Desarrollo de una metodología como respuestas a incidentes de infección por ransomware

Juan David Rojas Rosero, juanrojas043@gmail.com
Freyder Alejandro Urbano Rosales, freurbano@gmail.com

Informe final para optar por el título de ingeniero de sistemas
Asesor: Edgar Rodrigo Enríquez, Magister,

Universidad Cesmag
Facultad de ingeniería
Programa ingeniería de sistemas
Pasto, Colombia
2023

Citar/How to cite	[1]	
Referencia/Reference	[1]	J. David Rojas Rosero, F. Alejandro Urbano Rosales, “Desarrollo de una metodología como respuesta a infecciones por ransomware.”, Trabajo de grado Ingeniería de Sistemas, Universidad Cesmag Pasto, Facultad de Ingeniería, 2023.
Estilo/Style: IEEE (2014)		

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Jurado 1

_____

Jurado 2

Nota de Exclusión

El pensamiento que se exprese en las obras e investigaciones publicadas o divulgadas por la Universidad CESMAG es de exclusiva responsabilidad de sus autores y no compromete la ideología de la institución.

Dedicatoria

Quiero aprovechar este momento para expresar mi más sincero agradecimiento a mi amada familia por su apoyo incondicional durante el proceso de completar mi proyecto de grado. Sin su aliento constante, su comprensión y su amor inquebrantable, este logro no habría sido posible. A mis padres, quienes siempre han sido mi mayor inspiración, les agradezco por su constante apoyo y por inculcarme el valor del esfuerzo y la perseverancia. Su sabiduría y ejemplo me han guiado a lo largo de este camino y me han impulsado a dar lo mejor de mí. A mi hermano, su apoyo y palabras de aliento han sido un bálsamo para mi alma en los momentos más difíciles. Gracias por creer en mí y por recordarme constantemente que puedo lograr cualquier cosa que me proponga. A mis abuelos, tías, tíos, primos y demás familiares que siempre han estado presentes en mi vida, gracias por su apoyo inquebrantable y por sus palabras de aliento en los momentos más importantes de mi carrera académica. Su amor y respaldo significan el mundo para mí. Finalmente, quiero expresar mi gratitud a todos mis amigos y seres queridos que me han apoyado a lo largo de este viaje. Sus palabras de aliento, su ayuda práctica y su presencia constante han sido un verdadero regalo. Su amor y apoyo incondicional han sido el pilar que me ha sostenido en este camino. Sin ustedes, esto no habría sido posible. Gracias de todo corazón.

Juan David Rojas Rosero

Dedicatoria

A mis familiares, que me brindaron su apoyo en las largas horas de trasnocho, esfuerzo, frustración y gozo; a mis amigos, que me aclararon tantas dudas y me acompañaron a través de un tema que no dominaba; a mis docentes y tutores, que ampliaron mi conocimiento mostrándome nuevos temas y maneras de comprenderlos, edificando siempre sobre conocimientos previos y retando mi capacidad de entender el mundo con perspectivas cada vez más ingeniosas; y a mis mascotas, que estuvieron siempre a mi lado, acompañándome en silencio. Este trabajo de grado es la cúspide de mi recorrido académico y va dedicado a todos y todas aquellas que lo hicieron posible. Gracias a ellos y ellas hoy estoy a tan solo un par de pasos de obtener mi título de pregrado.

Freyder Alejandro Urbano

Agradecimientos

Agradecimientos especiales al profesor Magister Edgar Rodrigo Enríquez R. que nos acompañó, entendió y nos guio con paciencia durante la concepción de esta idea con propuestas y maneras de ejecutarla.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Esta investigación estudia la problemática relacionada con infecciones tipo ransomware. Su objetivo principal es la creación de una metodología para afrontar este mal. Esta última se presenta a los usuarios en una página web la cual, de forma interactiva, fácil de manejar y entender, los capacitará y guiará en los pasos que la conforman.

Para la construcción de la página web se usa la metodología RUP la cual maneja fases claras de construcción las cuales se ajustan al tipo de software que se requiere erigir.

Mediante el uso de formularios dentro de la página creada se realizan encuestas a los usuarios, relacionadas con la aplicación de la metodología, evaluando varios aspectos de esta como son: facilidad de consulta, manejo, aplicación, y principalmente efectividad contra el ransomware involucrado.

La finalidad de la investigación se alcanzó porque mediante procedimientos de ingeniería de sistemas se logró implementar una metodología que al ser usada por los usuarios dieron buenas referencias con respecto a los beneficios que esta ofrece.

Palabras clave: Metodología, Capacitación, Ransomware.

ABSTRACT

This research studies the problems related to ransomware infections. Its main objective is the creation of a methodology to deal with this evil. The latter is presented to users in a web page which, in an interactive, easy to handle and understand way, will train and guide them through the steps that comprise it.

For the construction of the web page, the RUP methodology is used, which manages clear construction phases that are adjusted to the type of software that needs to be built.

Through the use of forms within the created page, user surveys are carried out, related to the application of the methodology, evaluating several aspects of it such as: ease of consultation, management, application, and mainly effectiveness against the ransomware involved.

The purpose of the research was achieved because by means of systems engineering procedures it was possible to implement a methodology that when used by the users gave good references regarding the benefits it offers.

Key words: Methodology, Training, Ransomware.

I. INTRODUCCIÓN

En la sociedad actual es muy común el uso de Internet, muchas personas usan dispositivos tecnológicos que hacen de la vida en línea algo común y accesible para todos. Pero existe un lado negativo que empaña todo este avance y por el cual el uso de la web necesita de una orientación, la cual se debe enfocar en el modo correcto de usar todas estas herramientas y aplicaciones que facilitan muchas actividades diarias pero que a su vez exponen a peligros a sus usuarios.

Según la organización internacional del trabajo [1] Se ha incrementado el uso de internet mediante el trabajo remoto y educación virtualizada todo por consecuencia de la pandemia provocada por el COVID 19 en 2020, lo que ha llevado a más gente a usar servicios que en algunos casos son desconocidos o nuevos para ellos. En consecuencia, los riesgos en la red son mayores ya que existen personas que se aprovechan de estos nuevos usuarios. Aquí aparecen los peligros más comunes como son la suplantación de identidad, el engaño web y el robo de contraseñas. Por este motivo la inseguridad informática se ha incrementado, según Portafolio [2] afirma que se han elevado en un 30 % los ataques cibernéticos a personas comunes como a organizaciones en Colombia.

Dentro de esta investigación, la cual está alineada a principios de seguridad informática, se estudia el problema relacionado con ataques cibernéticos, dentro de los muchos existentes se enfoca sobre uno de los más usados como es el Ransomware. Dicho esto, los autores muestran un estudio profundo sobre las variantes del malware nombrado, el cómo es usado, el para qué es usado y como fin de la investigación se explica el cómo hacer frente a un ataque como este, mediante el uso de una metodología que guíe a los usuarios a fortalecer su seguridad en la red.

Dicha metodología será implementada en un sitio web donde será utilizada por empresas que hayan sufrido ataques ransomware o que deseen capacitarse para reducir la posibilidad de ser infectados y así hacer frente a este problema.

II. PROBLEMA DE INVESTIGACIÓN

A. Objeto o tema de estudio

Infecciones por malware tipo ransomware.

B. Línea de investigación

La línea de investigación para este proyecto es la seguridad informática bajo el enfoque de mantener la integridad, disponibilidad y confiabilidad de la información.

Según Aguilera la seguridad informática se define como la "disciplina que se encarga de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable." [3]

C. Planteamiento del problema

La situación actual del mundo con respecto a la seguridad de la información cambio en 2020 por efecto de la pandemia por COVID 19, esto ha llevado a las personas en general a cambiar su manera de vivir incluyendo la forma de trabajar. La población en general ha tenido que reinventarse y adaptarse modificando su forma de avanzar para seguir subsistiendo, lo que ha llevado a buscar un nuevo bienestar tanto para sí mismo como para los suyos. Según Alarcón [4] Esto ha hecho que la economía cambie a un mercado que se denominó de bajo contacto, en muchos casos se implementó el trabajo y estudio desde casa además se empezaron a usar más herramientas tecnológicas básicamente porque la situación así lo requirió. Todo esto está directamente relacionado o vinculado al uso de Internet y para el caso puntual se relaciona con la seguridad de la información. Por motivo de estas nuevas implementaciones obligatorias se incrementaron los peligros, ya que la gente en general empezó a estar más conectada a la red lo que conlleva a estar más vulnerables a posibles ataques.

Dentro de todos los aspectos positivos que ha conllevado el uso de nuevas maneras de trabajo ligadas al uso de internet y sus herramientas, también se han generado muchos problemas, uno de los más importantes es la seguridad de la información. No obstante es correcto afirmar que el problema de seguridad para con la información ha estado presente desde tiempo atrás, y que ha tenido falencias y las seguirá teniendo, ya que en este sentido existe una constante evolución que abre las posibilidades a que aparezcan nuevos vectores de ataque por donde seguir realizando intentos maliciosos, uno de los más conocidos es el ransomware que según Varela [5], en su página web define como: tipo de software hostil que compromete a equipos atacados, secuestrando su información sensible para luego solicitar un rescate a cambio de la recuperación de dicha información, esto último genera infinidad de problemas ya que dentro de una computadora puede haber información sensible y de uso diario e inmediato.

Dentro de la sociedad actual tanto empresas como personas naturales están vulnerables a estos tipos de ataques, según la investigación realizada por Diazgranados [6], en su artículo expuesto en la página Kaspersky daily en su informe anual del Equipo de Investigación y Análisis de la compañía revela que: “se han incrementado en un 24% los ciberataques en la región latino americana durante los primeros ocho meses del año, comparándolo a 2020, el informe tiene en cuenta 20 de los malwares más usados o famosos, los cuales registran más de 728 millones de intentos de infección, un promedio de 35 ataques por segundo”.

Uno de los principales promotores de que los ataques informáticos sean cada vez más comunes es la desinformación, lo cual eleva el nivel de desconocimiento en materia de seguridad en la web para los usuarios que no conocen los protocolos de seguridad al exponer su información a todo tipo de conexiones. Otro promotor muy importante en este momento fue la pandemia en 2020, la cual ha causado un aumento exponencial en este tipo de ataques. De acuerdo a estadísticas de incursiones con ransomware realizadas actualmente se ha encontrado que Según Passeri [7], las estadísticas de ataques cibernéticos hacia las campañas por motivo de la pandemia de COVID-19 movieron las motivaciones de los atacantes con un aumento del 78,2% en agosto al 86.7% en septiembre de 2021. Por último y posiblemente el problema raíz para esta temática es el mal manejo de las mínimas estrategias de seguridad por parte de los usuarios, los cuales no hacen uso de estas últimas, siendo vulnerables al momento de usar dispositivos y redes domésticas o públicas.

El mundo actual está en constante evolución cibernética, lo que da paso a la creación constante de nuevas tecnologías de software. Por consiguiente, siempre existirá una nueva actualización para un ciberataque malicioso. Un ransomware liberado por sus mismos creadores es tomado por otros atacantes los cuales lo modifican y lo utilizan nuevamente para otros ataques. Según Alonso [8], esto crea una cadena de malware que es muy difícil de detener generando versiones actualizadas cada vez más sofisticadas y peligrosas.

D. Formulación del problema

¿Cómo afrontar incidentes de seguridad por infección de software malicioso tipo ransomware?

E. Objetivos de la investigación

1) Objetivo General

Realizar una metodología que apoye el cómo afrontar incidentes de infección por ransomware.

2) Objetivos Específicos

- Caracterizar los principales tipos de ataque relacionados a ransomware existentes, para que integren el músculo principal de la metodología.

- Desarrollar las actividades que integran la metodología planteada, en un entorno web enfocadas en la prevención y defensa en casos de ataque ransomware.

- Validar la implementación de la metodología en el sistema web mediante la realización de evaluaciones a usuarios dentro del sitio.

F. Justificación

La situación actual relacionada a ciberataques ransomware es problemática, ya que se ha incrementado el uso de este método para obtener beneficios económicos por parte de delincuentes que se dedican a esto. La protección de datos personales es importante para cualquier usuario, es

por eso que el ransomware está en constante evolución y cada vez sus ataques son más organizados y precisos, el cifrado de información genera tanto pérdidas de datos como económicos, es por eso que cada vez se hace más común que dirijan sus ataques a organizaciones, dentro de los datos almacenados por las empresas existe información delicada, es por esto que según Medina [9], las empresas recopilan datos necesarios y primordiales para poder seguir funcionando. Éstos deben estar protegidos de toda amenaza interna o externa, manteniéndolos confidenciales, íntegros y disponibles.

Es importante el conocimiento sobre seguridad informática, y puntualmente los tipos de ataque existentes, siendo el ransomware uno de los más usados, esto es muy importante para que la sociedad actual se actualice en métodos para hacer frente a este tipo de males. Los usuarios están indefensos frente a la posibilidad de caer de manera fácil en alguna de las trampas para infectar sus sistemas, según Palacio [10], en su artículo denominado ¡ojo!, usted puede ser la próxima víctima de ransomware dice que más del 90% de los ciberataques y sus filtraciones de datos resultantes comienzan con un correo de suplantación de identidad Spear. Mediante la creación de esta metodología, se darán a conocer los pasos a seguir para hacerle frente a un ataque de este tipo. Motivo por el cual se busca fortalecer las maneras de hacer respuesta frente a estos posibles ataques, actualizando su visión en este sentido, para formar un criterio general que logre orientar los pasos que se deben seguir de manera segura y profesional para recuperar la información sustraída.

Hacer que la población en general sea consciente de la existencia de este tipo de males y cómo enfrentarlos, es la meta a conseguir con esta investigación. Mediante el uso de la metodología que muestre los pasos para hacer respuesta frente a un mal tan famoso como es el ransomware. Esto sería un gran avance para la comunidad, ya que este mal es uno de los más usados y dañinos que existe.

G. *Delimitación*

Esta investigación está destinada a la obtención del título de ingeniero de sistemas lo cual se proyecta un tiempo estimado de 24 meses. Esta se realizará en la ciudad de San Juan de Pasto en el área de seguridad informática más concretamente relacionada con ciberataques y puntualmente

sobre la problemática del ransomware. La finalidad de la investigación es construir una metodología que apoye a los usuarios para hacerle frente a infecciones por dicho malware.

III. TÓPICOS DEL MARCO TEÓRICO

A. Antecedentes

1) Internacionales

El constante crecimiento del malware en la sociedad en los últimos años ha generado diferentes tipos de ciberataques en donde se han visto afectadas muchas empresas. Es por ello que hoy en día se busca tener unos estándares de seguridad que garanticen mitigar los riesgos que se puedan llegar a tener. Se tendrán en cuenta diferentes investigaciones existentes que ayudarán en el desarrollo del proyecto. A continuación, se muestran los antecedentes que se consideraron para la investigación.

En primer lugar, se optó por estudiar la investigación "**Metodología para la implementación de la gestión automatizada de controles de seguridad informática**" [11]. Realizada en el año 2016, en la ciudad de La Habana - Cuba tiene como objetivo general proponer una metodología para implementar la gestión automatizada de los controles de seguridad informática a través de la integración de los elementos que aportan los modelos, normas y metodologías. Como resultados de la investigación se observó durante el desarrollo del experimento la disminución de la complejidad y el aumento de la eficiencia tras la implementación de la gestión automatizada de controles de seguridad informática, en ambos casos en un factor cercano al 90%. Finalmente, las conclusiones establecidas son la implementación de gestión automatizada de controles de seguridad informática, esta es la combinación de varios métodos enfocados a la gestión de riesgos con un enfoque de automatización durante las etapas de operación, monitorización y revisión de un SGSI. Las tareas definidas en la fase de planificación, donde se incluye el análisis de riesgo como componente central, están destinadas a definir los objetivos de control para la determinación de controles automatizables. Otra consideración importante consiste en el carácter iterativo e incremental de la metodología, con el que el SGSI crece a medida que se culmina un ciclo tras haber implementado un nuevo control automatizado. Esta investigación brinda un aporte muy importante ya que implementa una metodología para la gestión de controles de seguridad, para la construcción de esta se utilizaron MAGERIT y OCTAVE que son de tipo descriptivas. Estas están

basadas en el análisis de los riesgos que se exponen los activos informáticos. Esto brindará información para la implementación de la metodología.

Por otra parte, se cuenta con la investigación "**Análisis de estrategias de gestión de seguridad informática con base en la metodología open source security testing methodology manual (osstmm) para la intranet de una institución de educación superior**" [12]. Realizada en el año 2018, en la ciudad de Guadalajara - México plantea como objetivo general revisar el entorno de la Institución de Educación Superior objeto de estudio, conociendo la cultura organizacional y políticas de seguridad informática implantadas. Presenta los resultados representados en métricas o RAV; además con esta metodología, se pretende cubrir la mayoría de los entornos que posee la Institución de Educación Superior objeto de estudio, el alcance de la investigación es de tipo descriptivo, como resultados de la investigación en la fase de entorno organizacional se encontraron que el 74% de las organizaciones en Latinoamérica, incluyendo el Ecuador, ha implementado la creación de políticas de seguridad aplicando controles como antivirus, firewall, controles de acceso entre otros. En la Fase de interacción se puede observar que los controles de interacción o Tipo A son un total de 63 que afectan directamente a la visibilidad, acceso y confianza (porosidad); en cambio, de los controles de proceso o Tipo B, se cuantifica un total de 22, los cuales proporcionan seguridad ante amenazas. Finalmente se concluye que en este trabajo se realizó una auditoría de seguridad informática a una institución de educación superior, mediante la aplicación de la metodología OSSTMM y pruebas de hacking ético, estableciendo métricas para evaluar el nivel de impacto y criticidad de las vulnerabilidades encontradas, en donde el principal hallazgo encontrado fue el valor de 72,15% de seguridad, equivalente a una seguridad informática media. Este proyecto brinda información muy importante en donde se utilizó la metodología OSSTMM que es de tipo cuantitativo, esto se lo utilizó para medir los riesgos que se presentaban en la institución de educación superior, esta brindara los datos necesaria para la construcción de la metodología.

Por último, la investigación denominada "**Ethical hacking aplicado al sistema de gestión documental de la onpe para evitar vulnerabilidades y acceso no autorizado a la información**" [13]. Realizada en el año 2018, en la ciudad de Lima-Perú plantea como objetivo general Implementar Ethical hacking aplicado al Sistema de Gestión Documental de la ONPE para evitar vulnerabilidades y acceso no autorizado a la información. La metodología que se utilizó fue la de

gestión y desarrollo de los productos de software en la Oficina Nacional de Procesos Electorales que es de propia autoría de la Institución, está diseñada a partir de un conjunto de buenas prácticas que tienen aceptación internacional alineada a estándares como la NTP-ISO/IECC 12207:2006 Tecnología de la Información Procesos del ciclo de vida del software (NTP ISO/IEC 12207, 2011), NTP-ISO/IEC 15504, Evaluando los procesos con (NTP ISO/IEC 15504, 2012) e ISO/IEC 24774 Life cycle management - Guidelines for process description (IEEE 24774-2012, 2012). Como resultados de esta investigación se obtuvieron que la colaboración en el informe fue con el rol de analista programador para realizar la implementación de buenas prácticas en seguridad informática al sistema de gestión documental en los módulos: Configuración, Documentos, Mesa de Partes, Consultas. La participación principal del suscrito fue la de implementar validaciones de accesos por roles y privilegios a las diferentes opciones que cuentan los usuarios del Sistema de Gestión Documental, además de validar y restringir el acceso al detalle de los documentos administrativos, personales y de Mesa de partes a aquellos usuarios que intenten acceder y/o modificar información que no le corresponda. Finalmente se concluye que se realizó las validaciones de accesos por roles y privilegios a las diferentes opciones que cuentan los usuarios del Sistema de Gestión Documental y se evitó la manipulación de parámetros mediante la transferencia de información a través de la encriptación de parámetros en el envío de las peticiones. Este proyecto brinda un aporte muy importante ya que propone una forma de proteger el acceso no autorizado a la información, este tiene una gestión documental extensa, esto ayudará a una correcta implementación de la metodología.

2) Nacionales

Para iniciar con los antecedentes nacionales estudiamos la investigación "**Protocolo de informática forense ante ciber incidentes en la telemedicina para preservar información como primera respuesta"** [14] realizada en el año 2021, en la ciudad de Bogotá Colombia, plantea como objetivo general presentar un protocolo de preservación de rastros y evidencias digitales ante ciber incidentes por medio de diferentes niveles de acceso de usuarios, con base en la informática forense. Como metodología implementada para esta investigación desarrollada de forma, analítica y exploratoria, parte de tres preguntas específicas que los autores se plantearon sobre la incidencia de los delitos cibernéticos en la telemedicina las cuales son: ¿cómo se podría utilizar la informática

forense en la telemedicina?, cuáles son las herramientas y funcionalidades disponibles de la informática forense? y ¿Cómo se debe desarrollar un protocolo para preservar rastros y evidencias de los registros digitales en telemedicina con varios niveles de acceso?. Lo cual da inicio a 3 etapas de la investigación como son: Análisis de antecedentes, evaluación de herramientas de la informática forense y su funcionalidad en modo live forensics y desarrollo del protocolo para preservar rastros y evidencias en telemedicina con varios niveles de acceso. Como resultados el presente estudio tuvo como objetivo preservar la memoria, por ser el primer paso en el análisis forense. Según Dfir It (2015), el software MoonSols DumpIt es una forma fácil de obtener memoria, incluso si el investigador no se encuentra físicamente frente al equipo o el sistema. Está diseñado para ser usado por un usuario no técnico; puede hacerlo el first responder en telemedicina que opera el equipo de imágenes. Basta con un doble clic en el ejecutable para generar una copia de la memoria física en el directorio actual. Durante las pruebas, DumpIt asignó 780 kb de memoria, lo que Dfir It califica como un gran resultado. Finalmente, la investigación concluye que el protocolo desarrollado para la preservación de rastros y evidencias conforma la primera respuesta digital que, mediante informática forense, puede ayudar en la toma de decisiones frente a ciber incidentes en el contexto de la telemedicina. De esta forma, el protocolo para la conservación de rastros y evidencias para la primera respuesta digital, con definición de niveles de urgencia para las acciones, ayuda a tomar decisiones sobre los pasos que se deben emprender y su prioridad ante un determinado ciber incidente en el campo de la telemedicina. Como se puede evidenciar en el anterior resumen de investigación, esta última es de gran importancia para el desarrollo del trabajo a desarrollar ya que muestra cómo actúa la informática forense ante casos de ataques cibernéticos y principalmente muestra el cómo actuar frente a estos.

Para continuar con antecedentes nacionales se estudia la investigación llamada **“Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas”** [15] realizada en el año 2017 en la ciudad de Pereira Colombia, tiene como objetivo general desarrollar un modelo de simulación que permita evaluar el nivel óptimo de seguridad que deben tener las organizaciones considerando aspectos relacionados con la reducción del riesgo y la obtención de beneficios empresariales. La técnica empleada para la construcción del modelo fue dinámica de sistemas, la cual permite modelar y analizar el comportamiento de sistemas complejos en el corto, mediano y largo plazo. Como resultados arroja que el período de tiempo considerado en el modelo,

estuvo comprendido de cero a seis meses con una periodicidad mensual. En primer lugar, se presenta el comportamiento semestral de las vulnerabilidades, ataques y de la seguridad dando como resultado una serie de porcentajes útiles para el análisis y aplicación del modelo creado. Para finalizar concluye que, si las organizaciones no cuentan con un plan director que guíe los esfuerzos de protección de los activos, por más dinero que inviertan en seguridad nunca alcanzarán niveles de seguridad satisfactorios, debido al alto costo de la seguridad de la información y al hecho de que una organización ciento por ciento segura es una meta casi imposible de alcanzar. Las organizaciones deben aprender a determinar la cantidad óptima de inversión en seguridad, tomando como base modelos financieros o basados en análisis económicos de costo beneficio. Para la investigación este referente es de gran importancia ya que muestra el problema que puede existir en las empresas al no implementar medidas de seguridad y arroja conclusiones tajantes como la de realizar una inversión temprana en este sentido.

Para terminar con la temática de antecedentes nacionales se estudia la realizada en la ciudad de Cali, Colombia del año 2020 denominada **“Predicción de ciberataques en sistemas industriales scada a través de la implementación del filtro kalman”** [16], la cual centra su objetivo general en presentar un modelo de predicción de posibles ciberataques en un sistema SCADA, dicha predicción se hace con un filtro Kalman. Para la realización del estudio se usó la metodología en diferentes fases como son: Fase 1 IDS, Fase 2 configuración SCADA y filtro Kalman y Fase 3 Pruebas. Presenta los siguientes resultados: como primera aproximación a la ejecución de solo tres ataques, permite visualizar un amplio rango de posibles eventos de seguridad que se pueden generar. Con respecto a otros procesos de seguridad sobre los sistemas SCADA, varias técnicas de detección y mitigación hacen uso de Machine Learning (ML), mostrando una alta precisión en la detección de ataques, incluyendo *DDoS.* Dichas pruebas se realizaron utilizando el conjunto de datos KDD'Cup99 para las técnicas de árbol de decisión, algoritmo de *Random* Forest (RF) y método *Naive* Bayes (NB). Como resultado, el clasificador RF fue el mejor con una ocurrencia del 99.99 %, mientras que NB obtuvo un 97.74 %. Respecto a los resultados anteriores, y teniendo en cuenta que el filtro Kalman tuvo la mejor probabilidad de predicción (98 %) para ataque 514 (ataque de escritura) y mejor tendencia a la reducción del error, es claro que el filtro Kalman tiene mucho potencial y puede verse en igualdad de condiciones con respecto al uso de ML, con la diferencia de que el uso de Kalman se realizó sobre datos reales de ataques en línea (ejecutados y

recolectados por un IDS en tiempo real). Por lo último la investigación concluye que poder predecir posibles eventos de seguridad les permitirá a las organizaciones gestionar de manera más proactiva los riesgos en sus sistemas industriales. La prevención como elemento fundamental en los planes de tratamiento de riesgos permitirán establecer diferentes rutas de actuación para lograr mitigar posibles ciberataques. Esto último es muy pertinente para la actual investigación ya que permite establecer un método funcional que puede ser afinado y utilizado para actuar frente a posibles eventos de seguridad lo cual tiene gran afinidad con la investigación.

3) Regionales

El potencial de ejecución de la investigación, cuando ésta esté en sus fases finales, será en gran medida la región Nariñense, por tal motivo se estudiaron una serie de referentes, de los cuales se tomaron los 2 más relevantes para la investigación los cuales son:

La investigación **‘La aplicación de la metodología owisam en la red inalámbrica de la institución universitaria cesmag’** [17] realizada en la ciudad de San Juan de Pasto en el año 2018 plantea como objetivo general aplicar la metodología OWISAM para medir el nivel de seguridad en la red inalámbrica de la universidad Cesmag. Para la aplicación de la metodología mencionada la investigación se rige bajo un enfoque cuantitativo ya que su estudio se basa en datos que se analizaran con base a reportes generados por la metodología OWISAM a partir de las variables de estudio. Al implementar y poner en funcionamiento la metodología arroja valores positivos ya que para identificar debilidades con respecto a los dispositivos wifi de la red se aplicaron una serie de ataques englobados en los controles OWISAM-D, todo esto con el objetivo de saturar los recursos de cómputo. Para contrarrestar esto se aplicaron controles como OWISAM-F, OWISAM-CF, OWISAM-AU Y OWISAM-HS, esto logró verificar y analizar las fortalezas y falencias que pudo tener la infraestructura para proteger los elementos de la red con el fin de minimizar riesgos a ataques contra la organización. Para finalizar la investigación concluyó que al implementar la metodología OWISAM dentro de la red de la Universidad Cesmag, esta última se fortaleció ya que se encontraron tanto puntos fuertes como débiles los cuales fueron fortalecidos logrando así reforzar la red. El anterior antecedente es importante para el desarrollo de esta investigación ya que

muestra una metodología como es la OWISAM que sirve como método de evaluación de seguridad Wireless abierta la cual muestra otro método aplicable relacionado a seguridad de la información.

De igual modo se continúa con la investigación **"Implementación de técnicas hacking al modelo de red inalámbrica en la institución universitaria Cesmag"** [18]. Realizada en el año 2017, en la ciudad de San Juan Pasto Colombia, plantea como objetivo general: mejorar el nivel de protección de la red inalámbrica Netsky para el protocolo 802,11 b/g/n/ac de la institución Universitaria Cesmag. La metodología que se usó en el campo investigativo fue la cuantitativa y se contextualiza dentro del paradigma positivista. Se aborda a partir del método científico ya que parte de una realidad tangible que usa información cuantificable con el fin de obtener validez universal. Mediante el uso de la herramienta Snort la cual arrojó resultados positivos a la hora de aplicar su funcionamiento, uno de estos fue mitigar los posibles ataques que se puedan ejecutar en la red inalámbrica Netsky. Se realizó una intromisión con la herramienta NMAP realizando un escaneo a la red en un ambiente controlado en la cual se encontraron una serie de puertos abiertos que se detectaron en tiempo real. Finalmente, y como conclusión se obtuvo que la investigación arroja un estudio de la red inalámbrica Netsky de la Institución Universitaria Cesmag, mediante una encuesta se evaluaron aspectos como: Red inalámbrica, estructura, normas o políticas de seguridad, diseño y seguridad. Ítems que generaron resultados positivos haciendo viable la implementación de la red en la institución la cual garantiza wifi a todas las áreas requeridas. Para la investigación el anterior referente muestra la importancia de realizar estudios o sondeos a las redes ya sean institucionales o corporativas, con el fin de mejorarlas en cuanto a seguridad garantizando la confianza en su uso. Pero lo más relevante es el uso de herramientas tanto para localizar falencias como para detectar actividades de intromisión.

B. Supuestos teóricos de la investigación

1) Seguridad Informática

Gómez [19], afirma que la seguridad informática puede definirse como: el conjunto de métodos y de varias herramientas para proteger el principal activo de una organización como lo es la

información o los sistemas ante una eventual amenaza que se pueda suscitar. Para entender mejor el concepto de seguridad informática se deben conocer los siguientes conceptos:

2) Concepto de autenticación

Según Castro [20] en su trabajo Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades afirma que: La autenticación se puede definir como un proceso en el que se busca confirmar algo como verdadero, no se busca verificar un usuario, ya que la autenticación no siempre está relacionada con estos, en muchos casos se quiere saber si un cambio o un dato es correcto, no se debe cometer el error en pensar que solamente las personas necesitan este proceso, este puede ser para cualquiera, un sistema, un dispositivo o una persona.

3) Cifrado

Se define como cifrado a la actividad de convertir datos de un formato legible a un formato codificado los cuales solo se pueden leer después de ser descifrados. Esta es la base de la seguridad de datos, es la forma más sencilla para asegurar y garantizar que la información de una base de datos empresarial o de otra índole, no pueda ser leída al ser extraída de forma fraudulenta. Este método es usado tanto por usuarios comunes como por grandes organizaciones, aplicando lo que se conoce como algoritmo de cifrado el cual desarrolla un esquema de cifrado que en teoría solo se puede deshacer mediante el uso de gran potencia de cómputo. Afirma Pérez [21], que el día que elijan cifrar los documentos CAD/CAM o el código fuente de las múltiples aplicaciones o el código ya compilado y en ejecución, esto conllevara a diferentes efectos que pueden llegar a ser catastróficos.

El cifrado implica convertir texto sin formato legible por humanos en un texto incomprensible, conocido como texto cifrado. En esencia, esto significa tomar datos legibles y cambiarlos para que se vean como algo aleatorio. El cifrado implica utilizar una clave criptográfica; un conjunto de valores matemáticos que acuerdan tanto el emisor como el receptor. El receptor utiliza la clave para descifrar los datos y volver a convertirlos en texto sin formato legible [22].

C. Métodos de cifrado

Existen tres métodos para encriptar los cuales son: Simétrica: según Kaspersky [23], este tipo de criptografía está basado en métodos criptográficos que usan una misma clave para cifrar y descifrar el mensaje, estos extremos cuando establecen la comunicación deben establecer un acuerdo sobre la clave que tienen que usar, para posteriormente los dos tener acceso a la misma clave, en donde la remitente cifra el contenido de la misma y el destinatario la descifra con el mismo mecanismo. Se pueden indicar varios ejemplos de cifrado simétrico.

- Algoritmo de cifrado DES, usa claves basados en 56 bits
- Algoritmos de cifrado 3DES, *Blowfish*, e IDEA, usan claves de 128 bits
- Algoritmos de cifrado RC5 y AES

Asimétrico: Según Kaspersky [24] indica que este tipo de encriptación se basa en que si el emisor cifra la información el receptor lo puede descifrar o viceversa, en este caso cada usuario del sistema debe poseer una pareja de claves y se tiene dos tipos.

- Clave privada: Custodiada por el propietario, por lo tanto, solo él tiene acceso a ella sin darla a conocer a nadie.
- Clave pública: conocida por uno o todos los usuarios. Como ejemplo de este tipo de algoritmos usados por este tipo de cifrado se tiene a MD5 y SHA.

La Firma digital: Según la UPV [25]Es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje. El objetivo de la firma es autentificar la identidad de quién envía el mensaje y quién firma el documento, las firmas digitales acostumbran manejar diferentes datos, además de información que se envía, por ejemplo, la hora y la fecha en que se hizo. La firma digital es una forma matemática de adjuntar la identidad de una persona a un mensaje, está basada en la criptografía de clave pública, esto quiere decir que estos sistemas están utilizando dos claves, la primera sería la clave pública que es la que se conoce y la otra clave sería una clave privada qué es la que solamente el emisor del mensaje conoce.

Los protocolos WEP, WPA, WPA2 y WPA3 Según Antelec SL [26] son los estándares de seguridad inalámbrica más utilizados. Aunque tienen el mismo propósito, cada uno de ellos es diferente a su manera. Dichas normas no sólo evitan que se realicen conexiones no deseadas a las redes inalámbricas, sino que también cifran datos privados enviados a través de la red. Tienen algo en común, las cuatro son aplicadas a las señales inalámbricas y están basados en protocolos de conexión Wifi la primera y la segunda se basa en servidores de autentificación. Cuando la seguridad de cifrado consiste en la clave y no el algoritmo un sistema de cifrado se puede considerar como bueno. La mayoría de las aplicaciones que se dan a la encriptación hoy en día son:

- Mensajes de autenticidad
- Facturas electrónicas
- Banca electrónica
- Votos electrónicos
- Notificaciones
- Mensajería instantánea
- Correos electrónicos
- Almacenamiento de información

Tipos de software malicioso

Existen diferentes tipos de software malicioso como:

1) Virus informático:

Según Fernández [27] Se define a un virus informático como un tipo de malware cuyo objetivo es alterar el correcto funcionamiento de un dispositivo. Lo hace infectando los ficheros de un ordenador mediante un código maligno, y su principal característica es que necesita de la intervención del usuario para ser ejecutado. Momento en el que toma el control con el objetivo de infectar un ordenador y propagarse.

Aunque el primer virus informático apareció en 1971, no fue hasta los años 80 del siglo pasado que se adoptó oficialmente el término. Este nombre es debido a su parecido con los virus biológicos que infectan a una célula, y esta a su vez propaga el virus al resto de células de un organismo.

Hay diferentes tipos de virus, desde los que son simples bromas hechas con la única función de molestar hasta otros que pueden dañar muy seriamente los ordenadores borrando archivos que repercuten directamente en su funcionamiento. En cualquiera de los casos, su punto en común es que todos modifican el normal comportamiento de un ordenador.

Por lo general los virus son totalmente transparentes. No se esconden, sino que suelen viajar dentro de archivos ejecutables como los (.exe) de Windows. Eso sí, pueden hacerlo con los nombres de otras aplicaciones en un intento de engañar y tratar de inyectar el programa.

2) Troyano:

Según Muñoz [28], afirma que el troyano es un programa malicioso que pretende ser algo legal o inofensivo, intentando acceder a la computadora o dispositivo móvil de la víctima y realizar diferentes tipos de operaciones maliciosas. Se pueden ocultar de muchas formas, incluidos archivos de audio, archivos ZIP, RAR, extensiones de navegador, instaladores de software legítimos, archivos de actualización o aplicaciones de teléfonos móviles, etc.

3) Gusano informático:

Para González [29] El gusano informático es un software malintencionado que se duplica y se replica a sí mismo para propagarse a equipos no infectados. Los gusanos suelen utilizar partes del sistema operativo que son automáticas e invisibles para el usuario. Por lo general, los gusanos sólo se notan cuando la replicación incontrolada consume recursos del sistema, ralentizando o deteniendo otras tareas.

Cuando consigue penetrar en un equipo, el gusano intenta obtener las direcciones de otros ordenadores mediante las listas de contactos para enviarles copias y tratar de infectarlos también.

No tienen por qué manipular ningún programa ni hacer que el ordenador funcione incorrectamente, lo que los hace un poco más difíciles de detectar.

Para hacerlo es recomendable revisar los recursos que pudiera estar consumiendo, como la RAM, algo que hará que tareas ordinarias se vuelvan excesivamente lentas. De tener uno, también es posible que el equipo haya enviado mensajes sin permiso por correo electrónico o redes sociales.

En cuanto a su uso, hoy en día estos gusanos suelen utilizarse por ejemplo para crear botnets. Se tratan de redes de ordenadores zombis que pueden actuar de forma simultánea cuando un operador le da la orden para enviar SPAM de forma masiva, difundir malware o lanzar diferentes tipos de ataques informáticos ataques DDoS o de denegación de servicio [30].

4) Spyware:

Según Alestra [31] afirma que el spyware está diseñado para rastrear y utilizar contenido informático sin que el usuario se dé cuenta, siempre por motivos delictivos. Este software espía es el equivalente a un acosador web y como la mayoría de los otros programas infecciosos, ingresa a la computadora descargando archivos, correos electrónicos o sitios web sospechosos y maliciosos.

5) Ransomware:

Término que proviene del inglés que indica un tipo de software malicioso el cual bloquea el acceso a los datos almacenados en la computadora o cualquier dispositivo compatible con el malware. El atacante exige una recompensa por la recuperación de la información secuestrada. El término se forma de unir ransom (rescate, en inglés) y ware (producto o mercancía). El malware pide un rescate (ransom) a la víctima, a través de un mensaje o una ventana emergente, de ahí el nombre [32].

Este tipo de programa puede acceder al ordenador a través de un gusano informático u otro tipo de malware, y una vez cifre los datos bloqueará el ordenador mostrando una pantalla de advertencia

en la que se te informa que ha sido víctima del ataque. En esa pantalla se muestra también la cantidad a pagar y el método de pago, que puede ser por SMS, Paypal o mediante bitcoins.

Se trata de una de las amenazas que más está creciendo en los últimos años, por lo que es importante tener el ordenador siempre actualizado y seguir una serie de precauciones a la hora de enfrentarte a correos electrónicos o mensajes sospechosos, evitando siempre instalar nada que te manden por correo personas que no conozcas.

Otro consejo en el que coinciden casi todos los expertos en seguridad informática es que hay que tratar de no pagar nunca el rescate que se pide. Haciéndolo se logra que los criminales se salgan con la suya, y fomenta el que sigan recurriendo a este tipo de programa. El método más fácil de combatirlo es tener siempre copias de seguridad actualizadas de las bases de datos y formatear los equipos afectados recuperándose después con estas copias.

El Ransomware ha generado muchos casos que han impactado en la sociedad, según Rus [33] en su artículo, la curiosa historia del primer ransomware del mundo, su inventor y la víctima que consiguió eludirlo, dice que Eddy Willems un trabajador belga fue una de las primeras víctimas de ransomware de la historia informática. Para el año 1989 le fue sugerido revisar un disquete recibido de la OMS (Organización Mundial de la Salud), el cual estaba relacionado a estudios de Sida y se encontró un hackeo que le pedía 189 dólares. Cuando Eddy ingresó el diskette en los ordenadores no se desplegó la investigación médica sino el que es conocido como el primer ransomware de la historia del mundo. Solicitaba 189 dólares los cuales deberán ser enviados a una cuenta en Panamá, al final no se pagó el rescate y no se perdió la información sensible del disquete, la cual fue de fácil reversión y recuperación. Pero el caso no fue el único, se habían enviado 20.000 disquetes por correo postal a todo el mundo todos iban con el que luego se conoció como AIDS Troyan el cual logró causar muchos estragos ya que era nuevo a pesar que eludirlo era relativamente fácil. Las fuerzas del orden, de la época, rastrearon el origen del envío de los discos y llegaron a un biólogo evolutivo de Harvard llamado Joseph Popp el cual fue judicializado.

Otros casos sensibles son los presentados en la página de Kaspersky [34] la cual, en su artículo, Identificación de ransomware: en que se diferencian los troyanos de cifrado, muestra los siguientes casos:

Ransomware para WordPress el cual está dirigido a los archivos de los sitios web. Este malware ataca al cliente más popular cifrando sus datos y solicitando un rescate para la recuperación de los mismos. La probabilidad de ser víctima está directamente relacionada al número de visitas del sitio web desarrollado en la plataforma.

El caso Wolverine el cual trata sobre la empresa Wolverine Solutions Group empresa que presta servicios para el sector salud fue víctima en septiembre de 2018 de un ataque ransomware. El cual cifró una gran cantidad de archivos y dejó a sus empleados sin acceso a ninguno de ellos. Para octubre, personal especializado en técnicas de informática forense habían logrado descifrar y restaurar la información. Pero durante el ataque una gran cantidad de información médica fue expuesta y es posible que los ciber delincuentes hayan retenido nombre, direcciones, información médica y otros datos confidenciales.

Por último, pero no menos importante tenemos a él que es conocido como el más grande ataque ransomware de la historia el cual se denomina Kaseya, nombrado así por el nombre de la empresa atacada. La compañía de servicio de proveedor remoto y actualizaciones de sistemas operativos para dispositivos de red está especializada en brindar una alta automatización en la gestión de todos los dispositivos de red a través de una única solución, aquí fue encontrada su debilidad ya que se podía visualizar todo lo que estaba pasando en la red con todos los privilegios en esta, este fue el punto que trataron de explotar los hackers para para causar desperfectos.

El grupo Revil causante del ataque, implantó un ransomware en la última actualización del software y cuando los usuarios descargaron e instalaron el archivo este venía con el malware el cual rápidamente se multiplicó por toda la red cifrando los datos de millones de usuarios. Para la liberación de este cifrado exigieron la suma de 70 millones de dólares. Algunos tipos de Ransomware más comunes son:

- Ryuk: Según Pastor [35], define a Ryuk como un tipo de ransomware que cifra dispositivos de red junto con la eliminación de instantáneas almacenadas en los puntos finales. Este se dirige a grandes organizaciones y agencias gubernamentales que terminan pagando grandes sumas de dinero.

- Sodinokibi: Jiménez [36] explica que sodinokibi es uno de los ransomware más peligrosos y comunes, es una amenaza que intenta cifrar los archivos de la víctima. A cambio de permitirles abrir esos archivos les exigen un rescate financiero, con el tiempo ha perfeccionado sus técnicas de ataque y ocultación. Lógicamente hablando, este problema pondrá en peligro la seguridad y privacidad de los usuarios. Sodinokibi ha implementado realizar el pago a través del Monero, lo que imposibilita el seguimiento de los pagos. Así que no pueden averiguar quién recibió el dinero.

- WannaCry: Ramírez [37], define a WannaCry como un malware de tipo troyano que ha estado causando varios ataques de ransomware y es considerado uno de los malwares más peligrosos. De hecho, en 2017 el concepto de rescate fue de lleno al público, afectando a unos 200.000 usuarios de unos 150 países. Estos usuarios incluyen grandes empresas e instituciones públicas.

- Cryptolocker: Belcic [38], explica que este tipo de malware cifra los archivos en un ordenador con Windows y luego exige un rescate a cambio de la clave de descifrado. Cryptolocker Apareció en septiembre del 2013 y este lanzó un ataque continuo que tuvo una duración hasta mayo del 2014. Este tipo de ransomware engaña a su objetivo para que descarguen archivos maliciosos adjuntos que le envían a su correo electrónico. Una vez abiertos, estos troyanos ejecutan su malware oculto.

- STRRAT: Romero [39], afirma que STRRAT es un tipo de malware basado en Java que se disfraza como ransomware, pero en realidad es un troyano de administración remota. Este infecta las computadoras a través de una campaña de correos electrónicos fraudulentos. Es una amenaza en la que hay que prestarle más atención, este puede generar daños realmente importantes.

D. Informática Forense

Según Hidalgo [40], se considera que el Análisis Forense Informático consiste en la aplicación de técnicas científicas y analíticas especializadas a una infraestructura tecnológica que permite identificar, preservar, analizar, y presentar datos que sean válidos dentro de un proceso legal. Cuando se requiere de servicios profesionales para ejecutar un análisis forense o peritaje, es prioritario salvaguardar toda la información que luego será o no judicializada. El conocimiento del informático forense abarca aspectos no solo del software, sino también de hardware, redes, seguridad, hacking, cracking, recuperación de información. Es muy importante tener clara la diferencia entre informática forense, seguridad informática y auditoría, para evitar confusiones como la que vincula a la primera con la prevención de delitos, cuando la que se encarga de esto es la seguridad informática.

1) Perito Forense

Según la redacción de la página MCPRO [41] Un Perito Informático Forense es un profesional con conocimientos, habilidades y experiencia que se necesitan para ayudar en los juicios y los tribunales a esclarecer delitos cibernéticos. Los ordenadores, teléfonos inteligentes, tabletas, Internet… almacenan todos los datos que se realizan, y un perito informático tiene que ser capaz de extraer las evidencias electrónicas irrefutables que sean esenciales para resolver cualquier conflicto. En muchas ocasiones, son los encargados de encontrar las pruebas de los delitos. Pero además de la rama judicial, también pueden trabajar para las grandes empresas con el objetivo de evitar espionajes, fraudes, robos de información, manipulación de datos y programas, etc., que pueden ocasionar grandes pérdidas a las compañías.

2) Metodología para el análisis forense de evidencias digitales

Según el artículo presentado en la página Welivesecurity [42] by ESET, Usualmente está dividido en cinco fases que nos ayudan a mantener un estudio estructurado, facilitando la verificabilidad, la reproducibilidad del análisis. Las etapas del análisis forense son:

Adquisición: En esta fase se obtienen copias de la información que se sospecha que puede estar vinculada con algún incidente. De este modo, hay que evitar modificar cualquier tipo de dato utilizando siempre copias bite a bite con las herramientas y dispositivos adecuados. Cabe aclarar que este tipo de copia es imprescindible, debido a que dejará recuperar archivos borrados o particiones ocultas, arrojando como resultado una imagen de igual tamaño al disco estudiado.

Preservación: En esta etapa se debe garantizar la información recopilada con el fin de que no se destruya o sea transformada. Es decir que nunca debe realizarse un análisis sobre la muestra incautada, sino que deberá ser copiada y sobre la copia se deberá realizar la pericia. De este modo, aparece el concepto de cadena de custodia, la cual es un acta en donde se registra el lugar, fecha, analista y demás actores que manipularon la muestra. En muchos casos se deben utilizar técnicas de Hashes para identificar de forma unívoca determinados archivos que podrían ser de gran utilidad para la investigación.

Análisis: Finalmente, una vez obtenida la información y preservada, se pasa a la parte más compleja. Sin duda, es la fase más técnica, donde se utilizan tanto hardware como softwares específicamente diseñados para el análisis forense. Si bien existen métricas y metodologías que ayudan a estructurar el trabajo de campo, se podrán obtener grandes diferencias dependiendo de las herramientas que se utilicen, las capacidades y experiencia del analista. Además, es muy importante tener en claro qué es lo que se investiga, debido a que esto dará un enfoque más preciso a la hora de ir a buscar pruebas. Sin embargo, el estudio de la línea de tiempo (timeline), logs de accesos y una descarga de la memoria RAM será muy útil para la mayoría de las pericias. Es muy importante en esta instancia la evaluación de criticidad del incidente encontrado y los actores involucrados en él.

Documentación: Si bien esta es una etapa final, se recomienda documentar todas las acciones a medida que vayan ocurriendo. Aquí ya se debe tener claro por el análisis realizado qué fue lo que sucedió e intentar poner énfasis en cuestiones críticas y relevantes a la causa. Se debe citar y adjuntar toda la información obtenida, estableciendo una relación lógica entre las pruebas obtenidas y las tareas realizadas, asegurando la repetibilidad de la investigación.

Presentación: Normalmente se suelen usar varios modelos para la presentación de esta documentación. Por un lado, se entrega un informe ejecutivo mostrando los rasgos más importantes de forma resumida y ponderando por criticidad en la investigación sin entrar en detalles técnicos. Este informe debe ser muy claro, certero y conciso, dejando afuera cualquier cuestión que genere algún tipo de duda.

Un segundo informe llamado “Informe Técnico” es una exposición que detalla en mayor grado y precisión todo el análisis realizado, resaltando técnicas y resultados encontrados, poniendo énfasis en modo de observación y dejando de lado las opiniones personales.

E. Entornos virtuales

Es aquel entorno en el que se unen diferentes aplicaciones que necesitan de una pantalla de computador, en donde recrean un entorno real generando una sensación de interacción. Usan un modelo de entorno que representa un tipo de vida real, un lugar o estructura artificial por medio de gráficos tridimensionales. Existen varios tipos de entornos virtuales los cuales son: entornos virtuales comparativos, los cuales incorporan entornos visuales de interacción donde los participantes pueden actuar mutuamente o con objetos del entorno creado en 2 o 3D. Siguiendo con los tipos de entornos el siguiente es el colaborativo, el cual está desarrollado con entornos en los cuales los participantes pueden compartir documentos y artefactos de forma colaborativa. Y para terminar el entorno virtual multiusuario, el cual es usado para juegos de rol donde muchos usuarios se conectan, como ejemplo están Fortnite, League of Legends entre otros.

1) Máquinas Virtuales

Según Red hat [43], una máquina virtual (VM) es un entorno virtual que funciona como sistema informático virtual con su propia CPU, memoria, interfaz de red y almacenamiento, pero se crea en un sistema de hardware físico, ya sea en las instalaciones o no. El sistema de software se llama hipervisor, y se encarga de separar los recursos de la máquina del sistema de hardware e implementarlos adecuadamente para que la VM pueda utilizarlos.

