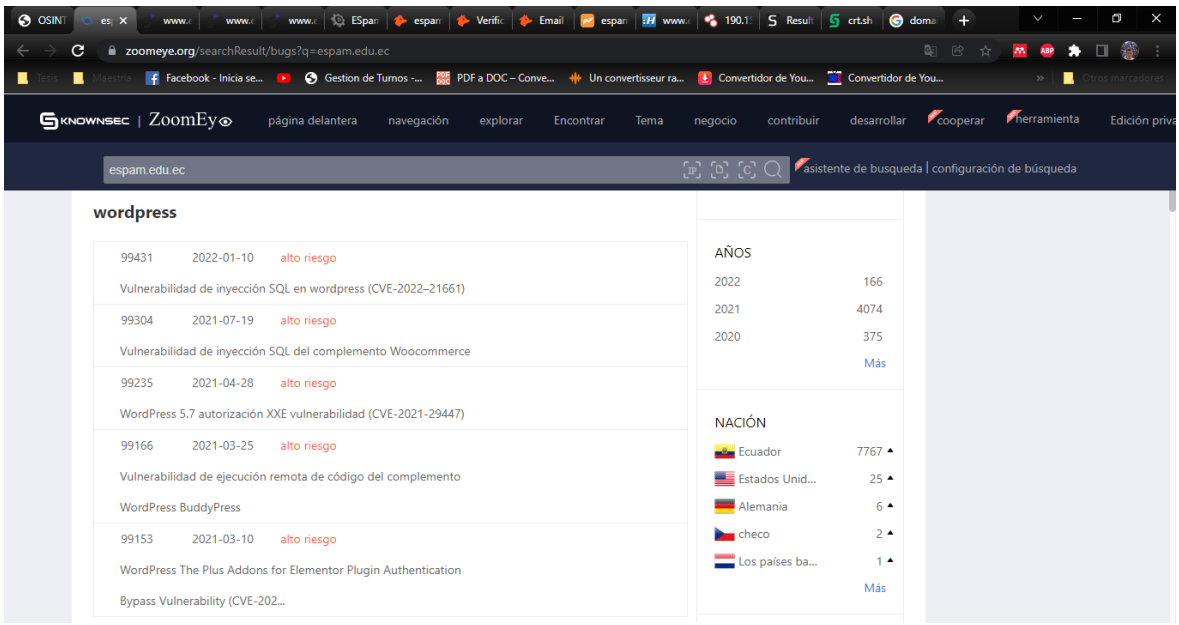
web/informativo/noticia.aspx?key=9108	ESPAM MFL	23	62 Kb	500	23:51, 21 Jan, 2022	500	100%	1	500	100%	1	0	40	1		
web/informativo/noticia.aspx?key=9109	ESPAM MFL	23	58 Kb	461	23:51, 21 Jan, 2022	39	8%	3	330	72%	4	0	40	1		
web/informativo/noticia.aspx?key=9095	ESPAM MFL	23	55 Kb	452	23:51, 21 Jan, 2022	68	15%	6	354	78%	31	0	40	1		
web/informativo/noticia.aspx?key=9094	ESPAM MFL	23	56 Kb	396	23:51, 21 Jan, 2022	0	0%	0	295	74%	6	0	40	1		
web/informativo/noticia.aspx?key=9090	ESPAM MFL	23	59 Kb	420	23:51, 21 Jan, 2022	0	0%	0	317	75%	6	0	40	1		

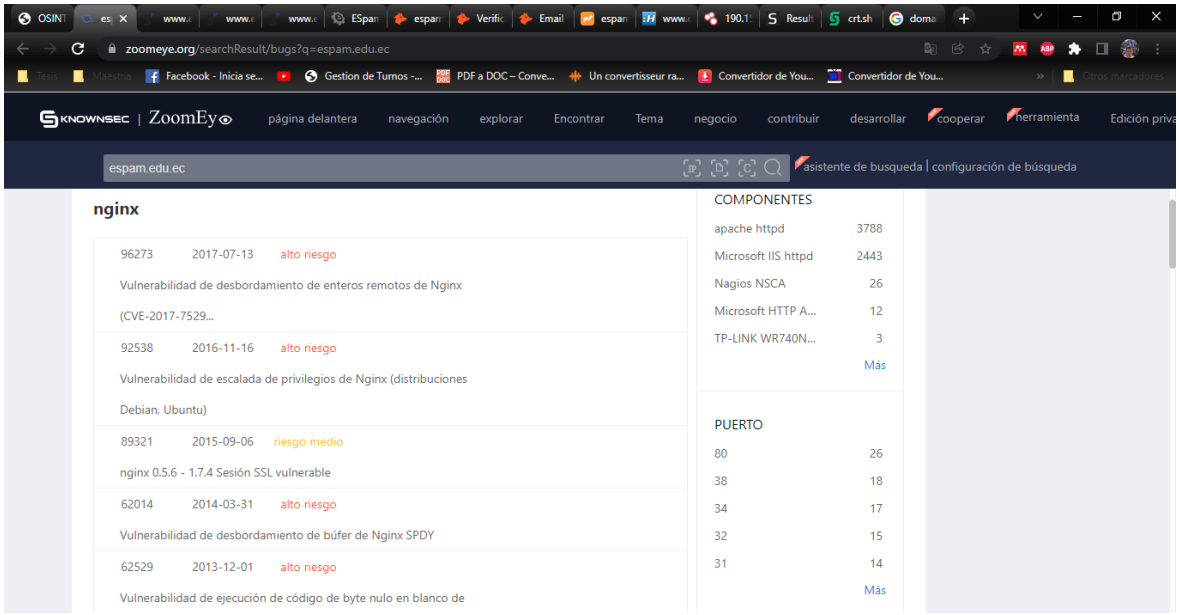
URL	Title	Page Power	Size	Words	Modified	Match Words	Match %-age	Match Pages	Match Words (w cmn)	Match %-age (w cmn)	Match Pages (w cmn)	Broken Links Out	Links Out	Links In	Skip Reason	Redirected to
web/informativo/noticia.aspx?key=9079	ESPAM MFL	23	59 Kb	476	23:51, 21 Jan, 2022	40	8%	2	320	67%	4	0	40	1		
web/informativo/noticia.aspx?key=9080	ESPAM MFL	23	57 Kb	432	23:51, 21 Jan, 2022	0	0%	0	311	72%	5	0	40	1		
web/informativo/noticia.aspx?key=9081	ESPAM MFL	23	59 Kb	474	23:51, 21 Jan, 2022	20	4%	1	332	70%	8	0	40	1		
web/informativo/noticia.aspx?key=9082	ESPAM MFL	23	58 Kb	412	23:51, 21 Jan, 2022	44	11%	2	342	83%	8	0	40	1		
web/informativo/noticia.aspx?key=7078	ESPAM MFL	23	58 Kb	505	23:51, 21 Jan, 2022	17	3%	1	317	63%	6	0	40	1		
web/informativo/noticia.aspx?key=7079	ESPAM MFL	23	57 Kb	409	23:51, 21 Jan, 2022	15	4%	1	312	76%	3	0	40	1		
web/informativo/noticia.aspx?key=7080	ESPAM MFL	23	55 Kb	430	23:51, 21 Jan, 2022	17	4%	1	328	76%	5	0	40	1		
web/informativo/noticia.aspx?key=7082	ESPAM MFL	23	61 Kb	449	23:51, 21 Jan, 2022	0	0%	0	329	73%	7	0	40	1		
web/informativo/ponencias_vinc.aspx	ESPAM MFL	24	108 Kb	1,880	23:51, 21 Jan, 2022	16	1%	1	293	16%	3	0	40	1		

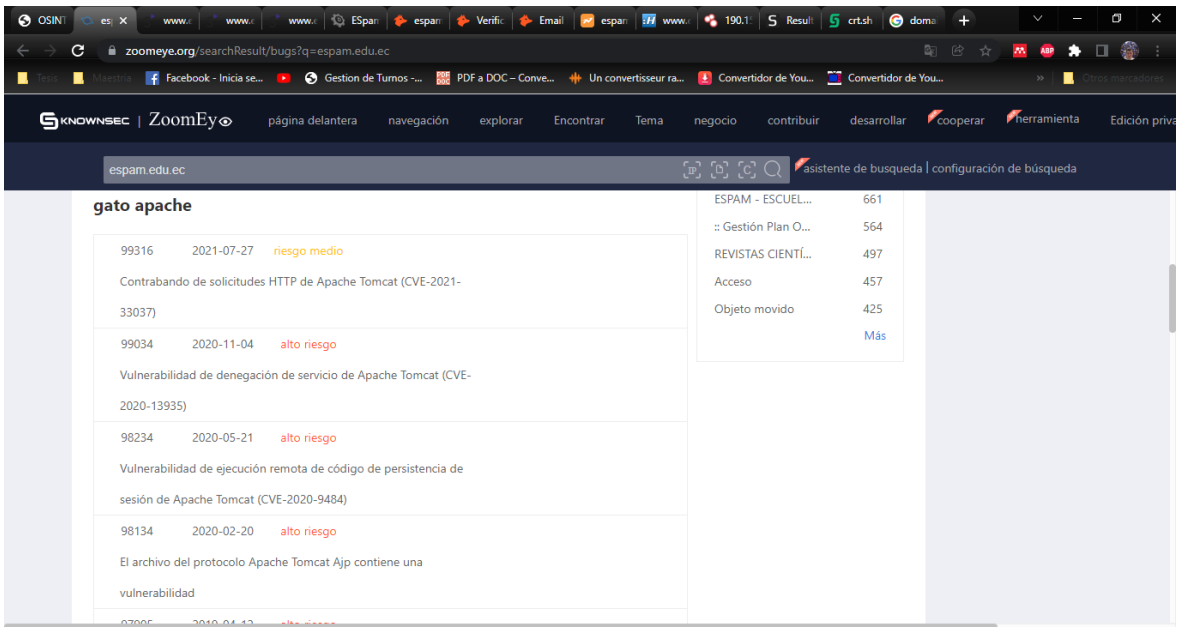
Anexo 5 Informe técnico sobre el dominio de la ESPAM MFL presentado por una de las herramientas OSINT ejecutadas en el experimento.
Fuente: Los autores.

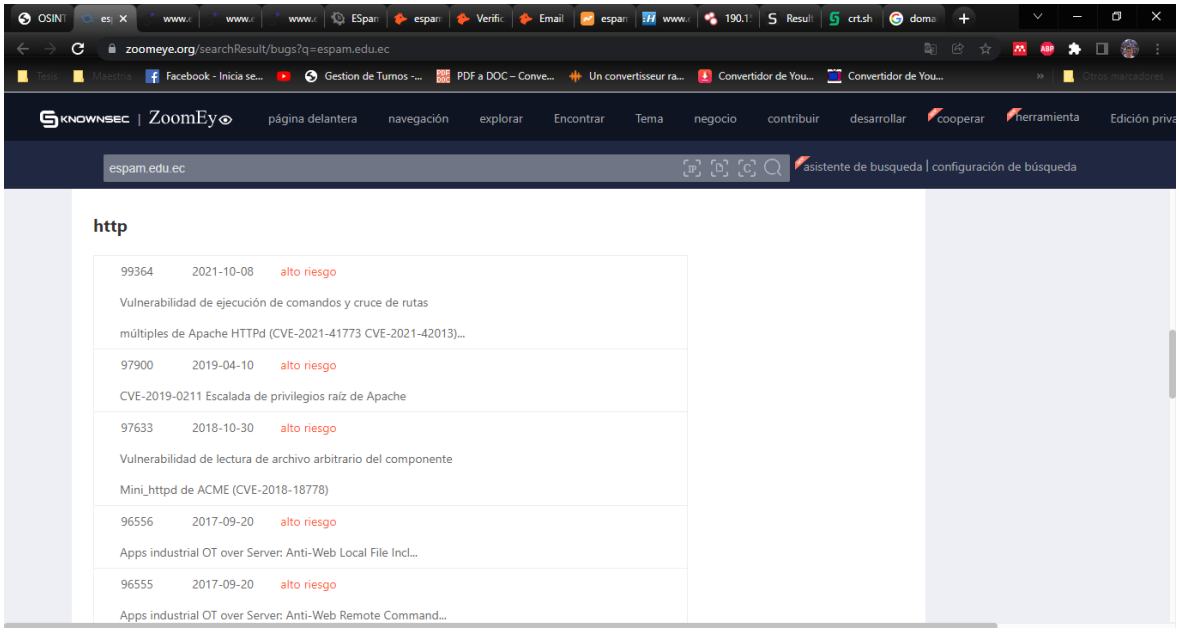
ANEXO 5. VULNERABILIDADES ENCONTRADAS CON SU NIVEL DE RIESGOS.