Las máquinas físicas equipadas con un hipervisor, como la máquina virtual basada en el kernel (KVM), se denominan máquinas host, computadoras host, sistemas operativos host o simplemente *hosts*. Las diversas máquinas virtuales que usan sus recursos son máquinas guest, computadoras guest, sistemas operativos guest, o simplemente *guests*. El hipervisor utiliza los recursos informáticos, como la CPU, la memoria y el almacenamiento, como un conjunto de medios que pueden redistribuirse fácilmente entre los guests actuales o en las máquinas virtuales nuevas. Las VM se encuentran aisladas del resto del sistema, pero puede haber varias VM en una sola pieza de hardware, como un servidor. Además, pueden trasladarse entre los servidores host en función de la demanda, o para utilizar los recursos de forma más eficiente. Las VM permiten que se ejecuten varios sistemas operativos diferentes a la vez en una misma computadora, como una distribución de Linux en una computadora portátil MacOS. Cada sistema operativo funciona de la misma manera en que un SO o una aplicación lo haría normalmente en el hardware del host. Por eso, la experiencia del usuario final emulada dentro de la máquina virtual es casi idéntica a la experiencia de un sistema operativo en tiempo real que se ejecuta en una máquina física.

2) Hipervisores

Ranchal [44] dice que un hipervisor es una pantalla de máquina virtual que permite trabajar con tecnologías de virtualización, y es una forma rápida, conveniente y segura de ejecutar o probar un sistema operativo, aplicación, juego o emulador, independientemente con el sistema principal actuando como host. Existen 2 tipos de hipervisores los cuales son:

- Hipervisor Tipo 1: Según Ortiz [45], dice que el Hipervisor de Tipo 1 es un sistema muy básico en el que se ejecutan las máquinas virtuales. Esto significa que el hardware real en el que se ejecuta el hipervisor solo se utiliza con fines de virtualización, no se podrán utilizar para ninguna otra función.

- Hipervisor Tipo 2: “También conocidos como hipervisores alojados, se ejecutan en un sistema operativo como un programa más. Algunos de los más conocidos son VMware, Workstation y Oracle VirtualBox” [46].

3) Virtualización

Para Maldonado [47], la virtualización es la creación de una forma virtual de un recurso de computación como una computadora, servidor, otro componente de hardware, o un recurso de software como un sistema operativo. El ejemplo más común de virtualización es partir un disco duro durante la instalación de un sistema operativo, en la que el disco duro físico se divide en múltiples discos lógicos para proveer un mejor almacenamiento y recuperación de datos".

- Virtualización de red.
- Virtualización de servidor.
- Virtualización de escritorio.
- Virtualización de hardware.
- Virtualización de software.

De todos los anteriores, la virtualización de servidor es la más usada. Esta requiere agrupar recursos de uno o más servidores físicos y partirlos en múltiples servidores virtuales. Las Ventajas de la virtualización son obtener un mejor desempeño y eficiencia de los recursos en los componentes de computación existentes, mejorar la seguridad de la máquina virtual, ahorro de dinero en el hardware y tranquilidad ya que las máquinas virtuales son más confiables en cuanto a recuperación ante desastres, respaldos y recuperación de capacidades.

F. Conexiones

1) USB Tipo A

Llamados oficialmente Standart-A, los conectores USB tienen una forma rectangular plana y sus versiones más comunes son USB 3.0, 2.0 y 1.1. Son utilizados para conectar muchos dispositivos y se pueden encontrar en casi cualquier dispositivo moderno. Según neoguias.com, estos conectores también se encuentran en otros dispositivos similares a ordenadores, como consolas de videojuegos (PlayStation, Xbox, Wii, etc.), receptores caseros de audio/vídeo, televisores

"inteligentes", DVRs, reproductores Streaming (Roku, etc.), reproductores DVD y Blu-ray, entre otros [48].

2) USB Tipo C

Según Xataka, el conector USB Type C (o tipo C) es un formato pequeño que permite la conexión de cables y dispositivos USB de diferentes estándares. Es importante destacar que el tipo C es solo un tipo de conector y no influye directamente en la velocidad de transmisión ni en la tecnología que se utiliza detrás [49].

3) Cable Ethernet (Rj45)

Según Telecocable Es una interfaz física usada para conectar redes de cableado estructurado, (categorías 5e, 6 y 6A). Posee ocho pines o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado. Es utilizada comúnmente con estándares como TIA/EIA-568-B, que define la disposición de los pines. Su principal aplicación es el uso en cables de red Ethernet, donde suelen usarse 8 pines (4 pares) [50].

4) Conexión Wifi:

WiFi utiliza ondas electromagnéticas para comunicarse con su entorno sin requerir de una guía de ondas. Según GEEKNETIC, las conexiones wifi utilizan ondas electromagnéticas para comunicarse sin necesidad de guía de ondas. Aunque su alcance está limitado, es ampliamente utilizado en redes inalámbricas. Para aislar un equipo infectado, se recomienda desconectarlo de la red wifi. Es importante cambiar todas las contraseñas de la red y actualizar las credenciales de las cuentas online registradas. Para desconectar un portátil de la red wifi, basta con desactivar la opción wifi del dispositivo, mientras que para los equipos de escritorio se debe desconectar el cable RJ45 [51].

5) Conexión Bluetooth.

De acuerdo con Digital Guide IONOS, Bluetooth es una tecnología de red estandarizada por el grupo de trabajo IEEE 802.15.1 del Institute of Electrical and Electronics Engineers

estadounidense. Esta tecnología permite la transferencia de voz y datos punto a punto entre dos dispositivos digitales diferentes sin necesidad de conexión física. Su principal objetivo es sustituir las conexiones por cable, lo que resulta especialmente beneficioso para dispositivos móviles como smartphones o tablets [52].

G. Variables de estudio:

- Dependiente: vector de infección, variantes de ransomware.
- Independiente: sistema web.

1) Definición nominal de variables

a) Independiente

Sistema web: según San Juan [53] un sistema web son aquellas aplicaciones que se usan accediendo a un servidor web, son muy usados por su practicidad, bajos costes de hardware y software, facilitan el trabajo colaborativo, su actualización es sencilla, provocan menos errores y sus datos están más seguros ya que se encuentran en servidores con altísimas medidas de seguridad. A través del sistema web se presenta la metodología desarrollada en el transcurso de la investigación.

b) Dependientes

Vector de infección: Según la página de la empresa Optical Networks [54], Los vectores de ataque en ciberseguridad son las formas o medios que permiten a ciberdelincuentes transmitir códigos maliciosos, con el propósito de obtener beneficios económicos. Actualmente, existen 5 vectores de ataques los cuales son las principales fuentes de ataques informáticos los cuales son el correo electrónico, la navegación, los endpoint, las aplicaciones web y la red.

Las variantes de ransomware, según Gutiérrez [55], son una forma de malware que se modifica o mejora a través de actualizaciones para ser utilizado en ataques específicos. Estas modificaciones

dan origen a nuevas variantes, las cuales suelen recibir el nuevo nombre del ataque realizado o elegido por los ciberdelincuentes.

H. Definición operativa de variables

Sistema web: esta variable se va a medir con base al cumplimiento a todas las fases de la metodología propuesta, actividad realizada por los investigadores o peritos informáticos haciendo uso de su criterio profesional.

Variantes de ransomware: esta variable se medirá con los diferentes casos acumulados que lleguen para ser evaluados con la metodología implementada en la web. Estos casos serán almacenados lo cual sirva como herramienta para observar cuales son las variantes más usadas.

Vector de infección: esta variable será medida mediante la acumulación de casos registrados dentro de la página web. Estos registros se realizan al ingresar los casos de infección tomando datos relacionados al modo usado para la infección.

I. Formulación de la hipótesis

- Hi: La metodología propuesta en el entorno web permite responder a incidentes de seguridad por infección de software malicioso de tipo ransomware.
- Ho: La metodología propuesta en el entorno web no permite responder a incidentes de seguridad por infección de software malicioso de tipo ransomware.
- Ha: La metodología propuesta en el entorno web permite informar a los usuarios sobre diferentes tipos de ataque ransomware.

IV. Metodología

A. Paradigma

Según lo descrito por Vodniza [56], el paradigma cuantitativo se guía por el positivismo en cuanto a su enfoque epistemológico y metodológico. Esto significa que se enfoca en la observación empírica y la medición numérica de los fenómenos. Además, se considera que los resultados obtenidos son reales, útiles, ciertos, precisos y relativos.

En el contexto de la construcción de la metodología que plantea esta investigación, el paradigma cuantitativo y su enfoque positivista pueden ser útiles para la recolección y análisis de datos empíricos que permitan identificar patrones y tendencias en cuanto a la seguridad informática se refiere.

B. Enfoque

La guía de investigación cuantitativa de Vodniza [57] establece que, debido al enfoque positivista que caracteriza este paradigma, las investigaciones cuantitativas son predominantes. Esto se debe a que la medición numérica de los fenómenos permite obtener valores cuantificables que corresponden a las propiedades, características o atributos de los objetos de estudio, los cuales se presentan en diferentes modalidades. Los proyectos desarrollados en el programa de ingeniería de sistemas tienen la característica de manejar un enfoque cuantitativo.

C. Método

Según Westreicher [58], el método científico es una técnica que permite obtener conocimientos efectivos desde el punto de vista científico. Por tanto, este incluye una forma de acercarse a la realidad y es el resultado de un proceso independiente de las creencias del investigador. Incluso, con el paso del tiempo, el conocimiento científico se perfecciona y solo se intenta averiguar cómo funciona el mundo, siempre basado en evidencias e investigaciones rigurosas. Existen diversos pasos para aplicar el método científico los cuales son: observación, obtener información real,

inducción, realizar preguntas sobre lo obtenido, hipótesis, plantear una idea de experimentación, demostrar la hipótesis, análisis, condensar la información para facilitar la comprensión y conclusión, se demuestra o refuta la hipótesis. En el presente trabajo se realizaron la recopilación de información y análisis de información.

D. Tipo de investigación

En el desarrollo de la investigación se utilizará el tipo correlacional, el cual permite ver la relación entre dos variables que conceden obtener resultados conformes a los objetivos de la investigación.

E. Diseño de la investigación

La presente investigación tendrá el diseño preexperimental que según Vodniza [59], dentro de su apartado de preexperimental y de diseño de preprueba-postprueba describe que se le aplica una pre prueba antes del tratamiento experimental, después se le administra el tratamiento y, finalmente, se le aplica una prueba posterior al tratamiento. Para la investigación se realizarán pruebas antes y después de la implementación de la metodología todo con el fin de comparar si al usarla existen mejoras o se lograron contrarrestar problemas al seguir los pasos planteados por la misma.

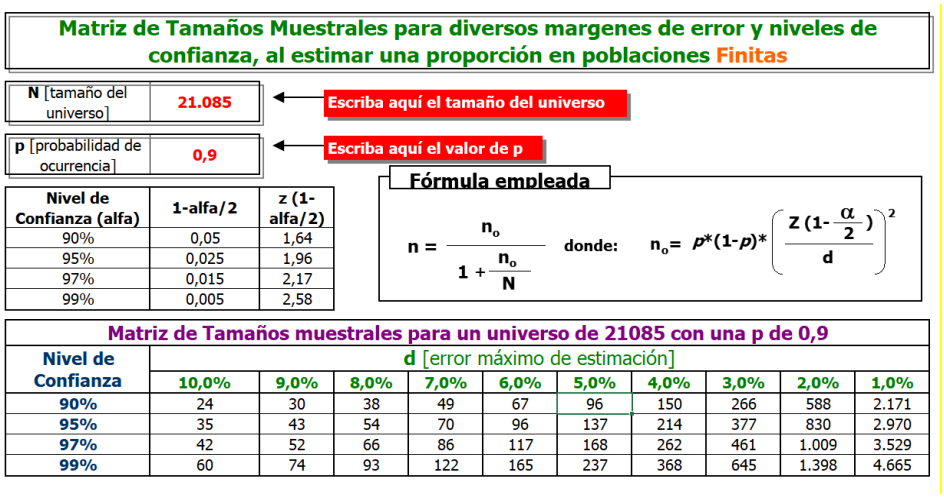
F. Población

La investigación enfoca sus lineamientos hacia la población de empresas de la ciudad de San Juan de Pasto. La cual cuenta con un número de 21.085 organizaciones comerciales [60].

G. Muestra

Se tomaron estadísticas de la Cámara de comercio de San Juan de Pasto de todas las empresas de la ciudad que en total suman 21.085 organizaciones. Aplicando la matriz de tamaños muestrales nos arroja que la muestra con un 90% de nivel de confianza y un 5%.

Fig. 1 Matriz muestra



Matriz de Tamaños Muestrales para diversos margenes de error y niveles de confianza, al estimar una proporción en poblaciones Finitas

N [tamaño del universo]	21.085
p [probabilidad de ocurrencia]	0,9

Escriba aquí el tamaño del universo

Escriba aquí el valor de p

Nivel de Confianza (alfa)	1-alfa/2	z (1-alfa/2)
90%	0,05	1,64
95%	0,025	1,96
97%	0,015	2,17
99%	0,005	2,58

Fórmula empleada

$$n = \frac{n_o}{1 + \frac{n_o}{N}} \quad \text{donde:} \quad n_o = p^*(1-p)^* \left(\frac{Z\left(1-\frac{\alpha}{2}\right)}{d} \right)^2$$

Matriz de Tamaños muestrales para un universo de 21085 con una p de 0,9

Nivel de Confianza	d [error máximo de estimación]									
	10,0%	9,0%	8,0%	7,0%	6,0%	5,0%	4,0%	3,0%	2,0%	1,0%
90%	24	30	38	49	67	96	150	266	588	2.171
95%	35	43	54	70	96	137	214	377	830	2.970
97%	42	52	66	86	117	168	262	461	1.009	3.529
99%	60	74	93	122	165	237	368	645	1.398	4.665

El proceso de exclusión es el siguiente:

- Según Bedoya [61], en San Juan de Pasto el 96.5% de empresas son microempresas, para efectos de la investigación se toma alrededor de un 80% de la muestra. Por tal motivo este porcentaje arroja un total de 77 microempresas que no cuentan con infraestructura sistematizada.

- cuántas empresas cumplen con los requisitos buscados por la investigación: 20.

La muestra final para implementar la encuesta con el fin de obtener datos relevantes para la investigación es de 20 empresas las cuales cumplen con el único requisito requerido para la investigación el cual es no ser microempresa.

H. Técnicas de recolección de la información

Análisis Documental: Según Machuca [62] en su página Future of people, la revisión documental consiste en recopilar información de diversas fuentes mediante la investigación de documentos, lo que la convierte en una técnica de recolección de datos.

Encuesta: Según Thomson [63], la encuesta es un instrumento de la investigación de mercados que consiste en obtener información de las personas encuestadas mediante el uso de cuestionarios

diseñados en forma previa para la obtención de información específica. Para la actual investigación se desarrollaron una prencuesta y una posencuesta.

I. Validez de las técnicas de recolección de la información

La técnica utilizada es la encuesta, la cual fue evaluada por docente de la materia investigación 2 Ing. José María Muñoz y el Magister Edgar Enríquez quien la ajustó según su criterio como profesional y que va alineada con el cumplimiento de los objetivos de esta investigación. Según Romo [64] esta es una de las más confiables técnicas a la hora de recolectar datos que buscan verificar y sondear el estado de un hecho o actividad la cual requiere de una serie de muestras para llegar a generar información que sea válida para la investigación.

J. Confiabilidad de las técnicas de recolección

Esta información se tomará directamente del personal del departamento TIC (Tecnología de la información y las Comunicaciones) de las organizaciones, garantizando la confiabilidad de la información recolectada la cual sería veraz, sucinta y real.

K. Instrumentos de recolección de datos

La caracterización de los ransomwares más utilizados se construyó a través de la técnica de análisis documental. Esta técnica consiste en la revisión y análisis de diferentes fuentes documentales para obtener información relevante y precisa sobre el tema de interés. En este caso, se llevaron a cabo investigaciones exhaustivas y se recopiló información de diversas fuentes como artículos científicos, informes técnicos y noticias relevantes en el campo de la ciberseguridad.

Se utilizó la encuesta como herramienta para respaldar la recolección de datos de la población empresarial en la ciudad de San Juan de Pasto. El objetivo era obtener una muestra real y fiable para el estudio de esta investigación. Además, se llevaron a cabo tres encuestas adicionales: una para evaluar la metodología utilizada, otra para validar el conocimiento adquirido por los usuarios

sobre los ataques de ransomware y una última para validar la página web. Para garantizar la precisión de esta información, se adjuntan los anexos 1, 2, 3 y 4.

V. RESULTADOS DE LA INVESTIGACIÓN

A. Caracterizar los principales tipos de ataques relacionados a ransomware existentes, para que integren el músculo principal de la metodología.

Según Porto y Gardey [65] Un ransomware es un tipo de malware; es decir, un software maligno o malicioso. Dicho programa informático infecta una computadora, impidiendo su uso normal o restringiendo el acceso a documentos, por lo que se solicita un pago para su restablecimiento. Lo normal es que un usuario instale el ransomware sin saberlo, mediante un link engañoso que puede aparecer en un sitio web o en un mail. Cuando se instala, el programa cifra los archivos o incluso bloquea la pantalla del ordenador. Con el sistema ya infectado, el creador del malware exige un "rescate" para su liberación.

Este trabajo de investigación centra su objetivo en el estudio de los diferentes tipos de ataques ransomware para integrar el músculo principal del procedimiento creado el cual tiene como finalidad lograr la desinfección, descifrado y recuperación si es posible de la información secuestrada.

Recolección de información: Se recolectó la información de los 10 tipos de ataques más relevantes relacionados con ransomware que se visualizan en las siguientes tablas, en las cuales se investigan aspectos como:

- El nombre del malware
- El tipo de ransomware
- Metodología de desinfección estudiando los principales vectores de transmisión.
- Algoritmo de cifrado que usa el malware.
- Método de pago solicitado por los atacantes.
- Fecha de aparición del malware.

La finalidad de estudiar los tipos de ransomware siguientes es fortalecer los conocimientos para integrarlos a la investigación y así robustecer la metodología a desarrollar.

TABLA I. RANSOMWARE WANNACRY

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
WannaCry	Es un ransomware de cifrado, esta cifra los archivos valiosos para que no puedas acceder a ellos	Este ransomware posee una función que comprueba la disponibilidad de un dominio web, y si está disponible, este infecta toda la red.	Algoritmo de cifrado AES, la clave aleatoria es generada con la función de Windows "CryptGenRandom". Esta se guarda con una clave cifrada de RSA pública, el descifrado de los archivos solo es posible por la clave privada RSA que se está utilizando durante el ataque.	Los atacantes exigieron un rescate en bitcoins por valor de 300 dólares y, posteriormente, aumentaron el rescate en bitcoins a un valor de 600 dólares. A las víctimas del ataque de ransomware WannaCry se les comunicó que, si no pagaban el rescate en un plazo de tres días, sus archivos se eliminarán de forma permanente.	Mayo de 2017

TABLA II RANSOMWARE LOCKY

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
Locky	Locky es un tipo de malware que puede cifrar archivos importantes en su equipo y exigir el pago de un rescate para recuperarlos. Aprenda cómo funciona el ransomware Locky, qué puede hacer para que no infecte su equipo y cómo detectar y bloquear los ataques de ransomware mediante un potente software antimalware.	El vector de infección más usado por los ciberdelincuentes es el correo electrónico. Usan mensajes fraudulentos relacionados a cobros de bancos o deudas, usando ingeniería social siembran incertidumbre en la posible víctima. Si esta última cae y abre el correo encontrará que tiene que descargar un archivo adjunto en Word el cual al momento de visualizarse solicita la activación de macros de Word. Este es el método como Locky se instala en el equipo y cifra los archivos.	Locky usa el algoritmo AES-128. Advanced Encryption Standard. Algoritmo de cifrado simétrico. Su nombre original es Rijndael. AES es una especificación para cifrado de datos establecido por el instituto nacional de estándares y tecnología de América 2001. El instituto seleccionó 3 sistemas de cifrado de 128 bits de la familia Rijndael para el estándar AES. Esta última se utiliza ampliamente en diversas aplicaciones de negocios. Sin embargo, crypto-malware ha descubierto una manera de tomar ventaja de ella y usarla contra los usuarios de PC. Al ser infectado por Locky utiliza los métodos de AES y cifra archivos que coincidan con las siguientes extensiones: .medio, .wma, .flv, .mkv, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .qcow2, .vdi, .vmdk, .vmx, .gpg, .aes, .ARCO, .PAQ, .tar.bz2, .Tbk, .detrás, .toma, .tgz, .rar, .cremallera, .DJV, .djvu, .svg, .bmp, .png, .gif, .prima, .cgm, .jpeg, .jpg, .tif, .pelea, .NEF, .psd, .cmd, .murciélago, .clase, .tarro, .Java, .áspid, .brda, .SCH, .DCH, .inmersión, .vbs, .pers, .no, .cpp, .php, .LDF, .mdf, .EII, .VENDIDO, .MYD, .frm, .odb, .dbf, .CIS, .sql, .SQLITEDB, .sqlite3, .asc, .lay6, .laico, .MS11 (copia de seguridad), .sldm, .sldx, .PPSM, .PPSX, .PDMA, .docb, .MML, .sxm, .OTG, .respuesta, .uop, .Potx, .senderos, .pptx, .pptm, .std, .sxd, .maceta, .pps, .STI, .ella, .OTP, .Responder, .semanas, .xltx, .XLTM, .xlsx, .xlsm, .xlsb, .ch, .xlw, .XLT, .XLM, .xlc, .dif, .STC, .sxc, .ots, .párrafo, .pliegue, .dotm, .DOTX, .docm, .docx, .PUNTO, .max, .xml, .txt, .CSV, .UOT, .RTF, .pdf, .XLS, .PPT, .STW, .sxw, .hay, .odt, .DOC, .pem, .RSE, .crt, .clave, wallet.dat. Estos archivos se renombran y cambian sus extensiones a, por ejemplo: aesir,. odin, osiris,. thor o .locky etc.	Al ser infectado Locky muestra la nota de rescate en el idioma de la zona correspondiente. Pedirá instalar el navegador Tor y solicita transferir bitcoins a cambio de una clave de cifrado. Los rescates varían según los deseos de los atacantes y quien sea el afectado. Si el afectado tiene en su equipo una cartera de Bitcoins puede llegar a cifrarla.	Locky apareció en 2016 y se extendió rápidamente por muchas regiones del mundo, incluidas Norteamérica, Europa y Asia. Uno de los primeros ataques importantes afectó a un hospital de Los Ángeles, que se vio obligado a pagar un rescate de más de 17.000 USD. A lo largo del año siguió con una serie de ataques dirigidos contra otras instituciones sanitarias.

TABLA III RANSOMWARE BAD RABBIT

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
Bad Rabbit	Ransomware de cifrado.	Se hace pasar por un instalador de Adobe Flash, se descarga desde páginas infectadas con tan solo visitar un sitio web. El malware se integra a las páginas mediante JavaScript inyectándose en el HTML de la página. Bad Rabbit se propaga a través de una falsa actualización de Adobe Flash Player. Sin embargo, tales virus se distribuyen probablemente a través de correos basura (adjuntos infecciosos), fuentes de descarga de software no oficiales (redes P2P, sitios web de descarga de software gratuito, sitios web de alojamiento de archivos, etc.) y troyanos. Los correos basura vienen a menudo con documentos de ofimática adjuntos, códigos JavaScript o archivos maliciosos que, cuando se abren, descargan e instalan malware. Las fuentes de descarga no oficiales presentan a menudo ejecutables maliciosos como software legítimo, por lo que engañan a las víctimas para que descarguen e instalen software malicioso. Los troyanos son los más simples; solo abren "puertas traseras" para que entren otros programas maliciosos en el sistema.	Bad Rabbit se sirve de criptografía AES (simétrica) y RSA-2048 (asimétrica). Los archivos se cifran con un algoritmo AES que genera una clave única usada para encriptar y desencriptar los archivos. La clave generada se encripta luego a través de criptografía RSA-2048 (para ver más información sobre los algoritmos de cifrado y claves, haga clic aquí). El precio de la clave es 0,05 Bitcoins (actualmente, equivalente a ~$280). Tras pagar el rescate, las víctimas recibirán supuestamente la clave de desencriptación. No obstante, los usuarios nunca deberían fiarse de los ciberdelincuentes. Los estudios demuestran que estos individuos suelen ignorar a las víctimas una vez que realizan el pago. Por este motivo, el pago no garantizará que esos archivos sean recuperados. Es más que probable que las víctimas resulten estafadas. Por tanto, le recomendamos que haga caso omiso a las peticiones de pago. Por desgracia, no hay herramientas capaces de restaurar los archivos encriptados por Bad Rabbit. Por tanto, la única solución es restaurar el sistema desde una copia de respaldo.	En la pantalla del infectado aparece un archivo readme.txt el cual lanza un mensaje en pantalla el cual informa a las víctimas que sus archivos fueron cifrados y anima a pagar un rescate por ellos. La manera de pago es generalmente en Bitcoins.	Surgió en Julio 2017 y es similar a Wanna Cry y Petya.

TABLA IV RANSOMWARE RYUK

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
Ryuk	Es un ransomware de cifrado	La metodología del ataque se llama triple amenaza. El primer paso es un correo electrónico con phishing, este correo tiene un documento de Microsoft office con un código en su interior. Este ejecuta un comando en PowerShell donde descargara el troyano EMOTET sin utilizar archivos de script, es de esta manera como comienza el cifrado de RYUK.	RYUK es un algoritmo de cifrado RSA y AES son irrompibles con tres claves, su modelo de cifrado base es CTA que utiliza un clave RSA global privada, la segunda RSA se entrega al sistema a través de la carga útil principal y se cifra con la clave RSA global privada de la CTA. Ryuk escanea los sistemas infectados y cifra casi todos los archivos, directorios, unidades, recursos compartidos y recursos de red.	Es día de pago para los hackers. La cantidad del rescate se basa en el tamaño y el valor de la organización objetivo. El rescate puede variar, pero en general, la cantidad es bastante elevada.	2018

TABLA V RANSOMWARE SHADE/TROLDESH

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
Shade/Troldesh	Ransomware de cifrado.	Este Ransomware se divulga a través de mensajes de correo electrónico en el apartado de SPAM, este contiene archivos tipo zip que son presentados como el receptor. El zip extraído es un JavaScript que descarga el malware, una vez la víctima le da apertura al mensaje con malware, este inicia el cifrado de archivos del usuario utilizando la extensión XBTL. Una vez terminado el proceso de cifrado, la víctima ve un mensaje de rescate que dice "LÉAME". Los atacantes buscan la comunicación directa con la víctima.	El algoritmo que utilizan es AES 246 en modo CBC. Para cada archivo que cifran utilizan dos claves AES de 246 bits aleatorias, una de ellas cifra el contenido del archivo, mientras que la otra cifra el nombre del archivo. Troldesh busca extensiones en unidades fijas, extraíbles y remotas como pueden ser: 1cd, .3ds, .3fr, .3g2, .3gp, .7z, .accda, .accdb, accdc, accde, accdt, accdw, adb, .adp, .ai3, .ai4, .ai5, .ai6, .ai7, .ai8, anim, arw, as, asa, .asc, .ascx, .asm, .asmx, .asp, .aspx, asr, asx, avi, .avs, .backup, .bak, .bay, .bd, .bin, .bmp, .bz2, .c, .cdr, .cer, .cf, .cfc, .cfm, .cfml,.cfu, .chm, .cin, .class, .clx, .config, .cpp, .cr2, .crt, .crw, .cs, .css, .csv, .cub, .dae, .dat, .db,dbf .dbx, .dc3, .dcm, .dcr, .der, .dib, .dic, .dif, .divx, .djvu, .dng, .doc, .docm, .docx, .dot. . dotm,. dotx, .dpx, .dqy, .dsn, .dt, .dtd, .dwg, .dwt, .dx, .dxf, .edml, .efd, .elf, .emf, .emz, .epf, .eps, .epsf, .epsp, .erf, .exr, .f4v, .fido, .flm, .flv, .frm, .fxg, .geo, .gif, .grs, .gz, .h, .hdr, .hpp .hta, .htc, .htm, .html, .icb, .ics, .iff, .inc, .indd, .ini, .iqy, .j2c, .j2k, .java, .jp2, .jpc,. jpe,.jpeg,, .jpf, .jpg.	Este ransomware conocido como TROLDESH cifra documentos, fotos y archivos de oficina. Este solicita a las víctimas un pago a cambio del descifrado, este rescate por lo general lo cobran en 118 Euros y hacen la transferencia por QIWI.	Existió desde el 2014 pero en el 2015 se registró su primer ataque con un total de 311. En el 2016 fue su pico más alto con 9039 ataques a usuarios registrados y en el 2020 los responsables abandonaron el proyecto publicando las 750000 claves para descifrar los archivos. Este apareció en Rusia.

TABLA VI RANSOMWARE JIGSAW

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
Jigsaw	Ransomware de encriptación	También conocido como BitcoinBlackmailer.exe. Es conocido por mostrar la marioneta de la película Saw en la pantalla al hacer la infección. Cuenta con más de 240 extensiones. El vector de infección más usado son los correos maliciosos. El malware se activa en cuanto el usuario lo descarga y cifra todos los archivos y el MBR el cual es el sistema de arranque. Jigsaw se hace pasar por DROPBOX o FIREFOX como fue escrito en .NET framework se puede realizar ingeniería inversa para eliminar el cifrado. Usando actualizaciones falsas de software, troyanos, e-mails maliciosos y redes P2P como Torrent	El algoritmo de cifrado es AES el cual afecta a los tipos de archivos: .jpg, .jpeg, .raw, .tif, .gif, .png, .bmp , .3dm, .max, .accdb, .db, .dbf, .mdb, .pdb, .sql, .dwg, .dxf, .c, .cpp, .cs, .h, .php, .asp, .rb, .java, .jar, .class, .py, .js, .aaf, .aep, .aepx, .plb, .prel, .prproj, .aet, .ppj, .psd, .indd, .indl, .indt, .indb, .inx, .idml, .pmd, .xqx, .xqx, .ai, .eps, .ps, .svg, .swf, .fla, .as3, .as, .txt, .doc, .dot, .docx, .docm, .dotx, .dotm, .docb, .rtf, .wpd, .wps, .msg, .pdf, .xls, .xlt, .xlm, .xlsx, .xlsm, .xltx, .xltm, .xlsb, .xla, .xlam, .xll, .xlw, .ppt, .pot, .pps, .pptx, .pptm, .potx, .potm, .ppam, .ppsx, .ppsm, .sldx, .sldm, .wav, .mp3, .aif, .iff, .m3u, .m4u, .mid, .mpa, .wma, .ra, .avi, .mov, .mp4, .3gp, .mpeg, .3g2, .asf, .asx, .flv, .mpg, .wmv, .vob, .m3u8, .dat, .csv, .efx, .sdf, .vcf, .xml, .ses, .Qbw, .QBB, .QBM, .QBI, .QBR , .Cnt, .Des, .v30, .Qbo, .Ini, .Lgb, .Qwc, .Qbp, .Aif, .Qba, .Tlg, .Qbx, .Qby , .1pa, .Qpd, .Txt, .Set, .1if , .Nd, .Rtp, .Tlg, .Wav, .Qsm, .Qss, .Qst, .Fx0, .Fx1, .Mx0, .FPx, .Fxr, .Fim, .ptb, .Ai, .Pfb, .Cgn, .Vsd, .Cdr, .Cmx, .Cpt, .Csl, .Cur, .Des, .Dsf, .Ds4, , .Drw, .Dwg.Eps, .Ps, .Prn, .Gif, .Pcd, .Pct, .Pcx, .Plt, .Rif, .Svg, .Swf, .Tga, .Tiff, .Psp, .Ttf, .Wpd, .Wpg, .Wi, .Raw, .Wmf, .Txt, .Cal, .Cpx, .Shw, .Clk, .Cdx, .Cdt, .Fpx, .Fmv, .Img, .Gem, .Xcf, .Pic, .Mac, .Met, .PP4, .Pp5, .Ppf, .Xls, .Xlsx, .Xlsm, .Ppt, .Nap, .Pat, .Ps, .Prn, .Sct, .Vsd, .wk3, .wk4, .XPM, .zip, .rar. Método usado para descifrar jigsaw: **1:** Haga clic en el icono de la batería en la bandeja del sistema (al lado del reloj digital) en Windows y luego haga clic en Más opciones de energía. **2:** Opciones de poder Aparecerá el menú. En el plan de energía, haga clic en Cambiar la configuración del plan. **3:** En la configuración de su plan asegúrese de que establece "Apagar la pantalla" y "Poner equipo de dormir" a "Nunca" Del menú desplegable minutos. **4:** Haga clic en "Cambiar la configuración avanzada del Plan" y haga clic para expandir la opción "disco duro" en la lista que hay. **5:** Desde allí, configurar los ajustes de potencia (En la batería y encendido) "Nunca".	Solicitan rescate en Bitcoins 150 dólares durante la primera hora de infección, aparece un reloj en cuenta atrás el cual muestra exactamente una hora si el tiempo termina proceden a borrar archivos. Si el pago no se realiza en el tiempo enviado se empiezan a borrar archivos progresivamente hasta terminar borrando todos en 72 horas. cada vez que el usuario intente reiniciar el equipo se eliminan 1000 archivos.	2016

TABLA VII RANSOMWARE CRYPTOLOCKER

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
CryptoLocker	Es un ransomware que cifra los archivos de Windows.	Este ransomware para infectar a sus víctimas utilizaron la red de robots o más conocida como botnet denominada Gameover ZeuS. Esta se trata de una red de equipos infectada anteriormente con un malware cuyo operador podría controlar la máquina de forma remota, sin el consentimiento de sus propietarios. De esta manera propagaron CryptoLocker a una infinidad de usuarios.	Este utiliza un método de cifrado asimétrico, este sistema utiliza dos claves vinculadas, una pública RSA de 2048 bits para el cifrado de extensiones de documentos, fotos e información del usuario y la otra es privada para el descifrado. El atacante utiliza conexiones anónimas a través de TOR para solicitar el pago del rescate.	El ransomware CryptoLocker ha obtenido de sus víctimas millones de dólares en bitcoins.	Surgió en septiembre del 2013 y su ataque se prolongó hasta el 2014

TABLA VIII RANSOMWARE PETYA

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
Petya	Ransomware de cifrado bloquea discos duros enteros e intenta impedir que el equipo no pueda arrancar.	Diseminado mediante archivos adjuntos maliciosos de correo electrónico. Cuando dichos archivos se descargan y abren, el malware cae sobre el equipo de la víctima. El ataque pudo haber sido iniciado como tradicionalmente hacen los cibercriminales con el ransomware: mediante phishing. Aunque las pruebas de que esto fuese así cada vez son más débiles. La hipótesis de este vector de ataque se sustenta en una posible propagación de documentos de MS Office que explotaría una vulnerabilidad de esa plataforma ofimática como vía de entrada a un equipo de la red y luego, de forma que detallaremos más adelante, se propagara en la red local de los equipos infectados mediante ese primer vector. Se habla de que podría tratarse de un falso currículo alojado en Dropbox. Este documento sería enlazado desde un email fraudulento, aunque no disponemos de evidencias certeras.	El ransomware Petya cifra la tabla maestra de archivos (MFT). Esta tabla es una guía de referencia rápida de todos y cada uno de los archivos que contiene un equipo. Sin acceso a la tabla, un equipo no puede encontrar ninguno de sus archivos, por lo que no es capaz siquiera de arrancar, y mucho menos funcionar con normalidad. Cuando la víctima instala inadvertidamente Petya en un equipo Windows, el malware infecta el registro de arranque maestro (MBR). El MBR es la parte de la programación de un equipo responsable de cargar el sistema operativo cada vez que el equipo se enciende. Una vez dentro del MBR, Petya fuerza el reinicio del equipo y, a continuación, comienza a cifrar la MFT mientras muestra la nota de rescate.	La pantalla de solicitud de rescate de Petya indica el identificador de una cartera de Bitcoins en la que deben ingresar el equivalente a 300 dólares. A continuación, los cibercriminales solicitan que se les envíe un email en el que se especifique el identificador de la cartera desde la que se ha hecho la transferencia y un número de identificación de la computadora.	Apareció en 2016, fue el 27 de junio de 2017 cuando explotó mundialmente con una nueva versión llamada NOT PETYA afectando a empresas ucranianas y luego se extendió a Francia, Alemania, Italia, Polonia, Reino unido y Estados Unidos.

TABLA IX RANSOMWARE GRANDCRAB 5.2

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
GandCrab 5.2	Es un Ransomware de cifrado que cifra los datos almacenados y los mantiene encriptados.	Este tipo de ransomware se distribuye por lo general a través de campañas de correos basura (Spam), herramientas falsas y programas infectados por malware. Los archivos adjuntos que vienen en los correos por lo general son documentos de Microsoft Office, ficheros PDF, archivos (ZIP), juegos descargados por TORRENT. Si se ejecutan estos archivos se descargan e instalan en la computadora de la víctima.	Actualmente no se sabe si es simétrico o asimétrico, pero usa el cifrado en este caso.	Para hacer el pago, las víctimas tienen que usar criptomoneda DASH o Bitcoin y transferirla haciendo clic en un enlace que apunta a una dirección de monedero de criptomonedas. El sitio web tiene un tiempo limitado que, si no se cumple, hará que el precio se duplique. El precio que te daban primero por la clave de descifrado es de $1200, después de un tiempo determinado se incrementará hasta los $2400.	Este apareció en enero del 2018.

TABLA X RANSOMWARE GOLDENEYE

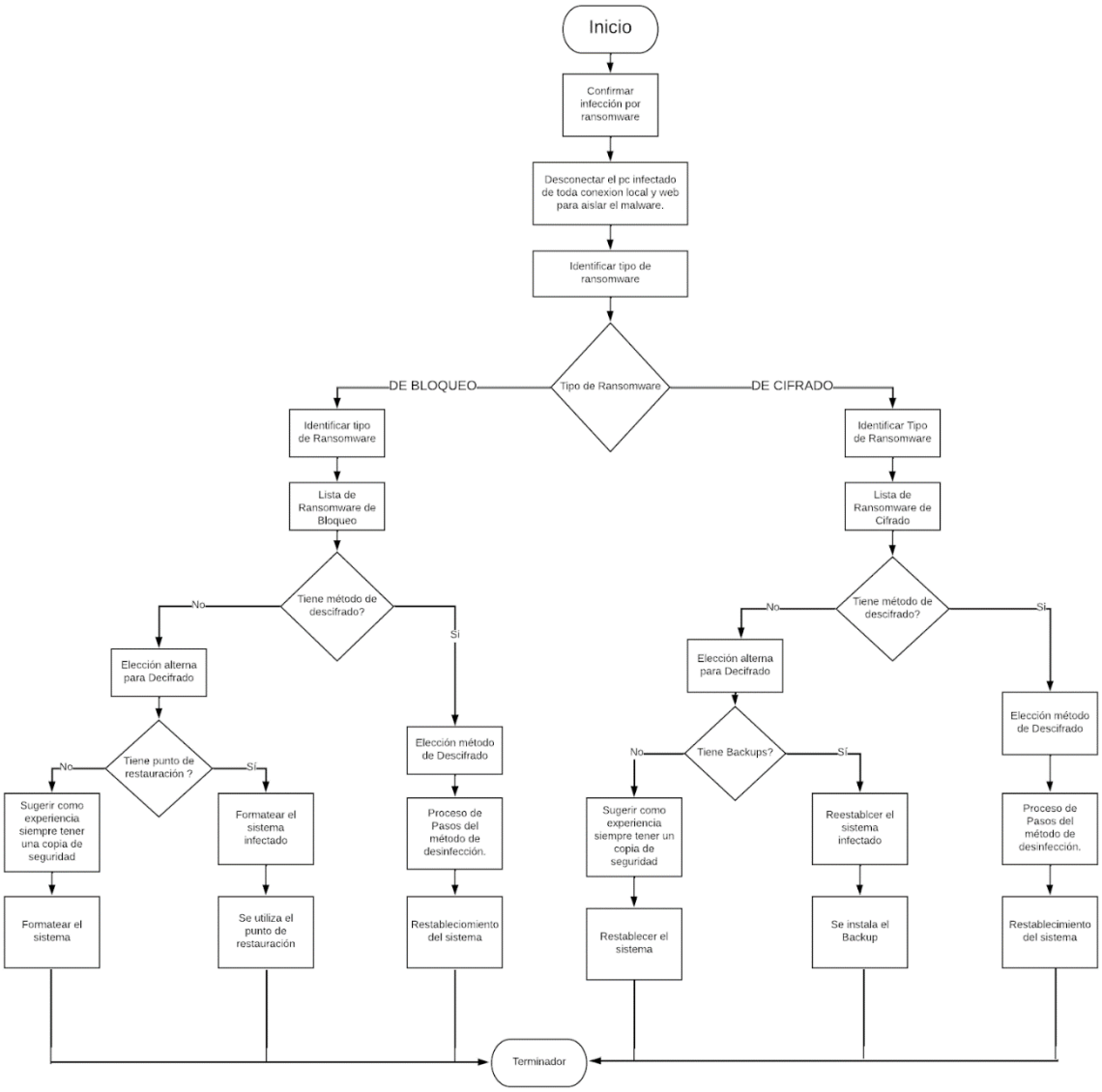
Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
GoldenEye	Ransomware de cifrado. Cifra todos los documentos del ordenador a los cuales les añadirá una extensión de 8 números al azar. A partir de este momento la víctima perderá control de todo y cada vez que intente realizar alguna actividad le saldrá un mensaje de texto en formato TXT.	Es una variante de Petya. Su vector de infección son correos electrónicos camuflados como solicitudes de empleo o spam los cuales tienen dos archivos adjuntos, el primero es un archivo pdf que contiene una carta de presentación; su finalidad es la credibilidad. El segundo es un documento en formato xls que contiene macros maliciosos y solicita validarlos para poderse ejecutar.	Usa el mismo método de Petya Mischa. Golden Eye encripta primero los archivos de la computadora y luego intenta instalar el MBR (Máster Boot Record). A continuación, añade una extensión aleatoria de 8 caracteres a cada archivo al que se dirige. Después de eso, modifica el proceso de arranque del sistema, haciendo que el ordenador sea inútil al restringir el acceso de los usuarios.	Solicitan pago por rescate en bitcoins.	2017

B. Desarrollar las actividades que integran la metodología planteada, en un entorno web enfocadas en la prevención y defensa en casos de ataque ransomware.

1) Diagrama de flujo para la metodología

El siguiente es el diagrama para entender cómo funciona la metodología creada en esta investigación.

Fig. 2 Diagrama de flujo



2) Metodología planteada para hacer frente a una infección por Ransomware

La siguiente metodología fue creada pensando en el asesoramiento o capacitación de empleados frente a una infección por ransomware. Los siguientes pasos fueron diseñados para capacitar a personas sin experiencia en el tema siendo estos de fácil entendimiento y manejo. Los pasos son:

a) Pasos 1 metodología cerrar la escena de la infección

Como en una escena del crimen se debe cerrar el lugar de los hechos para encontrar posibles pistas que ayuden a solucionar el problema. Para empezar no se debe permitir el ingreso ni salida de equipos posiblemente involucrados. Siguiendo el paso anterior se sugiere no apagar el equipo infectado para mantener evidencia y posibles maneras de recuperar la información que el mismo virus puede traer consigo.

Hacer inventario de todos los objetos externos que pudieron haber tenido contacto con la infección para aislarla de inmediato y que no se propague hacia otras dependencias de la empresa involucrada.

Según el sitio web del Ministerio público fiscal de Argentina, la escena del crimen hace referencia al lugar donde ocurrieron los hechos delictivos y su cierre total o parcial corresponde inmediatamente a la preservación para garantizar la intangibilidad de elementos, rastros e indicios que puedan llevar a una posible solución en menor tiempo [66].

b) Paso 2 metodología No apagar el ordenador afectado.

Para evitar la pérdida de información y posibles soluciones ante una infección por ransomware, los expertos recomiendan no apagar los equipos involucrados. En una encuesta realizada por educaciónIT en Estados Unidos, se encontró que el 30% de los encuestados reinició su computadora en modo seguro para mantener información del atacante en memoria en casos de ransomwares antiguos de bloqueo. Sin embargo, para ataques de cifrado, que son más difíciles de manejar, se sugiere no reiniciar ni apagar el equipo. [67].

Para preservar la evidencia digital del delito en un sistema infectado por un virus, es importante no manipular el medio informático. En muchos casos, los atacantes dejan rastros y contraseñas para desbloquear el sistema, pero al apagar o reiniciar el equipo se pueden perder o borrar estas pistas. Por lo tanto, se recomienda no manipular el equipo infectado para mantener la integridad de la evidencia y maximizar las posibilidades de recuperación de datos.

Se recomienda hibernar los dispositivos afectados por la infección para preservar las evidencias y soluciones potenciales. Aunque apagar el ordenador es una opción aceptable, la hibernación es más viable, ya que guarda una copia de la memoria según Microsoft en su página oficial [68].

Después de estas acciones previas se recomienda realizar una denuncia a autoridades no antes de establecer los siguientes puntos como ayuda para los funcionarios públicos:

1. Fecha exacta y hora de cuando tuvo conocimiento que fue infectado.
2. Acciones que realizaba al momento de darse cuenta de la infección.
3. Acciones detalladas de que hizo al momento de darse cuenta de la infección.
4. Aportar el modo de contacto con los ciberdelincuentes (mails) a fin de estudiar el encabezado de estos.
5. Aportar todos los medios de almacenamiento posiblemente afectados por la infección.

Con toda esta información se procede a hacer una investigación sobre los medios informáticos infectados aportados.

c) Paso 3 metodología desconectar todas las conexiones

Según Fernández, se deben desconectar las conexiones, tanto virtuales como físicas, para evitar la propagación de la infección a otros equipos. Para lograr esto, es necesario desconectar todos los dispositivos cableados e inalámbricos, los discos duros externos, los dispositivos de almacenamiento y las cuentas en la nube. De esta manera, se puede prevenir la propagación del ransomware por la red a otras dependencias o terceros [69].

Para realizar esta tarea, es importante considerar que las conexiones se refieren a cualquier tipo de interacción que los equipos infectados tienen con el exterior de su hardware. Por lo tanto, las conexiones principales a deshabilitar son la conexión inalámbrica o por cable a Internet, seguida de la revisión de todos los puertos del PC donde se encuentran los conectores periféricos. Los más comunes son: USB tipo A, USB tipo C, Cable Ethernet (Rj45), conexión wi-fi, conexión bluetooth que se encuentran en el marco teórico.

d) Paso 4 metodología identificar qué ransomware es el que infectó al sistema si es de Bloqueo o de Cifrado.

Después de cerrar la escena de infección, se realiza un chequeo de los equipos para determinar qué tipo de ransomware ha sido involucrado. Según Crowdstrike, existen varios métodos para identificar el tipo de ransomware utilizado. En primer lugar, se puede realizar una observación visual, ya que muchos ransomware colocan una imagen característica que informa al usuario de que se ha producido un problema y cómo solucionarlo. De esta manera, se puede determinar tanto el tipo de ransomware como la variante específica que se ha utilizado. Otra forma de identificar el ransomware es revisar los archivos infectados y comprobar si han sido renombrados con extensiones extrañas [70]

En el paso 4 de la investigación, se utilizará la herramienta ID Ransomware, que es gratuita y permite identificar el tipo de malware utilizado en la infección del usuario [71]. Esta herramienta es capaz de detectar hasta 807 tipos distintos de ransomware a partir de uno de los archivos cifrados. Fue desarrollada por Malware Hunter Team, un grupo de investigadores especializados en seguridad informática que se dedican al análisis y combate del malware.

e) Paso 5 metodología ransomware de cifrado y bloqueo

1. Ransomware de Cifrado

Kaspersky describe el ransomware de cifrado como un malware que selecciona ciertos tipos de archivos previamente estudiados por el atacante y los cifra, lo que impide que el usuario acceda a ellos. El último paso es pedir un rescate para entregar las claves de restablecimiento [72].

Como paso 5 de la metodología planteada por los investigadores se recomienda, tras haber seguido los pasos anteriores, continuar con los siguientes.

- Navegar hacia las herramientas sugeridas dentro del sistema web según sea la necesidad del usuario.
- Estudiar y elegir la mejor herramienta según la necesidad del cliente.
- Mediante la guía construida en el sistema web el usuario ingresa a las páginas oficiales de descarga de las herramientas que necesite.
- Descargar la herramienta usando la explicación que entrega el sistema web.
- Utilizar la herramienta descargada para ransomware de cifrado, siguiendo la guía del sistema web donde se explican de forma más detallada los siguientes pasos:

1. instalar la herramienta
2. usar la herramienta
3. desencriptar los archivos infectados
4. restaurar archivos
5. crear copias de seguridad

Al finalizar la guía anterior si el resultado es negativo se sugiere consultar dentro de la organización si cuenta con backups o discos duros de respaldo, ya que de esto dependen los siguientes pasos:

- Si poseen Backups o discos de respaldo se invita a usarlos.
- Si no poseen Backups o discos de respaldo la única alternativa es formatear el sistema. (esto como última opción).

2. Ransomware de bloqueo

El ransomware de Bloqueo, según Microsoft, es un tipo de malware que bloquea completamente el sistema operativo del usuario, impidiendo el acceso a cualquier parte del equipo. Sin embargo, este tipo de ransomware es poco común debido a que su solución es bastante sencilla: basta con apagar el sistema y cambiar el disco duro a otro equipo para eliminar el problema, ya que este malware no cifra ningún archivo [73].

Con base en la investigación del trabajo de grado se recopilan o se incluyen los diferentes métodos de desbloqueo creados para los ransomware.