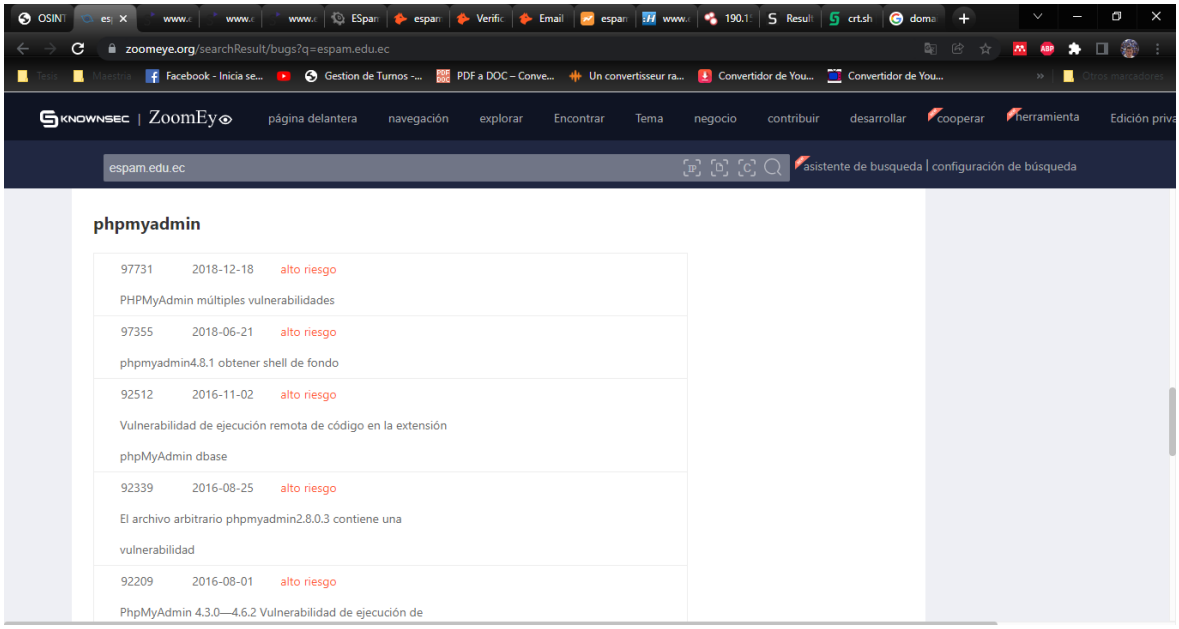


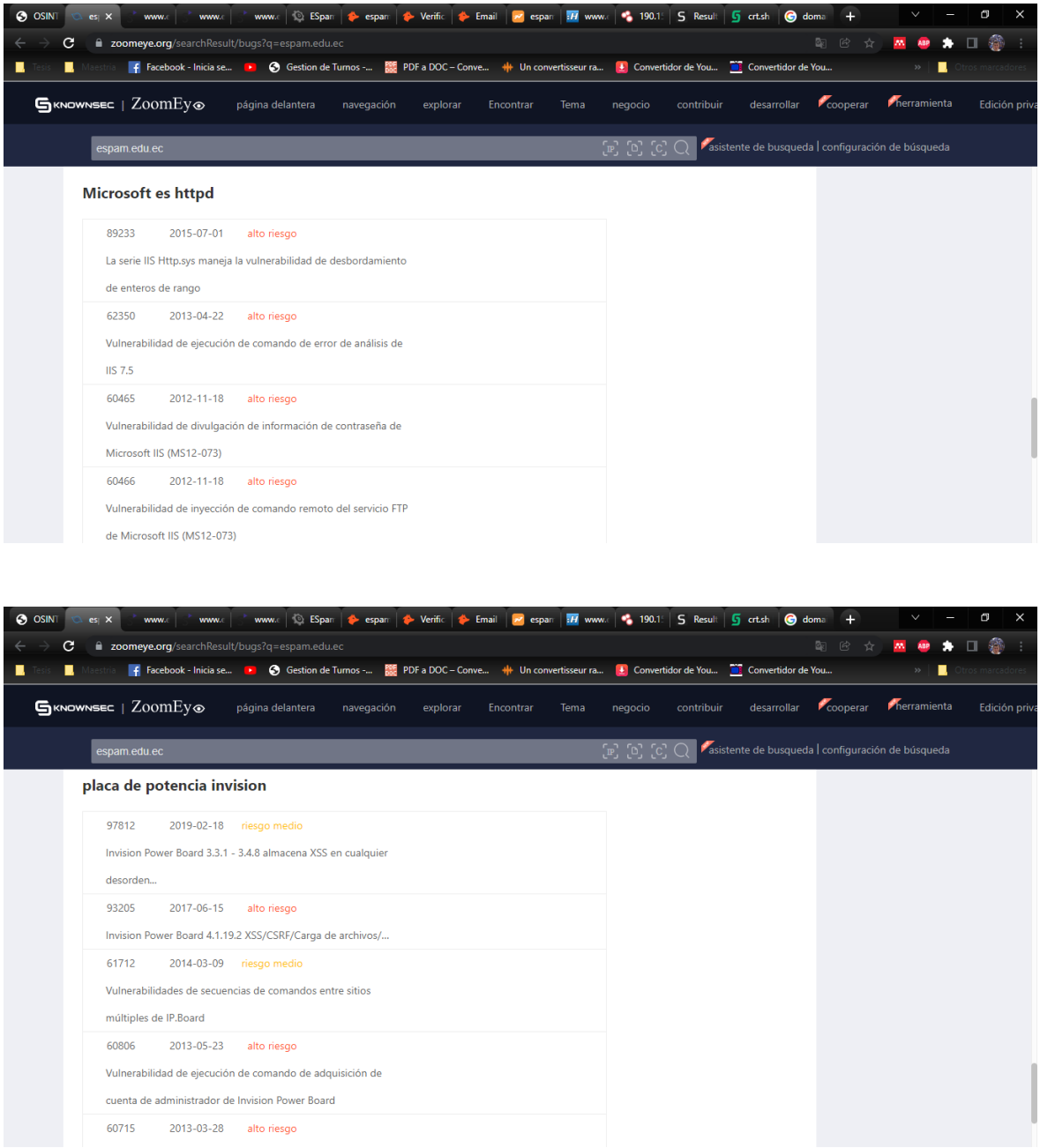



zoomeye.org/searchResult/bugs?q=espam.edu.ec
KNOWNSEC | ZoomEye
página delantera
navegación
explorar
Encontrar
Tema
negocio
contribuir
desarrollar
cooperar
herramienta
Edición priva
espam.edu.ec
asistente de busqueda | configuración de búsqueda
nginx
96273 2017-07-13 alto riesgo
Vulnerabilidad de desbordamiento de enteros remotos de Nginx (CVE-2017-7529...
92538 2016-11-16 alto riesgo
Vulnerabilidad de escalada de privilegios de Nginx (distribuciones Debian, Ubuntu)
89321 2015-09-06 riesgo medio
nginx 0.5.6 - 1.7.4 Sesión SSL vulnerable
62014 2014-03-31 alto riesgo
Vulnerabilidad de desbordamiento de búfer de Nginx SPDY
62529 2013-12-01 alto riesgo
Vulnerabilidad de ejecución de código de byte nulo en blanco de
COMPONENTES
apache httpd 3788
Microsoft IIS httpd 2443
Nagios NSCA 26
Microsoft HTTP A... 12
TP-LINK WR740N... 3
Más
PUERTO
80 26
38 18
34 17
32 15
31 14
Más


zoomeye.org/searchResult/bugs?q=espam.edu.ec
KNOWNSEC | ZoomEye
página delantera
navegación
explorar
Encontrar
Tema
negocio
contribuir
desarrollar
cooperar
herramienta
Edición priva
espam.edu.ec
asistente de busqueda | configuración de búsqueda
gato apache
99316 2021-07-27 riesgo medio
Contrabando de solicitudes HTTP de Apache Tomcat (CVE-2021-33037)
99034 2020-11-04 alto riesgo
Vulnerabilidad de denegación de servicio de Apache Tomcat (CVE-2020-13935)
98234 2020-05-21 alto riesgo
Vulnerabilidad de ejecución remota de código de persistencia de sesión de Apache Tomcat (CVE-2020-9484)
98134 2020-02-20 alto riesgo
El archivo del protocolo Apache Tomcat Ajp contiene una vulnerabilidad
ESPAM - ESCUEL... 661
:: Gestión Plan O... 564
REVISTAS CIENTÍ... 497
Acceso 457
Objeto movido 425
Más


zoomeye.org/searchResult/bugs?q=espam.edu.ec
KNOWNSEC | ZoomEye
página delantera
navegación
explorar
Encontrar
Tema
negocio
contribuir
desarrollar
cooperar
herramienta
espam.edu.ec
asistente de busqueda | configuración de búsqueda
http
99364 2021-10-08 alto riesgo
Vulnerabilidad de ejecución de comandos y cruce de rutas
múltiples de Apache HTTPd (CVE-2021-41773 CVE-2021-42013)...
97900 2019-04-10 alto riesgo
CVE-2019-0211 Escalada de privilegios raíz de Apache
97633 2018-10-30 alto riesgo
Vulnerabilidad de lectura de archivo arbitrario del componente
Mini_httpd de ACME (CVE-2018-18778)
96556 2017-09-20 alto riesgo
Apps industrial OT over Server: Anti-Web Local File Incl...
96555 2017-09-20 alto riesgo
Apps industrial OT over Server: Anti-Web Remote Command...


zoomeye.org/searchResult/bugs?q=espam.edu.ec
KNOWNSEC | ZoomEye
página delantera
navegación
explorar
Encontrar
Tema
negocio
contribuir
desarrollar
cooperar
herramienta
espam.edu.ec
asistente de busqueda | configuración de búsqueda
phpmyadmin
97731 2018-12-18 alto riesgo
PHPMyAdmin múltiples vulnerabilidades
97355 2018-06-21 alto riesgo
phpmyadmin4.8.1 obtener shell de fondo
92512 2016-11-02 alto riesgo
Vulnerabilidad de ejecución remota de código en la extensión
phpMyAdmin dbase
92339 2016-08-25 alto riesgo
El archivo arbitrario phpmyadmin2.8.0.3 contiene una
vulnerabilidad
92209 2016-08-01 alto riesgo
PhpMyAdmin 4.3.0—4.6.2 Vulnerabilidad de ejecución de



Anexo 6 Vulnerabilidades encontradas en los servidores de la ESPAM MFL.
Fuente: Los autores.