- Aplicar los pasos recomendados para la desinfección que son los siguientes:
    1. Extraer los discos duros y formatearlos.
    2. Si existen usar los respaldos usar las copias de seguridad. Si tiene copia de seguridad, aplicarla a su última fecha y recuperar el sistema.
    3. Si no existen formatear el sistema. Si no tiene copia de seguridad, se hace énfasis en la sugerencia de tener siempre copias ya sea locales o en la nube por seguridad.
    4. Formatear todos los equipos infectados.

3) Encuesta como sondeo y base para desarrollo del sistema web

La seguridad informática es cada día más necesaria dentro de las organizaciones y también para personas naturales, ya que la exposición a internet es cada vez más común y necesaria para desarrollar cualquier actividad económica. Por este motivo es necesario implementar capacitaciones dentro de organizaciones sin importar su tamaño. Ya que en investigaciones realizadas por Advisor Smith en EEUU dice que el 42% de medianas y pequeñas empresas sufrieron ciberataques. usando las modalidades más comunes como son phishing, violacion de datos y ransomware. Esto es evidencia de que los piratas informáticos se interesan por empresas de cualquier tamaño.

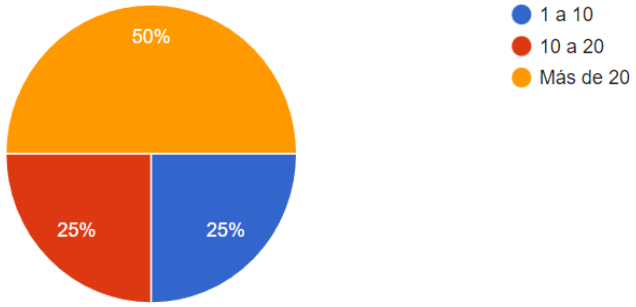
La importancia de las capacitaciones [74] en ciberseguridad de los empleados de organizaciones y/o personas naturales radica en que los ciberdelincuentes se fijan en los puntos más débiles situacionales y mediante el uso de phishing o implementando ingeniería social manipulan a la persona haciendo que involuntariamente de ingreso a el posible ataque a la empresa. Las capacitaciones oportunas ayudan a reducir errores que puedan cometer los empleados, ahorrar dinero e incrementar la productividad y reforzar la confianza en los empleados.

Con motivo de esta investigación se realizó una encuesta trabajada en google forms que se encuentra en el anexo 1, con la finalidad de encontrar estadísticas reales sobre la problemática trabajada (ransomware). Para este efecto se realizaron dos encuestas, cada una a un grupo selecto de personas. Una de las encuestas venía acompañada de una capacitación y la otra fue realizada sin capacitación.

El fin de la realización de las dos capacitaciones es enfrentar los resultados para así obtener primero, datos reales del conocimiento o desconocimiento sobre ciberseguridad y por otro lado se obtienen datos ya con una previa explicación sobre el tema; obteniendo estadísticas que indiquen diferencias entre los dos grupos.

1. ¿Cuántos puntos de cómputo maneja su organización?

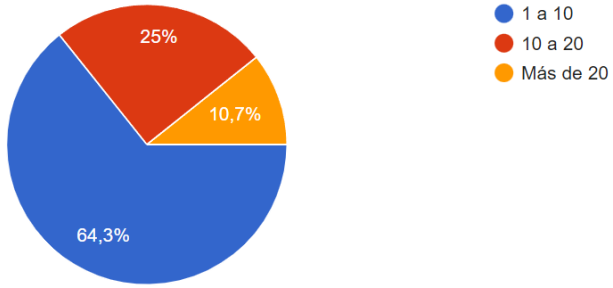
Fig. 3 Gráfica 1 encuesta sondeo



Elaboración propia

Según el resultado de la encuesta realizada a empresas sin previa capacitación, arroja el resultado expuesto en la anterior gráfica. Lo que denota que un 50% manejan más de 20 puntos de cómputo, y el otro 50% está dividido entre empresas de menos de 20.

Fig. 4 Gráfica 2 encuesta sondeo

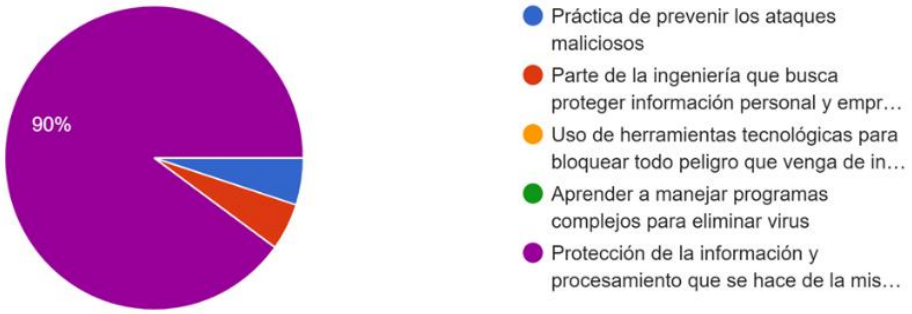


Elaboración propia

La imagen muestra el resultado de la encuesta realizada a empresas con previa capacitación mostrando que en un 64.3 % se usan de 1 a 10 puntos de cómputo, un 25% de 10 a 20 y en un 10% más de 20. Lo que evidencia que con previa capacitación los encuestados mejoraron el concepto de puntos de cómputo descartando algunos equipos que no entran en la lista involucrada en el proceso laboral de la organización.

2. ¿Qué concepto de seguridad informática tiene la empresa a la que está vinculado?:

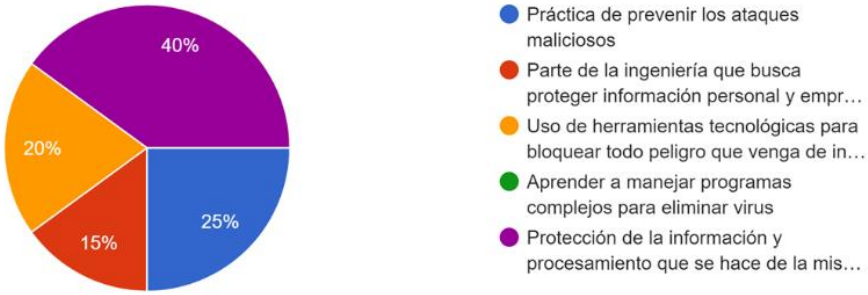
Fig. 5 Grafica 5 encuesta sondeo



Elaboración propia

En respuesta a este cuestionamiento sin previa capacitación se obtiene la anterior grafica donde el 90 % de los encuestados eligió la respuesta de color morado la cual es la más acertada denotando que muchos de los 20 encuestados tenía conocimiento sobre el tema.

Fig. 4 Gráfica 6 encuesta sondeo

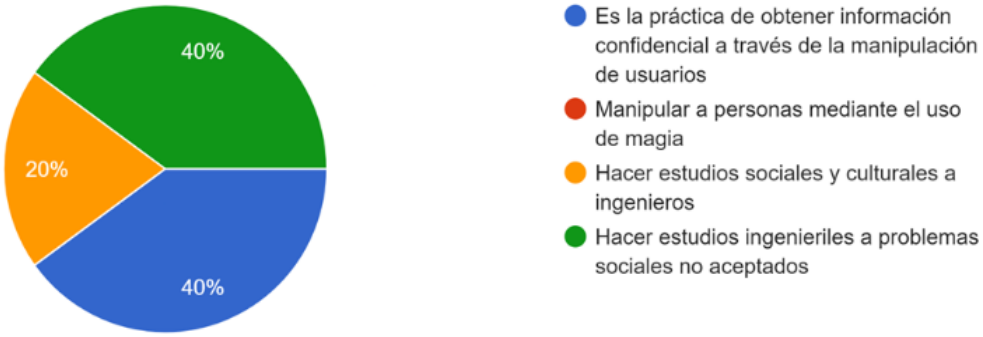


Elaboración propia

La gráfica obtenida en relación a la misma pregunta, pero con capacitación previa muestra confusión en los conceptos. Lo que denota que al haber tomado una guía previa es posible que los conceptos se hayan generalizado o dividido según el criterio propio.

3. ¿Qué concepto maneja su organización sobre ingeniería social?

Fig. 5 Gráfica 7 encuesta sondeo



Elaboración propia

La gráfica muestra el resultado de consultar un concepto un poco complejo sin previa capacitación. Lo que arroja resultados divididos en cuanto al concepto. También denota poco conocimiento del tema.

Fig. 6 Gráfica 8 encuesta sondeo

Elaboración propia

Al grupo encuestado se le hizo una previa presentación del tema lo cual cambia radicalmente el resultado en la gráfica en comparación de la anterior. En este caso se muestra que el 90 % de las organizaciones entendieron el concepto lo cual es positivo para la investigación.

4. ¿Su organización conoce el concepto de DUMPSTER DIVING o Buceo en la Basura?

Fig. 7 Gráfica 11 encuesta sondeo

Elaboración propia

La gráfica muestra lo divido de este concepto entre los encuestados ya que no había conocimiento del tema y no es muy común entre las organizaciones. Ya que muchos de los encuestados trabajan en empresas donde se manejan sistemas de cómputo.

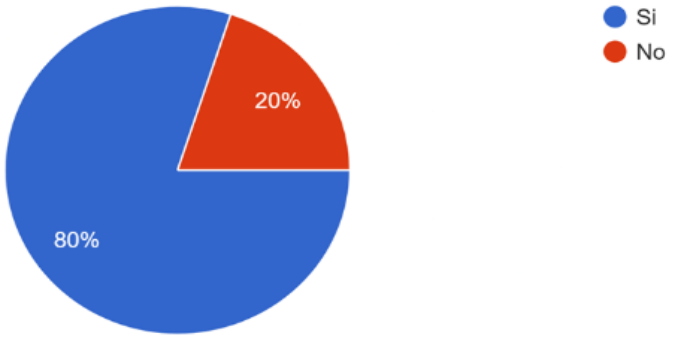
Fig. 8 Gráfica 12 encuesta sondeo

Elaboración propia

La gráfica muestra que al realizar la capacitación previa igual el concepto no quedó muy claro. Se muestran casi los mismos resultados que sin capacitación.

5. ¿La presentación anterior realizada a su organización dejó claro que es un ciberataque conocido como ransomware?

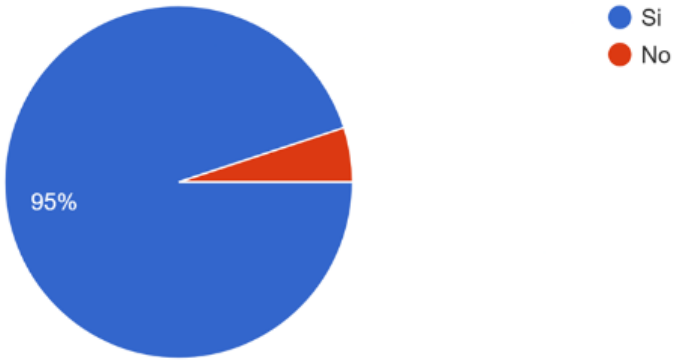
Fig. 9 Grafica 17 encuesta sondeo



Elaboración propia

La gráfica muestra que en un 80 % las personas encuestadas tienen conocimiento de que es un ciberataque sin previa capacitación.

Fig. 10 Grafica 18 encuesta sondeo

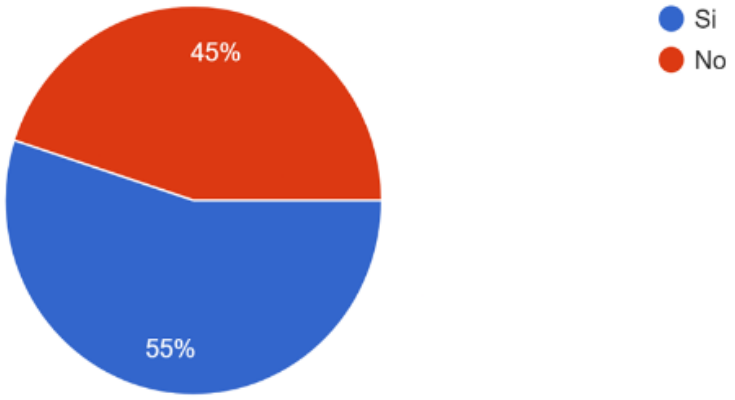


Elaboración propia

La gráfica muestra que posterior a la capacitación se tiene claro que es un ciberataque ransomware para un 95 % de los encuestados.

6. ¿Ha conocido empresas involucradas en casos de ciberataques?

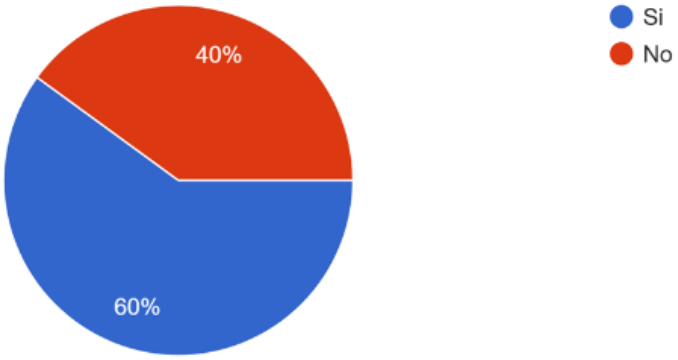
Fig. 11 Grafica 19 encuesta sondeo



Elaboración propia

La gráfica muestra en los encuestados sin previa capacitación que prácticamente en un 50 % se conocen ciberataques a organizaciones. Lo que deja claro que es común para las empresas este problema.

Fig. 12 Grafica 20 encuesta sondeo

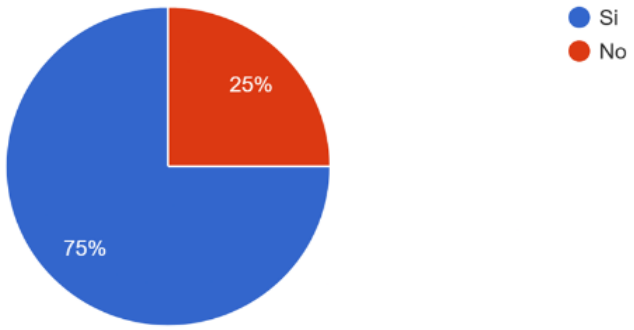


Elaboración propia

La respuesta por parte de los encuestados con previa capacitación eleva en un 10% aproximadamente el conocimiento de ciberataques a empresas. La gráfica de los encuestados con previa capacitación muestra que es posible que en un 50% las organizaciones donde laboran han sido víctimas de este flagelo. Es posible que por la previa capacitación hayan caído en cuenta de casos que fueron tomados de otra manera y con la explicación sobre conceptos de ingeniería social y phishing llevaron a relacionar casos sospechosos y por eso el porcentaje aumentó en relación a la gráfica sin previa capacitación.

7. ¿Dentro de su organización ha sufrido intentos de fraude que puedan causar fugas de información ya sea vía mail o celular?

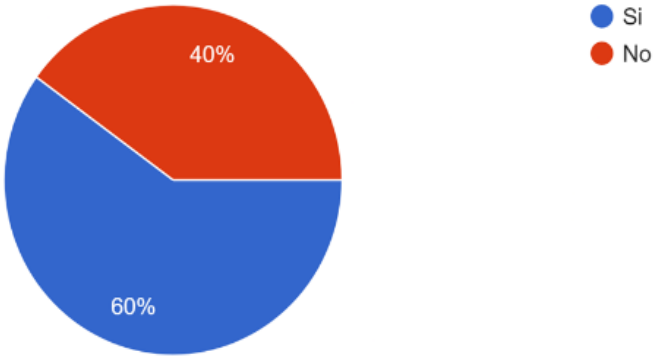
Fig. 13 Grafica 23 encuesta sondeo



Elaboración propia

Esta gráfica muestra que es muy común el intento de fraude entre los encuestados lo que refleja la realidad de la situación de las empresas.

Fig. 14 Grafica 24 encuesta sondeo

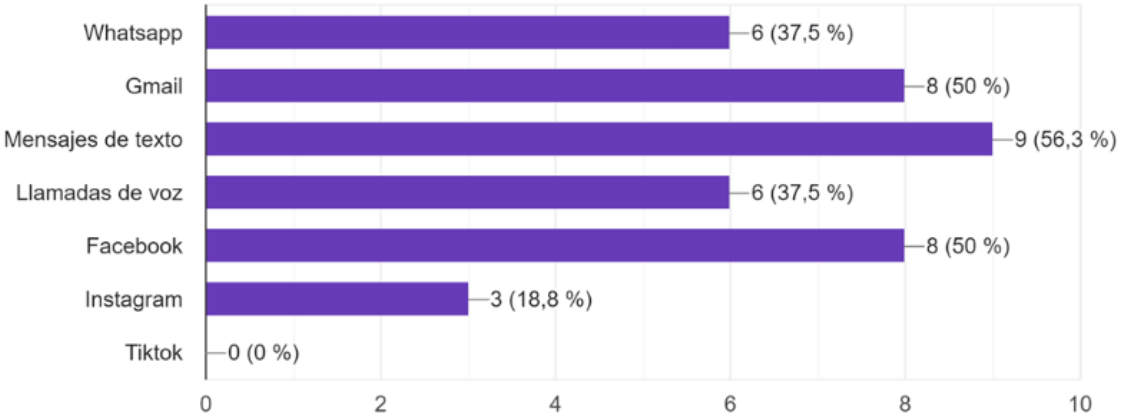


Elaboración propia

La gráfica muestra la misma tendencia referente al tema igual que en la encuesta sin previa capacitación.

8. Si la respuesta anterior fue positiva, describa mediante qué medios ha presenciado intentos de fraude dentro de su organización. Esta pregunta es de selección múltiple.

Fig. 15 Grafica 25 encuesta sondeo



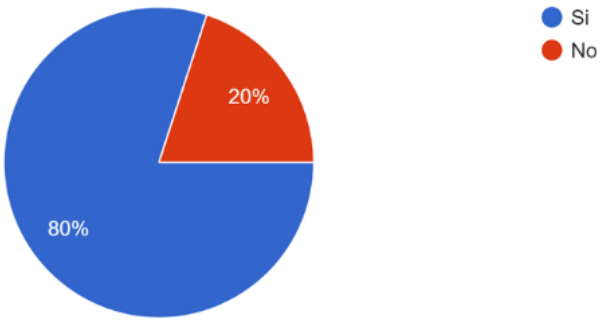
Elaboración propia

La pregunta fue en cuál de las siguientes plataformas ha encontrado intentos de fraude mostrando el resultado plasmado en la gráfica. Los resultados de la gráfica muestran que el mensaje de texto es el medio más usado para intentos de fraude según las elecciones de los encuestados.

Para los encuestados con previa capacitación el resultado varía dando a WhatsApp como ganador pero en general los resultados son similares en los dos casos.

9. ¿Cuándo estás navegando en redes sociales, revisando emails o leyendo mensajes de texto organizacionales, reconoce cuáles podrían ser intentos de fraude?

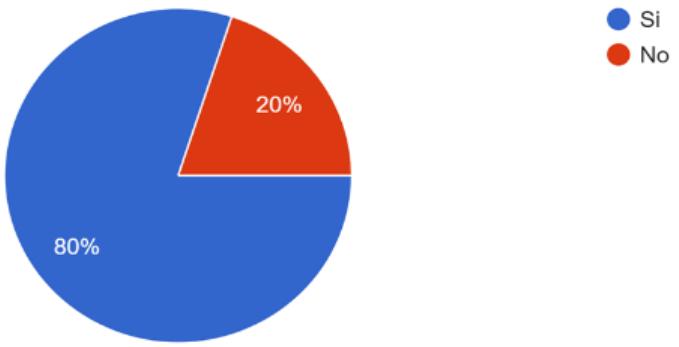
Fig. 16 Grafica 26 encuesta sondeo



Elaboración propia

La gráfica muestra que los encuestados sin previa capacitación reconocen los posibles intentos de fraude.

Fig. 17 Grafica 27 encuesta sondeo

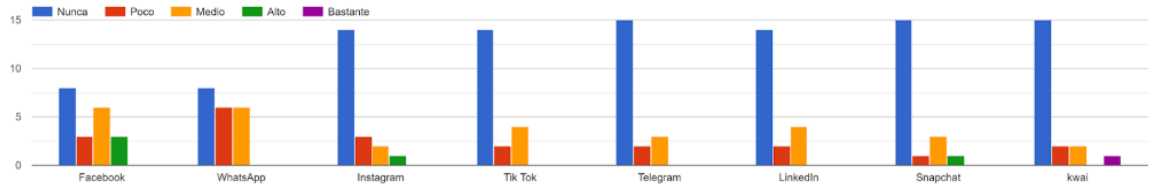


Elaboración propia

La gráfica arroja información similar respecto al tema hasta con previa capacitación esto se debe a que los ciberdelincuentes usan muchas estrategias muy estudiadas para hacer caer a los usuarios.

10. ¿Si la anterior respuesta fue positiva, con qué frecuencia se te presentan posibles intentos de fraude o phishing?

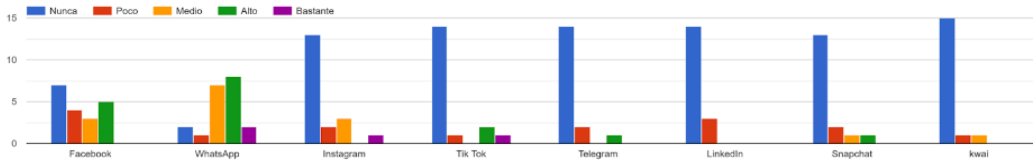
Fig. 18 Grafica 28 encuesta sondeo



Elaboración propia

Esta gráfica muestra las diferentes plataformas donde se pueden usar métodos de fraude como phishing

Fig. 19 Grafica 29 encuesta sondeo

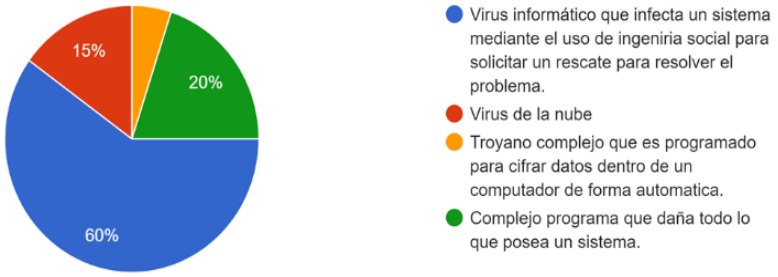


Elaboración propia

La gráfica muestra similitud en las respuestas realizadas por encuestados con previa capacitación.

11. ¿Posterior a la capacitación dada, cuál es el concepto sobre RANSOMWARE que le quedó a su organización?

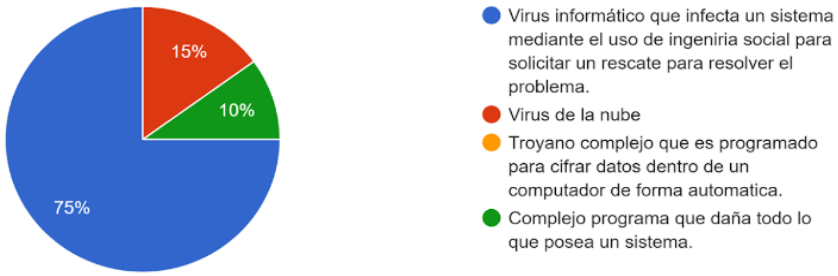
Fig. 20 Grafica 30 encuesta sondeo



Elaboración propia

La gráfica muestra que en un 60% de los encuestados sin previa capacitación tiene un concepto positivo sobre qué es un ransomware. Pero es confundido con un troyano o virus lo que no es muy acertado.

Fig. 21 Grafica 31 encuesta sondeo

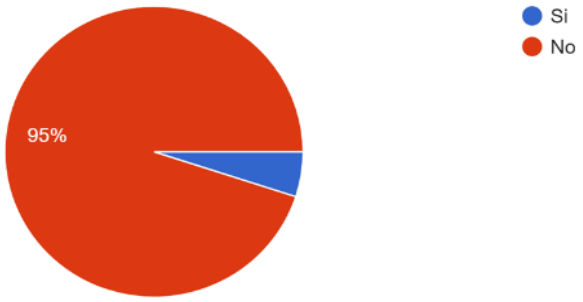


Elaboración propia

La gráfica muestra que los encuestados con previa capacitación mejoran en la elección de la respuesta correcta, además el gráfico denota que no hay muchas dudas y el concepto es más claro.

12. ¿Posterior a la capacitación dada, su organización sabría qué hacer en caso de infección por RANSOMWARE?

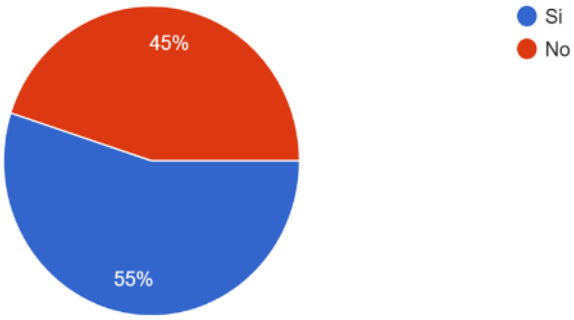
Fig. 22 Grafica 32 encuesta sondeo



Elaboración propia

La gráfica muestra que la gran mayoría de los encuestados sin capacitación desconoce qué se debe hacer en caso de infección por ransomware.

Fig. 23 Grafica 33 encuesta sondeo

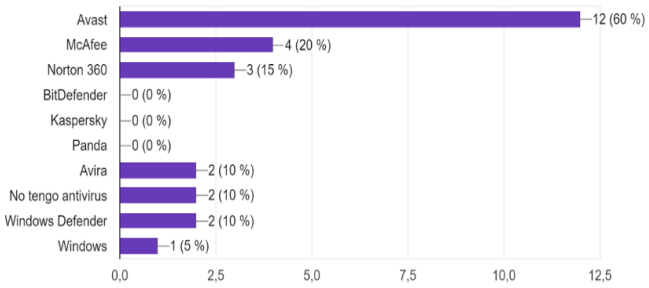


Elaboración propia

La gráfica muestra que mediante la aplicación de la capacitación los encuestados entienden cómo se debe actuar en caso de una infección por ransomware. Lo que es uno de los fines de la investigación. Aquí se denota la gran ayuda de las capacitaciones a empleados.

13. ¿Cuáles de los siguientes antivirus tiene instalado en el sistema de su organización?

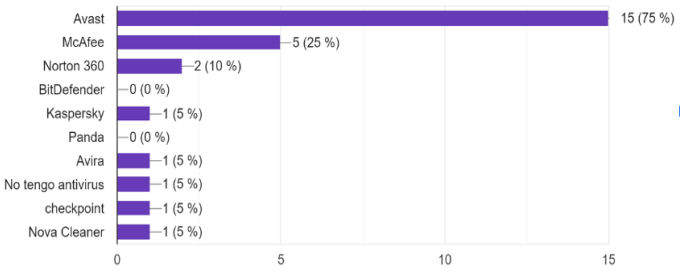
Fig. 24 Grafica 34 encuesta sondeo



Elaboración propia

La gráfica muestra la respuesta que realizaron los encuestados sin previa capacitación sobre el uso de antivirus.

Fig. 25 Grafica 35 encuesta sondeo

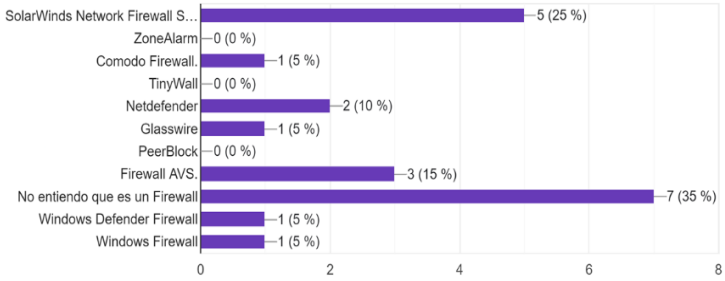


Elaboración propia

La gráfica muestra que el antivirus Avast es el más conocido y por ende el más usado según las dos encuestas.

14. ¿Cuáles de este firewall está instalado en el sistema de su organización?

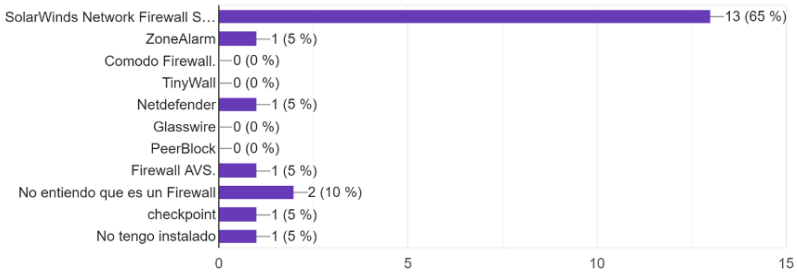
Fig. 26 Grafica 36 encuesta sondeo



Elaboración propia

Según la gráfica muestra que SolarWinds es el más usado por los encuestados sin previa capacitación, pero también se dispara el no conocimiento sobre el tema lo cual es preocupante ya que esto puede ser el origen de futuros ataques.

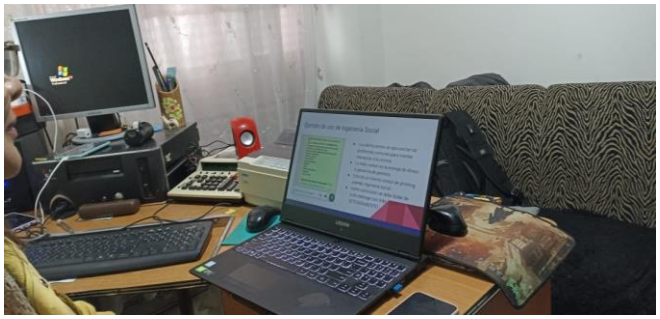
Fig. 27 Grafica 37 encuesta sondeo



Elaboración propia

Como evidencia se muestra una de las personas quien realizó la encuesta bajo la supervisión de los investigadores

Fig. 28 Foto evidencia de capacitación

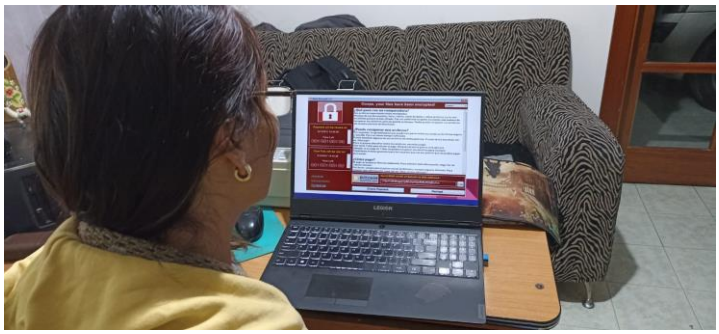


Elaboración propia

Fig. 29 Foto evidencia de capacitación

Elaboración propia

Fig. 30 Foto evidencia de capacitación



Elaboración propia

4) Elaboración del proyecto

Para el desarrollo de la aplicación se utilizó la metodología RUP. Según Lean-Management [75] RUP es un acrónimo y significa el Proceso Unificado Racional. Este proceso se usa preferiblemente para proyectos complejos con equipos grandes.

En la gestión de un proyecto, el sistema RUP promueve una solución disciplinada, que consiste en organizar las tareas y responsabilidades de todos dentro de una organización.

RUP se detalla desde 3 perspectivas dinámica, estática y práctica. Es en la Dinámica donde se desarrolla el ciclo de vida del proyecto. Para comprobar si se han alcanzado los objetivos de la fase, se realiza una evaluación al final de cada etapa.

Las fases de RUP son:

- Inicio: se planifica el desarrollo del proyecto definiendo los objetivos y requerimientos del sistema.
- Elaboración: se establece la construcción del sistema.
- Construcción: se aclaran los requerimientos que faltan y se elabora el sistema de información.
- Transición: se detalla el proyecto desde el punto de prueba hasta la implementación.

RUP desde el punto de vista estático se enfoca en actividades que se llevan a cabo durante el ciclo de vida del proyecto, estas actividades se denominan workflows. Desde lo práctico consta de buenas prácticas de proceso, las cuales son recomendaciones de método para que las actividades se preparen de la mejor manera.

Se eligió la metodología RUP por sus fases de iteración, que son cruciales para garantizar la creación de un software de alta calidad y, por tanto, para satisfacer las demandas de los usuarios.

a) Fase de iniciación

Este apartado tiene como objetivo acordar y definir el alcance del proyecto teniendo en cuenta el ciclo de vida de este, con el fin de proponer una visión general de la arquitectura del software.

1. Objetivos del sistema

Los objetivos del sistema nos permiten lograr las operaciones que se van a realizar dentro del sistema web. Entre los objetivos del sistema se encuentran:

TABLA XI REGISTRO DE USUARIOS COMO ADMINISTRADOR

OBJ–01	**Registro de usuarios administradores**
Versión	1.0 24/03/2022
Autores	Freyder Urbano - Juan David Rojas
Descripción	El sistema debe gestionar los usuarios administradores con sus respectivos roles y permisos específicos para la gestión del aplicativo.

Estabilidad	ALTA
Comentarios	Ninguno

Fuente: Elaboración Propia

TABLA XII. REGISTRO DE USUARIOS COMUNES

OBJ–02	**Registro de usuarios comunes**
Versión	1.0 24/03/2022
Autores	Freyder Urbano - Juan David Rojas
Descripción	El sistema debe gestionar los usuarios comunes estableciendo su información personal para el uso de la página y su metodología.
Estabilidad	ALTA
Comentarios	Ninguno

Fuente: Elaboración Propia

TABLA XIII. GESTIONAR LA INFORMACIÓN DE LOS CLIENTES O EMPRESAS

OBJ–03	**Gestionar la información de los usuarios.**
Versión	1.0 17/03/2022
Autores	Freyder Urbano - Juan David Rojas
Descripción	El sistema deberá gestionar la información de los clientes o empresas registradas en el sistema.
Estabilidad	ALTA
Comentarios	Ninguno

Fuente: Elaboración Propia

TABLA XIV. SOLUCIÓN DE INFECCIÓN POR RANSOMWARE

OBJ–04	**Hacer frente al problema del usuario relacionado a la infección por ransomware.**
Versión	1.0 24/03/2022
Autores	Freyder Urbano - Juan David Rojas

Descripción	El sistema web debe hacer frente al problema inicial planteado por el usuario relacionado a la infección por ransomware, usando la metodología implementada en él.
Estabilidad	ALTA
Comentarios	Ninguno

Fuente: Elaboración Propia

TABLA XV GESTIONAR LA INFORMACIÓN DE LAS HERRAMIENTAS TIPO RANSOMWARE

OBJ–05	**Gestionar la información de las herramientas tipo ransomware**
Versión	1.0 24/03/2022
Autores	Freyder Urbano - Juan David Rojas
Descripción	El sistema web proporciona la facilidad de obtener herramientas de descifrado que ayuden a una posible solución a la infección tipo ransomware.
Estabilidad	ALTA
Comentarios	Ninguno

Fuente: Elaboración Propia

TABLA XVI GESTIONAR LA INFORMACIÓN DE LA CAPACITACIÓN

OBJ–06	**Gestionar la información de la capacitación.**
Versión	1.0 24/03/2022
Autores	Freyder Urbano - Juan David Rojas
Descripción	El sistema web proporciona la facilidad de obtener ingreso a información relacionada a temas como phishing, ingeniería social entre otros, con el fin de capacitarse.
Estabilidad	ALTA
Comentarios	Ninguno

Fuente: Elaboración Propia

2. Requerimientos funcionales

Los requisitos funcionales muestran en esencia lo que el proyecto debe realizar. El levantamiento de requisitos funcionales se realiza con el fin de determinar las actividades principales que debe realizar la aplicación web. Para este fin se muestran las siguientes tablas.

TABLA XVII REQUERIMIENTO FUNCIONAL REGISTRO CLIENTE O EMPRESA

FRQ- 01	**Registro Usuarios**

Versión	1.0 21/03/2022
Fuentes	Usuarios
Módulo	MO-01 Usuarios
Descripción	El sistema debe permitir registrar los usuarios que buscan solución a ataques sufridos por ransomware.
Variables Involucradas	● Nombre: nombres de usuarios ● Apellidos: apellidos de usuarios ● Email: correo ● Password: contraseña ● Fecha: fecha de la creación de la cuenta
Duración	6 horas
Prioridad	Alta
Comentarios	Ninguno
Autores	Juan David Rojas y Freyder Urbano

Fuente: Elaboración Propia

TABLA XVIII REQUERIMIENTO FUNCIONAL CONSULTA HERRAMIENTA TIPO RANSOMWARE

FRQ- 02	***Consulta las herramientas tipo Ransomware***
Versión	1.0 22/03/2022
Fuentes	Usuarios
Módulo	MO-02 Listado de herramientas Ransomware
Descripción	El sistema debe brindar un listado de herramientas ransomware con su respectivo método de descifrado si lo tiene.
Variables Involucradas	• Ransomware: lista de herramientas.
Duración	6 horas
Prioridad	Alta
Comentarios	Ninguno
Autores	Juan David Rojas y Freyder Urbano

Fuente: Elaboración Propia

TABLA XIX REQUERIMIENTO FUNCIONAL CONSULTA Y USO DE LA METODOLOGÍA

FRQ- 03	***Consulta y uso de la metodología***
Versión	1.0 22/03/2022
Fuentes	Usuarios
Módulo	MO-03 Metodología paso a paso
Descripción	En este apartado se encuentra el total de usuarios registrados en la plataforma los cuales tendrán acceso a la información proporcionada por la misma.
Variables Involucradas	● Nombre: nombres de usuarios ● Apellidos: apellidos de usuarios ● Email: correo ● Password: contraseña ● Fecha: fecha de la creación de la cuenta
Duración	6 horas
Prioridad	Alta
Comentarios	Ninguno
Autores	Juan David Rojas y Freyder Urbano

Fuente: Elaboración Propia

TABLA XX REQUERIMIENTO FUNCIONAL REGISTRO DE ADMINISTRADOR

FRQ- 04	**Registro Administrador**
Versión	1.0 22/03/2022
Fuentes	Administrador
Módulo	MO-04 Administrador
Descripción	El sistema debe permitir registrar los administradores con sus roles y permisos específicos del sistema
Variables Involucradas	● Nombre: nombres de usuarios ● Apellidos: apellidos de usuarios ● Email: correo ● Password: contraseña ● Permisos: permisos con los que se va a contar ● Roles: el rol que va a desempeñar en el sistema
Duración	6 horas
Prioridad	Alta
Comentarios	Ninguno

Autores	Juan David Rojas y Freyder Urbano

Fuente: Elaboración Propia

TABLA XXI REQUERIMIENTO FUNCIONAL CAPACITACIÓN USUARIOS

FRQ- 05	***Capacitación usuarios***
Versión	1.0 22/03/2022
Fuentes	Usuarios
Módulo	MO-05 Capacitación
Descripción	El sistema proporciona información en temas como phishing, ingeniería social entre otros, con el fin de capacitar a los usuarios.
Variables Involucradas	• Capacitación.
Duración	6 horas
Prioridad	Alta
Comentarios	Ninguno

Autores	Juan David Rojas y Freyder Urbano

Fuente: Elaboración Propia

3. Requerimientos no funcionales

Los requerimientos no funcionales son características, cualidades y restricciones del software, independientemente a su finalidad. Estos se caracterizan por ser específicos, cuantificables y verificables. Se clasifican en atributos de calidad, restricciones, interfaces externas, interfaces de usuario y control de errores. Entre los requerimientos no funcionales se encuentran:

TABLA XXII REQUERIMIENTO NO FUNCIONAL DISPONIBILIDAD

NFRQ- [01]	**Disponibilidad**
Versión	1.0 22/03/2022
Fuentes	Administrador
Descripción	• El sistema debe estar disponible en horarios de trabajo.
Prioridad	*MoSCow: Must*
Comentarios	ninguno
Autores	Juan David Rojas y Freyder Urbano

Fuente: Elaboración Propia

TABLA XXIII REQUERIMIENTO NO FUNCIONAL SEGURIDAD

NFRQ- [03]	**Seguridad**
Versión	1.0 22/03/2022
Fuentes	Administrador
Descripción	• El sistema debe contar con protocolos https, http, ftp, smtp pop3.
Prioridad	*MoSCow: Must*
Comentarios	ninguno
Autores	Juan David Rojas y Freyder Urbano

Fuente: Elaboración Propia

TABLA XXIV REQUERIMIENTO NO FUNCIONAL EFICIENCIA

NFRQ- [04]	**Eficiencia**
Versión	1.0 22/03/2022
Fuentes	Administrador

Descripción	● El sistema debe realizar procesos en el menor tiempo posible, usando recursos necesarios para conformidad del cliente y el administrador.
Prioridad	*MoSCow: Must*
Comentarios	Ninguno
Autores	Juan David Rojas y Freyder Urbano

Fuente: Elaboración Propia

TABLA XXV REQUERIMIENTO NO FUNCIONAL MANTENIBILIDAD

NFRQ- [06]	**Mantenibilidad**
Versión	1.0 22/03/2022
Fuentes	Administrador
Descripción	● El sistema debe permitir ser modificado para realizar correcciones, implementar mejoras, o adaptaciones del software a cambios en el entorno.
Prioridad	*MoSCow: Must*
Comentarios	Ninguno

Autores	Juan David Rojas y Freyder Urbano

Fuente: Elaboración Propia

TABLA XXVI REQUERIMIENTO NO FUNCIONAL USABILIDAD

NFRQ- [07]	**Usabilidad**
Versión	1.0 24/03/2022
Fuentes	Administrador
Descripción	● El sistema debe ser sencillo de usar facilitando la lectura de los textos, debe presentar funciones y menús sencillos, para el usuario.
Prioridad	*MoSCow: Must*
Comentarios	Ninguno
Autores	Juan David Rojas y Freyder Urbano

Fuente: Elaboración Propia

4. Identificación de actores

La identificación clara de actores, sirve para comprender de forma completa el funcionamiento de la aplicación web. Ya que cada actor trae consigo una acción a realizar y esta dibuja de forma clara

el engranaje interno del software. Los siguientes son los actores principales involucrados que se visualizan en la tabla 16 y 17.

TABLA XXVII ACTOR USUARIO

ACT–01	**Usuarios**
Versión	1.0 24/03/2022
Autores	Juan David Rojas y Freyder Urbano
Descripción	Actor permanente del sistema. Cliente o empresa quien usará constantemente el sistema para seguir los pasos de la metodología implementada, con el fin de lograr capacitarse contra infecciones por ransomware y si es posible recuperar información cifrada o bloqueada.
Comentarios	Ninguno

Fuente: Elaboración Propia

TABLA XXVIII ACTOR ADMINISTRADOR

ACT–02	**Administrador**
Versión	1.0 24/03/2022
Autores	Juan David Rojas y Freyder Urbano

Descripción	Actor que lleva el control total del software. Gestiona usuarios, actualiza bases de datos, permisos específicos, roles y actualizaciones generales del sistema.
Comentarios	Ninguno

Fuente: Elaboración Propia

5. Descripción casos de uso

En este apartado de la investigación se muestran las tablas de los casos de uso implicados, con el fin de exponer las interacciones que se generan al momento de realizar actividades dentro de la aplicación web, las cuales describen cada una de las funcionalidades más relevantes del sistema entre los los cuales se encuentran:

TABLA XXIX CASO DE USO REGISTRO DE ADMINISTRADOR

CU-01	**Registro de administrador**
Versión	1.0 24/03/2022
Dependencias	FRQ-01 Registro de Administrador.
Relaciones	DCU-01 Administrador
Descripción	El sistema deberá permitir el registro de administradores con sus permisos y roles específicos.

<table>
<tr><td>Actores</td><td>Administrador</td></tr>
<tr><td>Precondición</td><td>El Administrador no debe estar registrado en la página.</td></tr>
<tr><td>Secuencia Normal</td><td>
<table>
<tr><th>Paso</th><th>Acción</th></tr>
<tr><td>1</td><td>El sistema muestra un apartado de login.</td></tr>
<tr><td>2</td><td>El actor selecciona el menú Administrador</td></tr>
<tr><td>3</td><td>El sistema le mostrará el formulario de registro de datos (Nombre, Apellido, Email, Password).</td></tr>
<tr><td>4</td><td>El actor selecciona la opción registrar.</td></tr>
<tr><td>5</td><td>Al momento de realizar el registro, el sistema mostrará un mensaje informando el registro exitoso.</td></tr>
</table>
</td></tr>
<tr><td>Flujo Alternativo</td><td>
<table>
<tr><th>Paso</th><th>Acción</th></tr>
<tr><td>4.1</td><td>Si el actor ingresa incorrectamente los datos o deja campo sin rellenar el sistema emitirá un mensaje de error respectivamente.</td></tr>
<tr><td>5.1</td><td>El actor puede seleccionar la opción Cancelar para abortar el proceso de registro</td></tr>
</table>
</td></tr>
<tr><td>Postcondición</td><td>Administrador o Perito Forense registrados correctamente</td></tr>
<tr><td>Importancia</td><td>Vital</td></tr>
</table>

Prioridad	Alta
Comentarios	Ninguno

TABLA XXX CASO DE USO REGISTRO DE USUARIO

<table>
<tr><td>CU-02</td><td>Registro de usuarios</td></tr>
<tr><td>Versión</td><td>1.0 24/03/2022</td></tr>
<tr><td>Dependencias</td><td>FRQ-01 Registro de usuarios</td></tr>
<tr><td>Relaciones</td><td>DCU-02 Administrador</td></tr>
<tr><td>Descripción</td><td>El sistema deberá permitir el registro de usuarios.</td></tr>
<tr><td>Actores</td><td>Administrador</td></tr>
<tr><td>Precondición</td><td>● El usuario no debe estar registrado en la página.</td></tr>
<tr><td>Secuencia Normal</td><td>
<table>
<tr><th>Paso</th><th>Acción</th></tr>
<tr><td>1</td><td>El sistema muestra un apartado de login.</td></tr>
<tr><td>2</td><td>El actor selecciona el menú usuario.</td></tr>
</table>
</td></tr>
</table>

	3 — El sistema le mostrará el formulario de registro de datos (Nombre, Apellido, Email, Password). 4 — El actor selecciona la opción registrar. 5 — Al momento de realizar el registro, el sistema mostrará un mensaje informando el registro exitoso.
Flujo Alternativo	**Paso** / **Acción** 4.1 — Si el actor ingresa incorrectamente los datos o deja campo sin rellenar el sistema emitirá un mensaje de error respectivamente. 5.1 — El actor puede seleccionar la opción Cancelar para abortar el proceso de registro.
Postcondición	Usuarios registrados correctamente
Importancia	Vital
Prioridad	Alta
Comentarios	Ninguno

Fuente: Elaboración Propia

TABLA XXXI CASO DE USO INGRESO USUARIO

CU-03	**Ingreso usuario**

<table>
<tr><td>Versión</td><td>1.0 24/03/2022</td></tr>
<tr><td>Dependencias</td><td>FRQ-01 Registro Clientes o empresas</td></tr>
<tr><td>Relaciones</td><td>DCU-03 Usuario</td></tr>
<tr><td>Descripción</td><td>El sistema deberá permitir el ingreso de un usuario a la página web.</td></tr>
<tr><td>Actores</td><td>Usuario</td></tr>
<tr><td>Precondición</td><td>● El usuario debe estar registrado en la página web.</td></tr>
<tr><td>Secuencia Normal</td><td>
<table>
<tr><th>Paso</th><th>Acción</th></tr>
<tr><td>1</td><td>El sistema muestra un apartado de login.</td></tr>
<tr><td>2</td><td>El sistema le mostrará el formulario de ingreso de datos (Usuario, Password).</td></tr>
<tr><td>3</td><td>El actor selecciona la opción ingresar al sistema.</td></tr>
<tr><td>4</td><td>El sistema muestra el inicio de la página web.</td></tr>
</table>
</td></tr>
<tr><td>Flujo Alternativo</td><td>
<table>
<tr><th>Paso</th><th>Acción</th></tr>
<tr><td>1.1</td><td>Si el actor ingresa incorrectamente los datos o deja campo sin rellenar el sistema emitirá un mensaje de error respectivamente.</td></tr>
</table>
</td></tr>
</table>

Postcondición	Usuario ingresado correctamente
Importancia	Vital
Prioridad	Alta
Comentarios	Ninguno

Fuente: Elaboración Propia

TABLA XXXII CASO DE USO REGISTRO DE CONSULTA DE HERRAMIENTA RANSOMWARE

CU-04	**Consulta de herramientas ransomware**
Versión	1.0 24/03/2022
Dependencias	FRQ- 02 Consulta listado de ransomware
Relaciones	Usuarios
Descripción	El sistema debe permitir al actor consultar el listado de herramientas de tipo ransomware
Actores	Usuarios

<table>
<tr><td>Precondición</td><td>

- El usuario debe estar registrado en la página web.

</td></tr>
<tr><td>Secuencia Normal</td><td>

<table>
<tr><th>Paso</th><th>Acción</th></tr>
<tr><td>1</td><td>El actor elige el módulo de herramientas.</td></tr>
<tr><td>2</td><td>El sistema debe mostrar las herramientas disponibles en la página web</td></tr>
<tr><td>4</td><td>El actor ingresa a la herramienta seleccionada</td></tr>
<tr><td>5</td><td>El sistema muestra al actor el método de descifrado planteado</td></tr>
<tr><td>6</td><td>El sistema muestra al actor los pasos planteados por el método de descifrado.</td></tr>
</table>

</td></tr>
<tr><td>Flujo Alternativo</td><td>

<table>
<tr><th>Paso</th><th>Acción</th></tr>
<tr><td>4.1</td><td>El sistema muestra al actor que el ransomware no tiene método de descifrado.</td></tr>
</table>

</td></tr>
<tr><td>Postcondición</td><td>Usuario ingresado correctamente</td></tr>
<tr><td>Importancia</td><td>Vital</td></tr>
<tr><td>Prioridad</td><td>Alta</td></tr>
<tr><td>Comentarios</td><td>Ninguno</td></tr>
</table>

Fuente: Elaboración Propia

TABLA XXXIII CASO DE USO METODOLOGÍA

<table>
<tr><td>CU-05</td><td>Consulta de la metodología</td></tr>
<tr><td>Versión</td><td>1.0 24/03/2022</td></tr>
<tr><td>Dependencias</td><td>FRQ- 03 Consulta metodología paso a paso</td></tr>
<tr><td>Relaciones</td><td>Usuarios</td></tr>
<tr><td>Descripción</td><td>El sistema debe permitir al actor constar el paso a paso de la metodología.</td></tr>
<tr><td>Actores</td><td>Usuarios</td></tr>
<tr><td>Precondición</td><td>● El usuario debe estar registrado en la página web.</td></tr>
<tr><td>Secuencia Normal</td><td>
<table>
<tr><th>Paso</th><th>Acción</th></tr>
<tr><td>1</td><td>El actor elige el módulo de metodología.</td></tr>
<tr><td>2</td><td>El sistema muestra la parte didáctica de la metodología siguiendo los pasos</td></tr>
<tr><td>3</td><td>El actor sigue los pasos de la parte didáctica.</td></tr>
<tr><td>4</td><td>El sistema muestra los pasos de la metodología individualmente.</td></tr>
<tr><td>5</td><td>El sistema genera una encuesta para el actor.</td></tr>
</table>
</td></tr>
</table>

	6 | El actor diligencia la encuesta planteada
Flujo Alternativo	**Paso** | **Acción** 4.1 | El sistema muestra al actor que el ransomware no tiene método de descifrado.
Postcondición	Usuarios ingresados correctamente
Importancia	Vital
Prioridad	Alta
Comentarios	Ninguno

Fuente: Elaboración Propia

TABLA XXXIV CASO DE CAPACITACIÓN

CU-06	**Consulta de la capacitación.**

<table>
<tr><td>Versión</td><td>1.0 24/03/2022</td></tr>
<tr><td>Dependencias</td><td>FRQ- 06 Consulta Capacitación</td></tr>
<tr><td>Relaciones</td><td>Usuarios</td></tr>
<tr><td>Descripción</td><td>El sistema debe permitir al actor usar la información de capacitación.</td></tr>
<tr><td>Actores</td><td>Usuarios</td></tr>
<tr><td>Precondición</td><td>● El usuario debe estar registrado en la página web.</td></tr>
<tr><td>Secuencia Normal</td><td>
<table>
<tr><th>Paso</th><th>Acción</th></tr>
<tr><td>1</td><td>El actor elige el módulo capacitación.</td></tr>
<tr><td>2</td><td>El sistema muestra de forma ágil la información relacionada con la capacitación.</td></tr>
<tr><td>3</td><td>El actor consume la información.</td></tr>
</table>
</td></tr>
<tr><td>Flujo Alternativo</td><td>
<table>
<tr><th>Paso</th><th>Acción</th></tr>
<tr><td></td><td>Ninguno</td></tr>
</table>
</td></tr>
<tr><td>Postcondición</td><td>Usuarios ingresados correctamente</td></tr>
</table>

Importancia	Vital
Prioridad	Alta
Comentarios	Ninguno

Fuente: Elaboración Propia

6. Requisitos de información

En este apartado se exponen los diferentes requisitos que el sistema debe lograr para alcanzar un funcionamiento óptimo. Su fin primordial es mostrar las actividades internas del sistema, funcionalidades y acciones que llevan a cabo los actores haciendo uso de la metodología planteada.

TABLA XXXV REQUISITO DE INFORMACIÓN DE REGISTRO DE ADMINISTRADOR

RIF–01	**Registro de Administrador**
Versión	1.0 24/03/2022
Objetivos asociados	OBJ-01 Registro de Usuarios como administradores
Descripción	Almacenar información en el sistema web acerca de los administradores
Datos específicos	• Identificador de clientes o empresas

Estabilidad	Alta
Comentarios	Ninguno

Fuente: Elaboración Propia

Tabla 26. Requisitos de información de registro de usuarios

RIF–02	**Registro de Usuarios**
Versión	1.0 24/03/2022
Objetivos asociados	OBJ-02 Registro de Usuarios.
Descripción	Almacenar información en el sistema web acerca de clientes o empresas
Datos específicos	• Identificador de clientes o empresas
Estabilidad	Alta
Comentarios	Ninguno

Fuente: Elaboración Propia

TABLA XXXVI REQUISITOS DE INFORMACIÓN DE RANSOMWARE Y HERRAMIENTA PARA SOLUCIONARLOS

RIF–03	**Información referente a tipos de ransomware y sus herramientas.**
Versión	1.0 24/03/2022
Objetivos asociados	OBJ-03 Gestionar la información
Descripción	Dentro del sistema web se implantará una metodología accesible para los usuarios, la cual guiará a los mismos a capacitarse y hacer frente a una probable infección. El usuario seguirá los pasos planteados por la metodología para hacer frente al problema.
Datos específicos	● Identificador tipo de ransomware
Estabilidad	Alta
Comentarios	Ninguno

Fuente: Elaboración Propia

TABLA XXXVII REQUISITOS DE INFORMACIÓN DE LA METODOLOGÍA

RIF–04	**Información relacionada a la metodología planteada**
Versión	1.0 24/03/2022

Objetivos asociados	OBJ-04 Gestionar la información de la metodología
Descripción	Dentro del sistema se mostrarán los diferentes pasos para la metodología planteada
Datos específicos	● Soluciones a clientes o empresas con respecto a infecciones de ransomware.
Estabilidad	Alta
Comentarios	Ninguno

Fuente: Elaboración Propia

TABLA XXXVIII REQUISITOS DE INFORMACIÓN DE CAPACITACIÓN

RIF–05	**Información relacionada a la capacitación**
Versión	1.0 24/03/2022
Objetivos asociados	OBJ-05 Gestionar la información de Capacitación.
Descripción	El sistema mostrará la información pertinente a capacitación para el usuario.
Datos específicos	● Capacitación en temas como phishing, ingeniería social entre otros.

Estabilidad	Alta
Comentarios	Ninguno

Fuente: Elaboración Propia

7. Módulos del sistema

Los módulos del sistema muestran las partes en las que se divide el software. Cada parte cumple con una función específica la cual complementa el funcionamiento total de la aplicación web. Los módulos en los que se divide el software son solidarios entre sí con el fin de cumplir con una tarea u objetivo mayor, por ende, dichos módulos pueden ser expuestos como fases de desarrollo del aplicativo, pero también pueden ser tomados como guía para avances tanto como para revisar pasos anteriores.

TABLA XXXIX MODULO DEL SISTEMA DE USUARIOS

Identificador	**MO-01**
Versión	1.0 24/03/2022
Nombre	Registro de administradores
Descripción	Módulo encargado de registrar los administradores con sus permisos específicos para manipular el sistema

Elementos a considerar	● Permite realizar el registro completo de datos de un administrador.
Definido por:	Freyder Urbano y Juan David Rojas

Fuente: Elaboración Propia

TABLA XL MODULO DEL SISTEMA DE USUARIOS

Identificador	**MO-02**
Versión	1.0 24/03/2022
Nombre	Registro de usuarios
Descripción	Módulo encargado de realizar el registro total de datos de usuarios dentro del sistema web para uso de metodología enfocada a capacitar y dar respuesta a infecciones por ransomware.
Elementos a considerar	● Permite realizar el registro completo de datos de un nuevo usuario.
Definido por:	Freyder Urbano y Juan David Rojas

Fuente: Elaboración Propia

TABLA XLI MODULO DEL SISTEMA DE HERRAMIENTAS DE RANSOMWARE

Identificador:	**MO-03**
Versión	1.0 24/03/2022
Nombre:	Herramientas de Ransomware
Descripción	Módulo encargado de listar tipos de ransomware más usados, con el fin de ser elegidos por los usuarios, para seguir los pasos planteados con el fin capacitarse y hacerle frente a la infección.
Elementos a considerar	● Permite elegir tipos de ransomware registrados en el sistema.
Definido por:	Juan David Rojas y Freyder Urbano

Fuente: Elaboración Propia

TABLA XLII MODULO DEL SISTEMA DE LA METODOLOGÍA PLANTEADA

Identificador	**MO-04**
Versión	1.0 24/03/2022
Nombre	Metodología planteada

Descripción	Módulo que muestra el paso a paso iterativo de la metodología
Elementos a considerar	● Muestra los pasos que se deben seguir
Definido por	Juan David Rojas y Freyder Urbano

Fuente: Elaboración Propia

TABLA XLIII MODULO DEL SISTEMA DE LA CAPACITACIÓN

Identificador	**MO-05**
Versión	1.0 24/03/2022
Nombre	Capacitación.
Descripción	Módulo que muestra la información relacionada con temas como phishing, ingeniería social entre otros.
Elementos a considerar	● Muestra la información sobre capacitación.
Definido por	Juan David Rojas y Freyder Urbano

Fuente: Elaboración Propia

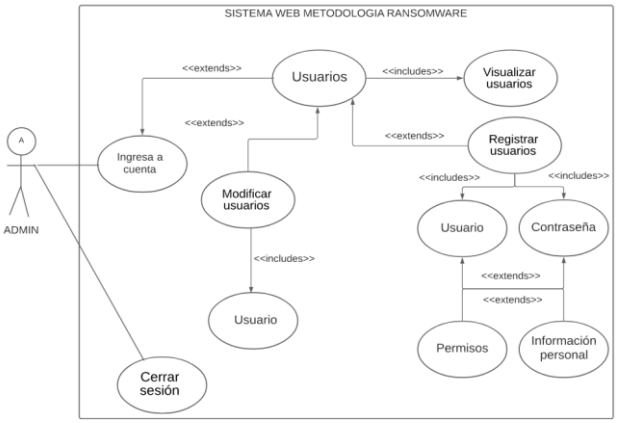
8. Diagramas de casos de uso

Los diagramas de casos de uso muestran las interacciones que se realizan entre los actores y el sistema. Se muestra de forma gráfica el cómo funcionan las acciones que realiza un actor dentro del software para realizar un proceso. Estos diagramas facilitan la realización del software ya que muestran gráficamente las actividades que realizan los actores implicados planteándose como pasos a seguir que los desarrolladores pueden tomar de forma fácil y clara para la construcción del programa.

8.1 Opción de registro de usuario del administrador

En la imagen 3 se puede apreciar el registro de usuarios, esta permitirá agregar usuarios con sus permisos respectivos y también cambiar si fuese pertinente.

Fig. 31 Caso de uso ingreso administrador

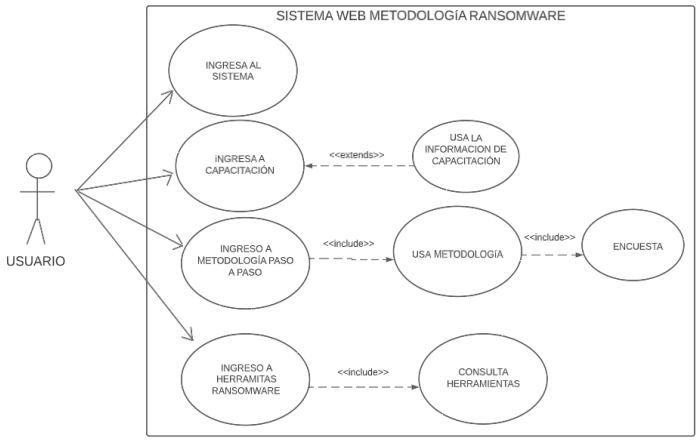


Fuente: Elaboración Propia

8.2 Opción de ingreso al sistema por parte del usuario

En la imagen 5 contará con las distintas opciones que tendrá el usuario al momento de manipular el sistema.

Fig. 32 Caso de uso usuario



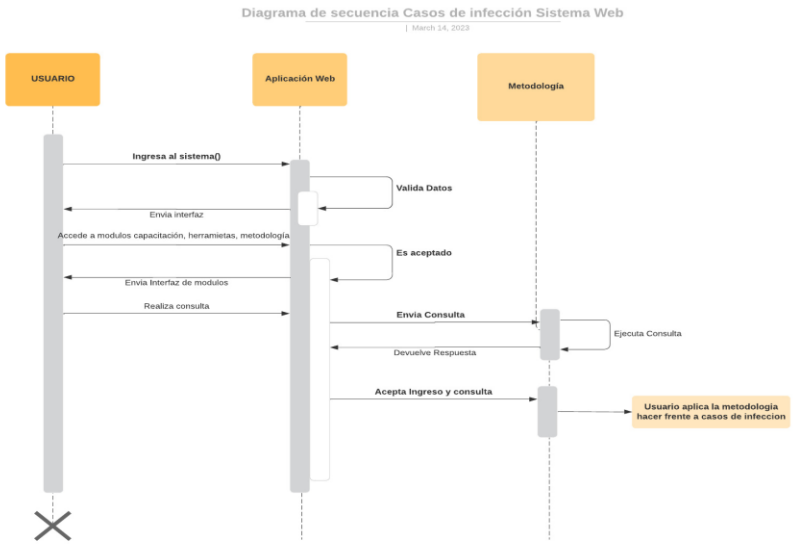
Fuente: Elaboración Propia

b) Fase de elaboración

1. Diagramas de interacción

Se muestra la forma como se comunican los objetos entre sí dentro de la aplicación durante el paso del tiempo. La siguiente figura muestra como un usuario realiza el ingreso al sistema. Primero ingresa de forma normal donde este le solicita entrar para lo cual el sistema le envía la interfaz de acceso. Al diligenciar sus datos se envía la solicitud formal de ingreso, el sistema compara los datos de ingreso y acepta o deniega el ingreso.

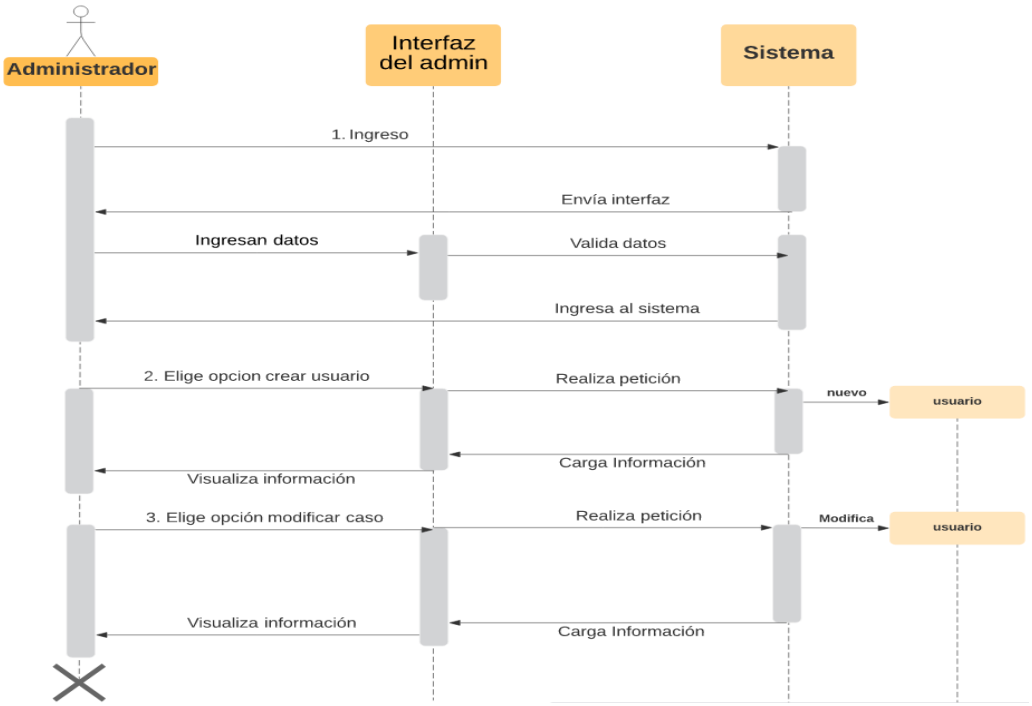
Fig. 33 Diagrama de secuencia ingresar al sistema



Fuente: Elaboración Propia

Se define en la imagen 6 la secuencia que el usuario realizará para ingresar al sistema y a sus diferentes módulos. Con el fin de capacitarse y hacer frente a un caso su caso de infección.

Fig. 34 Diagrama de secuencia ingreso al sistema administrador



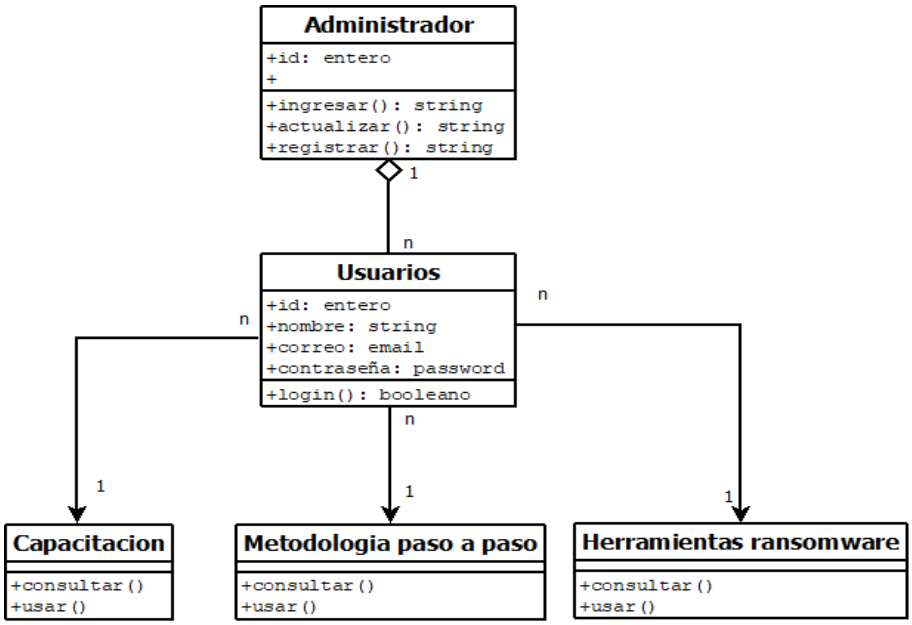
Fuente: Elaboración Propia

Se contrastó en la siguiente imagen 7 se expone el caso de uso el cual muestra la secuencia de pasos que realiza el sistema a la petición de ingreso, crear un usuario y modificar sus datos que hace el administrador.

2. Diagrama de clases

Se toman en el siguiente diagrama las diferentes clases involucradas en nuestro aplicativo web, el cual es de simple comprensión y manejo. Dentro del programa las clases son Usuario, quien se divide en dos tipos los cuales son Administrador usuario. La clase Administrador es encargada de controlar y crear nuevos usuarios y en general controla todo el sistema. La clase usuario es la encargada de consultar, estudiar y aplicar la metodología a los casos de infección por ransomware. En la Imagen 10 se muestra el diagrama de clases de nuestro sistema.

Fig. 35 Diagrama de clases

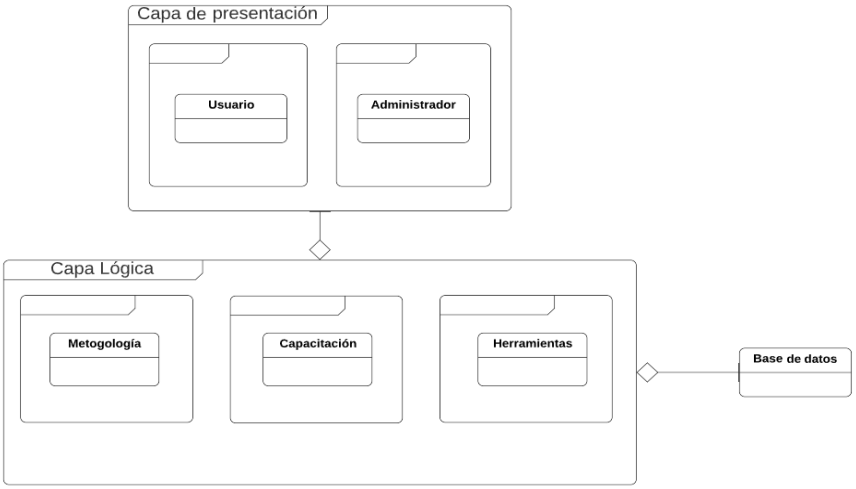


Fuente: Elaboración Propia

3. Diagrama de paquetes

Los diagramas de paquetes se emplean para mostrar la organización de diversos elementos en forma de elementos UML relacionados entre sí. Estos elementos pueden ser documentos o clases los cuales están relacionados jerárquicamente para proporcionar una organización visual de la arquitectura en capas dentro de la estructura del software. La imagen 11 muestra la organización interna del programa aplicando lo anteriormente dicho.

Fig. 36 Diagrama de paquetes del aplicativo



Fuente: Elaboración Propia

c) Fase de construcción

Sabiendo de los peligros relacionados a infecciones por ransomware que para esta época se han convertido en pan de cada día por el englobamiento que ha conseguido el internet llegando a ser un servicio común para casi todos. Esta investigación expone diferentes tipos de casos de infección y directamente exhibe los ransomware más usados para hacer dicho mal.

De aquí que sea de mucha importancia dar a conocer las formas o métodos para solucionar los inconvenientes provocados por caer en una infección de este tipo.

La investigación incluye una evaluación a muchos de los ransomware más usados a nivel mundial y también muchos de los métodos que se pueden implementar para hacerles frente como defensa.

Para lograr el objetivo de esta investigación la cual es la anteriormente mencionada, se hace uso de la metodología implementada en el aplicativo web con el fin de guiar a los peritos forenses para llegar a dar solución a los casos que lleguen a engrosar la lista incluida.

La aplicación se muestra en forma gráfica y está construida con el framework Django bajo el lenguaje de programación Python.

1. Arquitectura del aplicativo web

- Base de datos: la base de datos del aplicativo web es creada con *PostgresQL*. La cual es una excelente alternativa por su escalabilidad y seguridad en la nube AWS. Para nuestra investigación la seguridad que brinda este servicio es crucial ya que la información que se maneja es sensible.

- Lenguaje de programación: Python: Según Santander [76] *Python* es un lenguaje sencillo de leer y escribir debido a su alta similitud con el lenguaje humano. Además, se trata de un lenguaje multiplataforma de código abierto y, por lo tanto, gratuito, lo que permite desarrollar software sin límites.

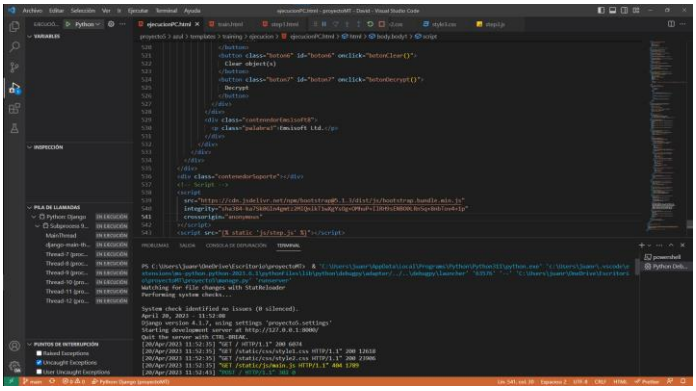
- Framework: Django Según *Mmdn* web *docs* [77]Django es un Framework web de alto nivel que permite el desarrollo rápido de sitios web seguros y mantenibles. Desarrollado por programadores experimentados, Django se encarga de gran parte de las complicaciones del desarrollo web, por lo que puedes concentrarte en escribir tu aplicación sin necesidad de reinventar la rueda. Es gratuito y de código abierto, tiene una comunidad próspera y activa, una gran documentación y muchas opciones de soporte gratuito y de pago.

- Lenguaje de diseño: Según Openwebinars.com [78]CSS3 es un lenguaje de diseño gráfico que permite definir y crear la presentación de un documento estructurado escrito en un lenguaje de marcado. Es muy usado para establecer el diseño visual de los documentos web e interfaces de usuario escritas en HTML.

- Lenguaje de Programación: Según MDN Plus [79]JavaScript es el lenguaje de programación que debes usar para añadir características interactivas a tu sitio web, (por ejemplo, juegos, eventos que ocurren cuando los botones son presionados o los datos son introducidos en los formularios, efectos de estilo dinámicos, animación, y mucho más). Este artículo te ayudará a comenzar con este lenguaje extraordinario y te dará una idea de qué es posible hacer con él.

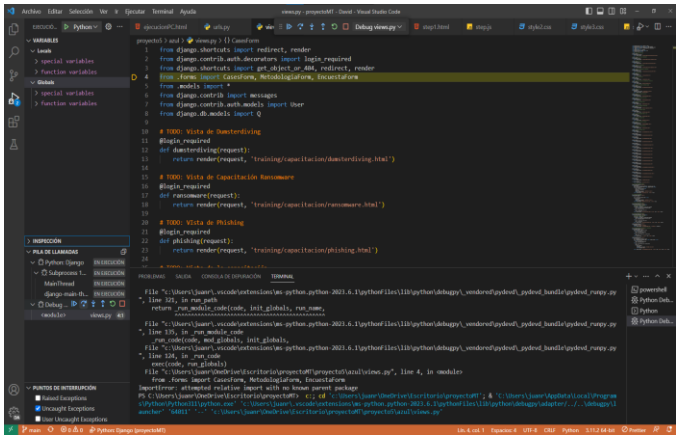
2. Pruebas

Fig. 37 Prueba 1



Fuente: Elaboración Propia

Fig. 38 Prueba 2

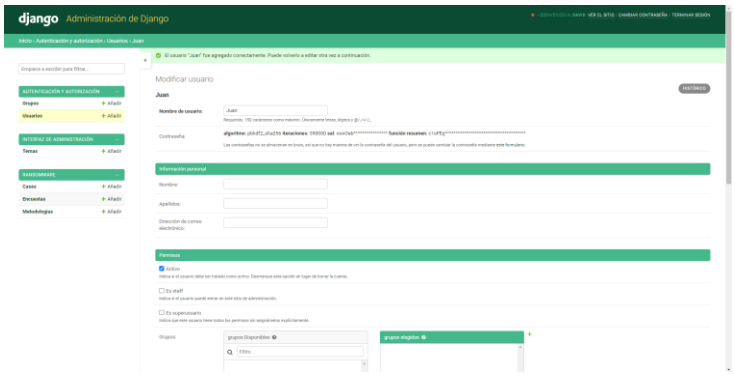


Fuente: Elaboración Propia

3. Módulos del sistema web

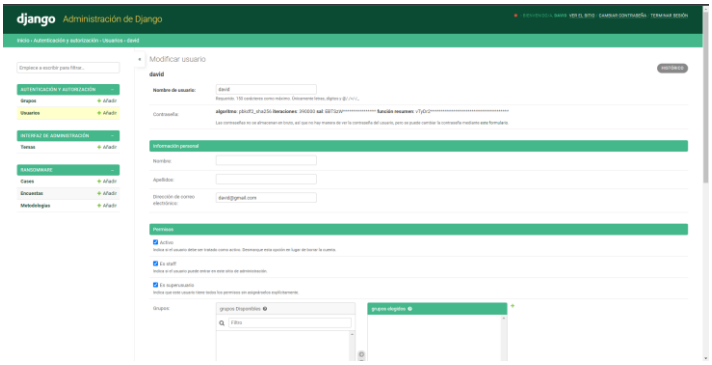
En este apartado se muestra mediante imágenes el sistema web creado por la investigación con la finalidad de implementar la metodología para capacitar a los usuarios que lo requieran.

Fig. 39 Vista Creación de usuario



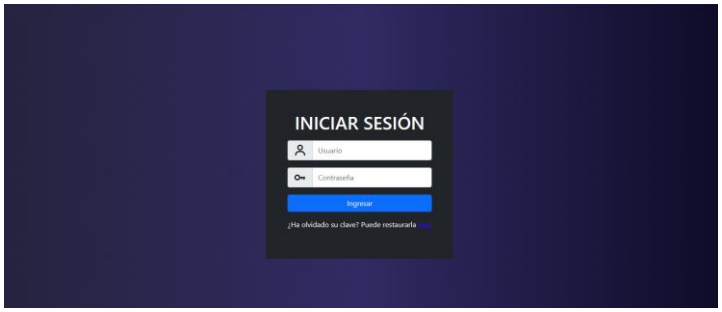
Fuente: Elaboración Propia

Fig. 40 Vista creación de un administrador



Fuente: Elaboración Propia

Fig. 41 Pantalla de inicio de sesión



Fuente: Elaboración Propia

Fig. 42 Pantalla inicial del sistema web

Fuente: Elaboración Propia

Vista de la metodología la cual contiene la parte interactiva creada para capacitar a usuarios de forma visual sumergiéndolos en una aplicación que simula la infección de un ransomware y cómo aplicar el paso a paso de la metodología. Como segunda parte se explican los pasos de la metodología creada por la investigación.

Fig. 43 Vista modulo metodología

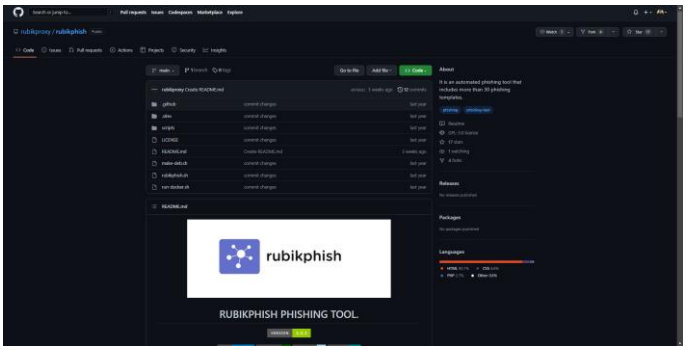
Fuente: Elaboración Propia

C. Validar la implementación de la metodología en el sistema web mediante la realización de evaluaciones a usuarios dentro del sitio.

1) Construcción de phishing falso como experimento de capacitación a usuarios

Para generar correos falsos se usó la herramienta GitHub, donde se usó un repositorio del cual se descargó el código de software para realizar el experimento de hacking ético. Este software crea servidores falsos y los camufla como diferentes páginas web o redes sociales.

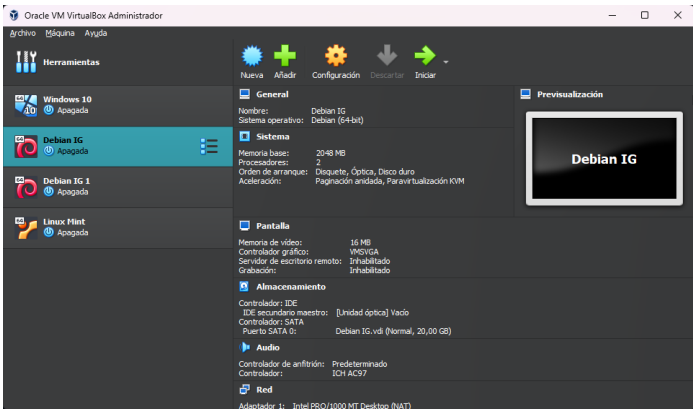
Fig. 44 Repositorio GitHub



Elaboración propia

Usando virtual box se crea una máquina virtual donde se instala el software para generar los servidores que se usarán dentro de un código HTML, el cual será enviado por correo a usuarios al azar.

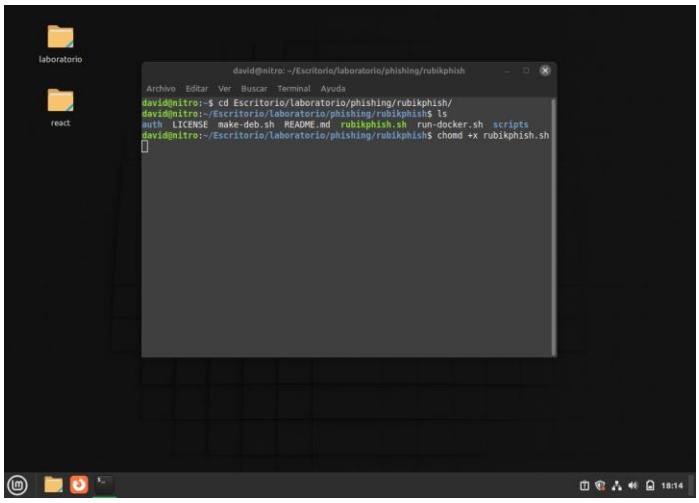
Fig. 45 Virtual box



Elaboración propia

Precisamente se realiza una clonación del software dentro de la máquina virtual otorgando todos los permisos mediante el comando +x rubikphish.sh

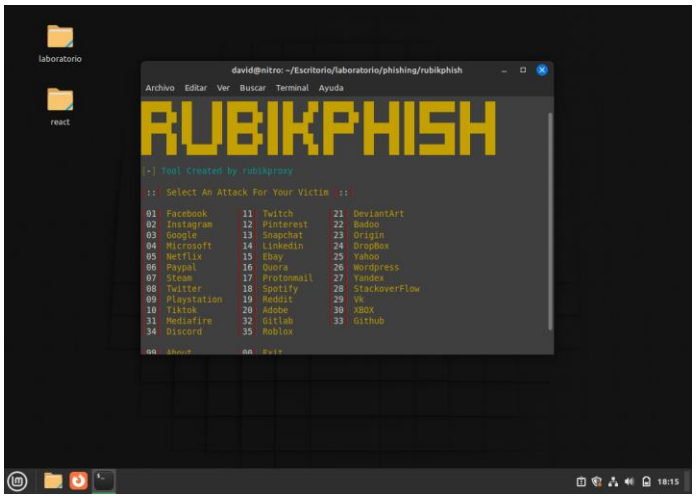
Fig. 46 Instalación Rubikfish



Elaboración propia

Se ejecuta el script para iniciar el software Rubik Phish

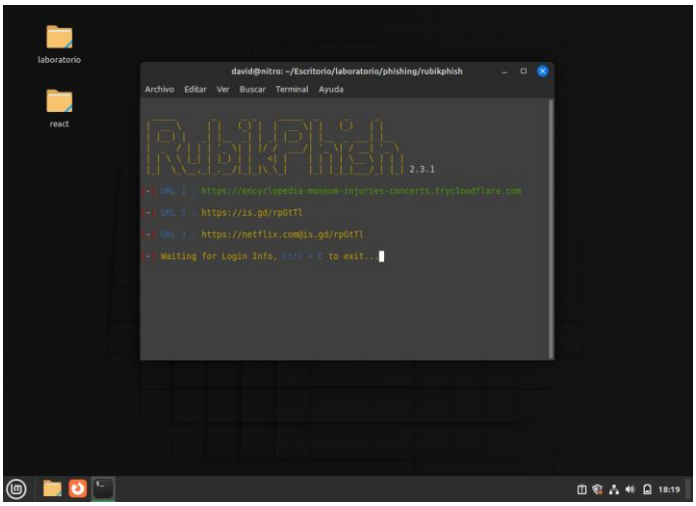
Fig. 47 Rubikphish



Elaboración propia

Los anteriores son todos los servicios que presta Rubik Phish, para la investigación usaremos Netflix ya que es uno de los servicios más usados. El siguiente paso es elegir el link que la aplicación genera para crear posteriormente el correo ficticio.

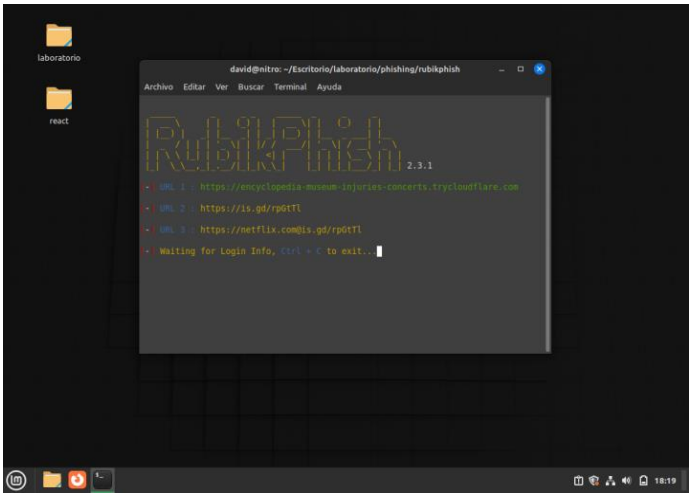
Fig. 48 Link Rubickfish



Elaboración propia

Cualquiera de los links elegidos lleva a una página falsa de Netflix

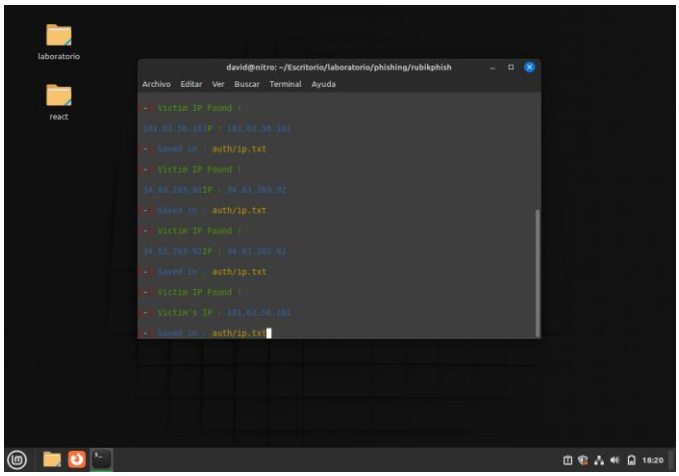
Fig. 49 Links Rubickfish



Elaboración propia

El servidor mientras tanto realiza un mapeo de ips de posibles víctimas

Fig. 50 Ips generadas por Rubickfish



Elaboración propia

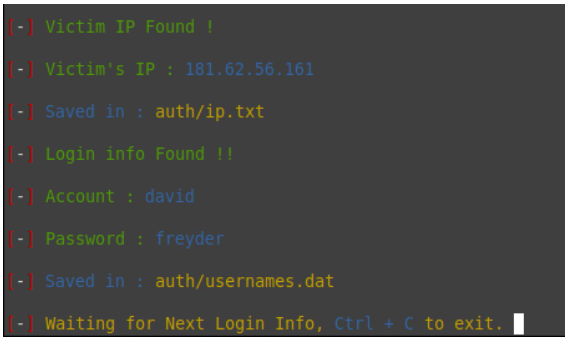
En el momento que la persona ingrese datos en la página falsa automáticamente las tomará en el servidor de la siguiente manera.

Fig. 51 Datos tomados por Rubickfish

Elaboración propia

Además, el programa registra la ip de la víctima

Fig. 52 Datos obtenidos Rubickfish



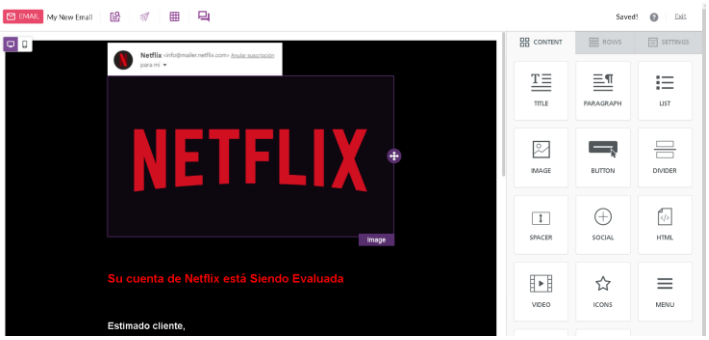
Elaboración propia

Lo que muestra lo anterior es el cómo se instala y usa el programa para generar links, los cuales son usados para robar datos mediante phishing a través de correo electrónico.

Lo siguiente es crear el código HTML que contendrá los links, para esto se usa la página BeePro.io la cual crea correos publicitarios los cuales se exportan como HTML y son enviados mediante correo electrónico de la siguiente manera.

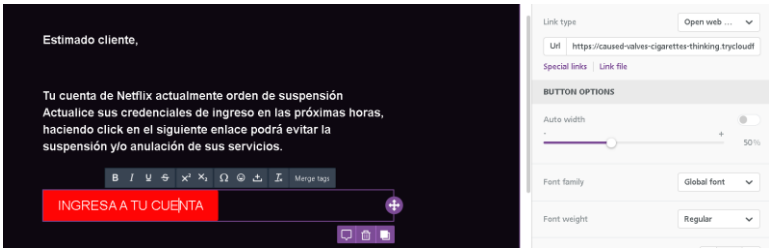
El correo se crea mediante el uso de la página Beepro.io donde se elige todo lo visual del documento y se conectan los botones con las direcciones generadas por Rubik Phis

Fig. 53 Phishing falso Netflix



Elaboración propia

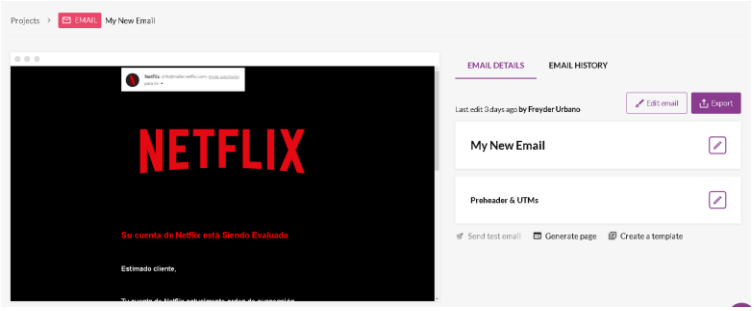
Fig. 54 Phishing falso Netflix



Elaboración propia

Se exporta el código HTML con el botón export y lo modificamos para configurar el código para que no haya problema al momento del envío

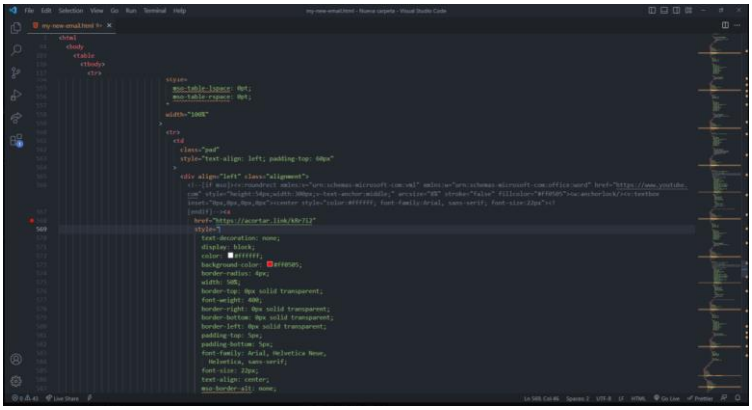
Fig. 55 Phishing falso Netflix



Elaboración propia

Se abre el código en Visual Studio Code para ser modificado.

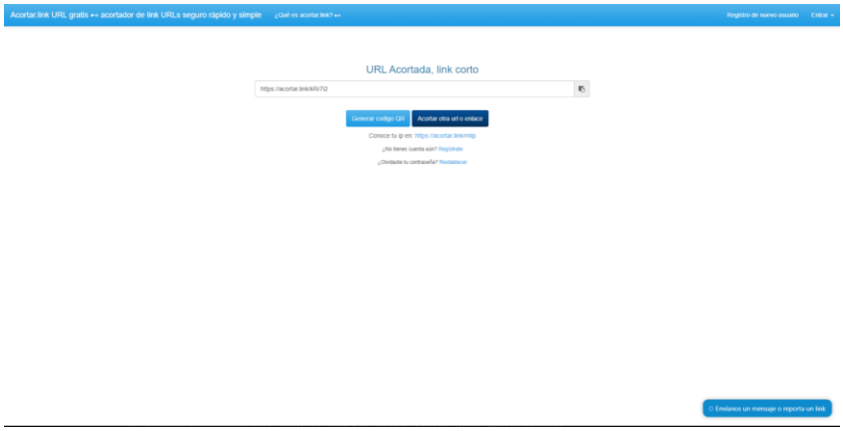
Fig. 56 VS code código phishing



Elaboración propia

Para el envío por correo se enmascara la url para poder enviar la publicidad falsa

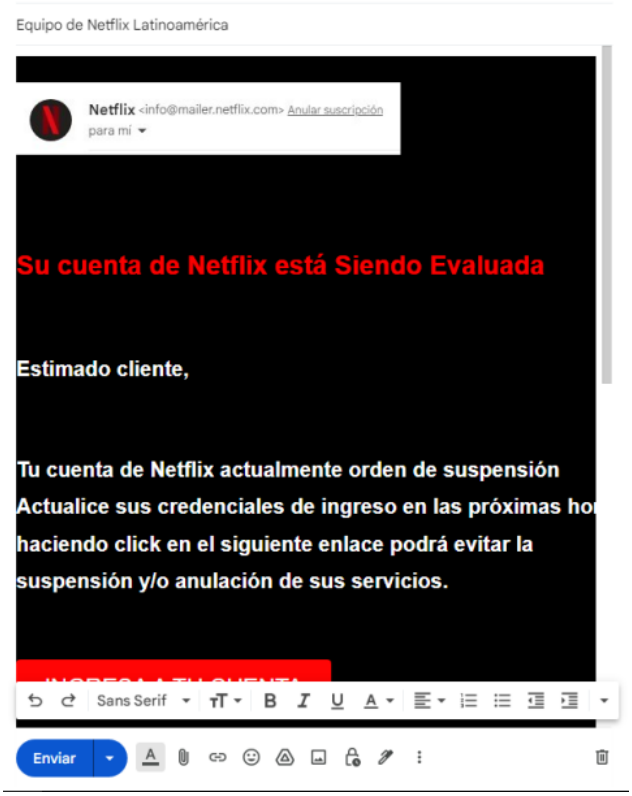
Fig. 57 Enmascaramiento correo falso



Elaboración propia

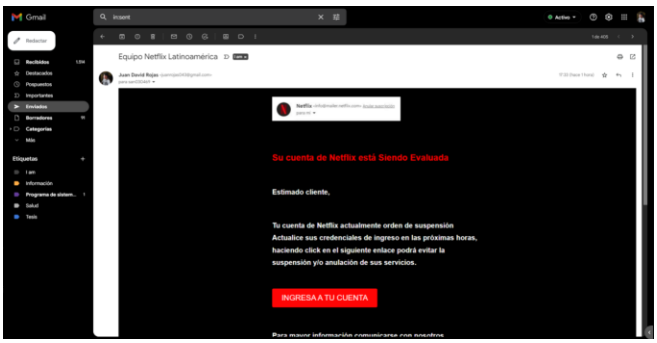
Se ingresa a Gmail para enviar el código.

Fig. 58 Envío correo falso



Elaboración propia

Fig. 59 Envío correo falso

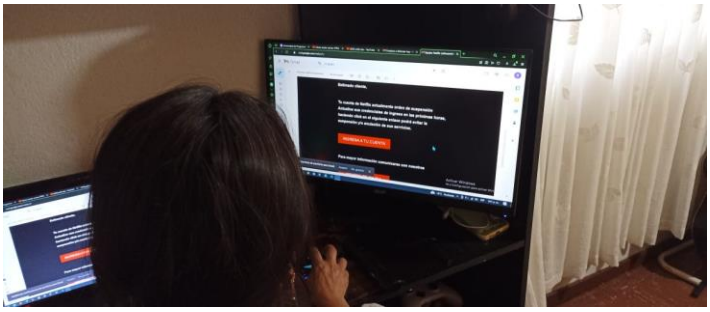


Elaboración propia

En este momento es enviado al correo de la víctima, la cual toma el mensaje y expresa que sería muy fácil caer con una trampa así ya que, según la persona, se mira igual que los mensajes que Netflix envía regularmente. En este momento se explica cómo detectar si se trata de un correo real o ficticio mostrándole primero que se debe fijar en la procedencia del correo, ósea la dirección y el nombre de usuario que envía el correo. También se debe fijar en la dirección de la página la cual

en este caso tendría que ser Netflix y no otra diferente o con nombres o textos muy extensos y por último el idioma en el que esta la página ya que para el ejercicio el lenguaje era inglés.

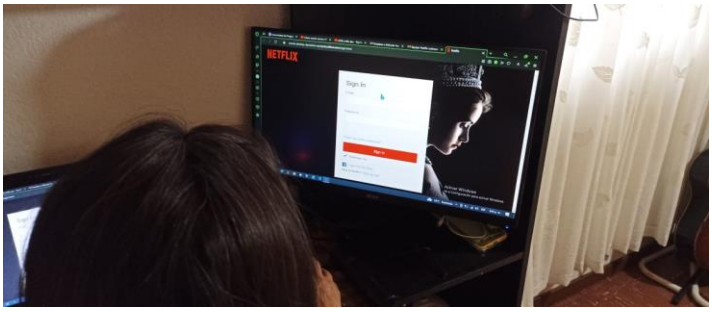
Fig. 60 Evidencia de intento Phishing



Elaboración propia

La víctima clic kea, bajo supervisión de los investigadores para seguir el ejercicio, en los botones cayendo en el phishing e ingresa a la página creada por Rubik phis

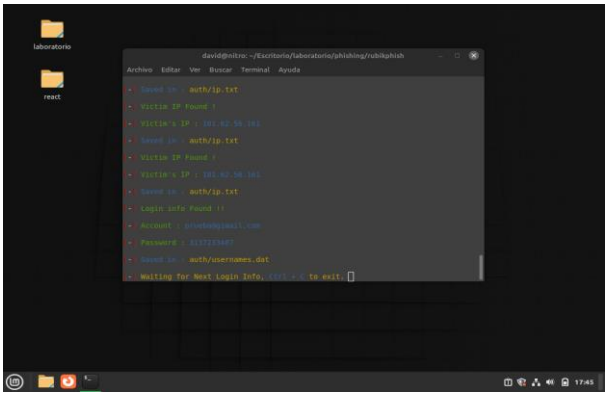
Fig. 61 Uso de phishing falso



Elaboración propia

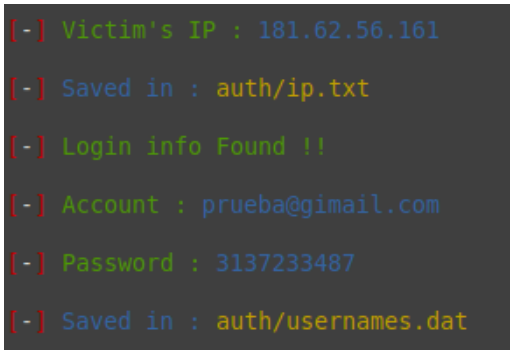
En este punto expresó que era idéntica a la página oficial de Netflix. E ingresó datos falsos para el ejercicio. El programa Rubik phis obtiene los datos que la persona ingresó.