ANEXO 6. POLITICAS DE DISTRIBUCIÓN Y DIFUSIÓN DE LA INFORMACIÓN.

ESPAM MFL
ESCUELA SUPERIOR POLITÉCNICA
AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

POLÍTICAS DE DISTRIBUCIÓN Y DIFUSIÓN DE INFORMACIÓN APLICADO A LA ESPAM MFL SEGÚN LA NORMA ISO/IEC 27002

KEVIN D. CUSME ZAMBRANO

LEYDI T. ZAMBRANO MENDOZA

ENERO, 2022

CONTENIDO

I. INTRODUCCIÓN

La seguridad de la información, es un tema que ha venido adquiriendo mayor relevancia a nivel mundial cada vez más. Las amenazas tanto externas como internas, cada día se incrementan y se diversifican los patrones y frecuencias de ataques, conllevando a que constantemente, se aumente el porcentaje de fuga de información. Por lo tanto, la finalidad de este documento es proponer políticas de seguridad, que permitan mejorar los aspectos de distribución y divulgación de la información, en los dominios no Gubernamentales del Ecuador.

En la elaboración de las Políticas se aplicó la Norma ISO/IEC 27002, tomando como caso de estudio los sistemas de información de la Universidad ESPAM MFL donde en base a sus necesidades generales, permitió sustentar la metodología utilizada a través de un experimento realizado. El mismo que describe las vulnerabilidades presentes en dichos sistemas, mediante el uso de herramientas de inteligencia de código abierto (OSINT).

Al realizar esta propuesta de Políticas de seguridad, se pretende socializar con la ESPAM MFL, que previo a la autorización, formo parte de este trabajo, el hecho de tomar medidas mediante estrategias que permitan mejorar en conocimientos de Ciberseguridad y mitigar los posibles riesgos que presentan las vulnerabilidades. Para la protección de los activos de información se basó en los pilares fundamentales de la seguridad de la información que son disponibilidad, integridad y confidencialidad, donde se definieron las políticas a seguir por el personal docente, administrativo y externos.

I.1. ALCANCE

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Universidad ESPAM MFL.

Es de aplicación para toda la comunidad universitaria: docentes, no docentes, estudiantes y toda aquella persona vinculada a la Unidad de Tecnología, o que trabajan o prestan un servicio bajo cualquier modalidad en la ESPAM MFL, y que en el desarrollo de sus actividades puedan acceder a Información privilegiada.

I.2. OBJETIVO DEL DOCUMENTO

Establecer políticas de distribución y difusión de información para mejorar el estado de Ciberseguridad de los sistemas de información de la ESPAM MFL con el fin de salvaguardar su confidencialidad y asegurar su correcta difusión al público en forma veraz y transparente.

I.3. PRINCIPIOS QUE RIGEN LA POLÍTICA

- **Respeto:** permite valorar el esfuerzo de todos los colaboradores, la confianza de los estudiantes y diversos grupos de interés.
- **Excelencia:** promueve el trabajo en equipo y la actitud innovadora orientados a lograr resultados más allá de lo esperado, contribuyendo al desarrollo personal.
- **Comunicación:** practicada con un estilo transparente que promueve una justa y oportuna distribución de información.
- **Responsabilidad:** permite comprometerse con las decisiones que se toman y con el resultado de ellas.

I.4. MARCO NORMATVO RELACIONADO

- ISO/IEC 27002:2013, Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información (ISO, 2013).

I.5. TÉRMINOS Y DEFINICIONES

Amenazas	Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información
Ciberseguridad	Es la encargada de la protección de infraestructura computacional y todo lo relacionado con esta, especialmente la información que se maneja.
Colaborador	Es toda persona que presta sus servicios personales y en relación de dependencia para la Universidad. Esta denominación comprende a Directivos, personal administrativo, docentes y practicantes.
Confidencialidad	Es la propiedad con la que cuenta la información que no se encuentre a disposición de cualquier persona o sea divulgada.
Dominio	Es como se encuentra dividida o clasificada las áreas de aplicación de la Ciberseguridad
Grupo de interés	Cualquier grupo o individuo identificable que pueda afectar o es afectado por el logro de los objetivos y acciones de la Universidad (docentes, estudiantes, proveedores, autoridades y gobierno, medios de comunicación etc.)
Herramientas para escaneo de vulnerabilidades	Son herramientas que se aplican para analizar el escaneo y explotación de vulnerabilidades en este caso en los sistemas de información de la ESPAM MFL
Información	Información denominamos al conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado
Mitigación de riesgos	La mitigación de riesgos sirve para aplicar acciones que permitan reducir la vulnerabilidad a ciertos peligros
Normativa interna	Lineamientos y documentación que rigen las actividades de la Universidad, tales como sus políticas, su Código de Ética, reglamentos, procedimientos, entre otros.
Política de ciberseguridad	Está orientada a gestionar eficazmente la seguridad de la información tratada por los sistemas informáticos
Riesgos	Es la probabilidad de que una amenaza se convierta en un desastre.
Seguridad	Es un estado en el cual los peligros y las condiciones que pueden provocar daños de tipo físico, psicológico o material son controlados para preservar la salud y el bienestar de los individuos y de la comunidad
Sistemas de información	Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
Vulnerabilidades	Es la incapacidad de resistencia cuando se presenta un fenómeno amenazante, o la incapacidad para reponerse después de que ha ocurrido un desastre o riesgos

2. POLÍTICAS DE SEGURIDAD

Una política de seguridad es una técnica de los activos de una organización, y la forma en que se debe de gestionar. De esta forma las instituciones de Educación Superior deben manejar una gestión de procesos, de manera organizada y eficiente, con el objetivo de poder identificar la comunicación y el transito que debe llevar la información (Navarro, 2017).

En otra definición las políticas de seguridad son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la institución. Esta a su vez establecen las reglas y procedimientos que regulan la forma en que una

organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos (IEDGE, 2022).

Con la implementación de la propuesta de Políticas de Seguridad de la información se pretende lograr que todos los miembros de la institución se rijan a las normas expuesta en el documento para así asegurar que los bienes y recursos sean y estén utilizados de una manera correcta, asegurando también que la información esté debidamente protegida, para tal efecto se debe realizar la difusión y concientización de lo que deberán cumplir para proteger todos los activos de la institución.

2.1. NORMA ISO 27002: 2013

La norma ISO 27002 anteriormente denominada ISO 17799, es un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional. La versión más reciente de la norma ISO 27002:2013.

La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como “la preservación de la confidencialidad, integridad y disponibilidad (ISOTools Excellence, 2017).