Fig. 62 Toma de datos a victima



Elaboración propia

Fig. 63 Evidencia de toma de datos a victima



Elaboración propia

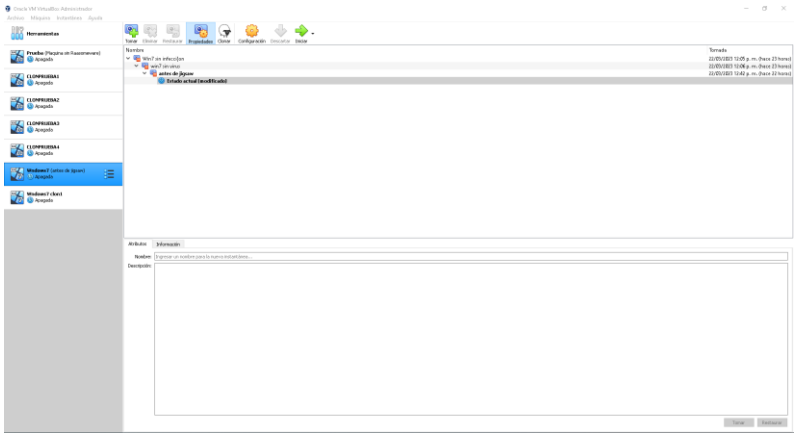
Y así es como funciona el phishing, se aprovecha del miedo y confusión de las personas para, mediante páginas muy bien realizadas, engañarlas y así obtener credenciales con las cuales son extorsionados directamente o usando ransomware.

2) Ejecución del ransomware Jigsaw dentro de entornos virtuales controlados.

Usando máquinas virtuales se presenta la infección del ransomware Jigsaw. Dicho malware fue descargado desde el repositorio (**the Zoo - A Live Malware Repository**) propiedad de Live Malware Repository. En las siguientes páginas se muestra la secuencia de acciones realizadas para descarga, instalación e infección de ransomware.

Como primer paso se descargó la Iso de Windows 7 pro y se crearon las máquinas virtuales utilizando VirtualBox.

Fig. 64 Máquina virtual



Elaboración propia

Como segundo paso se instala Windows 7 pro dentro de la máquina virtual creada dando ingreso a la misma con el usuario Unicesmag.

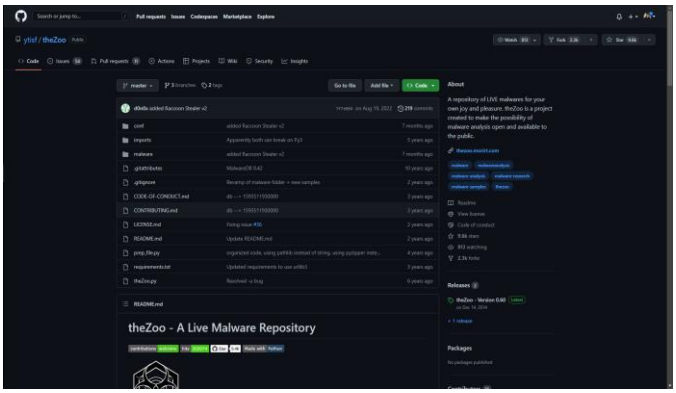
En el escritorio se crearon archivos como una imagen, un documento en blanco (txt) con el nombre de prueba y una carpeta con un archivo txt dentro. Esto se hizo para ver como el ransomware cambiaba el formato de los archivos

Fig. 65 Windows 7

Elaboración propia

Utilizando el repositorio de (**theZoo - A Live Malware Repository**) que es un repositorio en donde se encuentran diferentes malwares, se procedió a descargar el malware Jigsaw para infectar la máquina virtual.

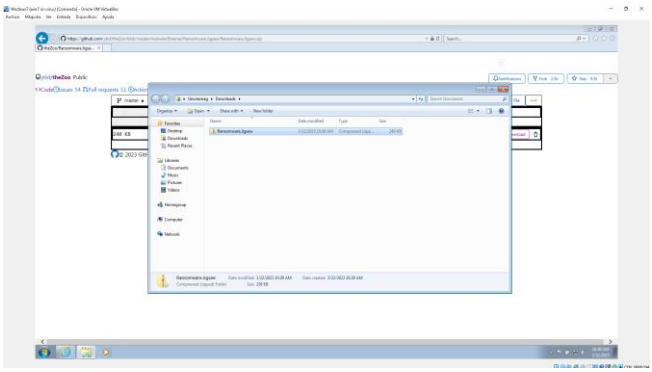
Fig. 66 GitHub thezoo



Elaboración propia

En la siguiente imagen se muestra el archivo de jigsaw.zip descargado dentro de la máquina virtual

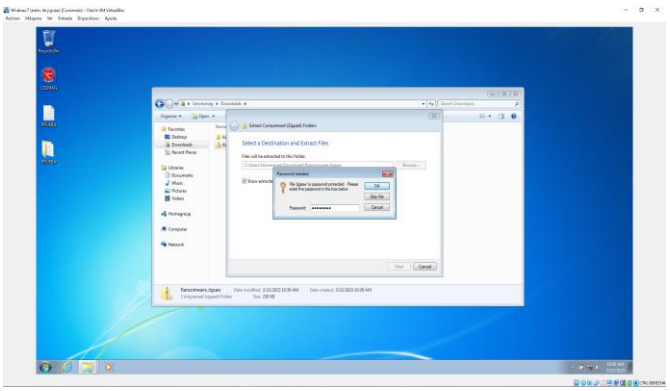
Fig. 67 Jigsaw descargado en máquina virtual



Elaboración propia

Se procedió a realizar la instalación completa del ransomware usando la clave de ingreso proporcionada por el repositorio.

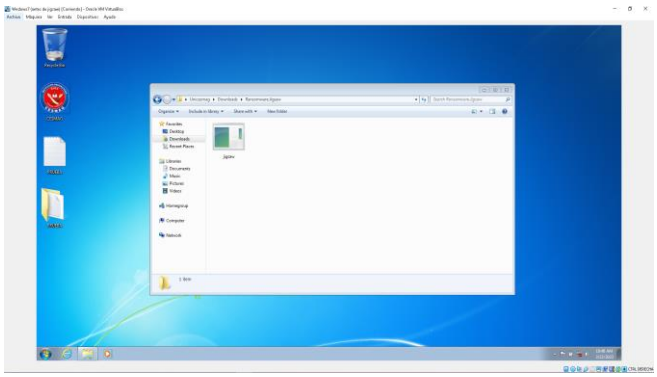
Fig. 68 Clave para Jigsaw ransomware



Elaboración propia

De esta manera se mira el archivo con el nombre de jigsaw.exe

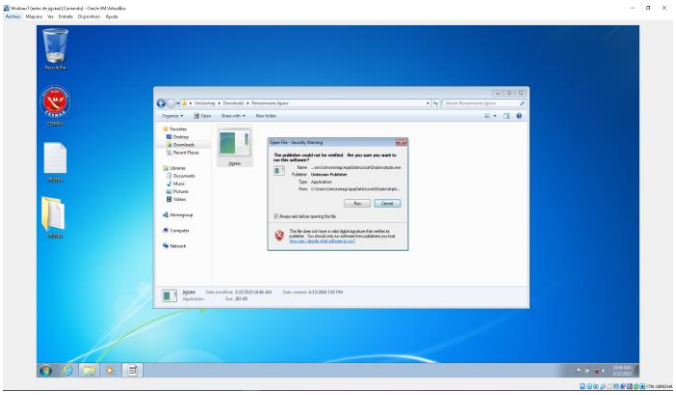
Fig. 69 Jigsaw descargado



Elaboración propia

Se ejecuta el archivo

Fig. 70 Ejecución Jigsaw



Elaboración propia

De esta manera si visualiza cuando el ransomware se empieza a ejecutar y los archivos son cifrados con una nueva extensión la cual es, .fun.

Fig. 71 Jigsaw

Elaboración propia

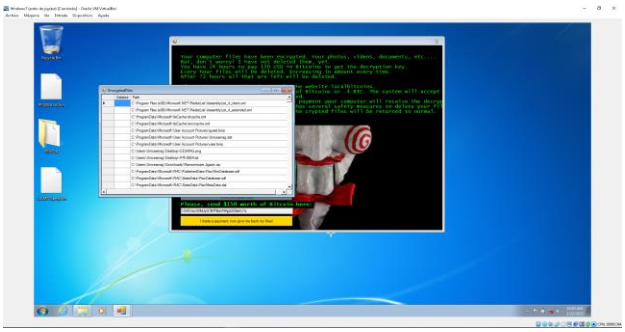
De esta manera se visualiza cuando ya se ha terminado de ejecutar el ransomware, y presenta un cronómetro en rojo con un tiempo límite para realizar el pago de la extorsión y se visualiza los archivos que cifró el ransomware.

Fig. 72 Ejecución del ransomware Jigsaw

Elaboración propia

El programa expone los archivos cifrados por el ransomware.

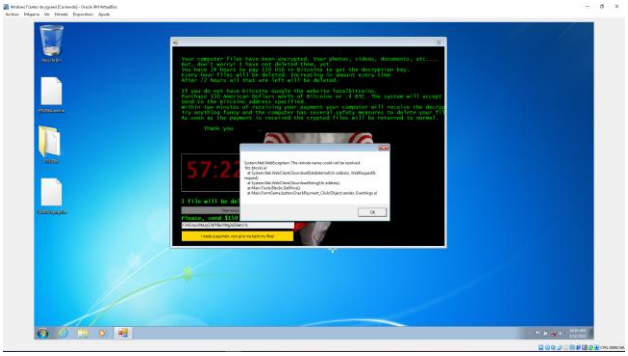
Fig. 73 Archivos a borrar



Elaboración propia

Colocando una clave incorrecta el programa expone el siguiente mensaje amenazante donde dice que tenemos poco tiempo para realizar el pago si queremos nuestros archivos descifrados.

Fig. 74 Extorción por Jigsaw



Elaboración propia

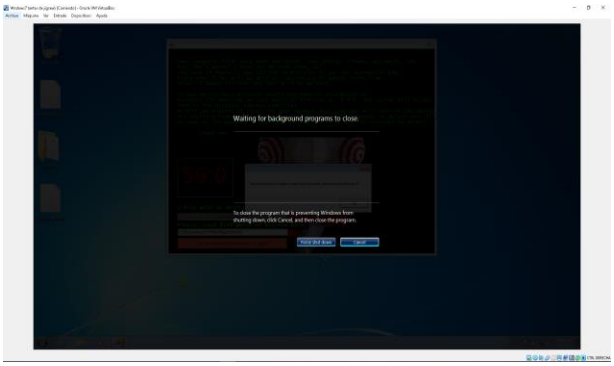
De esta manera se visualiza en rojo si se coloca mal la contraseña

Fig. 75 Cronometro Jigsaw

Elaboración propia

El programa no se cierra de forma correcta obligando a forzar el cierre de Windows en la máquina virtual.

Fig. 76 No cierra Windows 7 con facilidad



Elaboración propia

Y es así como se infecta un ransomware en un sistema el siguiente paso es mostrar el método de desinfección para el caso concreto explicando el paso a paso de cómo se debe aplicar.

3) Uso de herramienta de desinfección

a) Uso de ID ransomware

Tomando la infección controlada dentro de una máquina virtual anterior, se procede a explicar los pasos para el uso de la herramienta ID ransomware de la siguiente manera:

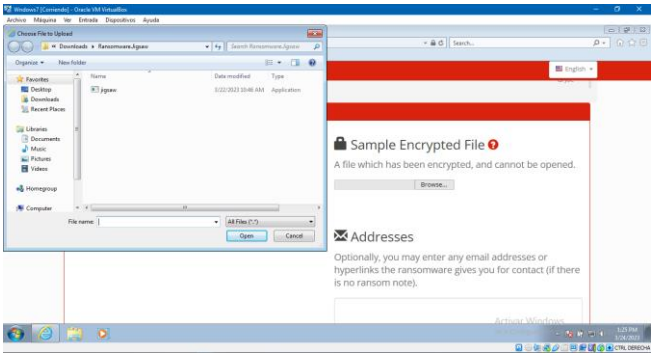
- Como paso 1 para el uso de la herramienta, se toma el archivo ejecutable del malware y uno de los archivos cifrados del ordenador afectado y los llevamos a la página Id ransomware con el fin de que nos diga qué tipo de infección es.

Fig. 77 ID ransomware

Elaboración propia

- Primero se toma el archivo original de infección y el archivo infectado para que la página los estudie.

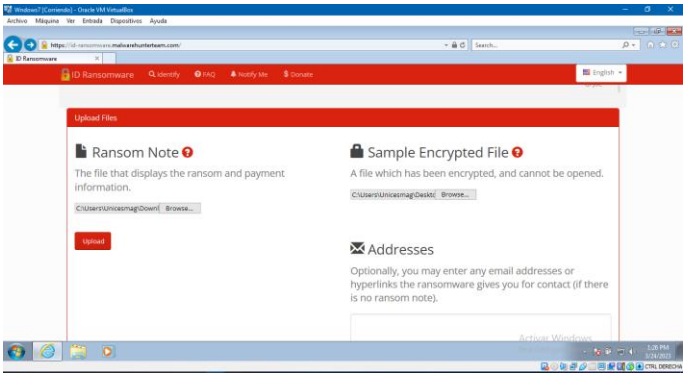
Fig. 78 ID ransomware archivos infectados



Elaboración propia

- Como se observa en la imagen se subieron los archivos y se procede a clicar en upload

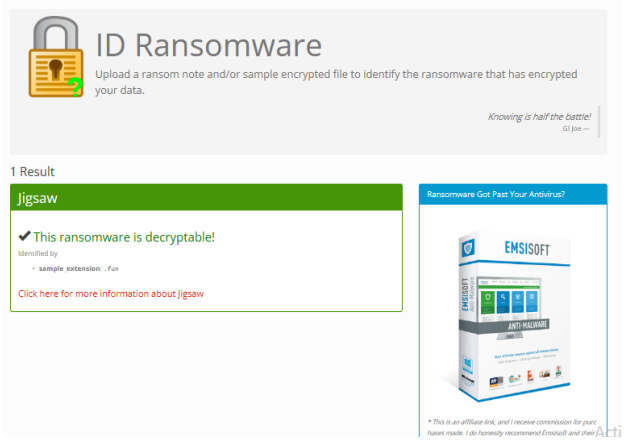
Fig. 79 ID ransomware página



Elaboración propia

- De esta manera se visualiza que la página de ID Ransomware detectó cual es el malware que está afectando al sistema operativo. Ingresando al link sugerido por ID ransomware se pasa a la página de descarga de la herramienta de descifrado creada por Emsisoft.

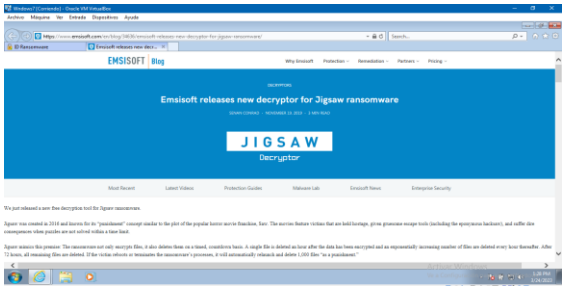
Fig. 80 ID ransomware herramienta desencriptado



Elaboración propia

- Como paso 2 se ingresa a la página de EMSISOFT para descargar la herramienta contra Jigsaw.

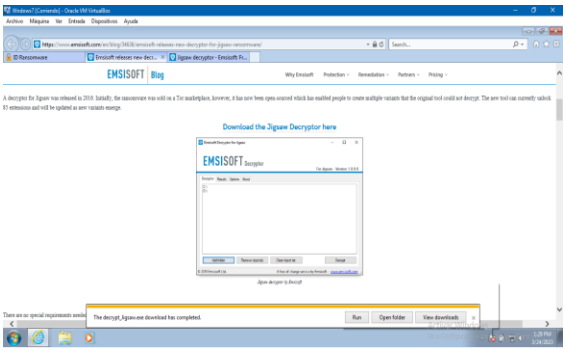
Fig. 81 Descarga herramienta desencriptado



Elaboración propia

- Click en Download para descargar la herramienta de forma segura.

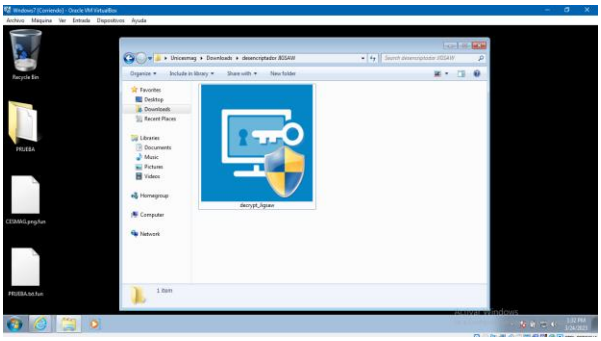
Fig. 82 Descarga herramienta desencriptado



Elaboración propia

- La herramienta es visualizada en nuestro sistema de Windows 7 de la siguiente manera.

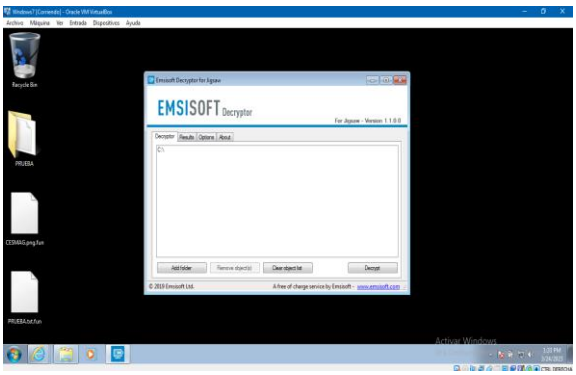
Fig. 83 Herramienta descargada



Elaboración propia

- Imagen de la herramienta instalada

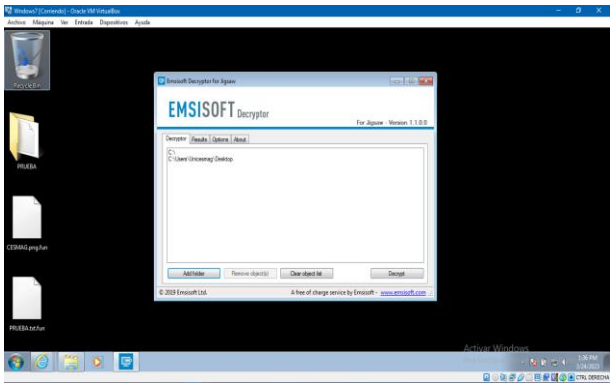
Fig. 84 Herramienta desencriptado



Elaboración propia

- Haciendo click en Add folder seleccionamos los archivos necesarios a desencriptar. Cuando ya tengamos seleccionada las carpetas le damos en Decrypt para iniciar el proceso.

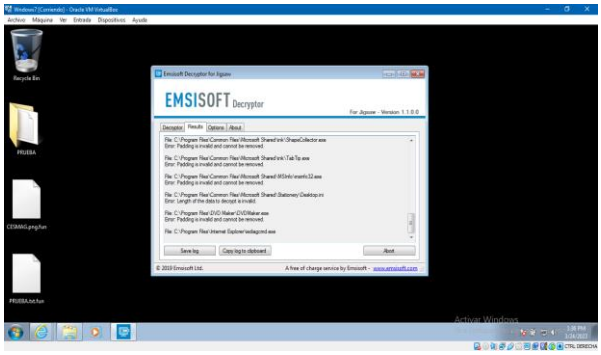
Fig. 85 Uso de herramienta desencriptado



Elaboración propia

- En esta imagen vemos todos los logs que se están ejecutando. Estos logs están revisando cada carpeta que se haya seleccionado buscando archivos para desencriptar

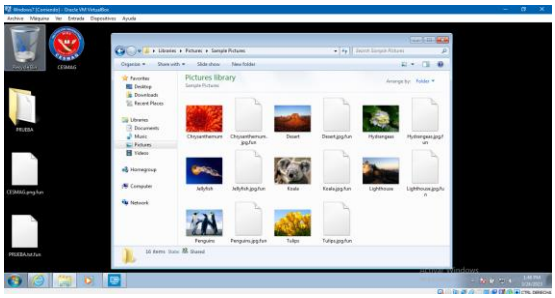
Fig. 86 Uso herramienta desencriptado



Elaboración propia

- Esta imagen muestra los archivos desencriptados por la herramienta.

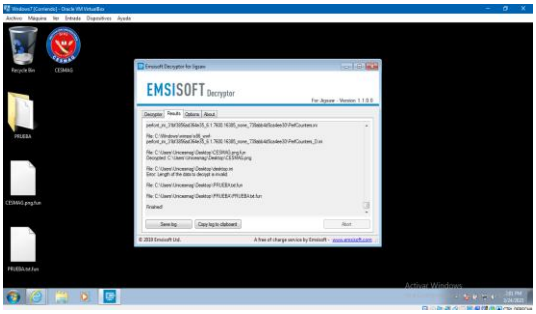
Fig. 87 Uso herramienta desencriptado



Elaboración propia

- En esta imagen se visualiza que ya finalizó el proceso de desencriptado

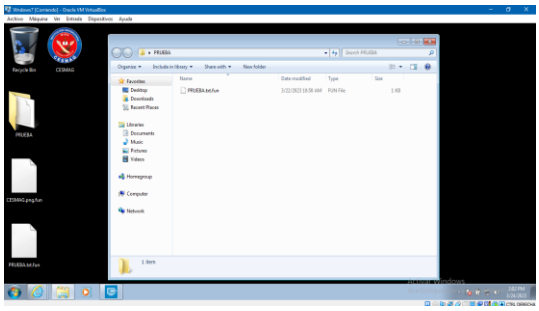
Fig. 88 Uso herramienta desencriptado



Elaboración propia

- En esta imagen vemos que los archivos con extensión en .txt no los desencripto la herramienta de Emisoft

Fig. 89 Uso herramienta desencriptado



Elaboración propia

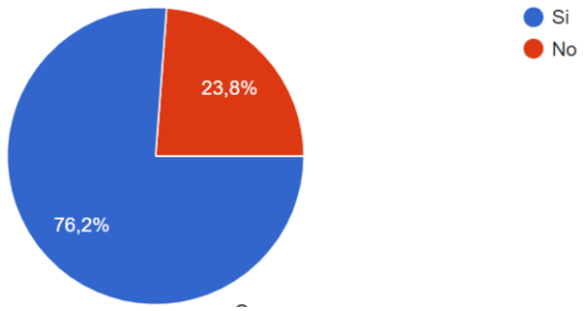
Aquí termina el experimento realizado en máquina virtual que expuso la infección del ransomware Jigsaw y el uso de la herramienta de desencriptado, dando como resultado que en general la aplicación es eficiente al momento de hacer lo solicitado pero que tiene sus limitantes como que hay ciertos tipos de archivos como los .txt que no son desencriptados por la herramienta.

Validar la implementación de la metodología en el sistema web mediante la realización de evaluaciones a usuarios dentro del sitio.

4) Encuesta validación metodología en el sistema web

a) Pregunta 1 Siendo el paso 1 de la metodología cerrar la escena de infección, ¿para su organización fue clara la información entregada por la metodología implementada en el sistema web?

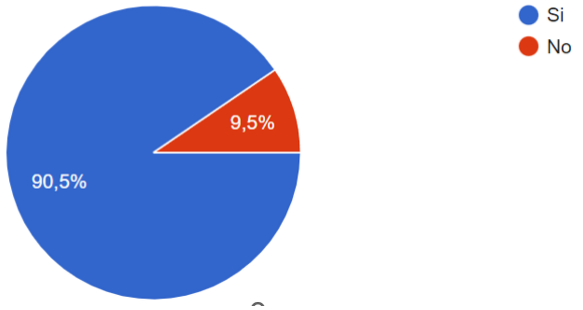
Fig. 90 Gráfica 1 encuesta validez



Elaboración propia

b) Pregunta 2 Siendo el paso 2 de la metodología no apagar el ordenador afectado, ¿para su organización fue clara la información entregada por la metodología implementada en el sistema web?

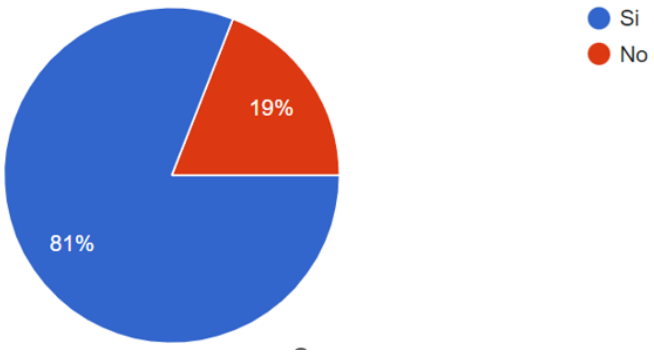
Fig. 91 Gráfica 2 encuesta validez



Elaboración propia

c) Pregunta 3 Siendo el paso 3 desconectar todas las conexiones, ¿Para su organización fue clara la información entregada por la metodología implementada en el sistema web?

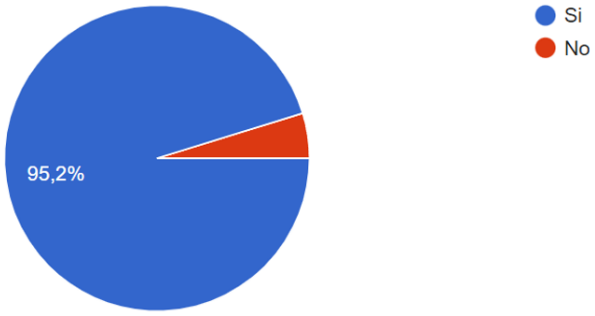
Fig. 92 Gráfica 3 encuesta validez



Elaboración propia

d) Pregunta 4 El paso 4 expone como identificar el tipo de ransomware involucrado en su infección, ¿Para su organización fue clara la información entregada por la metodología implementada en el sistema web?

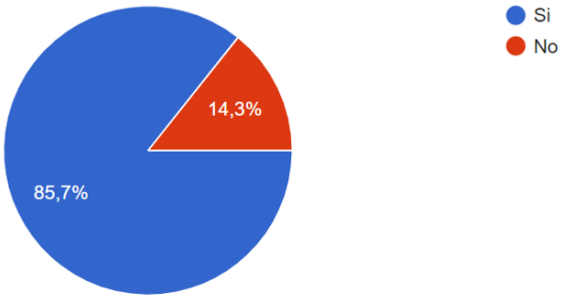
Fig. 93 Gráfica 4 encuesta validez



Elaboración propia

e) Pregunta 5 El paso 5 muestra que el ransomware involucrado es de cifrado, ¿la información entregada fue clara para hacerle frente a la infección?

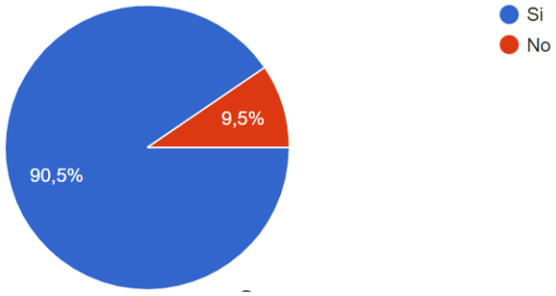
Fig. 94 Gráfica 5 encuesta validez



Elaboración propia

f) Pregunta 6 Cómo usuario al usar el sitio web en general, ¿Para usted fue fácil encontrar información relacionada a capacitación y específicamente sobre la metodología de desinfección planteada?

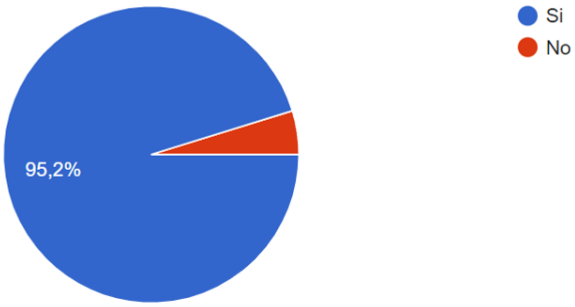
Fig. 95 Gráfica encuesta validez



Elaboración propia

g) Pregunta 6 ¿Cómo usuario el uso de la metodología planteada dentro del sistema web fue satisfactorio?

Fig. 96 Gráfica 6 encuesta validez



Elaboración propia

VI. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

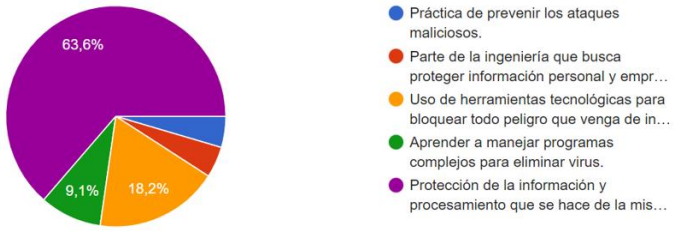
A. Resultados encuesta final postprueba validación sitio web y metodología.

Se realizo una encuesta final sobre el uso de la metodología en el sitio web, con el objetivo de obtener estadísticas claras sobre la facilidad de comprensión y la efectividad de la misma.

1) Después de utilizar el sitio web y usar la metodología planteada ¿Cuál es su concepto de seguridad informática?

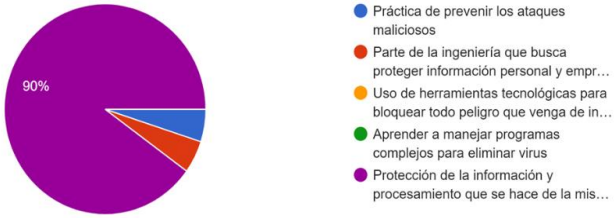
En la figura 97 se muestra el resultado obtenido en la encuesta presentada previo a la realización del sitio web. Por lo tanto, los resultados mostrados exponen que el concepto no estaba muy definido entre los encuestados, con un 63.6% la grafica muestra que los usuarios tienen claro el concepto de seguridad informática y mientras que para el 36.4% el concepto no esta claro.

Fig. 97 Grafica Encuesta Sondeo



En la figura 98, se exhiben los resultados de la encuesta final, en la cual los usuarios, tras utilizar el sitio web, demuestran una mejoría en el aprendizaje del concepto de seguridad informática. Estos resultados revelan que un 90% de los encuestados seleccionaron de manera acertada dicho concepto, brindando evidencia sólida de su comprensión mejorada.

Fig. 98 Gráfica Encuesta Final



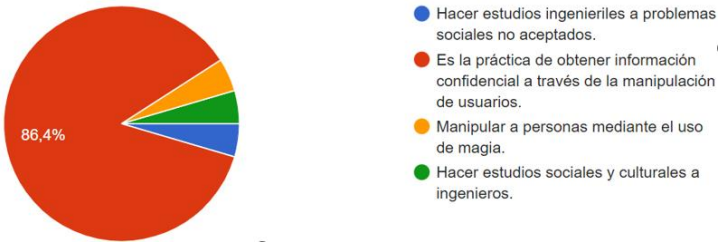
2) Después de utilizar el sitio web y usar la metodología planteada, ¿Cuál es su concepto sobre ingeniería social?

En la figura 99, se presenta el resultado de la encuesta de sondeo realizada antes del uso del sitio web, revelando que el concepto de ingeniería social no está claramente comprendido. Se observa que el concepto correcto, definido como "la práctica de obtener información confidencial mediante la manipulación de usuarios", obtuvo un 40%, cifra que coincide con el concepto erróneo que sugiere "realizar estudios ingenieriles en problemas sociales no aceptados".

Fig. 99 Gráfica Encuesta de Sondeo

El resultado del uso del sitio web en el área de ingeniería social se presenta en la figura 100, demostrando una mejora en el concepto para el 86.4% de los encuestados. Esto evidencia que el sitio web cumple con su propósito al clarificar los conceptos evaluados.

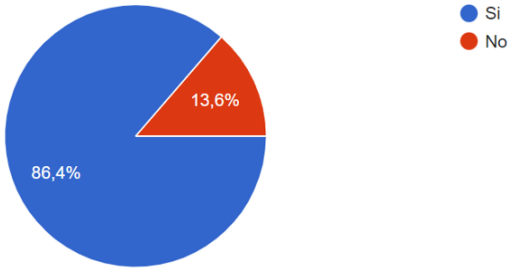
Fig. 100 Gráfica Encuesta Final



3) Después de utilizar el sitio web y usar la metodología planteada, ¿quedo claro que es un ciberataque conocido como ransomware?

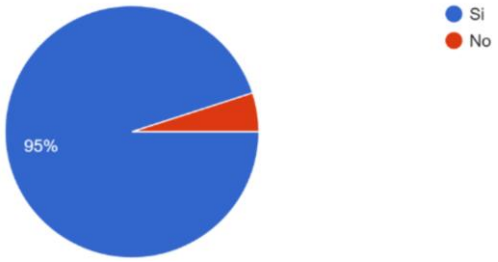
En la figura 101 se muestra el resultado de la encuesta previa a el uso del sitio web, la cual arroja que en un 86.4% de los encuestados el concepto de que es un ciberataque ransomware es positivo.

Fig. 101 Gráfica Encuesta Sondeo



En la figura 102 se muestra el resultado de la encuesta final luego del uso del sitio web y su metodología. Se expone que el concepto, que es un ciberataque ransomware, mejora en un 10% en relación al resultado expuesto de la encuesta de sondeo.

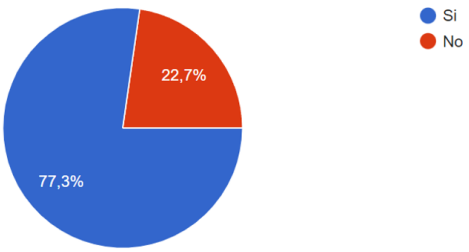
Fig. 102 Gráfica Encuesta Final



4) Después de usar el sitio web, ¿Le quedo claro como infecta un ransomware un sistema operativo?

La figura 103 muestra los resultados del uso de la metodología en el sitio web. Se puede apreciar que el 77% de los usuarios comprenden de manera clara la explicación interactiva sobre cómo un ransomware infecta un sistema operativo. Sin embargo, el 22% restante tiene dificultades para comprenderla.

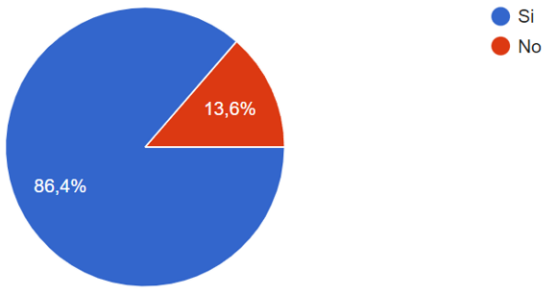
Fig. 103 Gráfica Encuesta Final



5) ¿El uso del paso a paso de la metodología contra ransomware fue claro y beneficioso para su organización?

La figura 104 expone que el uso del paso a paso de la metodología implementada en el sitio web fue en un 86.4% favorable para los usuarios. Lo que denota que el paso a paso es claro y fácil de manejar y alcanza su finalidad la cual es ayudar al usuario a cómo hacerle frente a un ataque tipo ransomware.

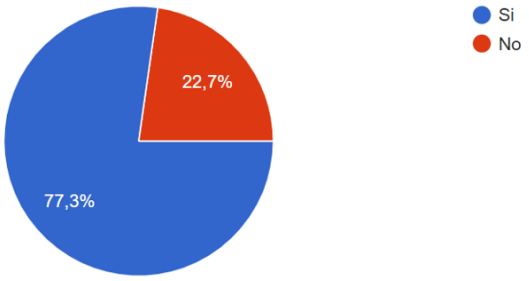
Fig. 104 Gráfica Encuesta Final



6) ¿La metodología plateada enseña de forma clara como hacerle frente a un ataque ransomware?

La figura 105 revela que, en el caso de los usuarios que utilizaron el sitio web y su metodología, se ofrece una explicación y capacitación clara sobre cómo enfrentar este problema. Esto indica que tanto el sitio como la metodología y sus pasos son comprensibles para el 77.3% de los usuarios, logrando así el objetivo de la investigación.

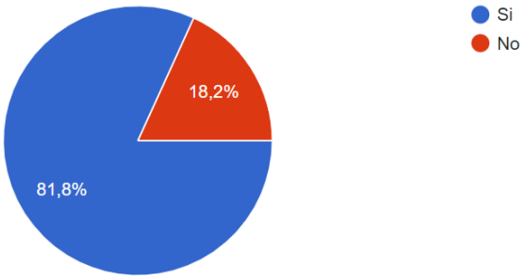
Fig. 105 Gráfica Encuesta final



7) ¿El módulo herramientas creado en el sitio web, fue útil y fácil de manejar para hacer frente a un caso específico de ataque ransomware?

La figura 106 revela que el apartado de herramientas en el sitio web fue útil y de fácil manejo para el 81.8% de los usuarios. En dicha página se presenta un listado de herramientas diseñadas para combatir el ransomware. Para cada una de estas herramientas, se proporciona información detallada sobre cómo encontrarlas, instalarlas y utilizarlas de manera efectiva.

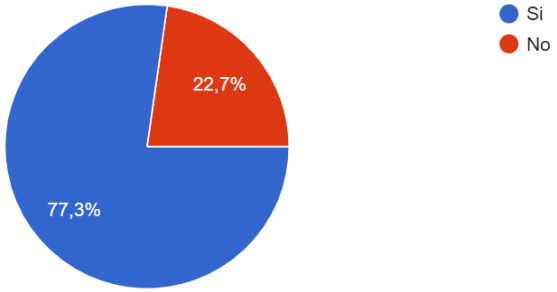
Fig. 106 Gráfica Encuesta Final



8) ¿El módulo de capacitación cree que proporciona la información adecuada para explicar los conceptos de seguridad informática?

La figura 107 muestra los resultados del módulo de capacitación del sitio web. Revela que el 77.3% de los usuarios consideró que la información contenida en dicho módulo fue apropiada para explicar los conceptos de seguridad informática.

Fig. 107 Gráfica Encuesta Final

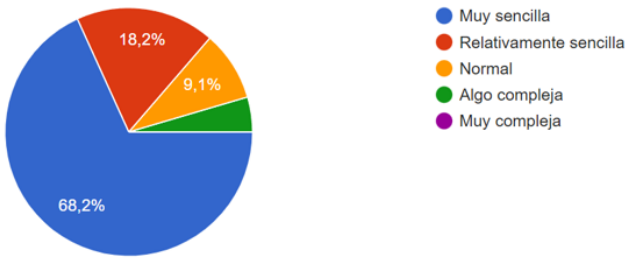


B. Resultados satisfacción del sistema

1) Navegabilidad

De acuerdo con la figura 108, la navegabilidad en el sitio web cumple satisfactoriamente su propósito para el 68.2% de los usuarios que la utilizaron. Esto indica que el sitio web es altamente accesible, lo que implica que su uso resulta sencillo para la mayoría de los usuarios.

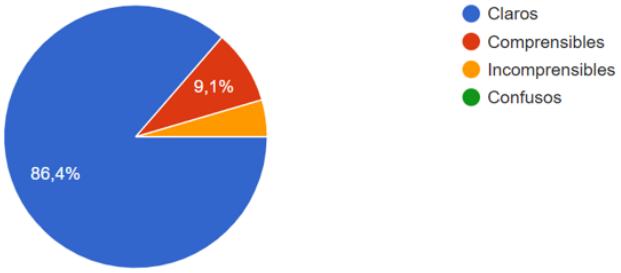
Fig. 108 Gráfica Evaluación Sitio Web



2) Contenidos

Según la figura 109 se expone que los contenidos para un 86.4% de los usuarios fueron claros. Lo que denota que el sitio web contiene la información necesaria para cumplir con la finalidad para la que fue creado.

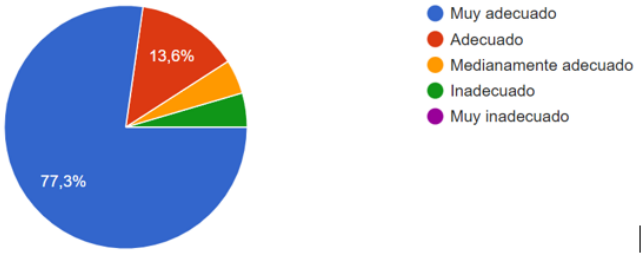
Fig. 109 Gráfica Evaluación sitio web



3) Variedad de Contenido

Según la figura 110 se expone que la variedad de contenidos es muy adecuada para el 77.3% de los usuarios. Lo que denota que el sitio web cumple con las expectativas de la investigación.

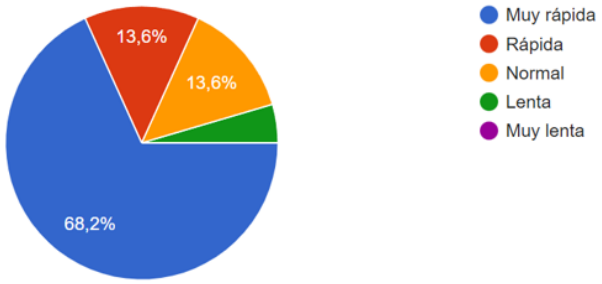
Fig. 110 Gráfica evaluación Sitio web



4) Descarga Contenido

Según la figura 111 se expone que para un 68.2% de los usuarios la descarga de contenido es muy rápida, esto depende de velocidades de los diferentes servicios de internet que tengan los usuarios. Lo importante para la investigación es que estas descargas sean fáciles de realizar dentro del módulo herramientas, todo encaminado en cumplir el 5to paso de la metodología el cual es usar una herramienta de desinfección contra ransomware.

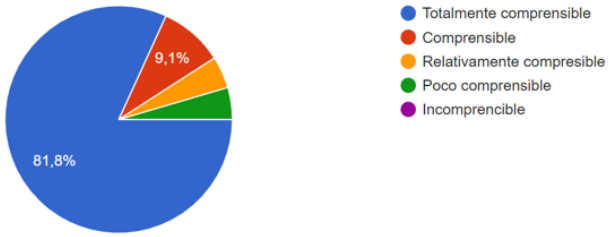
Fig. 111 Gráfica evaluación sitio web



5) Información comprensible

Según la figura 112 se expone que la información para el 81.8% de los encuestados es totalmente comprensible.

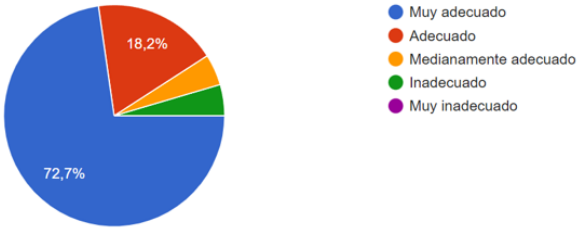
Fig. 112 Gráfica evaluación sitio web



6) Diseño

Según la figura 113 se expone que el diseño del sitio es muy adecuado para el 72.7% de usuarios que lo usaron.

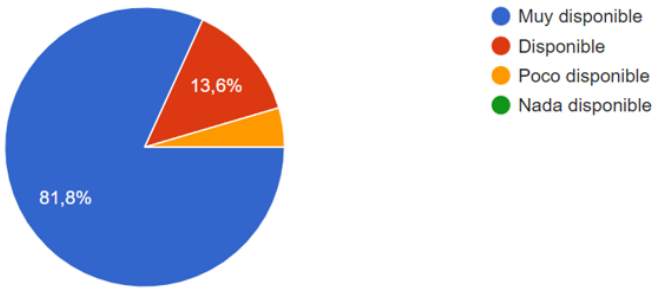
Fig. 113 Gráfica evaluación sitio web



7) Disponibilidad

Según la figura 114 expone que para el 81.8% de los usuarios el sitio web estuvo disponible para acceder a él.

Fig. 114 Gráfica evaluación sitio web



C. Discusión de resultados

Después de haber examinado detalladamente la información recopilada a través de la encuesta de sondeo, se pudo obtener información vital que fue utilizada para la creación del sitio web, así como también para sus distintos módulos, tales como la capacitación, la metodología y las herramientas.

Al comparar los resultados de la encuesta de sondeo con los de la encuesta final post-prueba de validación del sitio y su metodología, se puede concluir que los usuarios involucrados en esta investigación han logrado una capacitación efectiva en temas relacionados con la ingeniería social. Esto ha permitido que los conceptos sean comprendidos de manera clara y precisa.

Además, los usuarios han logrado comprender qué es un ransomware, cómo infecta un sistema y, sobre todo, cómo hacerle frente utilizando los pasos de la metodología. Esto ha permitido que los usuarios tengan un mayor conocimiento acerca de las amenazas cibernéticas y cómo protegerse contra ellas.

En resumen, la encuesta de sondeo ha sido fundamental para la obtención de información valiosa, la cual ha sido utilizada para la creación del sitio web y sus distintos módulos. La capacitación ofrecida ha permitido que los usuarios comprendan de manera efectiva los conceptos relacionados

con la ingeniería social y las amenazas cibernéticas, lo que ha resultado en una mejor preparación para enfrentar los riesgos en el entorno digital.

VII. CONCLUSIONES

La caracterización de los principales tipos de ataque relacionados al ransomware existentes, ha sido un aporte significativo para el cumplimiento del objetivo específico de la investigación, permitiendo una mejor integración de los mismos en la metodología. Esta información resulta de gran importancia para la prevención y gestión adecuada de los ataques de ransomware, siendo de gran utilidad para los usuarios involucrados en la investigación.

Después de un arduo trabajo en la creación de la metodología, se lograron desarrollar de manera exitosa las diferentes actividades necesarias para su implementación dentro del sitio web. Esto permitió que los usuarios pudieran acceder de forma interactiva a las herramientas y conceptos necesarios para la prevención y defensa en casos de ataque ransomware. Los usuarios ahora tienen acceso a una plataforma en línea que les permite aprender y practicar los pasos necesarios para hacer frente a este tipo de ataques.

Los equipos de cómputo modernos tienen características de seguridad integradas que los modelos más antiguos no tienen. Además, estos equipos tienen un mejor rendimiento y capacidad de procesamiento, lo que permite a los programas de seguridad funcionar, detectar y prevenir amenazas de manera más efectiva. Al actualizar los equipos de la empresa, se permite que se tengan las herramientas necesarias para trabajar de manera segura y eficiente.

La investigación llevada a cabo en el área de seguridad informática ha sido crucial para la creación de una metodología eficiente para la prevención de ataques ransomware. Sin embargo, se debe tener en cuenta que los conceptos relacionados con la seguridad informática evolucionan constantemente, por lo que es esencial seguir investigando nuevas formas de hacer frente a las amenazas emergentes.

VIII. RECOMENDACIONES

Como recomendación para futuras investigaciones, se sugiere continuar profundizando en este tipo de conceptos, de manera que se puedan desarrollar metodologías aún más efectivas para prevenir y combatir los ataques ransomware.

Los investigadores gracias a el arduo trabajo dentro de los problemas que conllevan las infecciones tipo ransomware, recomiendan que dentro de las organizaciones se realicen capacitaciones constantes, especialmente en temas de ingeniería social como puede ser el phishing. Esto último encaminado en reducir la posibilidad del ingreso de una infección a su sistema, ya que la tarea de la capacitación es hacer de fácil conocimiento para los empleados este tipo de engaños. Esta capacitación es de fácil realización ya que los conceptos no son difíciles de exponer, explicar y entender.

Mantener actualizados los equipos de las organizaciones debe ser una de las tareas obligatorias dentro del departamento de sistemas de la empresa. Ya que el uso de sistemas operativos desactualizados es uno de los vectores que más infecciones causa, al no contar con las medidas de seguridad y corrección necesarias para bloquear vulnerabilidades y amenazas.

REFERENCIAS

[1] ORGANIZACIÓN INTERNACIONAL DEL TRABAJO. COVID-19 y el mundo del trabajo [en línea]. OIT, Julio. 2021 [Online]. Avalible: <URL: https://www.ilo.org/global/topics/coronavirus/lang--es/index.htm>.

[2] PORTAFOLIO. Aumentan en 30% los ataques cibernéticos en Colombia 2021 [Online]. Avalible: <URL: https://www.portafolio.co/tendencias/aumentan-en-30-los-ataques-ciberneticos-en-colombia-553803>.

[3] AGUILERA, Purificación. Seguridad Informática. Madrid: EDITEX S.A, 2010. p. 9. ISBN 978-84-9771-761-8.

[4] ALARCÓN, Daniel. El impacto de la economía de bajo contacto. octubre. 2020 [en línea]. Disponible en: <URL: https://deltaxventures.com/el-impacto-de-la-economia-de-bajo-contacto-revision/>.

[5] VARELA, Joaquín. Ransomware: operativo rescate. [en línea]. Welivesecurity by ESET, oct. 2010 [citado el 3 noviembre 2021] Disponible en:<URL: https://www.welivesecurity.com/la-es/2010/10/20/ransomware-operativo-rescate/>.

[6] DIAZGRANADOS, Hernán. Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021 [en línea]. Kaspersky dayli, 31 agosto 2021 [citada 3 noviembre 2021]. Disponible en: <URL: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/.>.

[7] PASSERI, Paolo. September 2021 Cyber Attacks Statistics [en línea]. 1 ed. [Roma, Italia]: HACKMAGEDDON, sep. 2021 [citado 4 nov 2021]. Disponible en internet: <URL: https://www.hackmageddon.com/2021/10/28/september-2021-cyber-attacks-statistics/>.

[8] NEKANE, Alonso. La informática forense en la investigación de delitos. [en línea]. ATICO34, julio. 2021 [citado el 23 de nov de 2021] Disponible en: <URL: https://protecciondatos-lopd.com/empresas/informatica-for ense/ >.

[9] MEDINA F. Seguridad Informática: virus ransomware, el Secuestro virtual de datos es Posible. Proyecto Trabajo Final de Graduación Ingeniería en Software. Córdoba, Argentina: Universidad empresarial siglo 2. Facultad de ingeniería, Departamento Ingeniería de software, 2017. 10 p.

[10] PALACIO Juan, ¡OJO! USTED PUEDE SER LA PRÓXIMA VÍCTIMA DE RANSOMWARE [en linea]. 1 ed. [Medellín, Colombia]: Ransomware Help, enero 2021 [citado noviembre 04 2021]. Disponible en internet: URL: https://latam.ransomwarehelp.com/ojo-usted-puede-ser-la-proxima-victima-de-ransomware/ >.

[11] MIRANDA CAIRO, Michel, et al. Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. En: Revista Cubana de Ciencias Informáticas. Abril-junio, 2016. Vol. 10, no. 2, p. 14-26.

[12] GORDÓN REVELO, Diego, et al. Análisis de Estrategias de Gestión de Seguridad Informática con Base en la Metodología Open Source Security Testing Methodology Manual (OSSTMM) para la Intranet de una Institución de Educación Superior. En: ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica. Mayo-octubre, 2018. Vol. 7, no. 1, p. 1-21.

[13] CALIXTO, Juan. Ethical hacking aplicado al sistema de gestión documental de la ONPE para evitar vulnerabilidades y acceso no autorizado a la información. Trabajo de Suficiencia Profesional para optar el título de Ingeniero de Sistemas. Lima-Perú: Escuela Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, 2018. 140 p.

[14] Protocolo de informática forense ante ciber incidentes en telemedicina para preservar información como primera respuesta [en línea]. Volumen 19: Revista Científica General José María Córdova. 2020 [citado 4 noviembre 2021]. Anual. Disponible en internet: https://revistacientificaesmic.com/index.php/esmic/article/view/726/738. ISSN 1900-6586 (impreso), 2500-76.

[15] Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas [en línea]. Ed 2 vol. 22: Universidad Tecnológica de Pereira. 2017 [citado 4 nov 2021]. Anual. Disponible en internet: https://revistas.utp.edu.co/index.php/revistaciencia/article/view/11371/10511. ISSN 0122-1701.

[16] QUIROZ, Stephen y ZAPATA, Julián y VARGAS, Héctor. Predicción de ciberataques en Sistemas industriales SCADA a través de la implementación del filtro Kalman [en línea]. ed. 48 [Medellín, Colombia] agosto 2020 [citado 4 noviembre 2021]. Vol. 23 No. 48 pp

249-267. Disponible en internet: <https://dialnet.unirioja.es/servlet/articulo?codigo=7833456>.

[17] BASTIDAS, David y ZÚÑIGA, Luis. LA APLICACIÓN DE LA METODOLOGÍA OWISAM EN LA RED INALÁMBRICA DE LA INSTITUCIÓN UNIVERSITARIA CESMAG. Trabajo de grado Ingeniería de Sistemas: Pasto, Nariño: Universidad Cesmag. Facultad de Ingeniería. 2018. 287 p.

[18] DIAS ORDOÑEZ, Paulo y JARAMILLO BOLAÑOS, José. Implementación de técnicas hacking al modelo de red inalámbrica en la institución universitaria Cesmag. San Juan de Pasto: Universidad CESMAG, 2017.

[19] GÓMEZ, Álvaro. Seguridad informática y protección de datos [en línea]. 1 ed. CEUPE Magazín, ago. 2020 [citado 4 nov 2021]. Disponible en internet:<URL: https://www.ceupe.com/blog/seguridad-informatica-y-proteccion-de-datos.html>.

[20] CASTRO, Martha. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES [en línea]. 1 ed. [Alicante, España]. Editorial Área de Innovación y Desarrollo, S.L. octubre 2018. [citado 4 nov 2021]. Disponible en internet: <URL: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informática.pdf >.

[21] PÉREZ, Florián. Ciberseguridad: Ransomware, parte I – El negocio del secuestro digital [en línea]. En: Cantabria. Mayo, 2015. [citado el 3 de noviembre de 2021] Disponible en:<URL: http://www.cantabriatic.com/ciberseguridad-ramsonware-parte-i/>.

[22] KASPERSKY. ¿Qué es el cifrado de datos? Definición y explicación [en línea]. My Kaspersky: Kaspersky Total Security. 2020. [citado nov 4 2021]. Anual. Disponible en internet: https://latam.kaspersky.com/resource-center/definitions/encryption.

[23] Ibid. p. 2.

[24] Ibid. p. 3.

[25] UNIVERSITAT POLITÉCNICA DE VALENCIA. ¿Qué es una Firma Electrónica? [en línea]. 1 ed. [Valencia, España]: UPV, ago. 2020 [citado 4 nov 2021]. Disponible en internet: <URL: https://www.upv.es/contenidos/CD/info/711250normalc.html >.

[26] ANTELEC SL, Protocolos de seguridad inalámbrica: WEP, WPA y WPA2. ¿En qué se diferencian? [en línea] 1 ed. [Córdoba, España]: Antelec Newsletter, oct 2018 [citado 4 nov

2021]. Disponible en internet: <URL: https://www.antelec.es/protocolos-seguridad-wep-wpa-wpa2/>.

[27] FERNÁNDEZ, Yúbal. ¿Cuál es la diferencia: malware, virus, gusanos, spyware, troyanos, ransomware, ¿etcétera? [en línea]. 1 ed. [México, DC] Xataca Basics, 2 junio 2020 [citado 4 nov. 2021]. Disponible en internet: <URL: https://www.xataka.com/basics/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etcetera>.

[28] MUÑOZ, Facundo. Qué es un troyano en informática. [en línea]. Welivesecurity by ESET, may. 2021 [citado el 3 de Noviembre de 2021] Disponible en:<URL: https://www.welivesecurity.com/la-es/2021/05/14/que-es-virus-troyano-informatica/>.

[29] GONZÁLEZ, Yolanda. ¿Qué es un gusano informático? Tipos y ejemplos. [en línea]. En: ATICO34, ciberseguridad, sep. 2020 [citado el 4 de noviembre de 2021] Disponible en:<URL: https://protecciondatos-lopd.com/empresas/gusano-informatico/>

[30] FERNÁNDEZ, Yúbal. ¿Cuál es la diferencia: malware, virus, gusanos, spyware, troyanos, ransomware, ¿etcétera? [en línea]. 1 ed. [México, DC] Xataca Basics, 2 junio 2020 [citado 4 nov. 2021]. Disponible en internet: <URL: https://www.xataka.com/basics/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etcetera>.

[31] ALESTRA, Staff. Ciberseguridad básica: ¿Qué es el Spyware? [en línea]. En: Alestra, oct. 2020 [citado el 4 de noviembre de 2021] Disponible en:<URL: http://blog.alestra.com.mx/ciberseguridad-basica-que-es-el-spyware>.

[32] VILLARREAL, Rafael. Ransomware (secuestro de información) como delito informático en el ecuador. Trabajo de Titulación Modalidad Proyecto de Investigación presentado como requisito previo a la obtención del título de Abogado de los Tribunales y Juzgados de la República. Ecuador: universidad central del ecuador facultad de jurisprudencia y ciencias sociales carrera de derecho, 2019. 26 p.

[33] RUS, Cristian. La curiosa historia del primer ransomware del mundo, su inventor y la víctima que consiguió eludirlo [en línea]. 1 ed. [México, DC]: Xataka, junio 2021 [citado 4 nov 2021]. Disponible en internet: <URL: https://www.xataka.com/historia-tecnologica/curiosa-historia-primer-ransomware-mundo-su-inventor-victima-que-consiguio-eludirlo >.

[34] KASPERSKY. Identificación de ransomware: en qué se diferencian los troyanos de cifrado [en línea]. 1 ed. enero 2021. [citado 4 nov. 2021]. Disponible en internet: <URL: https://latam.kaspersky.com/resource-center/threats/ransomware-attacks-and-types >.

[35] PASTOR, Javier. Ciberataques los fines de semana: así actúan los ransomware de moda, BitPaymer y Ryuk. En: XATAKA. Noviembre. 2019 [citado el 1 de noviembre de 2021] Disponible en:<URL: https://www.xataka.com/seguridad/ciberataques-fines-semana-asi-actuan-ransomware-moda-bitpaymer-ryuk>.

[36] JIMÉNEZ, Javier. El último truco del ransomware Sodinokibi para no ser detectado. En: REDES ZONE. Abril. 2020 [citado el 29 de octubre de 2021] Disponible en:<URL: https://www.redeszone.net/noticias/seguridad/ransomware-sodinokibi-pago-no-detectado/>.

[37] RAMÍREZ, Helena. Ransomware: Definición, tipos y tendencias 2021-2022. En: ATICO34. Agosto. 2021 [citado el 28 de octubre de 2021] Disponible en:<URL: https://protecciondatos-lopd.com/empresas/ransomware/>.

[38] BELCIC, Ivan. Qué es el ransomware CryptoLocker y cómo eliminarlo. En: AVAST. Mayo. 2021 [citado el 28 de octubre de 2021] Disponible en:<URL: https://www.avast.com/es-es/c-cryptolocker>.

[39] ROMERO, Marta. El nuevo ataque informático 3 en 1: phishing, ransomware y troyano. En: Computer Hoy. Mayo. 2021 [citado el 25 de octubre de 2021] Disponible en:<URL: https://computerhoy.com/noticias/tecnologia/nuevo-ataque-informatico-3-1-phishing-ransomware-troyano-871459>.

[40] HIDALGO, Iván y PUCUNA, Saul y AYALA, Luis y CAJO, Byron. Informatice forense [en línea]. 17 ed. [Riobamba Ecuador]: Aval ESPOCH. 2017 [citado nov 4 2021]. Disponible en internet: <URL: http://cimogsys.espoch.edu.ec/direccion-publicaciones/public/docs/books/2019-09-19-133251-70%20Libro%20Informatica%20Forense.pdf>.

[41] MCPRO, Perito Informático Forense, una de las profesiones con más salidas [en línea]. [Madrid, España]: Redacción Mcpro, ago. 2014 [citato 4 nov, 2021]. Disponible en internet: <URL: https://www.muycomputerpro.com/2014/08/25/perito-informatico-forense>.

[42] WELIVESECURITY. 5 fases fundamentales del análisis forense digital [en línea]. ed. 1. [Latinoamérica]: WELIVESECURITY, abr. 2015. [citado 4 nov. 2021]. Disponible en

internet: <URL: https://www.welivesecurity.com/la-es/2015/04/15/5-fases-analisis-forense-digital/ >.

[43] RED HAT, ¿Qué es una máquina virtual? [en línea]. ed. 1. [Latinoamérica]: Red hat, sep. 2019 [citado 4 nov. 2021]. Disponible en internet: <URL: https://www.redhat.com/es/topics/virtualization/what-is-a-virtual-machine>.

[44] RANCHAL, Juan. GUÍAS ¿Qué es un hipervisor? ¿Cuáles son las diferencias entre VirtualBox, VMware e Hyper-V? En: MC. Marzo. 2020 [citado el 20 de octubre de 2021] Disponible en:<URL: https://www.muycomputer.com/2020/03/27/hipervisor-virtualbox-vmware-hyperv/>.

[45] ORTIZ, Angel. ¿Qué Es Un Hipervisor? Tipos De Hipervisores 1 Y 2. En: HOSTDIME. Septiembre. 2019 [citado el 14 de octubre de 2021] Disponible en:<URL: https://www.hostdime.com.ar/blog/que-es-un-hipervisor-tipos-de-hipervisores-1-y-2/>.

[46] RED HAT, ¿Qué es una máquina virtual? [en línea]. ed. 1. [Latinoamérica]: Red hat, sep. 2019 [citado 4 nov. 2021]. Disponible en internet: <URL: https://www.redhat.com/es/topics/virtualization/what-is-a-virtual-machine>.

[47] MALDONADO, Diego. Virtualización: ¿qué es y para qué sirve exactamente? [en línea]. 1 ed. [Mexico, DC]: icorp, ago. 2019 [citado 4 nov. 2021]. Disponible en internet: <URL: http://www.icorp.com.mx/blog/que-es-virtualizacion/#respond>.

[48] USB tipo A (2023) [En línea]. Disponible en: https://www.neoguias.com/conector-usb-tipo-a/ Acedido: 17 Mar. 2023

[49] F. Yúbal, (17 junio 2019) USB Type C: qué es exactamente y en qué se diferencia del resto [En línea] Disponible en: https://www.xataka.com/basics/usb-type-c-que-exactamente-que-se-diferencia-resto Acedido: 17 Mar. 2023

[50] R. Marta,,(22 Nov. 2017) Blog de Telecocable: actualidad en cables y conexión eléctrica [En línea] Disponible en: https://www.telecocable.com/blog/tipos-conectores-rj45/1467

[51] L. Pablo,,(04 Abr. 2020) ¿Wifi que es y para qué sirve? [En línea] Disponible en: https://www.geeknetic.es/WiFi/que-es-y-para-que-sirve Accedido: 17 Mar. 2023

[52] H. Know, (01 12 2022) ¿Qué es Bluetooth? Toda la información sobre el estándar inalambrico [En línea] Disponible en: https://www.ionos.mx/digitalguide/servidores/know-how/que-es-bluetooth/ Accedido: 17 Mar. 2023

[53] SAN JUAN, Victor. Ventajas de los sistemas web. [en línea]. AEURUS, abril. 2016 [citado el 4 de diciembre de 2021] Disponible en: <URL: http://www.aeurus.cl/blog/ventajas-de-los-sistemas-web >.

[54] OPTICAL NETWORKS. ¿Qué son los vectores de ataque en ciberseguridad? [en línea]. 1 ed. [Lima, Perú]: ON, dic. 2020 [citado 4 nov 2021]. Disponible en internet: <URL: https://www.optical.pe/blog/vectores-de-ataque-ciberseguridad/>.

[55] GUTIÉRREZ, Camilo. Nuevas variantes de ransomware en evolución constante. [en línea]. Welivesecurity by ESET, julio. 2016 [citado el 24 de noviembre de 2021] Disponible en: <URL: https://www.welivesecurity.com/la-es/2016/07/08/variantes-de-ransomware-evolucion/>.

[56] VODNIZA, Armando. Guía de Investigación Cuantitativa. 1 ed. San Juan de Pasto, Nariño: Cesmag, 2009. 75 p. ISBN: 9789588439129.

[57] VODNIZA, Armando. Guía de Investigación Cuantitativa. 1 ed. San Juan de Pasto, Nariño: Cesmag, 2009. 76 p. ISBN: 9789588439129.

[58] WESTREICHER, Guillermo. Método científico [en línea]. ed. 1 sep. 2020 [citado 4 nov 2021]. Disponibilidad en internet: <URL: https://economipedia.com/definiciones/metodo-cientifico.html>.

[59] VODNIZA, Armando. Guía de Investigación Cuantitativa. 1 ed. San Juan de Pasto, Nariño: Cesmag, 2009. 84 p. ISBN: 9789588439129.

[60] CÁMARA DE COMERCIO. Base General Establecimientos Activos. oct. 2021 [citado nov. 4 2021].

[61] Bedaya, Fernando Produccion y empleo en la pequeña industria en Nariño [en línea]. Revista Tendencias, diciembre. 2021 [citado el 24 de nov. De 2021] Disponible en: <URL:Dialnet-ProduccionYEmpleoEnLaPequenaIndustriaEnNarino-5029679.pdf>.

[62] Machuca, Fernando 8 tecnicas de recolecion de datos: descubre un mundo mas allá de la encuesta [en linea]. Future of people, junio 2022 [citado el 12 de may. De 2023] Disponible en:<https://www.crehana.com/blog/transformacion-digital/tecnicas-recoleccion-de-datos/>

[63] THOMSON, Ivan. Definición de Encuesta [en línea]. 1 ed. PromoNegocios.net jul. 2016 [citado 4 nov. 2021]. Disponible en internet: <URL: https://www.promonegocios.net/mercadotecnia/encuestas-definicion.html>.

[64] ROMO, Nilson. La importancia de hacen una encuesta. [en línea]. Economía I El Heraldo, enero. 2016 [citado el 4 de diciembre de 2021] Disponible en: <URL: https://www.elheraldo.co/economia/la-importancia-de-hacer-una-encuesta-236595>.

[65] Porto, Julián. Definición ransomware. [en línea]. Definición. DE, 2020 [citado el 9 de agosto 2022] Disponible en: <URL: https://definicion.de/ransomware/>

[66] Ministerio Publico Fiscal. (Junio del 2014) MANUAL DE PROCEDIMIENTO PARA LA PRESERVACIÓN DEL LUGAR DEL HECHO Y LA ESCENA DEL CRIMEN. [En línea] Disponible en: https://www.mpf.gob.ar/capacitacion/files/2015/07/Manual-Criminalistica.pdf.

[67] EducacionIT. (12 noviembre 2019) No reinicies tu PC después de un ataque de ransomware, según expertos, Disponible en: https://blog.educacionit.com/2019/11/12/no-reinicies-tu-pc-despues-de-un-ataque-de-ransomware-segun-expertos. Accedido 10 feb. 2023]

[68] Microsoft. (6 enero 2023) Apagar, suspender o hibernar tu PC. [En línea]. Disponible en https://support.microsoft.com/es-es/windows/apagar-suspender-o-hibernar-tu-pc-2941d165-7d0a-a5e8-c5ad-8c972e8e6eff Acedido 11 feb. 2023.

[69] F, Yúbal. (4 noviembre 2019) Qué es el ransomware y cómo te puedes proteger de él. [En línea]. Disponible en https://www.xataka.com/basics/que-ransomware-como-te-puedes-proteger Acedido 11 feb. 2023.

[70] CrowdStrike. Ransomware Detection: Attack Types & Techniques. (30 Enero. 2023). [En línea]. Disponible en: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-detection/ Accedido: 17 Mar. 2023

[71] ID Ransomware. Malware Hunter Team. [En línea]. Disponible en: https://id-ransomware.malwarehunterteam.com/ Accedido: 17 Mar. 2023

[72] Kaspersky. Reconocer el ransomware: en qué se diferencian los troyanos de cifrado. [En línea]. Disponible en: https://www.kaspersky.es/resource-center/threats/ransomware-attacks-and-types Accedido: 17 Mar. 2023

[73] Microsoft. ¿Qué es el ransomware?. [En línea]. Disponible en: https://www.microsoft.com/es-ar/security/business/security-101/what-is-ransomware Accedido: Accedido: 17 Mar. 2023

[74] Hillstone, Marketing. ¿Por qué es importante capacitar al personal de tu empresa en seguridad informática? [en línea] [EEUU] Hillstone NETWORKS, nov. 2022 [citado 11 enero 2023] Disponible en internet: <URL: https://www.hillstonenet.lat/blog/seguridad-de-la-red/importante-capacitar-al-personal-de-tu-empresa-en-seguridad-informatica/#:~:text=Mediante%20una%20capacitación%20integral%20en,de%20la%20empresa%20y%20conocer>

[75] Lean-Management. Metodología Rup: ¿Qué es, ¿cuál es su objetivo y como se utiliza? [en línea]. LM enero 3 2022 [citado 9 de agosto 2022] Disponible en: <URL: https://lean-management.site/rup/>

[76] Santander. Python: que es y porque deberías aprender a utilizarlo. [en línea]. Santander Universidades, abril 2021 [citado 9 de agosto 2022]. Disponible en: <URL: https://www.becas-santander.com/es/blog/python-que-es.html>

[77] Mdn Plus, Framework Web Django (Phyton) [en línea]. Mdn Plus, 2022 [citado 9 de agosto 2022] Disponible en: <URL: https://developer.mozilla.org/es/docs/Learn/Server-side/Django>

[78] Openwebinars.com. Curso Html5 y Css3 [en línea]. Openwebinars.com 2022 [citado 9 de agosto 2022]. Disponible en: <URL: https://openwebinars.net/cursos/html5-css3/>

[79] MDN Plus. JavaScript [en línea]. MDN Plus 2022 [citado 9 de agosto 2022]. Disponible en: <URL: https://developer.mozilla.org/en-US/docs/Web/JavaScript >

ANEXOS

Anexo 1. Encuesta

PROYECTO TESIS
DESARROLLO DE UNA METODOLOGÍA COMO RESPUESTAS A INCIDENTES DE INFECCIÓN POR RANSOMWARE
SAN JUAN DE PASTO 2021.
UNIVERSIDAD CESMAG
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS

Cordial saludo el siguiente cuestionario está dirigido a empresas que manejen softwares actualizados a las necesidades de hoy.

Objetivo: Recolectar información relevante a incidentes provocados por ciberataques, puntualmente ransomware. Este cuestionario está dirigido a empresas de la Ciudad de Pasto, con el fin de capacitarlas en lo relacionado al tema de seguridad informática.

Indicaciones: Lea cuidadosamente las preguntas, marque con una x la o las respuestas que considere correctas en los casos que se requiera o escriba la respuesta solicitada.

Datos personales

Nombres: _____

Apellidos: _____

Acepta los términos y condiciones de uso de sus datos personales a la universidad CESMAG bajo su política de tratamiento de información.

1. ¿Cuántos puntos de cómputo maneja su organización?
   5) 1 a 10
   6) 10 a 20
   7) Más de 20

2. ¿Qué sistema operativo usan en la empresa donde trabaja?

   8) Windows
   9) Mac - Apple
   10) Linux

3. ¿Qué concepto de seguridad informática tiene la empresa a la que está vinculado?
   - Práctica de prevenir los ataques maliciosos.
   - Parte de la ingeniería que busca proteger información personal y empresarial.
   - Uso de herramientas tecnológicas para bloquear todo peligro que venga de internet.
   - Aprender a manejar programas complejos para eliminar virus.
   - Protección de la información y procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos.

4. ¿Qué concepto maneja su organización sobre ingeniería social?

- Es la práctica de obtener información confidencial a través de la manipulación de usuarios.
- Manipular a personas mediante el uso de magia.
- Hacer estudios sociales y culturales a ingenieros.
- Hacer estudios ingenieriles a problemas sociales no aceptados.

5. ¿Qué concepto maneja su organización acerca del Phishing?

- Es la práctica de obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas.
- Pescar en la red.
- Trampas en internet para pescar personas.
- Navegar en la red pescando.

6. ¿Su organización conoce el concepto de DUMPSTER DIVING o Buceo en la Basura?

- Realizar un estudio profundo de una organización literalmente en su
- basura para recopilar información muy relevante.
- Recoger la basura todos los días a una hora predeterminada.
- Buscar en la basura cosas irrelevantes.
- Sumergirse en la basura de los demás.
-

7. ¿Dentro de su empresa se manejan conexiones mediante VPN?

- Si
- No

8. ¿Dentro de su empresa qué concepto se maneja sobre el término de VPN?

- Es una red que garantizará que no te puedan rastrear.
- Cifrado de extremo a extremo.
- Conectarse a internet de forma privada.
- "Virtual Prívate Network" (Red privada virtual) Permite crear conexiones protegidas en redes públicas.

9. ¿La presentación anterior realizada a su organización dejó claro que es un ciberataque conocido como ransomware?

- Si
- No

10. ¿Ha conocido empresas involucradas en casos de ciberataques?

- Si
- No

11. ¿Alguna vez su empresa se ha visto afectada por una infección de tipo ransomware?

- Si
- No

12. ¿Dentro de su organización ha sufrido intentos de fraude que puedan causar fugas de información ya sea vía mail o celular?

- Si

- No

13. Si la respuesta anterior fue positiva, describa mediante qué medios ha presenciado intentos de fraude dentro de su organización. Esta pregunta es de selección múltiple.

- Whatsapp
- Gmail
- Mensajes de texto
- Llamadas de voz
- Facebook
- Instagram
- Tik tok

14. ¿Cuándo estás navegando en redes sociales, revisando emails o leyendo mensajes de texto organizacionales, reconoce cuáles podrían ser intentos de fraude?

- Si
- No

15. ¿Si la anterior respuesta fue positiva, con qué frecuencia se te presentan posibles intentos de fraude o phishing?

	Nunca	Poco	Medio	Alto	Bastante
Facebook	○	○	○	○	○
WhatsApp	○	○	○	○	○
Instagram	○	○	○	○	○
Tik Tok	○	○	○	○	○
Telegram	○	○	○	○	○
LinkedIn	○	○	○	○	○
Snapchat	○	○	○	○	○
kwai	○	○	○	○	○

16. ¿Posterior a la capacitación dada, cuál es el concepto sobre RANSOMWARE que le quedó a su organización?

- Virus informático que infecta un sistema mediante el uso de ingeniería social para solicitar un rescate para resolver el problema.
- Virus de la nube
- Troyano complejo que es programado para cifrar datos dentro de un computador de forma automática.
- Complejo programa que daña todo lo que posea un sistema.

17. ¿Posterior a la capacitación dada, su organización sabría qué hacer en caso de infección por RANSOMWARE?

- Si
- No

18. ¿Cuáles de los siguientes antivirus tiene instalado en el sistema de su organización?

- Avast
- McAfee
- Norton 360
- BitDefender
- Kaspersky
- Panda
- Avira
- No tengo antivirus

19. ¿Cuáles de este firewall está instalado en el sistema de su organización?

- SolarWinds Network Firewall Security Management.
- ZoneAlarm
- Comodo Firewall.
- TinyWall
- Netdefender
- Glasswire
- PeerBlock
- Firewall AVS.
- No entiendo que es un Firewall
- Otra:

Anexo 2 Encuesta validez metodología

PROYECTO TESIS
DESARROLLO DE UNA METODOLOGÍA COMO RESPUESTAS A INCIDENTES DE INFECCIÓN POR RANSOMWARE
SAN JUAN DE PASTO 2023.
UNIVERSIDAD CESMAG
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS

Cordial saludo el siguiente cuestionario está dirigido a empresas que manejen softwares actualizados a las necesidades de hoy.

Objetivo: Validar la implementación de la metodología creada en el sitio web.

Indicaciones: Lea cuidadosamente las preguntas, marque con una x la o las respuestas que considere correctas en los casos que se requiera o escriba la respuesta solicitada.

Datos personales

Nombres: _____

Apellidos: _____

Acepta los términos y condiciones de uso de sus datos personales a la universidad CESMAG bajo su política de tratamiento de información.

1. ¿Siendo el paso 1 cerrar la escena de infección, para su organización fue clara la información entregada por la metodología implementada en el sistema web?

    - Si
    - No

2. ¿Siendo el paso 2 no apagar el ordenador afectado, para su organización fue clara la información entregada por la metodología implementada en el sistema web?

    - Si
    - No

3. ¿Siendo el paso 3 desconectar todas las conexiones, para su organización fue clara la información entregada por la metodología implementada en el sistema web?

    - Si
    - No

4. ¿El paso 4 expone como identificar el tipo de ransomware involucrado en su infección, para su organización fue clara la información entregada por la metodología implementada en el sistema web?

    - Si
    - No

5. ¿El paso 5 muestra que el ransomware involucrado es de cifrado, la información entregada fue clara para hacerle frente a la infección?

    - Si
    - No

6. ¿Como usuario al usar el sitio web en general, para usted fue fácil encontrar información relacionada a capacitación y específicamente sobre la metodología de desinfección planteada?

    - Si

- No

7. ¿Como usuario el uso de la metodología planteada dentro del sistema web fue satisfactorio?

   - Si
   - No

.

Anexo 3 Encuesta final

1). Después de utilizar el sitio web y usar la metodología planteada ¿Cuál es su concepto de seguridad informática?

- Práctica de prevenir los ataques maliciosos.
- Parte de la ingeniería que busca proteger información personal y empresarial.
- Uso de herramientas tecnológicas para bloquear todo peligro que venga de internet.
- Aprender a manejar programas complejos para eliminar virus.
- Protección de la información y procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos.

2). Después de utilizar el sitio web y usar la metodología planteada, ¿Cuál es su concepto sobre ingeniería social?

- Hacer estudios ingenieriles a problemas sociales no aceptados.
- Es la práctica de obtener información confidencial a través de la manipulación de usuarios.
- Manipular a personas mediante el uso de magia.
- Hacer estudios sociales y culturales a ingenieros.

3). Después de utilizar el sitio web y usar la metodología planteada, ¿quedo claro que es un ciberataque conocido como ransomware?

- Si
- No

4). Después de usar el sitio web ¿Le quedo claro como infecta un ransomware un sistema operativo?

- Si
- No

5). ¿El uso y el paso a paso de la metodología contra ransomware fue claro y beneficioso para su organización?

- Si
- No

6). ¿La metodología plateada enseña de forma clara como hacerle frente a un ataque ransomware?

- Si
- No

7). El módulo herramientas creado en el sitio web, ¿fue útil y fácil de manejar para hacer frente a un caso específico de ataque ransomware?

- Si
- No

8). ¿El módulo de capacitación cree que proporciona la información adecuada para explicar los conceptos de seguridad informática?

Si
No

Anexo 4 Encuesta de satisfacción

1). Navegabilidad

- Muy sencilla
- Relativamente sencilla
- Normal
- Algo compleja
- Muy compleja

2). Contenidos

- Claros
- Comprensibles
- Incomprensibles
- Confusos

3). Variedad de contenido

- Muy adecuado
- Adecuado
- Medianamente adecuado
- Inadecuado
- Muy inadecuado

4). Descarga contenido

- Muy rápida
- Rápida
- Normal

- Lenta
- Muy lenta

5). Información Comprensible

- Totalmente comprensible
- Comprensible
- Relativamente compresible
- Poco comprensible
- Incomprensible

6). Diseño

- Muy adecuado
- Adecuado
- Medianamente adecuado
- Inadecuado
- Muy inadecuado

7). Disponibilidad

- Muy disponible
- Disponible
- Poco disponible
- Nada disponible

Anexo 5 Manual de usuario

MANUAL DE USUARIO METODOLOGÍA RANSOMWARE

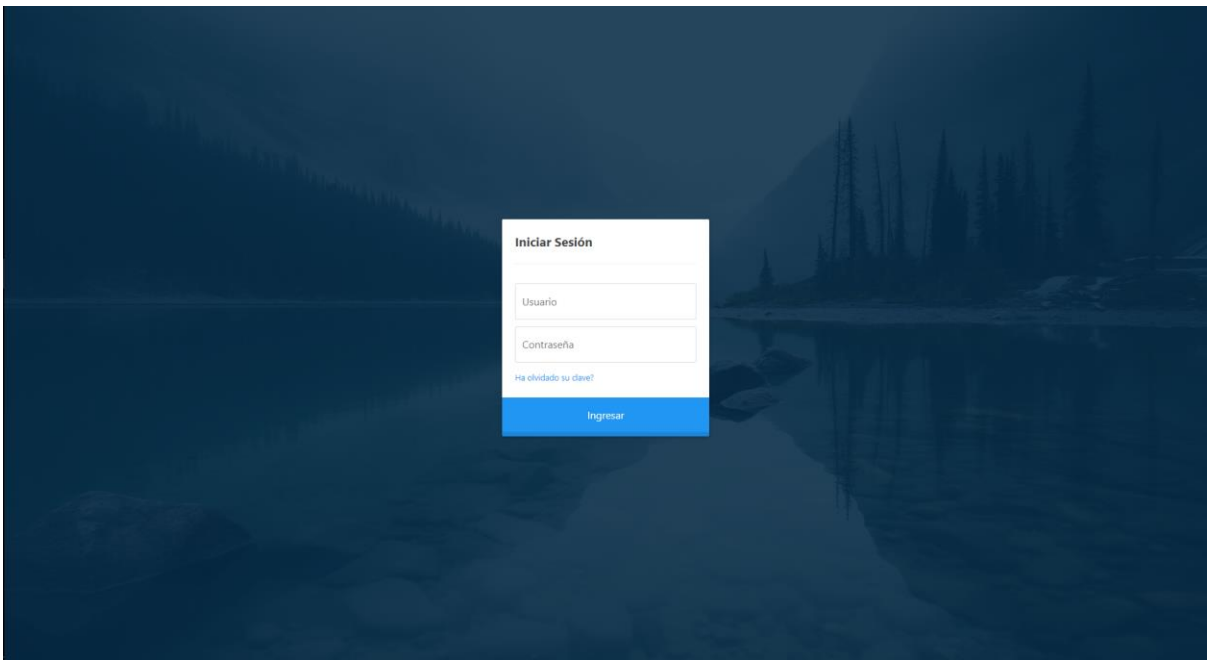
AUTORES:

Juan David Rojas

Freyder Alejandro Urbano

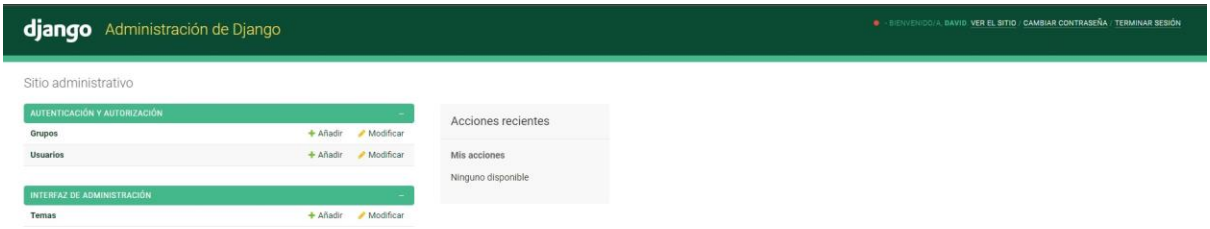
Inicio de Sesión

El inicio de sesión es una parte fundamental para acceder al sitio web y en la figura se muestra la interfaz que te permitirá iniciar sesión. En esta sección, deberás ingresar tu nombre de usuario y contraseña correspondiente para acceder a las funcionalidades del sitio. Es importante asegurarse de que tanto el nombre de usuario como la contraseña sean ingresados correctamente para evitar problemas de acceso. Además, se recomienda no compartir tus credenciales de inicio de sesión con terceros para garantizar la seguridad de tu cuenta. Una vez ingresados los datos correctamente, podrás acceder a todas las características del sitio web.

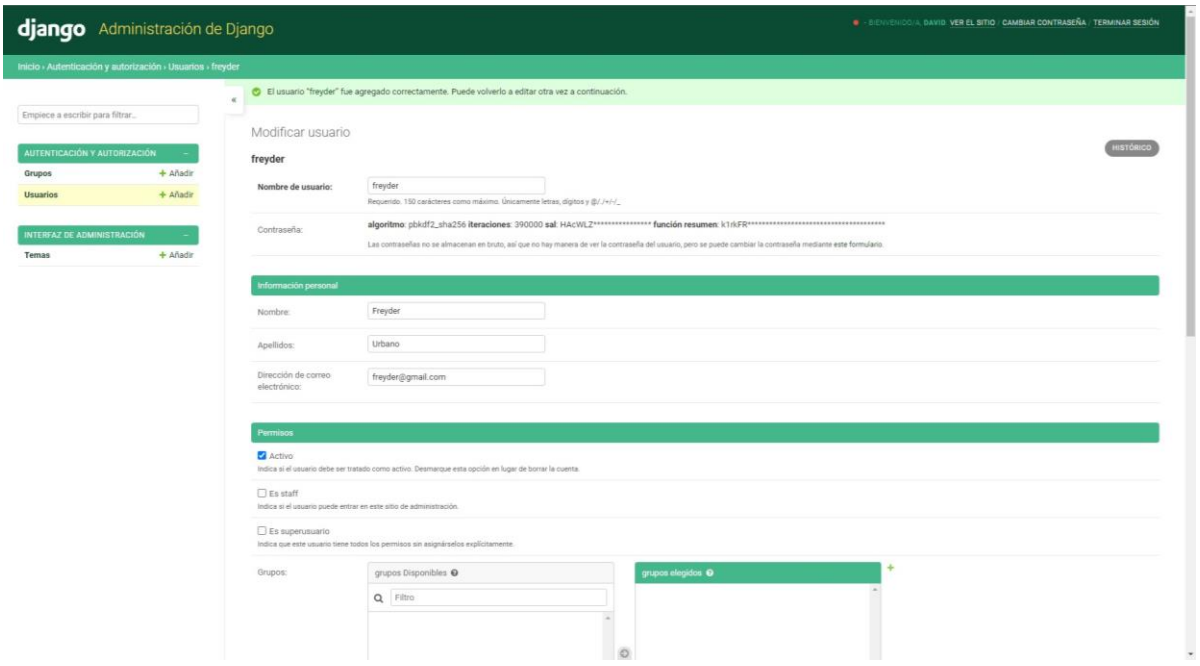


Interfaz de Administrador

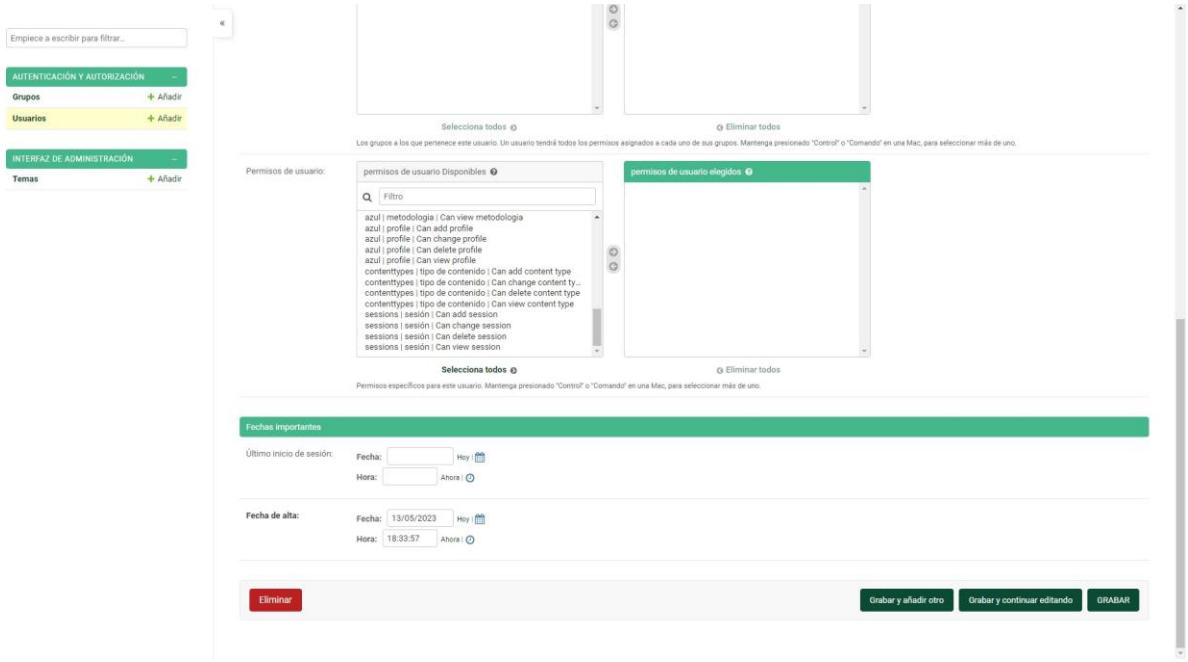
En la interfaz de administrador en la figura este puede crear y eliminar cuentas de usuario, modificar la información de los mismos y asignarles diferentes roles y permisos dentro del sitio. También puede generar informes y estadísticas sobre el uso del sistema y detectar posibles vulnerabilidades en la seguridad. Gracias al administrador de usuarios, se puede mantener un control total sobre el acceso al sitio web y garantizar la privacidad y seguridad de la información.



En la figura se visualiza la interfaz para crear un nuevo usuario en el sitio web, es necesario contar con permisos de administrador. Una vez dentro de la sección de administración de usuarios, se debe seleccionar la opción "Crear nuevo usuario". En la ventana que aparece, se debe ingresar la información del nuevo usuario, como su nombre, correo electrónico y contraseña. Es importante asegurarse de que la contraseña sea segura y cumpla con los requisitos de seguridad establecidos en la página web.

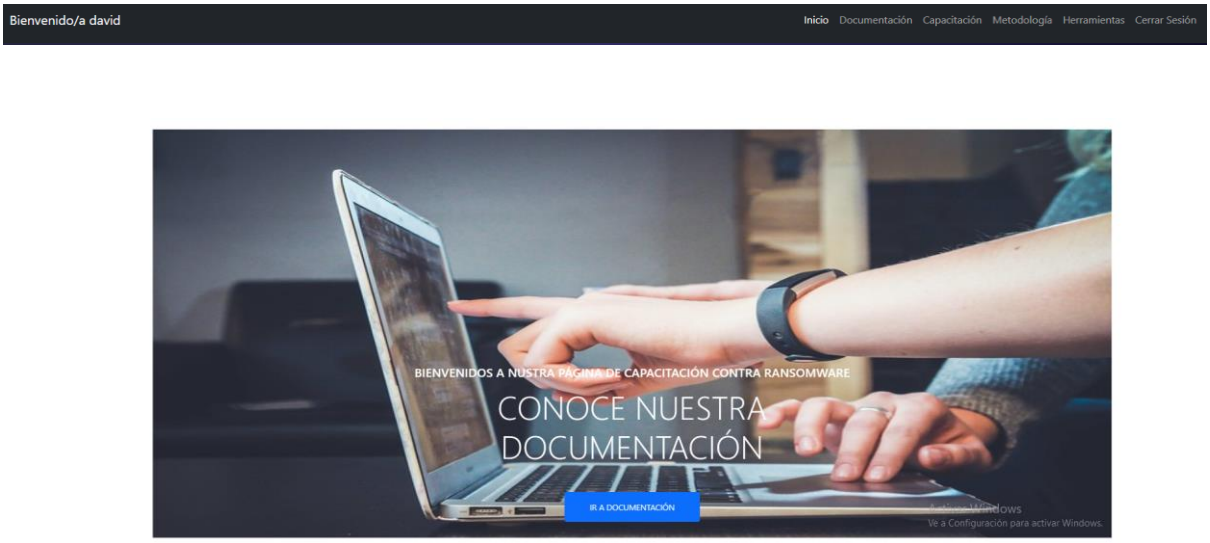


Eliminar usuarios es una tarea importante que solo puede ser realizada por el administrador del sitio web. Para eliminar un usuario existente en la figura el administrador debe seleccionar el usuario que quiere que ya no esté en el sistema web y pulsar en el botón de eliminar.



Página de presentación inicio

La barra de navegación ofrece todas las opciones del sistema tal como se visualiza en la figura se pulsa click derecho en inicio, documentación, metodología, herramientas y cerrar sesión para seguir interactuando con el sistema

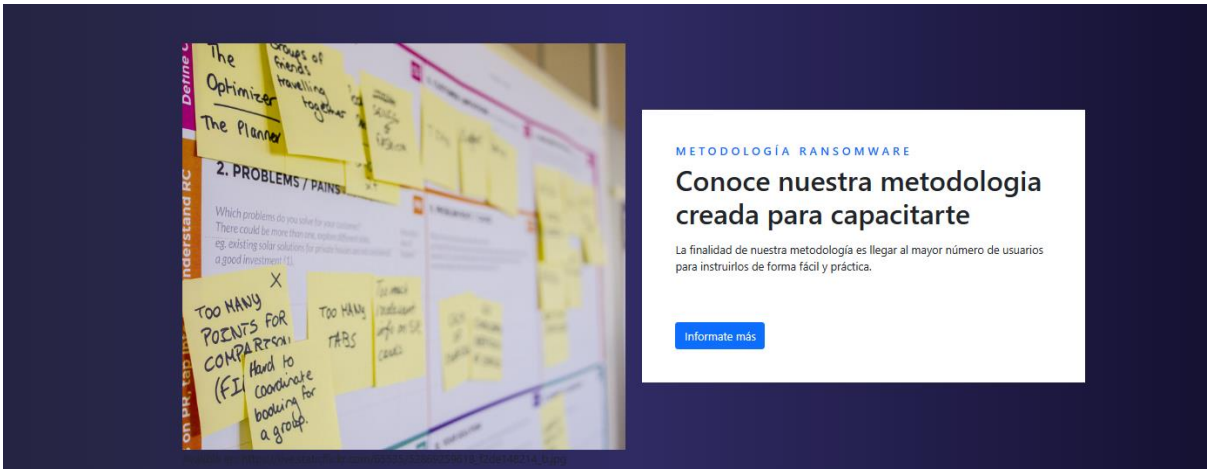


La figura presenta el encabezado inicial de la página de inicio del sitio web. El cual redirige hacia la documentación de la metodología, haciendo click en el botón IR A DOCUMENTACIÓN el sitio te lleva al apartado DOCUMENTACIÓN.

Fig. Barra de Módulo capacitación en la página inicio

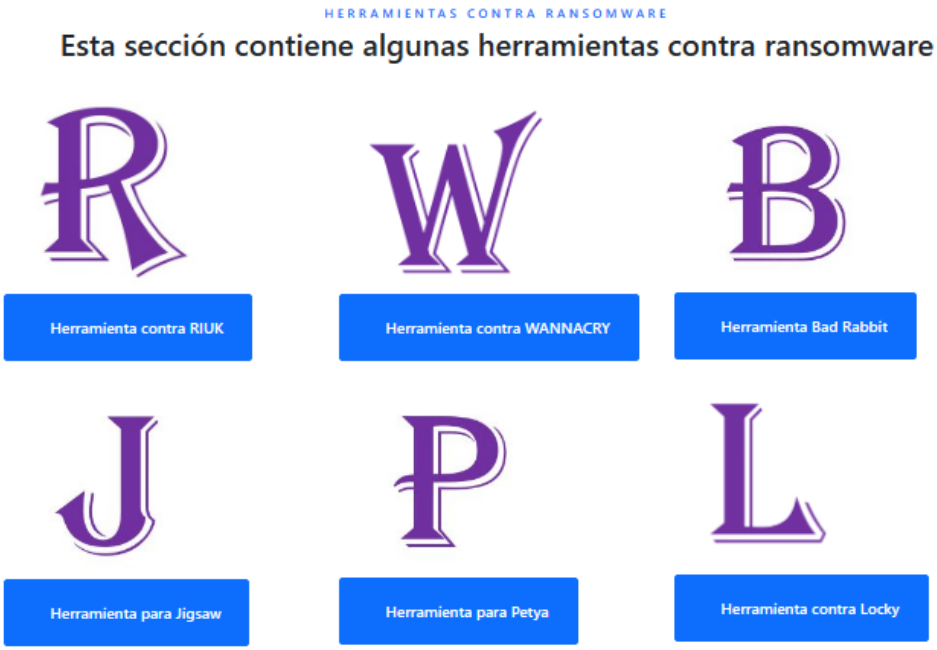
La figura expone la barra de navegación hacia temas directos relacionados a capacitación. Haciendo click en los botones de IR el sitio te dirigirá directamente hacia los temas expuestos en la barra de navegación.

Fig. Barra navegación metodología



La figura muestra el banner de navegación hacia la metodología interactiva creada dentro del sitio web. Haciendo click en el botón INFÓRMATE MAS, el sitio te redirigirá hacia el módulo metodología.

Fig. Barra Herramientas contra ransomware



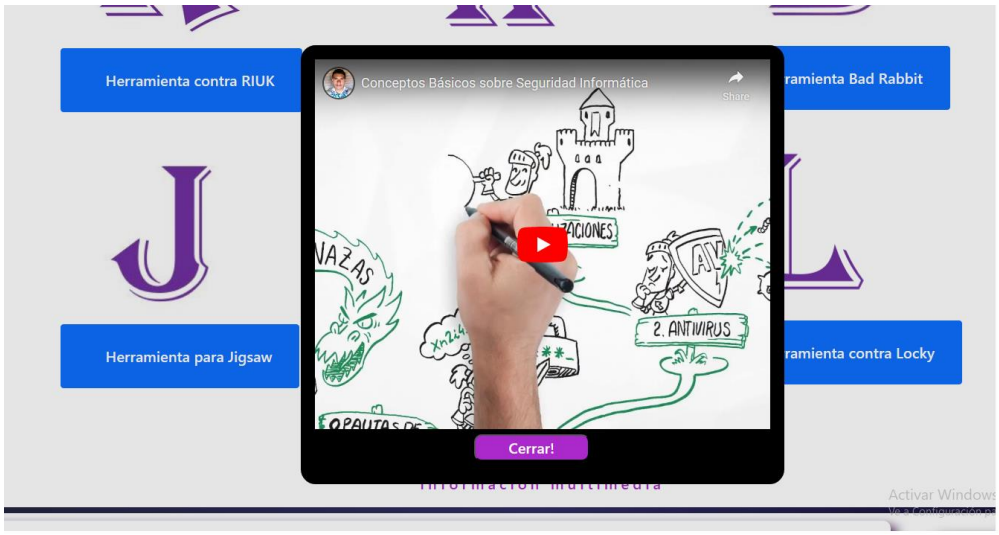
La figura expone el banner de navegación de las herramientas contra ransomware más conocidas. Haciendo click en el botón de su preferencia usted será redirigido hacia el módulo elegido.

Fig. Información multimedia

La figura expone tres vínculos los cuales exponen videos relacionados a los títulos relacionados a Ciberseguridad, ataque DDos y ransomware.

Haciendo click en el botón MOSTRAR del video de ciberseguridad se muestra el video de la siguiente manera:

Fig. Video Ciberseguridad



Haciendo click en el botón MOSTRAR del video Que es un ataque DDos se muestra el video de la siguiente manera:

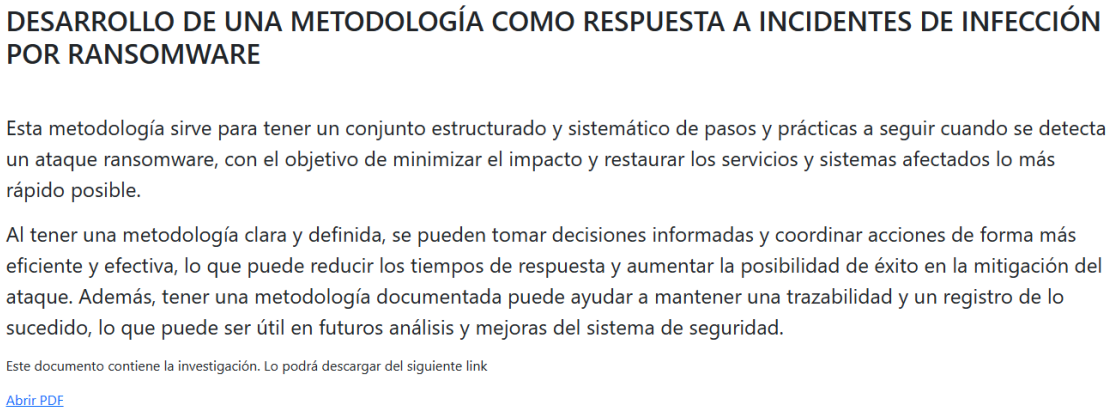
Fig. Video Ataque DDos

Haciendo click en el botón MOSTRAR del video Historia y evolución del ransomware se muestra el video de la siguiente manera:

Fig, Video Historia Ransomware

Módulo documentación

Fig. Modulo Documentación Metodología



La figura expone el módulo de documentación el cual contiene documentos en pdf relacionados con el músculo de la metodología contra ransomware creada.