La norma se encuentra organizada en base a los 14 dominios, 35 objetivos de control y 114 controles de la norma que se utiliza para el análisis y el desarrollo de la política de seguridad:

Tabla 6. Norma ISO IEC 27002:2013

DOMINIO	OBJETIVO DE CONTROL	CONTROLES	
5. POLÍTICAS DE SEGURIDAD	5.1. Directrices de la dirección en seguridad de la información	5.1.1.	Conjunto de políticas para la seguridad de la información.
		5.1.2.	Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	6.1. Organización interna.	6.1.1.	Asignación de responsabilidades para la seguridad de la información.
		6.1.2.	Segregación de tareas
		6.1.3.	Contacto con las autoridades.
		6.1.4.	Contacto con grupos de interés especial.
		6.1.5.	Seguridad de la información en la gestión de proyectos.
	6.2. Dispositivos para movilidad y teletrabajo	6.2.1.	Política de uso de dispositivos para movilidad.
		6.2.2.	Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	7.1. Antes de la contratación	7.1.1.	Investigación de antecedentes.
		7.1.2.	Términos y condiciones de contratación.
	7.2. Durante la contratación.	7.2.1.	Responsabilidades de gestión.
		7.2.2.	Concienciación, educación y capacitación en seguridad de la información.
		7.2.3.	Proceso disciplinario.
	7.3. Cese o cambio de puesto de trabajo	7.3.1.	Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.	8.1. Responsabilidad sobre los activos.	8.1.1.	Inventario de activos.
		8.1.2.	Propiedad de los activos.
		8.1.3.	Uso aceptable de los activos.
		8.1.4.	Devolución de activos.
	8.2. Clasificación de la información	8.2.1.	Directrices de clasificación.
		8.2.2.	Etiquetado y manipulado de la información.
		8.2.3.	Manipulación de activos.
	8.3. Manejo de los soportes de almacenamiento.	8.3.1.	Gestión de soportes extraíbles.
		8.3.2.	Eliminación de soportes.
		8.3.3.	Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.	9.1. Requisitos de negocio para el control de accesos.	9.1.1.	Política de control de accesos.
		9.1.2.	Control de acceso a las redes y servicios asociados.
	9.2. Gestión de acceso de usuario.	9.2.1.	Gestión de altas/bajas en el registro de usuarios.

		9.2.2.	Gestión de los derechos de acceso asignados a usuarios.
		9.2.3.	Gestión de los derechos de acceso con privilegios especiales.
		9.2.4.	Gestión de información confidencial de autenticación de usuarios.
		9.2.5.	Revisión de los derechos de acceso de los usuarios.
		9.2.6.	Retirada o adaptación de los derechos de acceso
	9.2. Responsabilidades del usuario.	9.2.1.	Uso de información confidencial para la autenticación.
	9.3. Control de acceso a sistemas y aplicaciones.	9.4.1.	Restricción del acceso a la información.
		9.4.2.	Procedimientos seguros de inicio de sesión.
		9.4.3.	Gestión de contraseñas de usuario.
		9.4.4.	Uso de herramientas de administración de sistemas.
		9.4.5.	Control de acceso al código fuente de los programas.
10. CIFRADO	10.1. Controles criptográficos.	10.1.1.	Política de uso de los controles criptográficos.
		10.1.2.	Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.	11.1. Áreas seguras	11.1.1.	Perímetro de seguridad física.
		11.1.2.	Controles físicos de entrada.
		11.1.3.	Seguridad de oficinas, despachos y recursos.
		11.1.4.	Protección contra las amenazas externas y ambientales.
		11.1.5.	El trabajo en áreas seguras
		11.1.6.	Áreas de acceso público, carga y descarga.
	10.1. Seguridad de los equipos	11.2.1.	Emplazamiento y protección de equipos.
		11.2.2.	Instalaciones de suministro.
		11.2.3.	Seguridad del cableado.
		11.2.4.	Mantenimiento de los equipos.
		11.2.5.	Salida de activos fuera de las dependencias de la empresa.
		11.2.6.	Seguridad de los equipos y activos fuera de las instalaciones.
		11.2.7.	Reutilización o retirada segura de dispositivos de almacenamiento.
		11.2.8.	Equipo informático de usuario desatendido.
		11.2.9.	Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.	12.1. Responsabilidades y procedimientos de operación	12.1.1.	Documentación de procedimientos de operación.
		12.1.2.	Gestión de cambios.
		12.1.3.	Gestión de capacidades.
		12.1.4.	Separación de entornos de desarrollo, prueba y producción.
	12.2. Protección contra código malicioso.	12.2.1.	Controles contra el código malicioso.
	12.3. Copias de seguridad.	12.3.1.	Copias de seguridad de la información

	12.4. Registro de actividad y supervisión	12.4.1.	Registro y gestión de eventos de actividad.
		12.4.2.	Protección de los registros de información.
		12.4.3.	Registros de actividad del administrador y operador del sistema.
		12.4.4.	Sincronización de relojes.
	12.5. Control del software en explotación	12.5.1.	Instalación del software en sistemas en producción.
	12.6. Gestión de la vulnerabilidad técnica.	12.6.1.	Gestión de las vulnerabilidades técnicas.
		12.6.2.	Restricciones en la instalación de software.
	12.7. Consideraciones de las auditorías de los sistemas de información.	12.7.1.	Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	13.1. Gestión de la seguridad en las redes.	13.1.1.	Controles de red.
		13.1.2.	Mecanismos de seguridad asociados a servicios en red.
		13.1.3.	Segregación de redes.
	13.2. Intercambio de información con partes externas.	13.2.1.	Políticas y procedimientos de intercambio de información.
		13.2.2.	Acuerdos de intercambio.
		13.2.3.	Mensajería electrónica.
		13.2.4.	Acuerdos de confidencialidad y secreto.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	14.1. Requisitos de seguridad de los sistemas de información	14.1.1.	Análisis y especificación de los requisitos de seguridad.
		14.1.2.	Seguridad de las comunicaciones en servicios accesibles por redes públicas.
		14.1.3.	Protección de las transacciones por redes telemáticas
	14.2. Seguridad en los procesos de desarrollo y soporte.	14.2.1.	Política de desarrollo seguro de software.
		14.2.2.	Procedimientos de control de cambios en los sistemas.
		14.2.3.	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
		14.2.4.	Restricciones a los cambios en los paquetes de software.
		14.2.5.	Uso de principios de ingeniería en protección de sistemas.
		14.2.6.	Seguridad en entornos de desarrollo.
		14.2.7.	Externalización del desarrollo de software.
		14.2.8.	Pruebas de funcionalidad durante el desarrollo de los sistemas.
		14.2.9.	Pruebas de aceptación
	14.3. Datos de prueba.	14.3.1.	Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES	15.1. Seguridad de la información en las relaciones con suministradores.	15.1.1.	Política de seguridad de la información para suministradores.
		15.1.2.	Tratamiento del riesgo dentro de acuerdos de suministradores.
		15.1.3.	Cadena de suministro en tecnologías de la información y

		15.1.4.	comunicaciones.
	15.2. Gestión de la prestación del servicio por suministradores.	15.2.1.	Supervisión y revisión de los servicios prestados por terceros.
		15.2.2.	Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	16.1. Gestión de incidentes de seguridad de la información y mejoras.	16.1.1.	Responsabilidades y procedimientos.
		16.1.2.	Notificación de los eventos de seguridad de la información.
		16.1.3.	Notificación de puntos débiles de la seguridad.
		16.1.4.	Valoración de eventos de seguridad de la información y toma de decisiones.
		16.1.5.	Respuesta a los incidentes de seguridad.
		16.1.6.	Aprendizaje de los incidentes de seguridad de la información.
		16.1.7.	Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	17.1. Continuidad de la seguridad de la información	17.1.1.	Planificación de la continuidad de la seguridad de la información.
		17.1.2.	Implantación de la continuidad de la seguridad de la información.
		17.1.3.	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
		17.1.4.	
	17.2. Redundancias.	17.2.1.	Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.	18.1. Cumplimiento de los requisitos legales y contractuales	18.1.1.	Identificación de la legislación aplicable.
		18.1.2.	Derechos de propiedad intelectual (DPI).
		18.1.3.	Protección de los registros de la organización.
		18.1.4.	Protección de datos y privacidad de la información personal.
		18.1.5.	Regulación de los controles criptográficos.
	18.2. Revisiones de la seguridad de la información.	18.2.1.	Revisión independiente de la seguridad de la información.
		18.2.2.	Cumplimiento de las políticas y normas de seguridad.
		18.2.3.	Comprobación del cumplimiento.

Fuente: (ISO, 2013)

2.2. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Por lo expuesto anteriormente y en base a los resultados obtenidos en el análisis de vulnerabilidades con herramientas OSINT en la investigación "**Análisis de"** se presentan las siguientes POLITICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ESPAM MFL:

1. POLÍTICAS DE SEGURIDAD

Objetivo: Proporcionar dirección y soporte de la gestión de la seguridad de la información, aplicables a la ESPAM MFL alineados a las leyes, reglamentos vigentes.

1.1. DIRECTRICES DE LA DIRECCIÓN EN SEGURIDAD DE LA INFORMACIÓN

- **Conjunto de políticas para la seguridad de la información. -** El Director de la Unidad de Tecnología deberá aprobar el documento de políticas de seguridad de la información, el mismo que será publicado y comunicado al personal docente y administrativo de la ESPAM MFL.

  Revisión de las políticas de seguridad de la información. - La política de seguridad de información debe ser revisada, documentada, actualizada y socializada de forma permanente como establece la norma de referencia o cada vez que ocurran cambios importantes, mediante la presente política se podrá evitar el acceso no autorizado de usuarios internos / externos.

2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización.

2.1. ORGANIZACIÓN INTERNA.

- **Asignación de responsabilidades para la seguridad de la información. -** El Director de la Unidad Tecnología puede delegar funciones sobre seguridad de la información, a uno o varios integrantes del área.

- **Segregación de tareas. -** El Director de la Unidad de tecnología de deberá asignar un responsable de cada una de las actividades que tiene el área de Tecnología de la Información, con el objetivo de mantener un control adecuado de los activos de información y poder evitar accesos no autorizados; además el área de Tecnología deberá implementar controles de monitoreo para las actividades realizadas por todo el personal de TI, con el fin de revisar el cumplimiento de las mismas.

2.2. DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO

- **Política de uso de dispositivos para movilidad. -** El área de Tecnología deberá definir unas reglas de autentificación entre el dispositivo y la red de la institución, mediante la cual se pueda realizar el intercambio de información con dispositivos autorizados

3. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Objetivo: Asegurar que los usuarios conozcan en cuanto a la seguridad de la información para reducir el riesgo de robo, fraude o uso inadecuado de la misma.

3.1. ANTES DE LA CONTRATACIÓN

- **Términos y condiciones de contratación. –** Los integrantes del área de Tecnología deben firmar un compromiso de confidencialidad y resguardo de la información, dado a que en esta área se maneja información sensible de cada usuario perteneciente a la institución.

3.2. DURANTE LA CONTRATACIÓN

- **Concienciación, educación y capacitación en seguridad de la información. -** La ESPAM MFL, mediante el área de Tecnología deberá realizar capacitaciones periódicas sobre las políticas de seguridad de la información, con el fin de concientizar a los colaboradores sobre la criticidad de la información;

- También se deberá brindar capacitaciones a los usuarios al inicio de cada semestre académico sobre del uso y manejo de las aplicaciones académicas que se manejan en la institución, dichas capacitaciones se deberán realizar en ambientes de prueba para reducir el riesgo de error humano.

- **Procesos disciplinarios. -** El Director de Tecnología designará a los integrantes que dominen el tema de seguridad de la información para realizar las capacitaciones en cada área de la institución.
  - Es compromiso de los usuarios, asistir a las capacitaciones de forma semestral y acatar las disposiciones expuestas en cada una de ellas.

3.3. CESE O CAMBIO DE PUESTO DE TRABAJO

- **Cese o cambio de puesto de trabajo. -** El área de Talento Humano de la ESPAM MFL, deberá comunicar de forma inmediata la renuncia o desvinculación del docente y/o administrativo al área de Tecnología, para que este pueda dar de baja al usuario de los sistemas informáticos. Los usuarios que no se rijan a esta política se responsabilizan de las acciones que se generen por la omisión.
  - El área de Talento Humano de la ESPAM MFL, debe notificar inmediatamente el inicio y fin de los periodos de vacaciones de docentes y/o administrativos de la institución, para que se proceda a dar de baja a los mismos de los sistemas académicos durante las fechas indicadas. Los usuarios que no cumplan esta política se responsabilizan de las acciones que se generen por la omisión.
  - El área de Tecnología, debe informar al empleado de las obligaciones y responsabilidades en seguridad de la información que tiene durante el proceso de cambio de puesto de trabajo en la Institución.
  - Los integrantes del área de TI que se desvinculen laboralmente de la institución deberán entregar los activos que les fueron proporcionados en las mismas condiciones y estado para el respectivo control de inventarios

4. GESTIÓN DE ACTIVOS

Objetivo: Identificar los activos de la organización y definir las responsabilidades de actividad.

4.1. RESPONSABILIDAD SOBRE LOS ACTIVOS

- **Inventarios de activos. –** La ESPAM MFL, debe mantener un inventario de todos los activos de información, y los responsables de los procesos deben clasificar la información dependiendo de su valor, sensibilidad, riesgo de pérdida y requerimientos legales de retención.
- **Devolución de activos. -** Los docentes y/o administrativos deben devolver todos los activos que estén en su poder al finalizar su empleo, contrato o acuerdo.

4.2. CLASIFICACIÓN DE LA INFORMACIÓN

- **Clasificación de la información. -** La información debe ser clasificada en términos de la importancia de su relevancia frente a requisitos legales, valor, sensibilidad, y criticidad ante revelación o modificación no autorizadas.

4.3. CLASIFICACIÓN DE LA INFORMACIÓN

- **Eliminación de soportes. -** La Institución, establece la siguiente política en materia de respaldo y borrado seguro de la información:
    - Periódicamente se debe efectuar copia de respaldo de toda la información considerada confidencial o sensible y que se encuentre contenida en los equipos de la Institución.
    - Se deben adoptar procedimientos para la aplicación de técnicas de borrado seguro de información, mediante herramientas o procesos manuales y/o automáticos que permitan eliminar toda la información contenida en el equipo o dispositivo asignado a un funcionario o proveedor cuando sea necesario, ya sea por su desvinculación o por la baja del activo tecnológico.
    - Los procedimientos establecidos en esta política se deben aplicar a todo dispositivo de almacenamiento que contenga información confidencial o sensible para la Institución, como discos duros, tabletas, equipos móviles, entre otros.

- **Soporte físico en tránsito. -** El Director de la Unidad de Tecnología junto con los demás integrantes del área, deberán crear un procedimiento para el trasporte seguro de medios físicos que contengan información como: Discos Duros, Unidades extraíbles, portátiles y otros dispositivos de la institución, cifrando la información

5. CONTROL DE ACCESO

Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.