Modulo Capacitación

El módulo Capacitación contiene información relacionada a ingeniería social para empezar inicia con una explicación general sobre el concepto de ingeniería social.

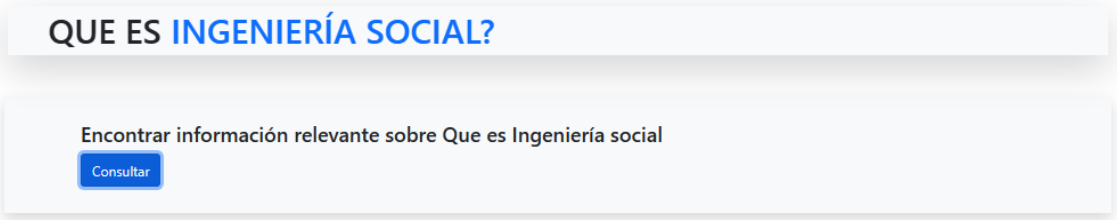
Fig. Ingeniería Social

La figura muestra la introducción y vínculo hacia el apartado de ingeniería social. Haciendo click en el botón infórmate más se ingresa a la siguiente página:

Fig. Página Ingeniería Social

Esta página expone primero el que es ingeniería social de la siguiente manera

Fig. que es ingeniería social



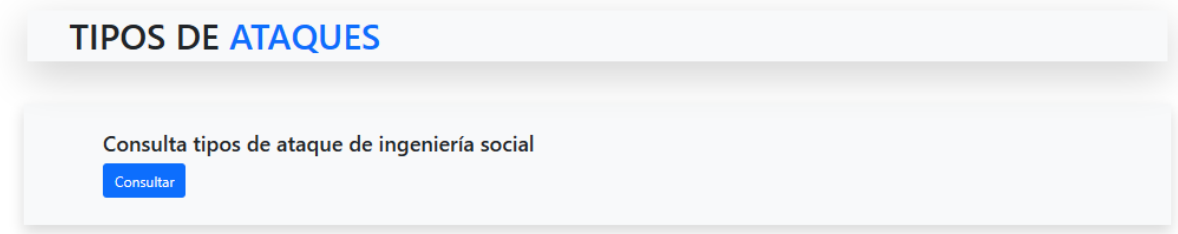
Haciendo click en el botón consultar muestra el concepto general sobre que es la ingeniería social

Fig. Que es ingeniería social

La figura muestra el concepto de ingeniería social.

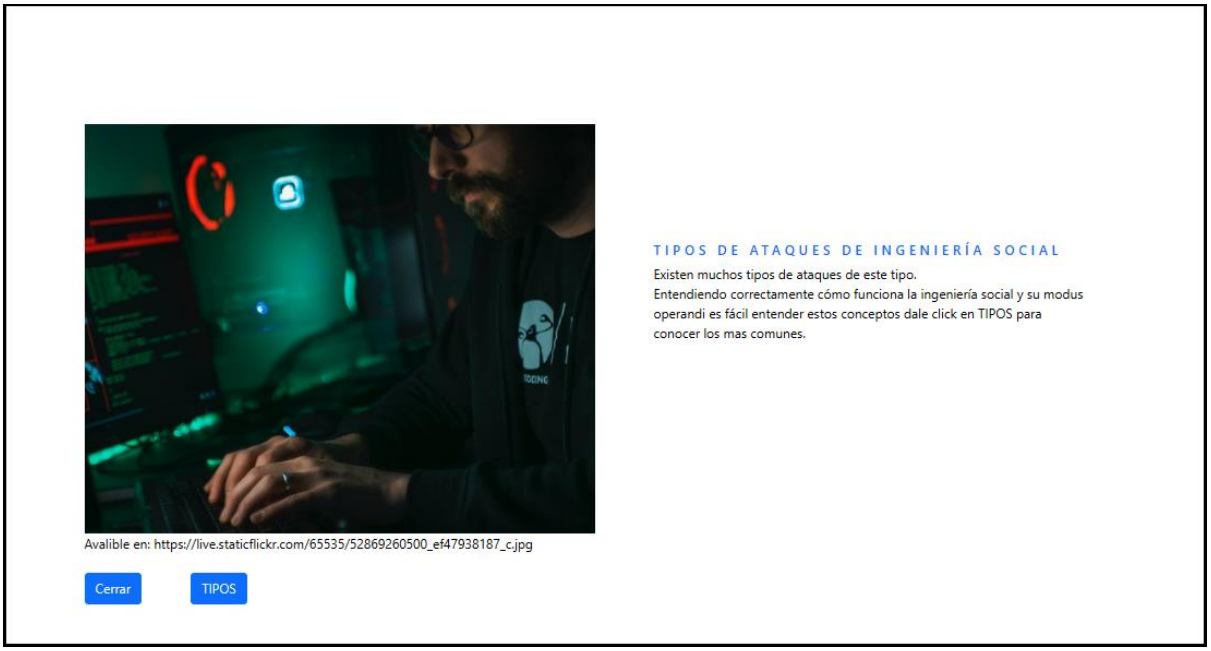
La página continúa con una explicación de cuáles son los tipos de ingeniería social así:

Fig. Tipos de ataques



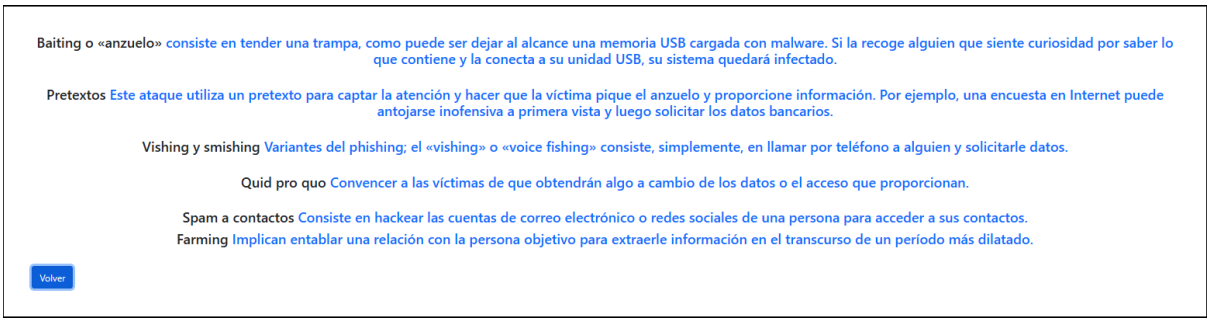
Haciendo click en el botón consultar se visualizan los diferentes tipos de ataques así:

Fig. Ataques ingeniería social



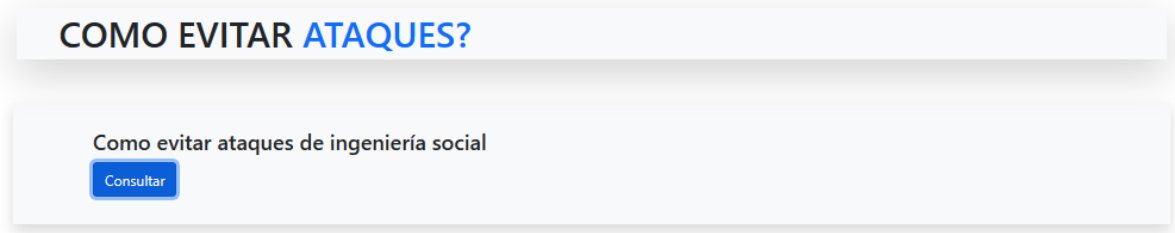
Haciendo click en el botón TIPOS pasamos a visualizar los diferentes tipos de ataques relacionados a ingeniería social.

Fig. Tipos Ataques Ingeniería Social



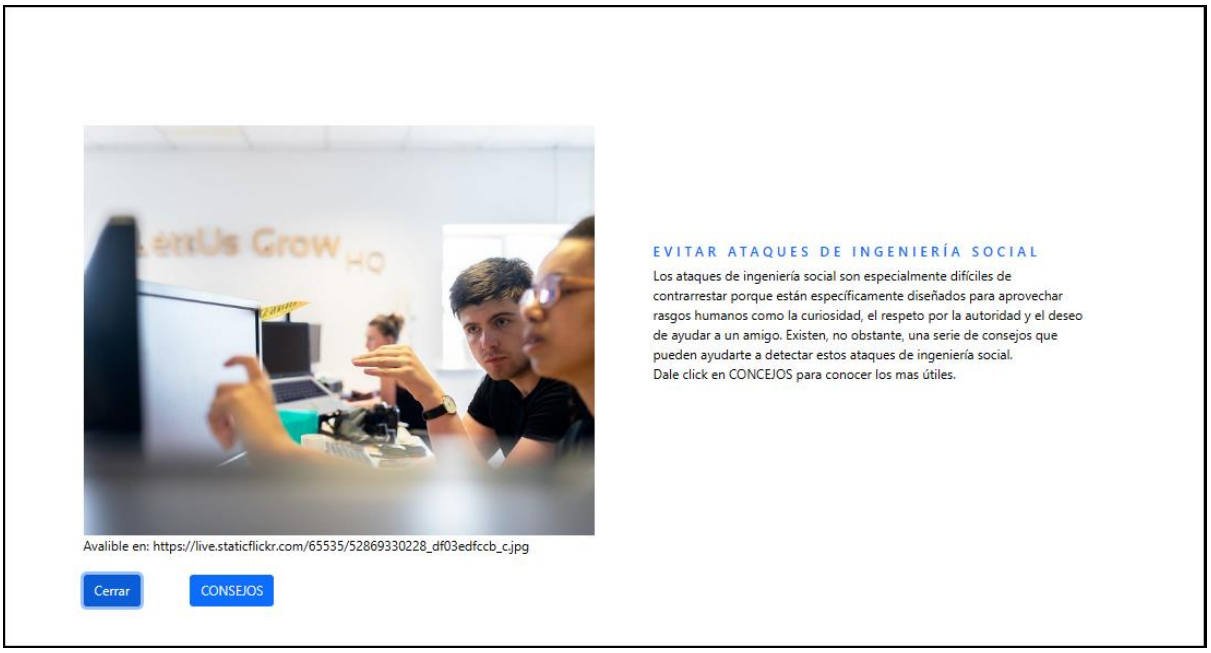
La página continúa con la sección de cómo evitar los ataques de ingeniería social así:

Fig. Cómo evitar Ataques



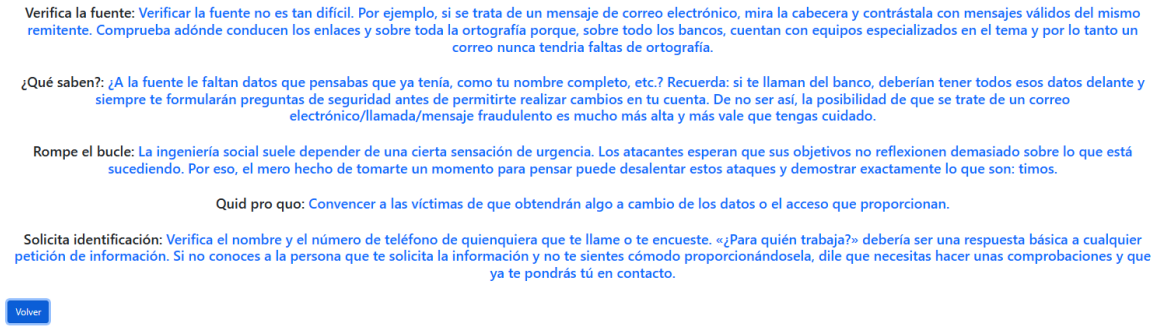
Haciendo click en el botón Consultar se muestra

Fig. Consejos



La figura muestra la introducción hacia los consejos siguientes. Haciendo click en el Botón consejos pasa a la ventana donde se exponen los consejos más oportunos para evitar un ataque por ingeniería social.

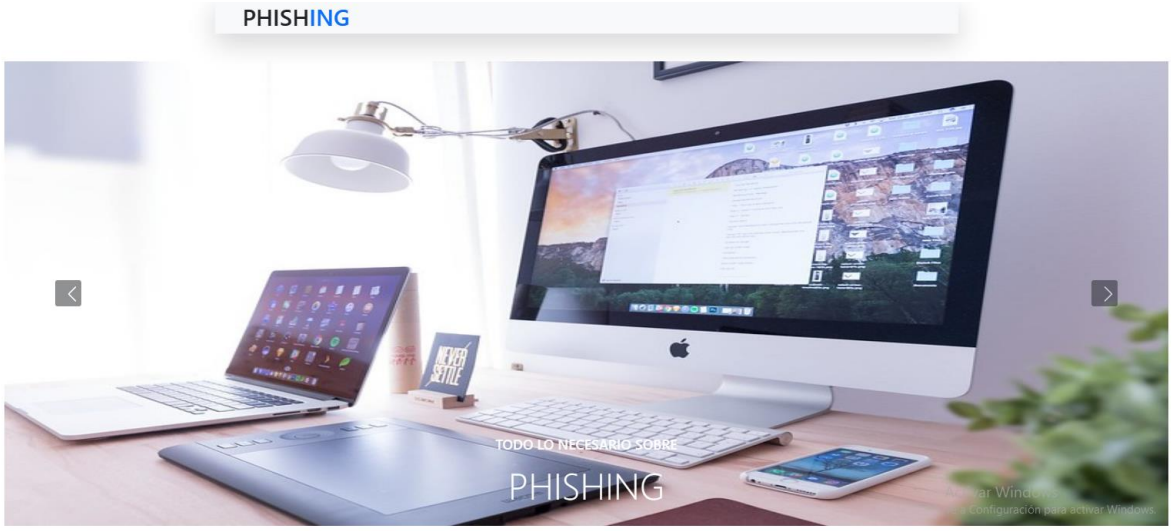
Fig. Consejos Ataques ingeniería social



La figura muestra los consejos más relevantes contra ataques de ingeniería social.

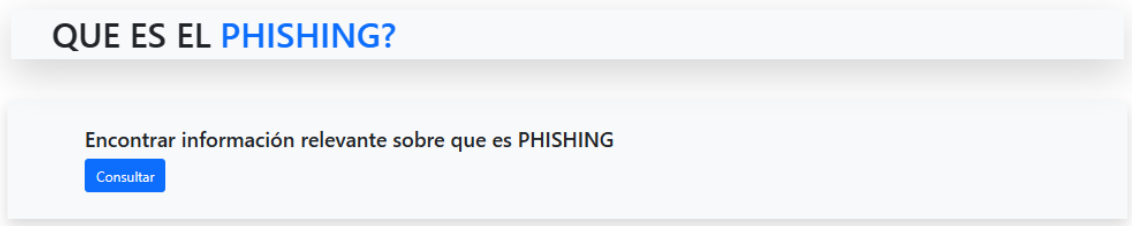
Módulo Phishing

Fig. phishing



La figura muestra la presentación de la página para phishing

Fig. Que es el phishing

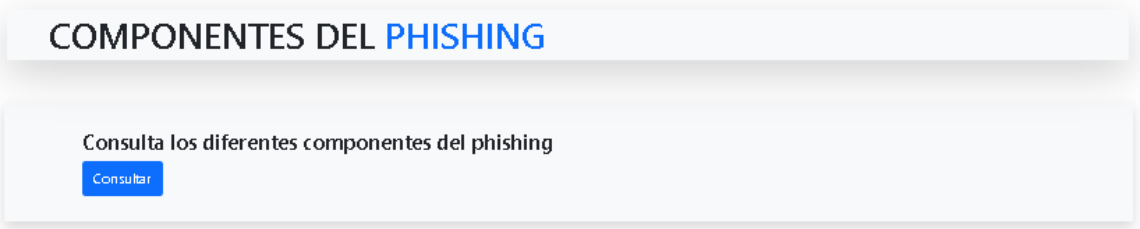


La figura muestra el banner de ingreso a ¿Que es el phishing? haciendo click en el botón Consultar ingresa a la ventana siguiente.

Fig. Phishing

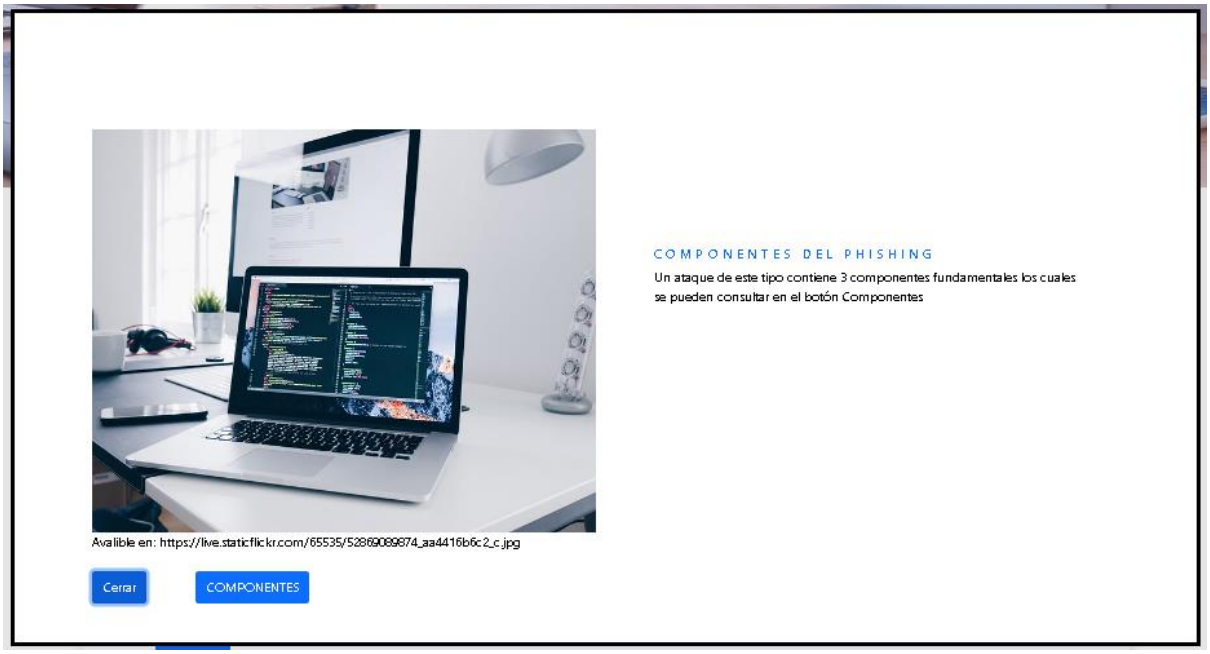
La figura muestra el contenido sobre qué es el phishing donde se encuentra una explicación sobre el tema.

Fig. Componentes del phishing



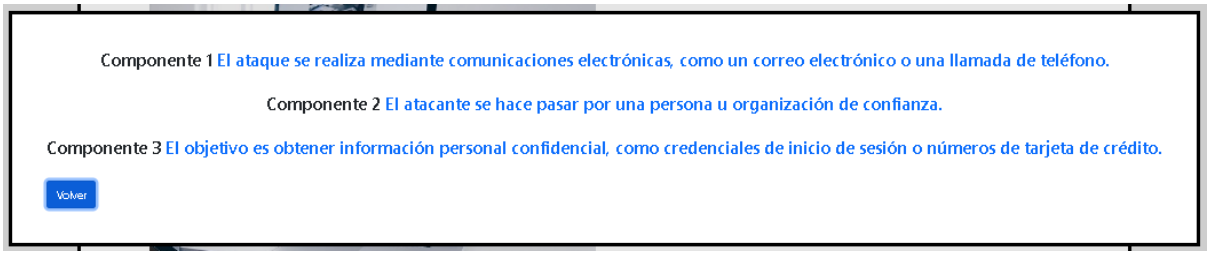
La figura muestra el banner de ingreso a componentes phishing.

Fig. Componentes phishing



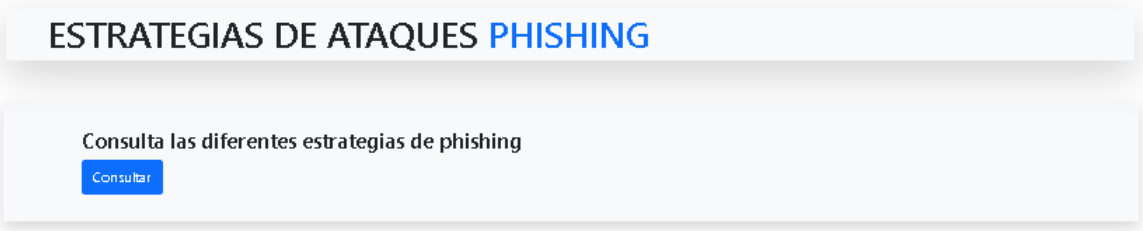
La figura muestra el banner de ingreso a componentes haz click en COMPONENTES.

Fig. Componentes



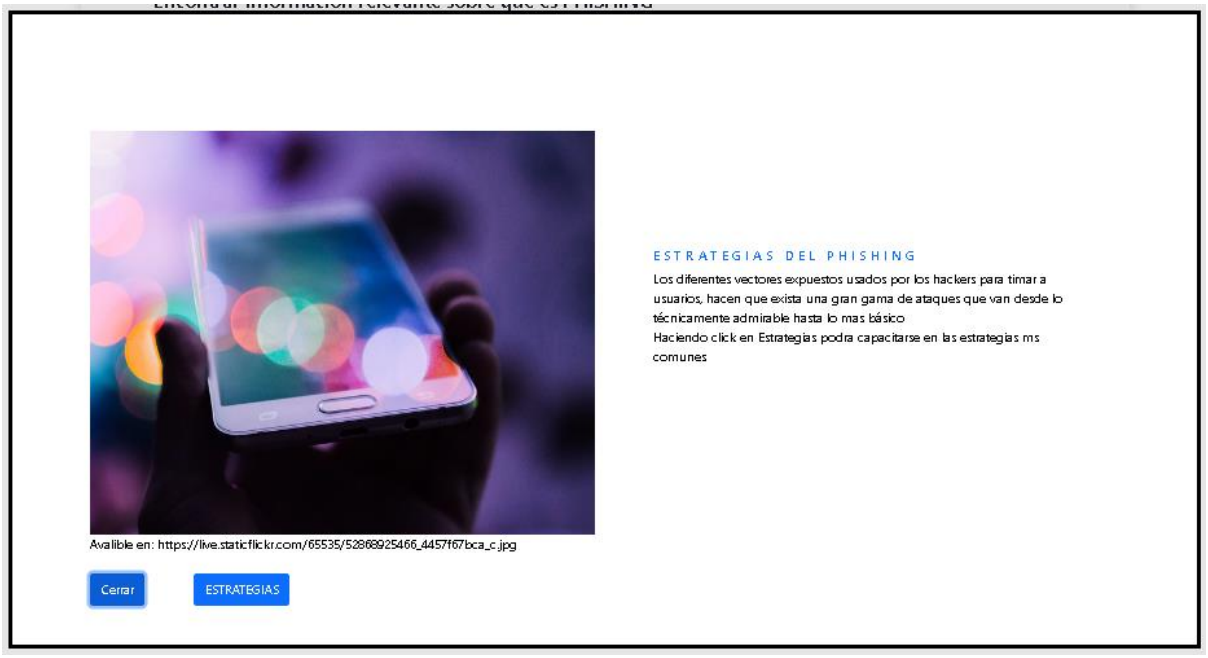
La figura muestra los componentes del phishing.

Fig. Estrategias phishing



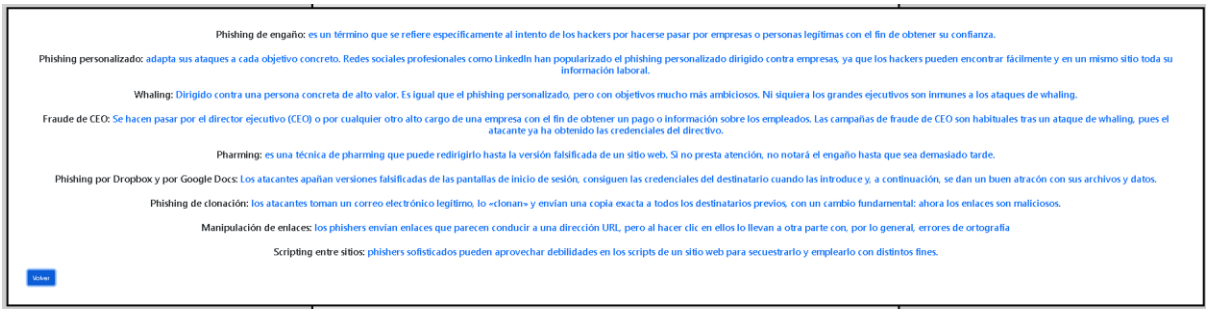
La figura muestra el banner de ingreso a estrategias de ataque de phishing haz click en CONSULTAR para pasar a la ventana siguiente.

Fig. Estrategias phishing



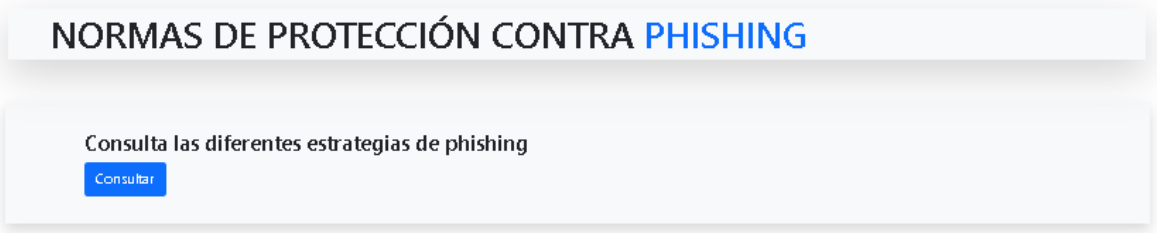
La figura muestra el ingreso a las estrategias del phishing. Haz click en ESTRATEGIAS para acceder a la siguiente ventana.

Fig. Estrategias



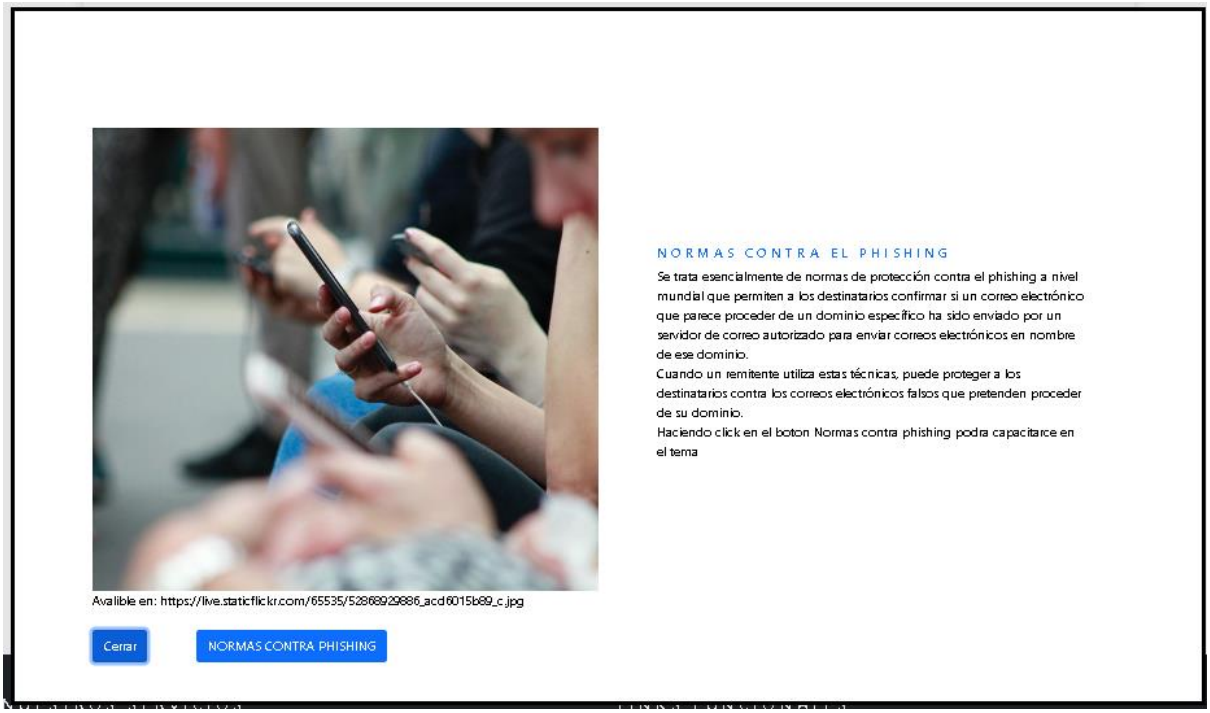
La figura muestra las estrategias usadas por los ciberdelincuentes para vectorizar un phishing.

Fig. Normas de Protección



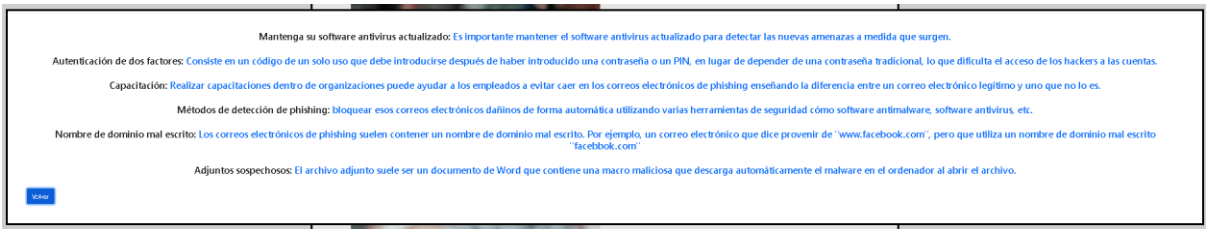
La figura muestra el banner de ingreso a normas de protección contra phishing. Haz click en CONSULTAR para acceder a la siguiente ventana.

Fig. Normas



La figura muestra la introducción a las normas contra el phishing haciendo click en NORMAS CONTRA PHISHING puedes acceder a la siguiente ventana.

Fig. Normas contra phishing

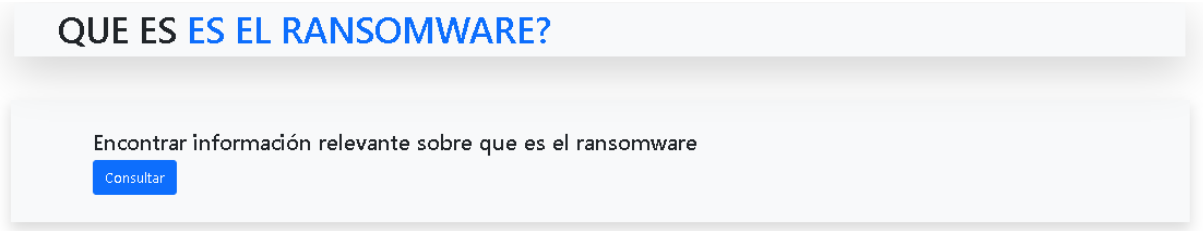


La figura muestra las normas contra el phishing

Fig. Ransomware

La figura muestra el banner inicial de la página de ransomware.

Fig. ¿Qué es el Ransomware?

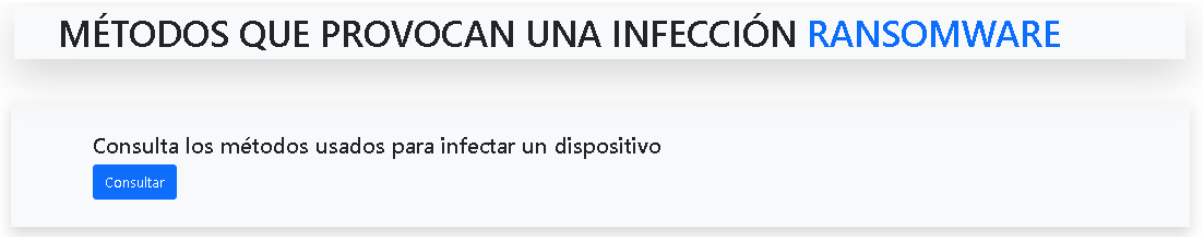


La figura muestra el banner de ingreso a ¿Que es el ransomware?, haciendo click en CONSULTAR accedes a la siguiente ventana.

Fig. ¿Qué es?

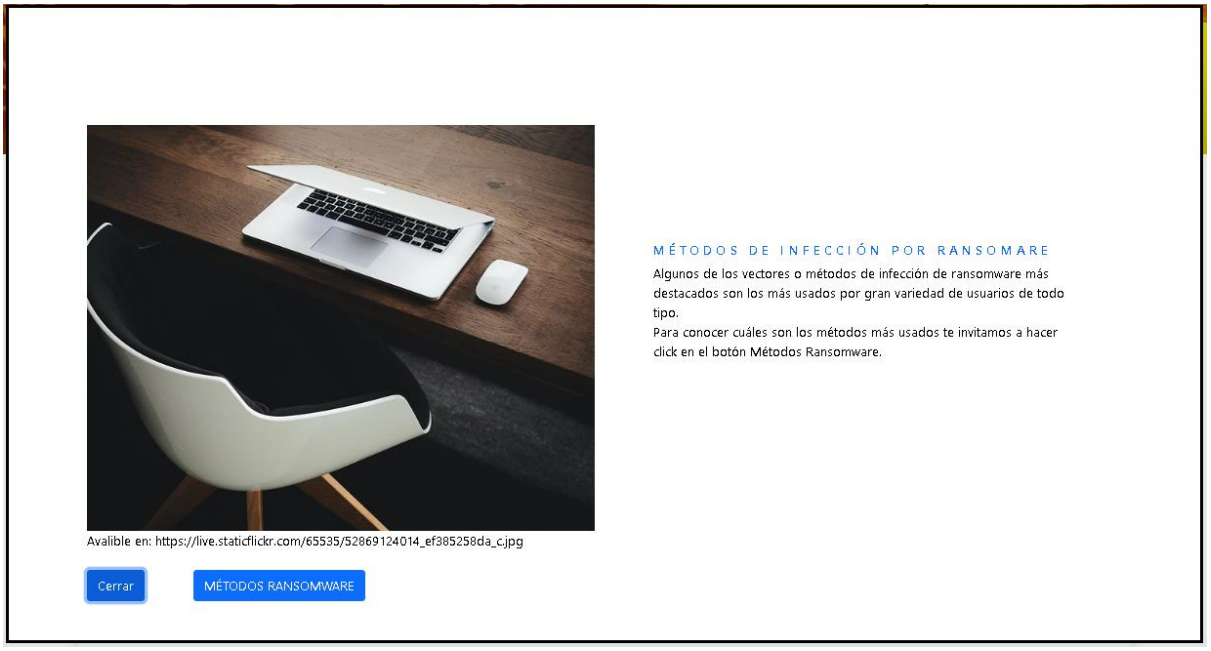
La figura muestra que es un ransomware de forma clara y concisa.

Fig. Métodos que provocan una infección Ransomware



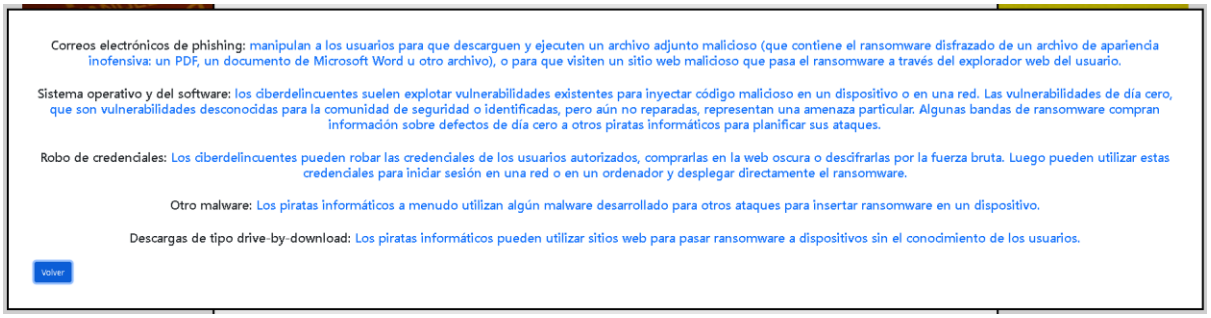
La figura presenta el banner de ingreso a los métodos de provocación de infección de ransomware. Haciendo click en CONSULTAR puedes acceder a la siguiente ventana.

Fig. Métodos



La figura muestra el banner de introducción a hacia los métodos de infección de ransomware. Haciendo click en MÉTODOS RANSOMWARE accedes a la siguiente ventana.

Fig. Métodos Ransomware

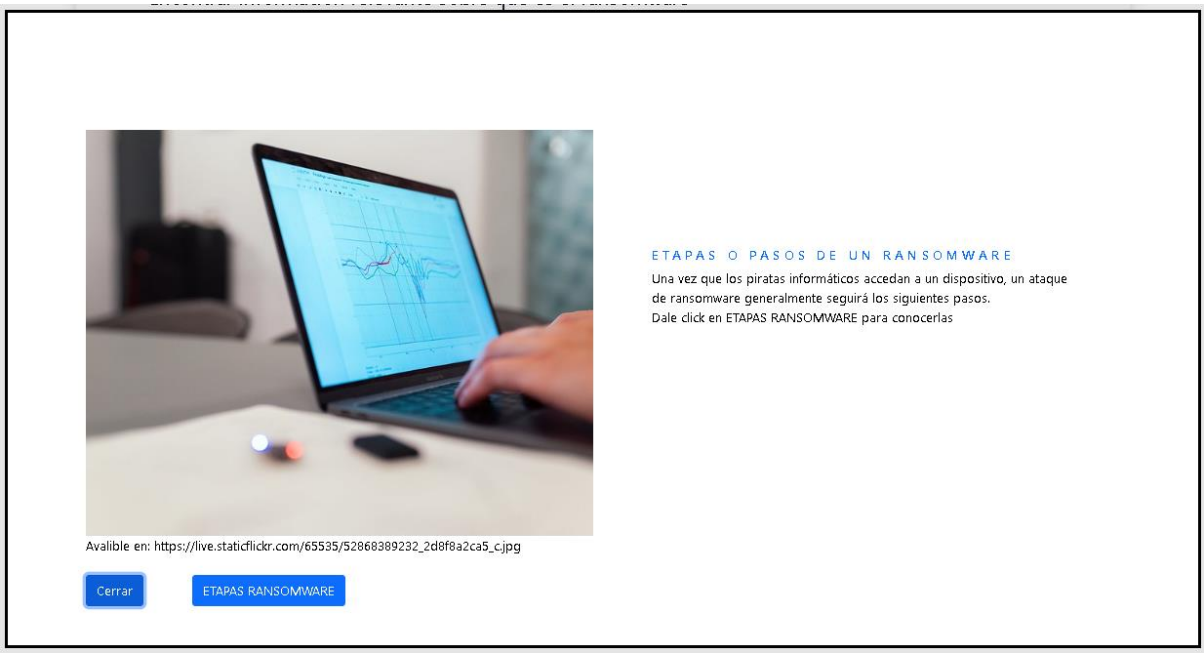


La figura muestra los métodos más usados de infección de ransomware de forma simple y concisa.

Fig. Etapas Ransomware

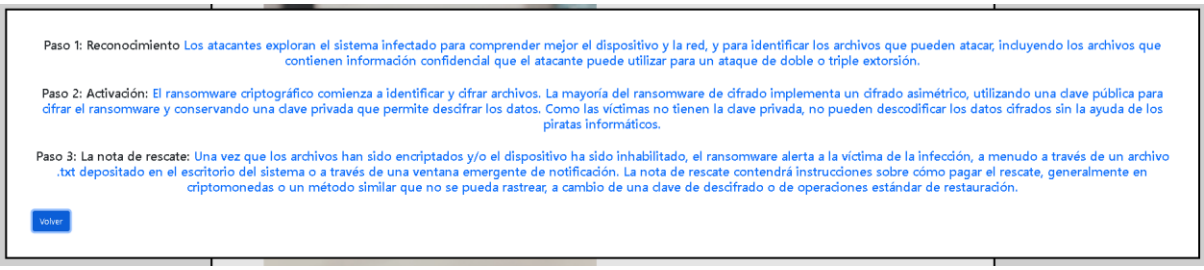
La figura muestra el banner de ingreso a las etapas de un ransomware. Haciendo click en CONSULTAR puedes acceder a la siguiente ventana.

Fig. Etapas



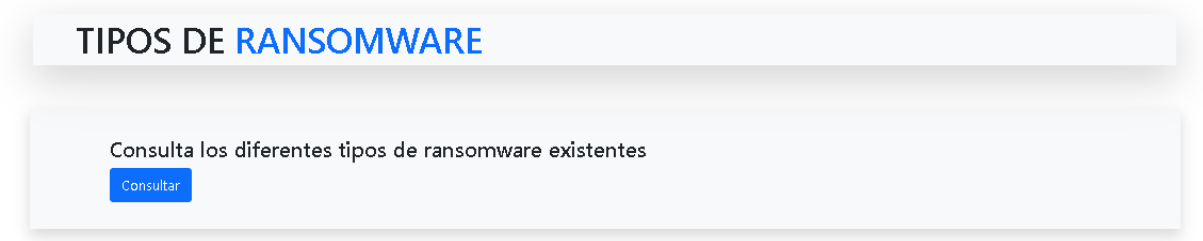
La figura muestra la introducción a las etapas de un ransomware. Haciendo click en ETAPAS RANSOMWARE accedes a la siguiente ventana.

Fig. Etapas Ransomware



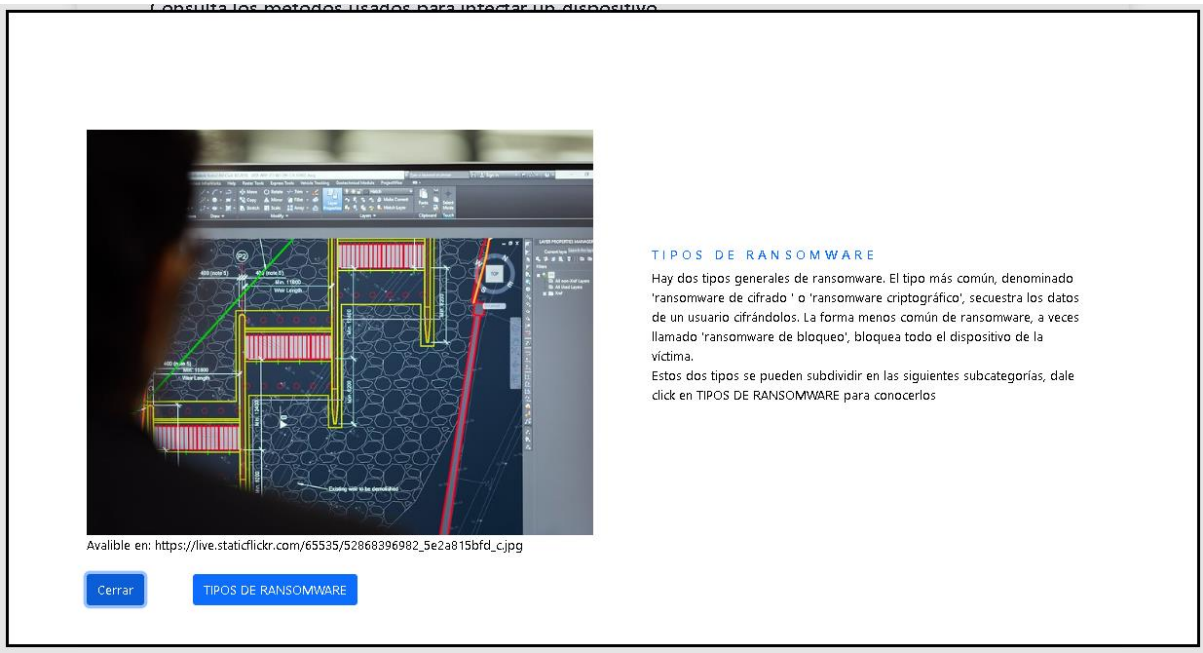
La figura muestra los pasos de un ransomware.

Fig. Tipos de Ransomware



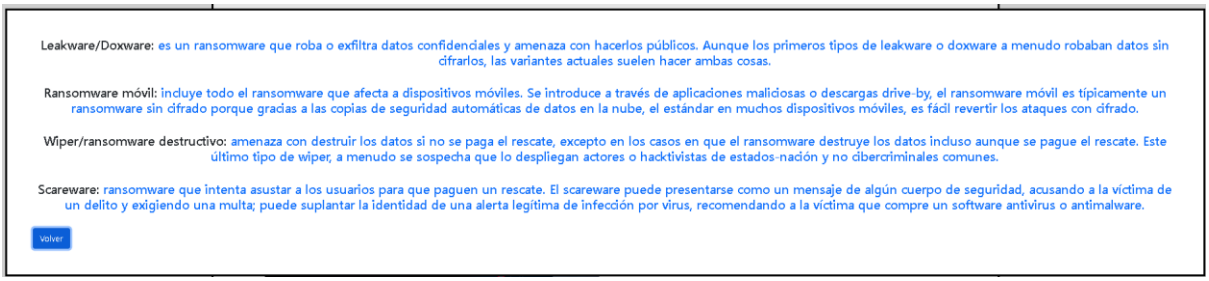
La figura muestra el banner de ingreso a los tipos de ransomware. Haciendo click en CONSULTAR accede a la siguiente ventana.

Fig. Tipos de Ransomware.



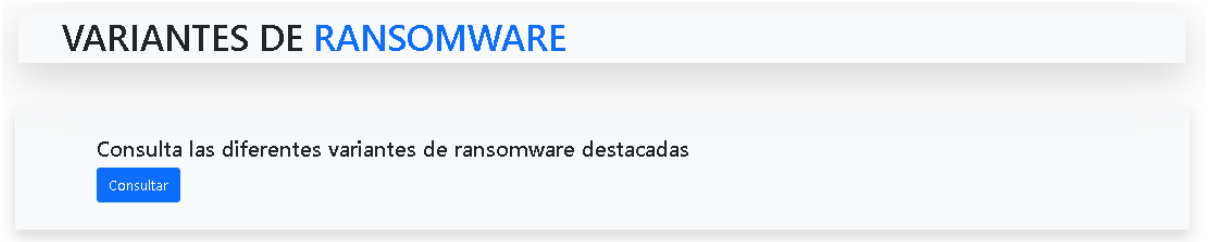
La figura muestra la introducción a los tipos de ransomware. Haciendo clic en TIPOS DE RANSOMWARE para acceder a la siguiente ventana.

Fig. Tipos de Ransomware



La figura muestra los tipos de ransomware más usados.

Fig. Variantes de Ransomware

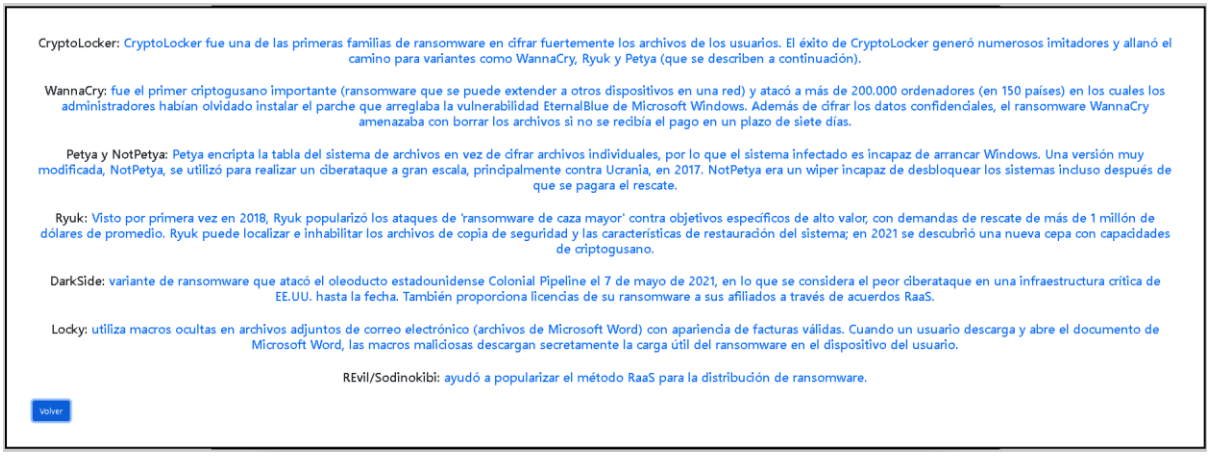


La figura muestra el banner de ingreso de variantes de ransomware. Haciendo click en CONSULTAR accede a la siguiente ventana.

Fig. Variantes de Ransomware

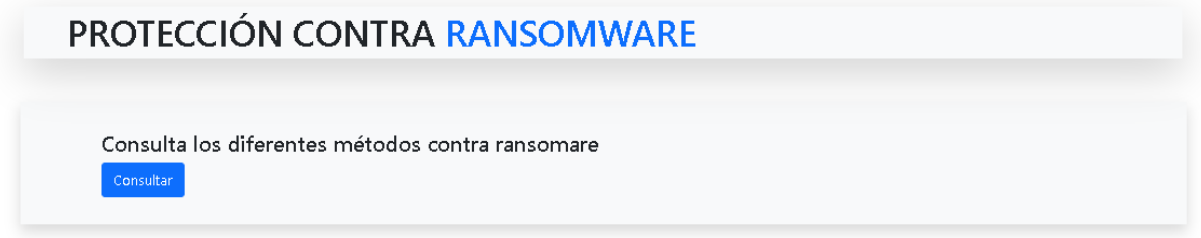
La figura muestra la introducción hacia las variantes de ransomware más destacadas. Haciendo clic en VARIANTES accede a la siguiente ventana.