5.1. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS

- **Política de control de accesos. -** El Director de la Unidad de Tecnología proporcionará a los usuarios el manual de usuario para el correcto uso y manejo de los sistemas académicos.
    - Es obligatorio para los docentes, administrativos y estudiantes cambiar las contraseñas temporales en su primer acceso a las aplicaciones académicas.
    - No mostrar las contraseñas en pantalla cuando el usuario está ingresando a los sistemas.
    - Utilizar contraseñas seguras, para lo cual se debe cumplir los siguientes requisitos:
        - La contraseña debe tener una longitud mínima de 8 caracteres y máxima de 12 caracteres.
        - Usar mínimo una letra mayúscula
        - Usar mínimo una letra minúscula
        - Utilizar mínimo un carácter especial
        - Utilizar mínimo un número
        - La contraseña debe tener un periodo de vigencia, luego se debe cambiar por una nueva, y diferente a la anterior
        - No usar contraseñas que contengan relación con el usuario, nombres, apellidos, fechas de nacimiento, fechas de matrimonio.

- **Control de acceso a las redes y servicios asociados. -** El acceso a la red de la institución, debe ser otorgado solo a usuarios autorizados, debidamente asignado todos los roles y perfiles a los diferentes sistemas informáticos.

5.2. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS

- **Gestión de altas/bajas en el registro de usuarios. -** El área de Talento Humanos de la ESPAM MFL, deberá notificar al área de Tecnología la nómina del personal nuevo para la asignación de los accesos correspondientes en las aplicaciones académicas que maneja la institución.
    - El área de Talento Humanos, deberá informar a la Unidad de Tecnología de manera inmediata la baja de algún usuario que se desvinculo de la institución para su proceso de inactivación de los diferentes sistemas académicos. Las cuentas de acceso deben colocarse en estado Inactivo
- **Gestión de los derechos a acceso con privilegios especiales. -** La asignación de privilegios a usuarios en los sistemas informáticos se los realizará previa autorización del Director de Tecnología, con un documento firmado o un correo de autorización.
- **Retirada o adaptación de los derechos de acceso. –** La Unidad de Tecnología deberá revocar de manera inmediata los privilegios de los usuarios que cambiaron de puesto, con sus respectivas tareas o de aquellos a los que se les revoco la autorización por la máxima autoridad de la institución.

5.3. RESPONSABILIDADES DE USUARIO

- **Uso de la información confidencial para la autenticación. -** El usuario es responsable directo de su estación de trabajo y es su responsabilidad bloquear la cuenta de usuario de su equipo de cómputo cuando no esté presente en su lugar de trabajo.
    - Ningún usuario deberá acceder a las aplicaciones académicas, utilizando la cuenta de otro usuario.

- Es responsabilidad de los usuarios el uso que realicen en las cuentas de acceso y contraseñas que fueron otorgadas a los sistemas académicos y equipos de cómputo.
- Las contraseñas no deben ser almacenadas en dispositivos que no estén cifrados o escritas en lugares de fácil acceso como en cuadernos, escritorio o pegados en la pantalla.
- Los usuarios deben informar de manera inmediata a la Unidad de Tecnología sobre daños, fallas o amenazas detectadas en las aplicaciones académicas, bases de datos o red.
- La Unidad e Tecnología de la Institución no se responsabiliza por el mal uso y manejo que se dé al correo electrónico institucional.
- La cuenta del correo electrónico de los usuarios que terminen su relación laboral con la Institución debe ser desactivada de forma inmediata.

5.4. CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

- **Procedimientos seguros de inicio de sesión. -** Todos los equipos de cómputo, que tengan acceso a los sistemas de información, bases de datos, reportes deben contar con mecanismos de autentificación y privilegios de usuarios apropiados, según el tipo de información que está manipulando el usuario.
- **Gestión de contraseñas de usuario. -** Todas las contraseñas por defecto de servidores, bases de datos, sistemas informáticos, aplicaciones, Routers, Switch, Acces Point debes cambiarse antes de sacarlos a producción.
  - La Unidad de Tecnología asignará una cuenta de usuario y una contraseña a los usuarios, el primer inicio lo realizarán con las credenciales entregadas, luego deberán cambiarla para acceder a sus servicios.
  - Los usuarios podrán realizar cambios de su contraseña cuando crean necesarios o cuando alguna política de seguridad requiera hacerlo.

6. CIFRADO

Objetivo: proteger la confidencialidad, autenticidad o integridad de la información mediante la ayuda de técnicas criptográficas.

6.1. CONTROLES CRIPTOGRÁFICOS

- **Política de uso de los controles criptográficos. -** La institución utilizará controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización.
- **Gestión de claves. –** La Unidad de Tecnología efectuará procedimientos y asignación de funciones respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.
    - El uso de algoritmos de cifrado y las longitudes de clave deberán ser revisadas periódicamente para aplicar las actualizaciones necesarias en atención a la seguridad requerida y los avances en técnicas de descifrado.

7. SEGURIDAD FÍSICA Y DE ENTORNO

Objetivo: Proteger los activos de información, fortaleciendo la confidencialidad, disponibilidad e integridad mediante la seguridad física y ambiental.

7.1. ÁREAS SEGURAS

- **Controles físicos de entrada. -** Todos los lugares que son identificados como áreas restringidas y tengan información sensible para la institución, deben ser protegidos contra accesos no autorizados, utilizando medios y procedimientos tecnológicos o registro de ingresos.
    - Los usuarios que ingresen a los lugares donde se encuentra los sistemas de información deben llevar obligatoriamente su credencial de manera visible.
    - Los usuarios que ingresen en áreas restringidas deben registrar de forma obligatoria el ingreso, detalle de la visita y hora de salida
- **Protección contra las amenazas externas y ambientales. –** Es prohibido consumir líquidos y alimentos dentro de los centros de cómputo o áreas restringidas de la institución.

- El personal de limpieza, deberá recibir capacitaciones sobre seguridad de la información, debido a que por su actividad tienen acceso a los distintos equipos informáticos.
- El personal de limpieza de la Institución tiene prohibido el ingreso de maletas o material que no sea el relacionado a sus funciones.
- La ESPAM MFL., debe contar con extintores de incendios en aquellos ambientes que cuenten con equipos de procesamiento de información, con la capacidad de mitigar el fuego generado por equipos eléctricos o papel.

7.2. SEGURIDAD DE LOS EQUIPOS

- **Instalaciones de suministro. -** Todos los equipos que proveen información a la institución como centros de datos, equipos del área de sistemas deben tener ininterrumpida la energía eléctrica.
- **Seguridad del cableado.** - El técnico de infraestructuras debe realizar mantenimientos periódicos del cableado estructurado de la institución, pare prevenir daños ambientales e interceptación de datos.
  - El cableado estructurado debe estar claramente codificado, permitiendo identificar la estructura de conexión entre sitios de la institución.
- **Mantenimiento de los equipos. -** El Director de Tecnología junto con el técnico de soporte de infraestructura deben realizar planificaciones anuales de mantenimiento de equipos de cómputo en toda la institución, los cuales deben ser en horarios que no afecte el correcto funcionamiento del personal operativo.
  - El Director de tecnología se encargará de llevar registros de mantenimiento preventivo y correctivo de los equipos de cómputo.
  - Los usuarios que hayan recibido mantenimiento en sus equipos deben ser informados previamente por el encargo de Tecnología.
- **Políticas de puesto de trabajo y bloqueo de pantalla. -** Cuando el usuario requiera ausentarse de su puesto de trabajo debe bloquear el acceso a su equipo de cómputo, con un protector de pantalla y contraseñas seguras.

- Los usuarios tienen totalmente prohibido mover, instalar, reubicar los equipos y retirar los sellos de seguridad de los dispositivos de cómputo.
- Al terminar su jornada laboral, el usuario es responsable de apagar sus equipos informáticos, para evitar el acceso de terceros

8. SEGURIDAD EN LA OPERATIVA

Objetivo: Definir las reglas para asegurar las operaciones correctas y seguras de la Unidad de Tecnología.

8.1. PROTECCION CONTRA CODIGO MALICIOSO

- **Controles contra el código malicioso. -** Todos los equipos de cómputo de la institución deben tener instalado un antivirus actualizado.
  - Es responsabilidad de cada usuario revisar que todos los medios extraíbles sean analizados por un antivirus, antes de procesarlos en los computadores personales.

8.2. COPIAS DE SEGURIDAD

- **Copias de seguridad de la información. -** Las copias de seguridad de la información de los sistemas académicos que maneja la ESPAM MFL deben contar con un control de acceso restringido al personal autorizado.

8.3. REGISTRO DE ACTIVIDAD Y SUPERVISIÓN

- **Protección de los registros de información. -** El Director de Tecnología definirá la periodicidad de generar copias de seguridad de los sistemas de información de la institución.
  - Las copias de seguridad de la información deben ser resguardadas en unidades de almacenamiento en discos duros extraíbles en buen estado.
  - Cuando las unidades de almacenamiento extraíbles se encuentren en mal estado, se debe realizar un proceso de eliminación de información de forma segura, y posteriormente dar de baja de los activos.
- **Registro de actividad del administrador y operador del sistema. -** El Director de Tecnología junto con los demás miembros del área, deben

revisar los logs de auditoría de los administradores y operadores de los sistemas informáticos, con el fin de identificar brechas de seguridad y revisar sus actividades dentro del sistema.

8.4. CONTROL DEL SOFTWARE EN EXPLOTACIÓN.

- **Instalación del software en sistemas en producción. -** El Director de Tecnología designará al responsable para la instalación de los sistemas informáticos en la institución con las siguientes recomendaciones: a) Realizar procedimientos de instalación para cada aplicativo. b) Verificación: contar con los contactos de los soportes de sistemas de terceros. c) Se asegurará del correcto funcionamiento y actualización.

8.5. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

- **Restricciones en la instalación de software. -** La instalación de software en las computadoras de la institución, son funciones exclusivas de la Unidad de Tecnología con el personal de soporte y se deben tomar las siguientes observaciones: a) Se debe mantener una lista actualizada del software autorizado para la instalación. b) De forma permanente, el área de tecnología junto con el responsable de seguridad de información deberá revisar el software instalado en cada estación de trabajo. c) El uso de otros programas no autorizados dentro de la institución será considerado como una falta a la política de seguridad de información.

9. GESTIÓN DE INCIDINTES EN LA SEGURIDAD DE LA INFORMACIÓN

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, para obtener una respuesta rápida, efectiva y adecuada ante los incidentes de seguridad de información.

9.1. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS

- **Notificación de puntos débiles de la seguridad. -** Todos los usuarios de la institución, de manera obligatoria deberán reportar algún evento de seguridad de la información, que observe en su puesto de trabajo o áreas visitadas, y debe informar fallas en los sistemas informáticos.

- **Respuesta a incidentes de seguridad de la información. -** EL Director de Tecnología deberá designar una persona que se encargue de investigar adecuadamente los incidentes de seguridad reportados por todo el personal de la institución, y su respectiva solución a los mismos.

10. CUMPLIMIENTO

- Corresponde a los involucrados de la Unidad de Tecnología el cumplimiento del presente manual de políticas y procedimientos descritos bajo la presente Norma.

11. RESPONSABLES

La Institución desarrolla e implementa políticas y procedimientos que garantizan que las personas que por razón de su cargo o función tengan acceso a información privilegiada, conozcan las regulaciones aplicables y las sanciones vinculadas con su revelación, recomendación o uso indebido.

La máxima autoridad de la ESPAM MFL como órgano rector, a través de la Unidad de Tecnología y coordinador de TI, debe asegurar que cada uno de los directores de carrera, colaboradores, áreas de desarrollo de aplicaciones, área de redes y al área de datos (data center) reciban una copia y capacitación respecto a la presente Política.

La presente Política, además de ser distribuida, debe estar disponible en la página web de la Institución.

12. REFERENCIAS

IEDGE. (2022). *Políticas de Seguridad Informática 2022*.

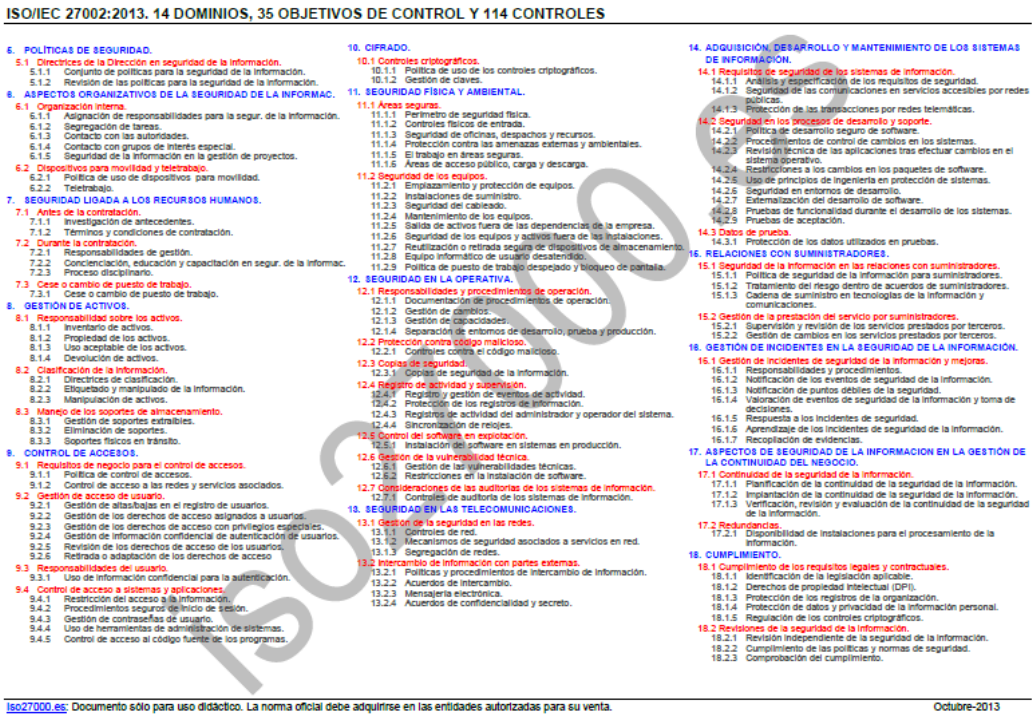
ISO. (2013). *ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES 5.*

ISOTools Excellence. (2017). *Norma ISO 27002: El dominio política de seguridad*. https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

Navarro, A. (2017). *Desarrollo de un modelo de Data Loss Prevention (DLP), en las instituciones de Educación superior (IES). Caso Universidad ECOTEC.*

ANEXOS

ANEXO INFORME DE POLITICAS 1. CONTROLES ISO/IEC 27002:2013



ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

Anexo 7 Políticas de distribución y difusión de la información.
Fuente: Los autores.