Fig. Variantes



La figura muestra las variantes ransomware más conocidas.

Fig. Protección contra ransomware



La figura muestra el banner de protección contra ransomware. Haciendo clic en CONSULTAR accede a la siguiente ventana.

Fig. Dumpster diving

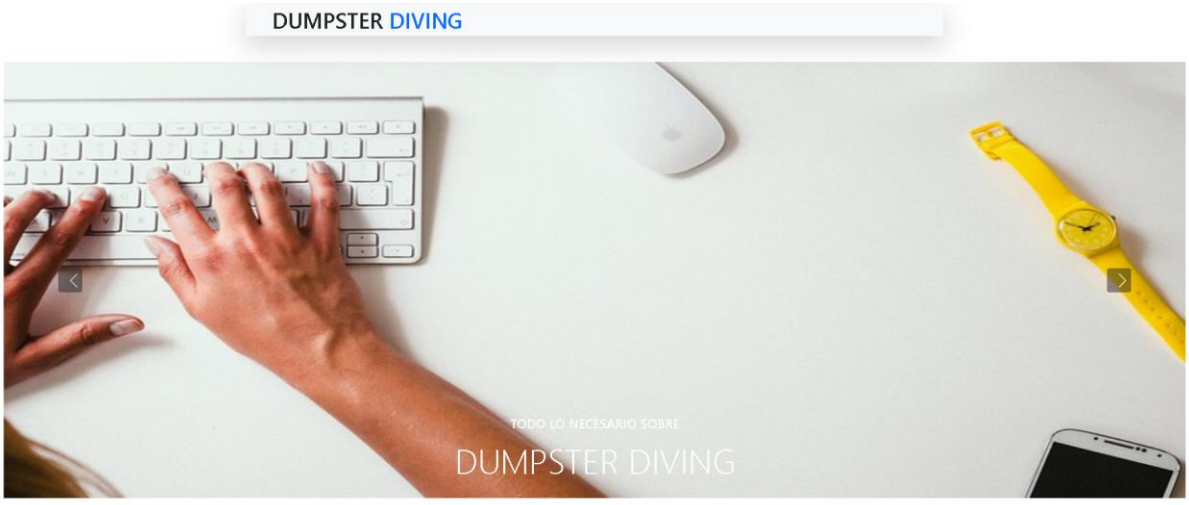
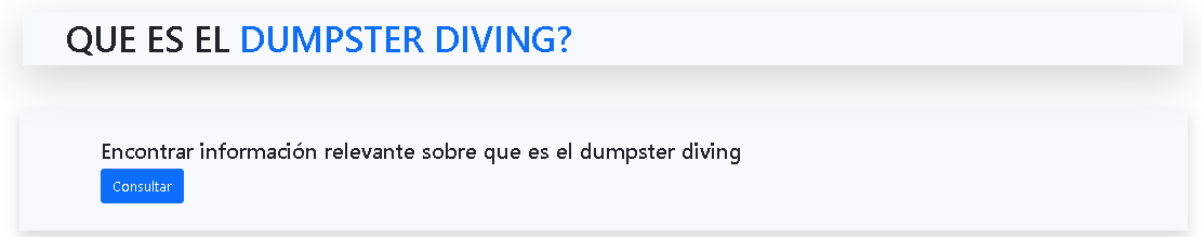
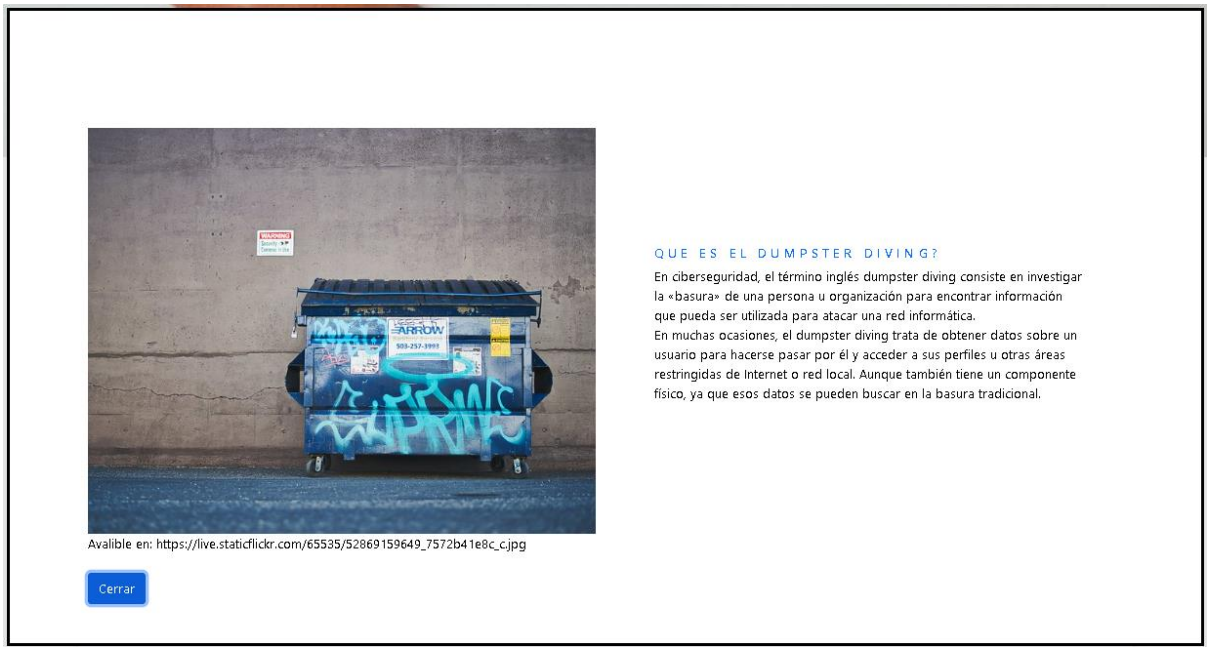


Fig. ¿Qué es el dumpster diving?



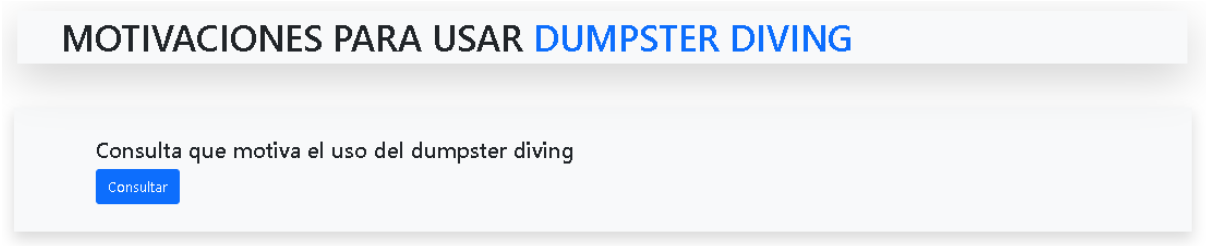
La figura muestra el banner sobre el ¿Que es el dumpster diving? Haciendo click en CONSULTAR accede a la siguiente ventana.

Fig. ¿Qué es el dumpster diving?



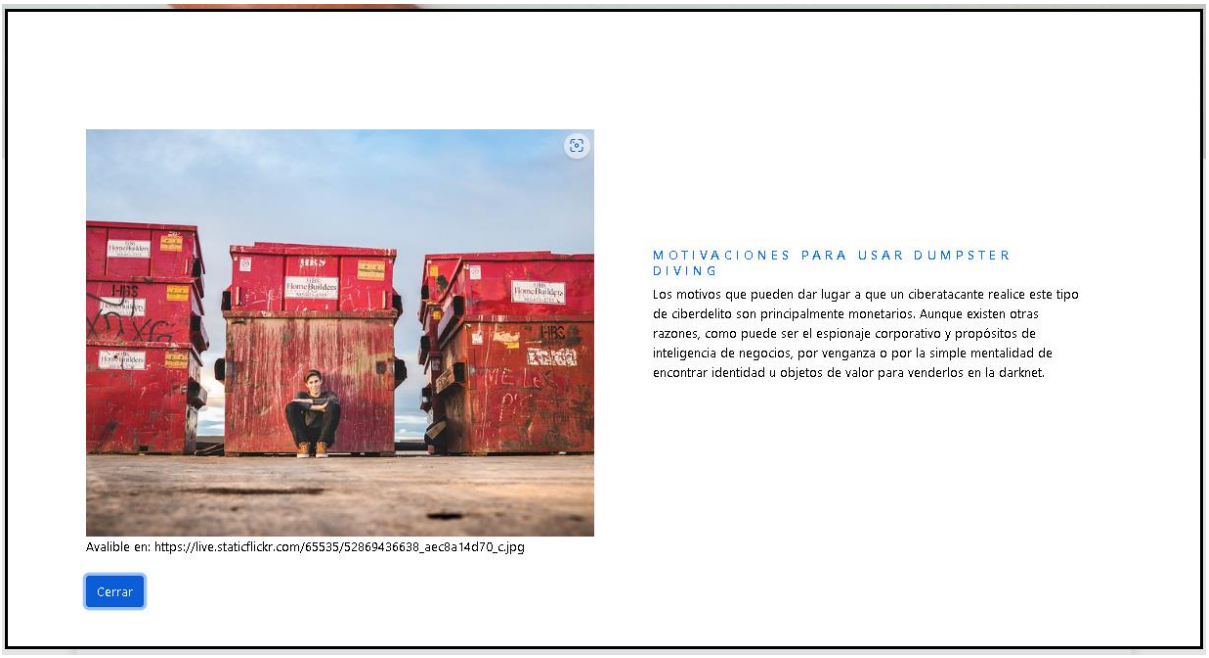
La figura muestra una introducción clara sobre lo que es el dumpster diving.

Fig. Motivación para usar dumpster diving



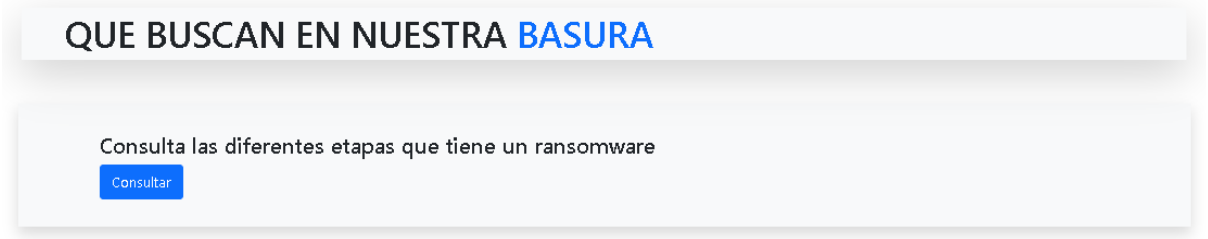
La imagen muestra el banner de acceso de motivaciones para usar dumpster diving. Haciendo clic en CONSULTAR accede a la siguiente ventana.

Fig. Motivaciones



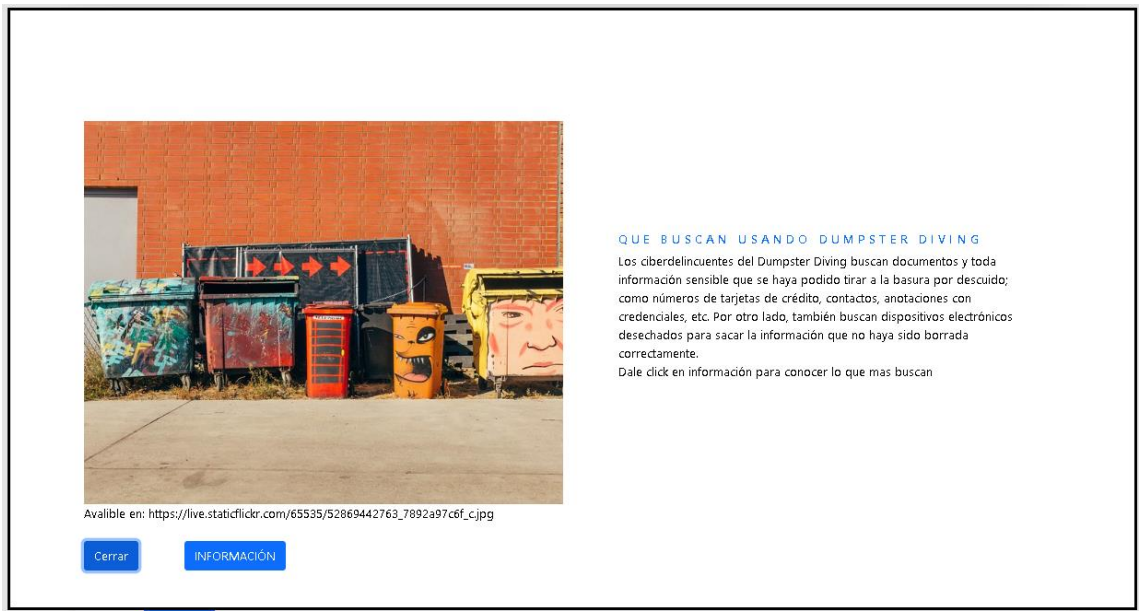
La imagen muestra las motivaciones para usar dumpster diving.

Fig. Que Buscan?



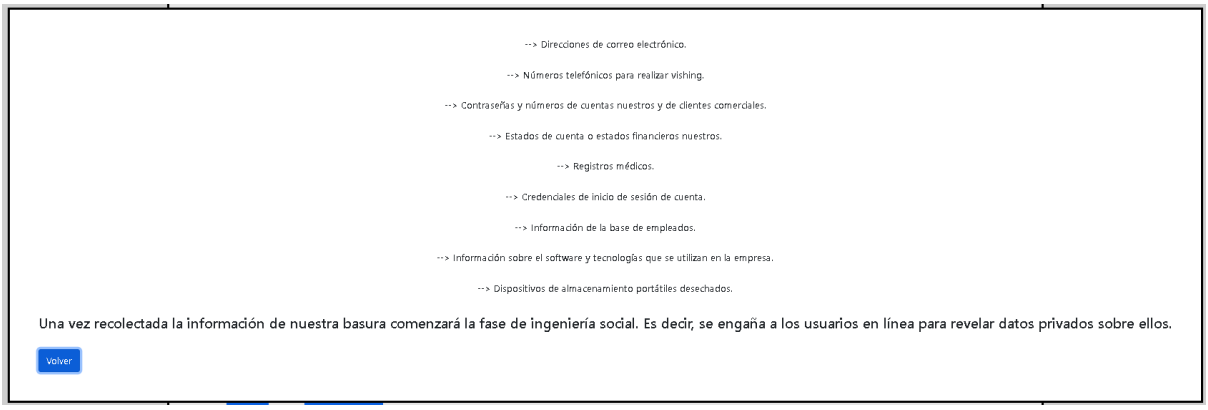
La imagen muestra el banner de ingreso hacia la ventana que buscan en nuestra basura. Haciendo click en CONSULTAR accede a la ventana siguiente.

Fig. Que Buscan?



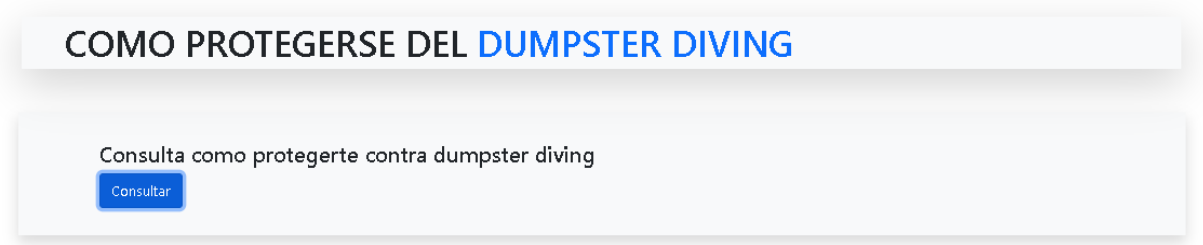
La imagen muestra la introducción hacía que buscan usando dumpster diving. Haciendo clic en RECOMENDACIONES accede a la siguiente ventana.

Fig. Recomendaciones



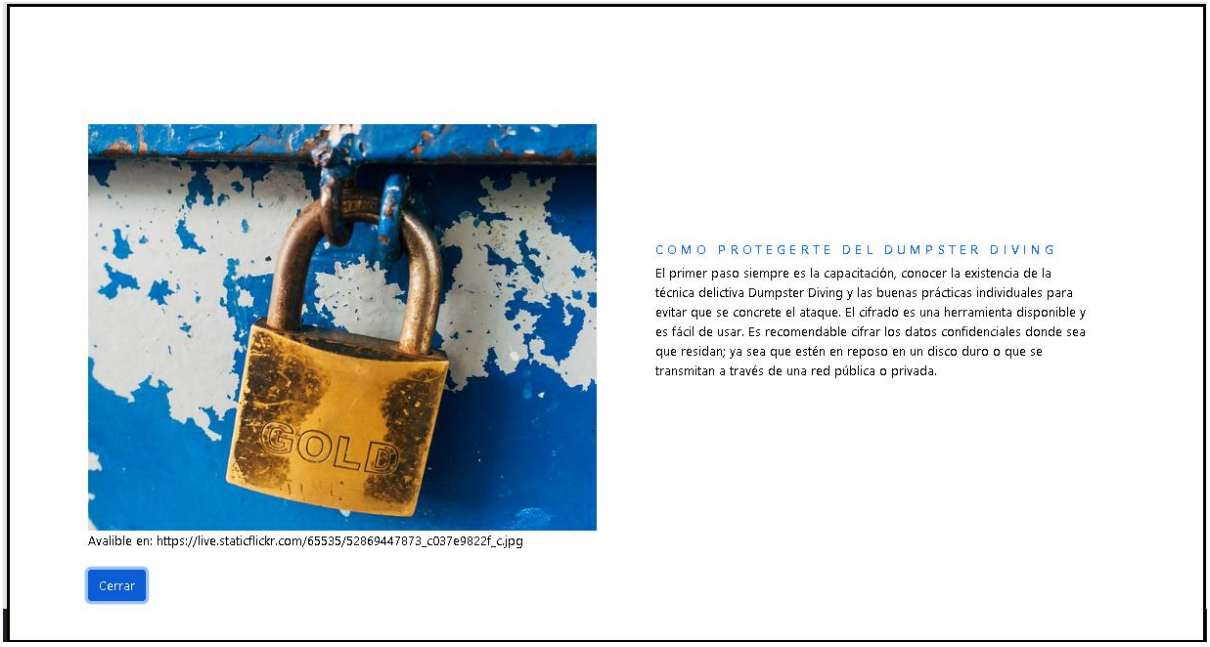
La figura muestra las recomendaciones más relevantes contra Dumpster diving.

Fig. Cómo protegerse del Dumpster diving



La figura muestra el banner de ingreso a cómo protegerse del dumpster diving. Haciendo click en CONSULTAR accede a la siguiente ventana.

Fig. Protegerse contra Dumpster Diving



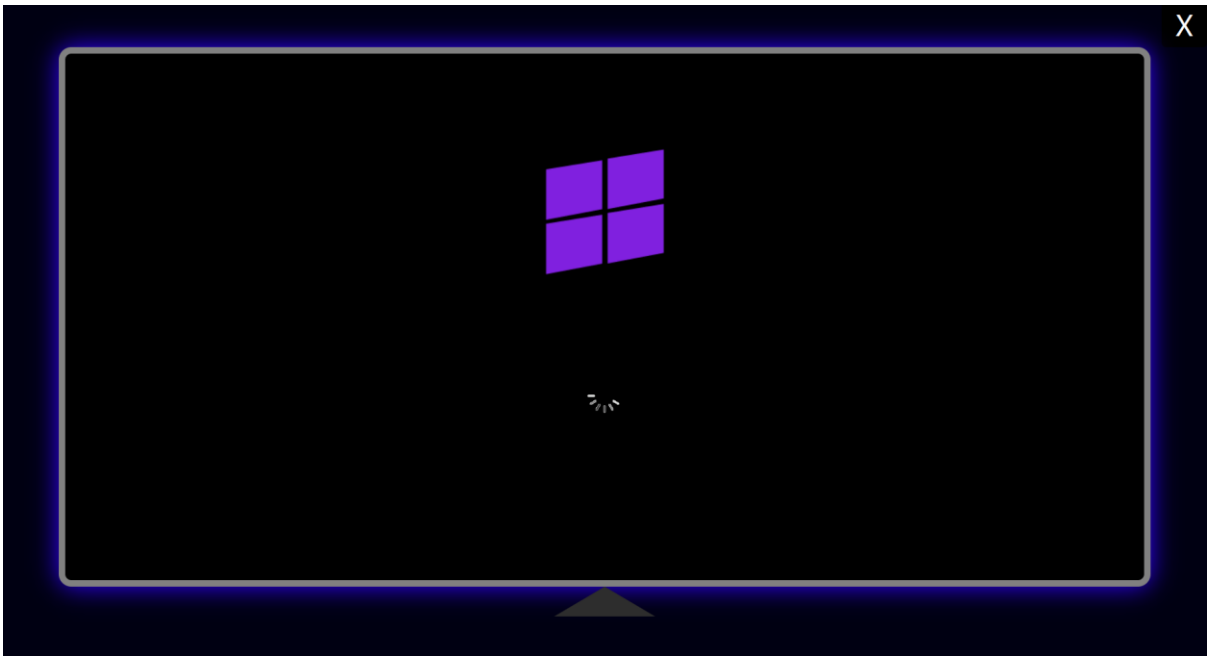
La figura muestra la forma de protegerse contra Dumpster diving.

Módulo de la Metodología

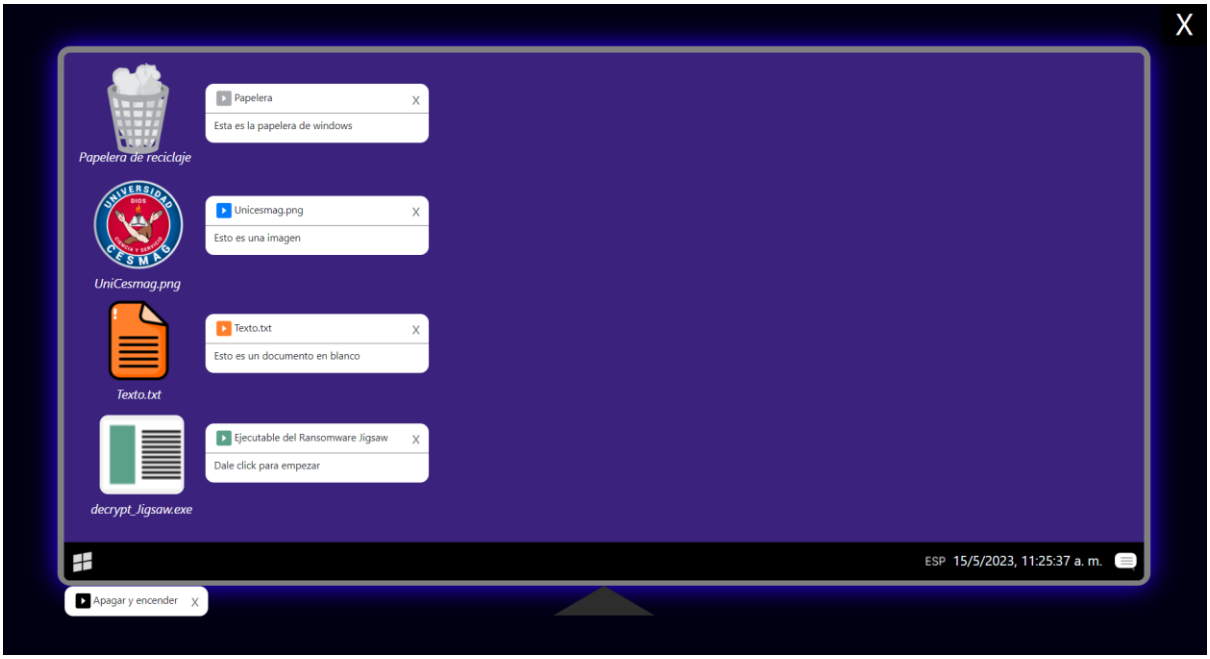
En la figura se presenta una imagen interactiva que cambia cuando se hace clic en ella, al hacer clic en esta imagen, se accederá a la sección de ejecución del PC, donde se proporcionará información detallada sobre el proceso de ejecución y funcionamiento del sistema operativo.

Esta sección es fundamental para comprender cómo funciona la metodología propuesta por los investigadores. Al explorar esta sección, los usuarios podrán adquirir conocimientos prácticos del funcionamiento de un Ransomware.

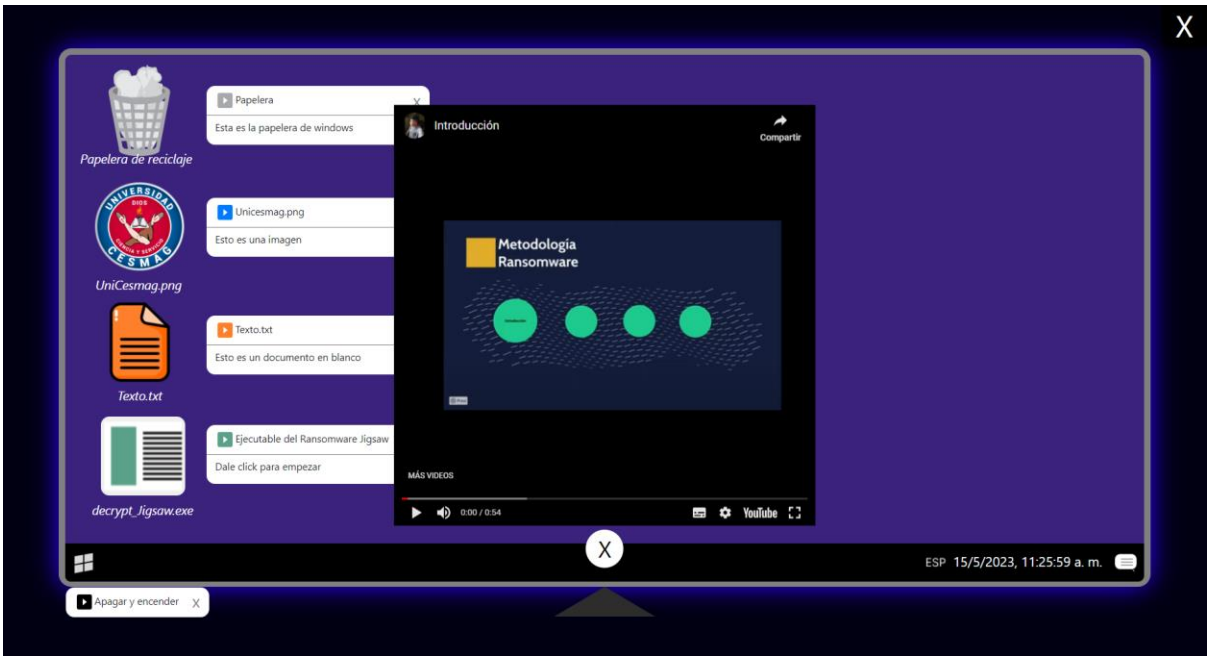
En la figura se muestra la interfaz de inicio del sistema operativo, donde se presenta la pantalla de bienvenida al usuario del sistema.



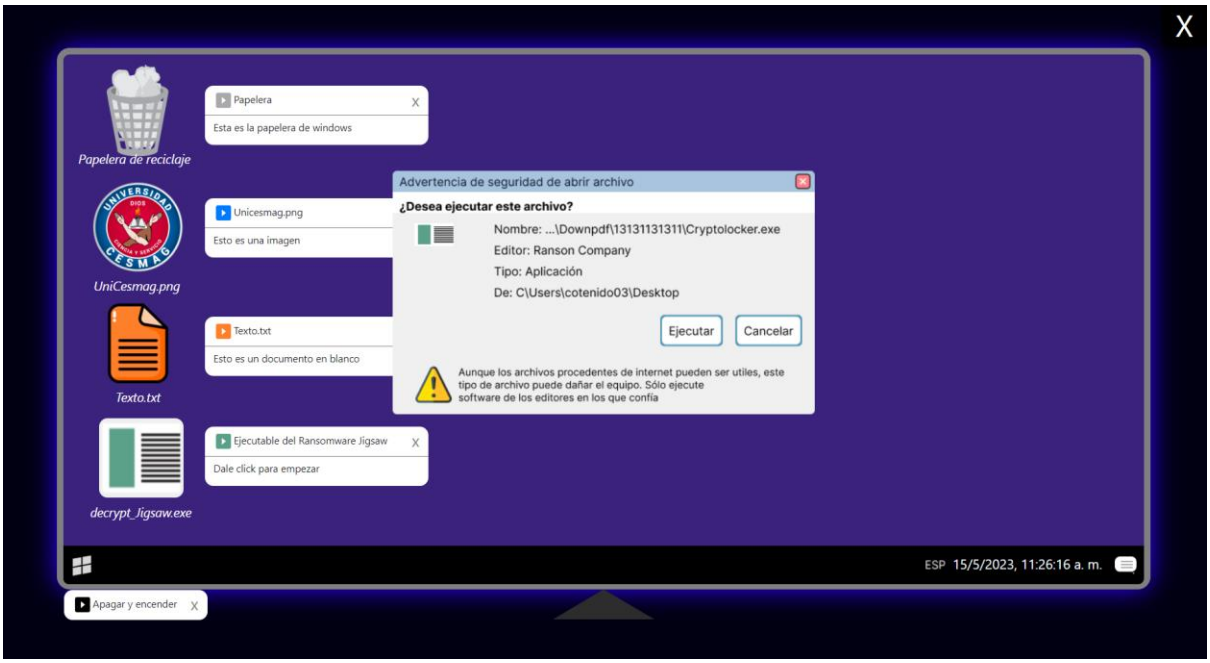
En la siguiente figura se puede apreciar el sistema operativo completamente iniciado y listo para su uso. En esta etapa, todas las funciones y características del sistema están disponibles para el usuario, y se puede comenzar a utilizar las aplicaciones, acceder a los archivos y llevar a cabo las tareas deseadas. Es importante destacar que el proceso de inicio del sistema operativo garantiza un arranque adecuado y confiable, brindando al usuario una experiencia fluida y segura en el uso de su dispositivo.



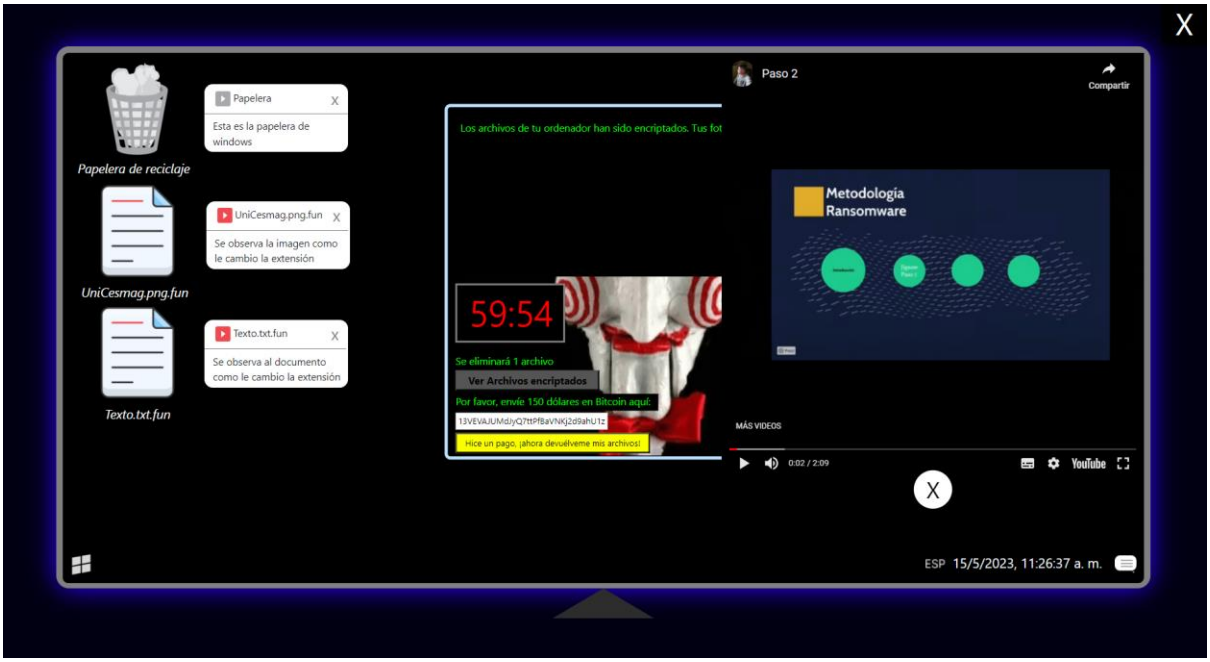
Si se hace clic en decryp_Jigsaw.exe, tal como se muestra en la siguiente figura se iniciará la ejecución del primer video, el cual proporciona una explicación detallada de la primera parte de la metodología.



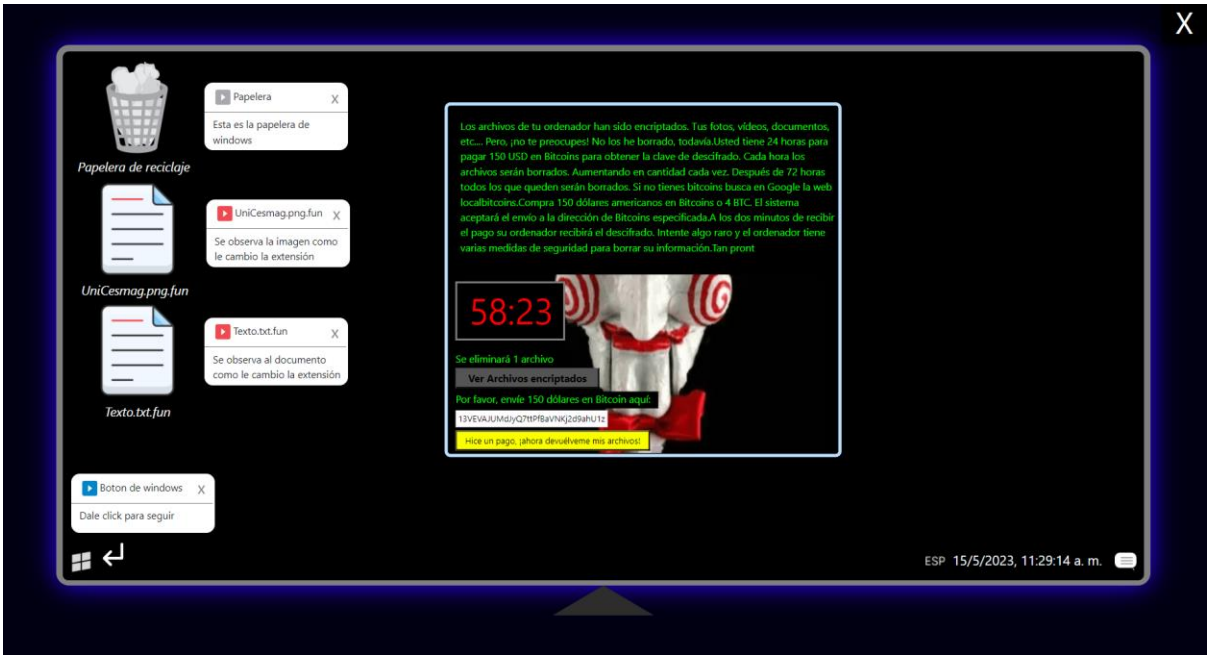
Una vez finalizado el video, en la siguiente figura se mostrará una ventana emergente que permite ejecutar el programa seleccionado. Esta etapa es fundamental para poner en práctica los conceptos aprendidos y avanzar en la implementación de la metodología en el contexto específico del usuario. A través de esta secuencia de pasos, se busca facilitar el aprendizaje y el uso efectivo de la metodología, brindando una experiencia interactiva y práctica para alcanzar los objetivos deseados.



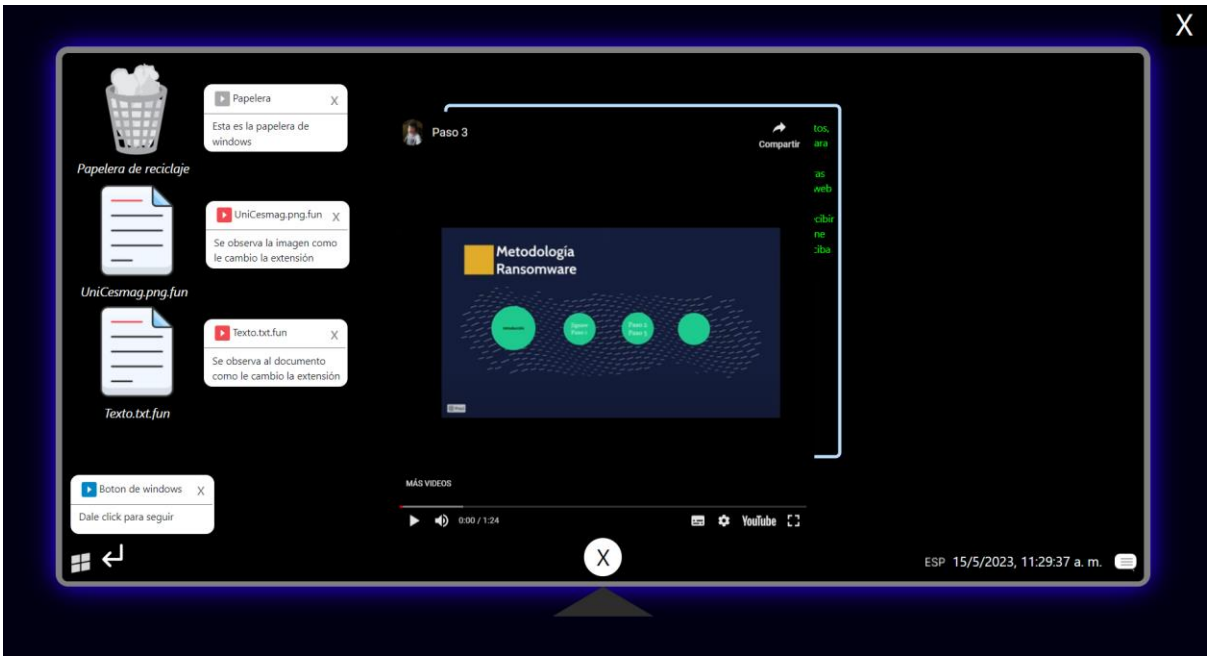
En la siguiente figura se muestra de manera visual el video de la ejecución del segundo paso de la metodología ransomware.



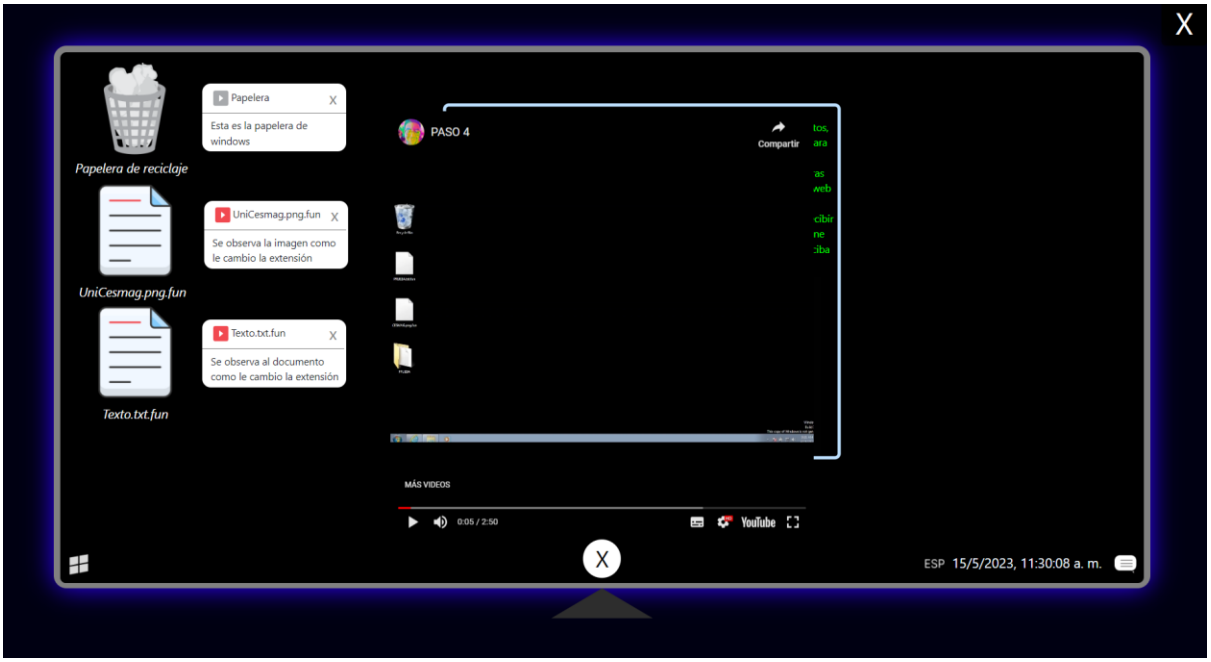
Al finalizar la reproducción del video, se puede observar en la interfaz de fondo la ejecución del ransomware Jigsaw en un entorno virtual, tal como se ilustra en la figura . Esta representación gráfica brinda una representación realista y detallada del proceso, permitiendo a los usuarios familiarizarse con las acciones y consecuencias asociadas al ransomware Jigsaw. Al visualizar esta etapa, los usuarios podrán comprender de manera más profunda cómo funciona el ransomware.



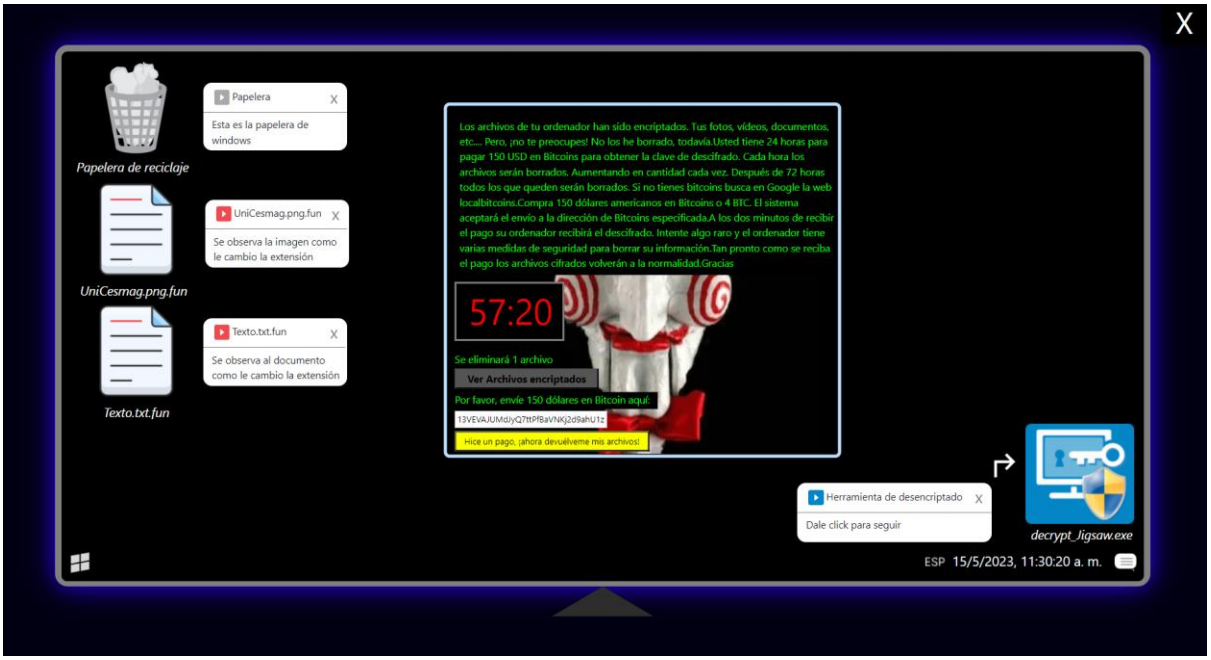
Cuando se hace clic en el botón de inicio, como se muestra en la siguiente figura se despliega de forma visual la ejecución del tercer paso de la metodología. Una vez que el video correspondiente finaliza, se activa automáticamente el video del cuarto paso de la metodología, donde se brinda una explicación detallada sobre cómo actuar en caso de una infección por ransomware.



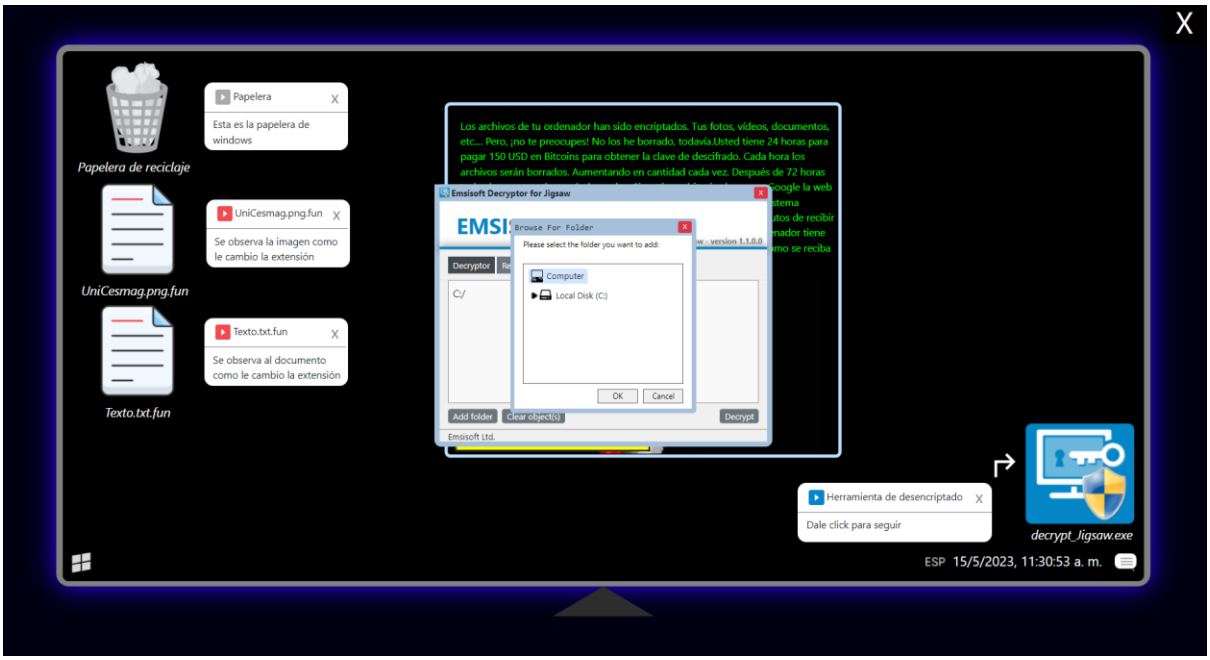
El video del cuarto paso proporciona una guía completa y detallada sobre las acciones recomendadas a tomar en caso de encontrarse con un caso de ransomware. Se abordan aspectos clave como la identificación de la infección, las medidas de contención y aislamiento, y las opciones disponibles para la recuperación de los archivos afectados.



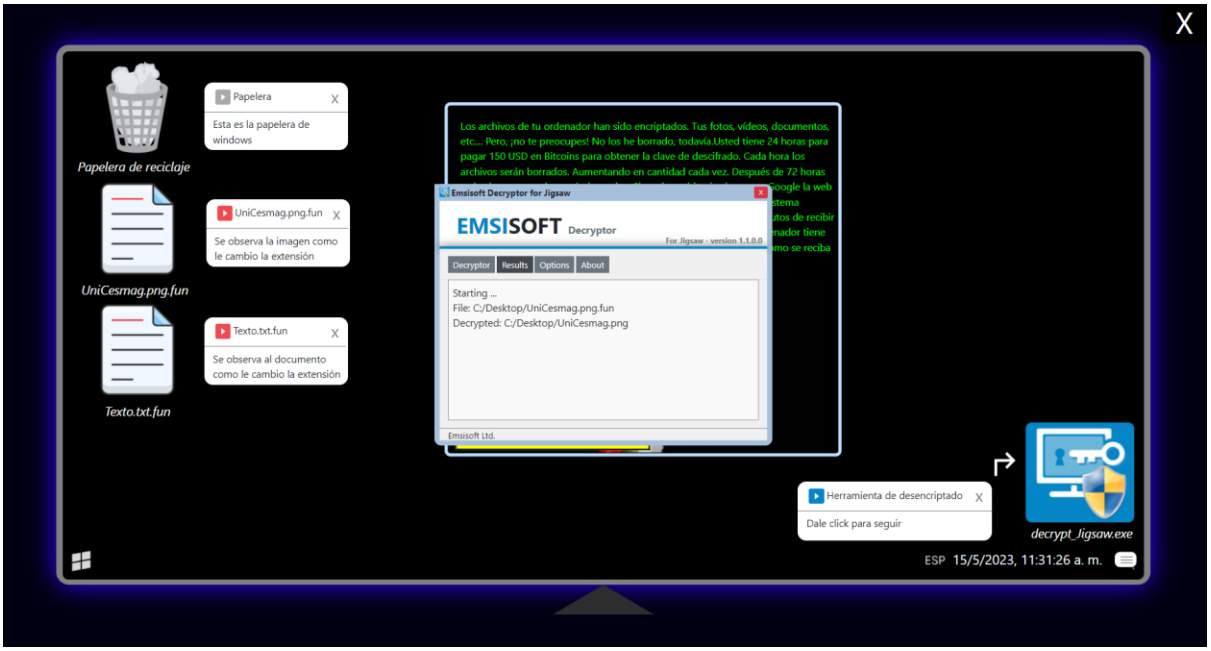
En la figura se puede apreciar en la parte inferior derecha de la interfaz la presencia de una herramienta de desencriptado específicamente diseñada para el ransomware Jigsaw. Esta herramienta se muestra como una solución efectiva para recuperar los archivos afectados por este tipo de malware.



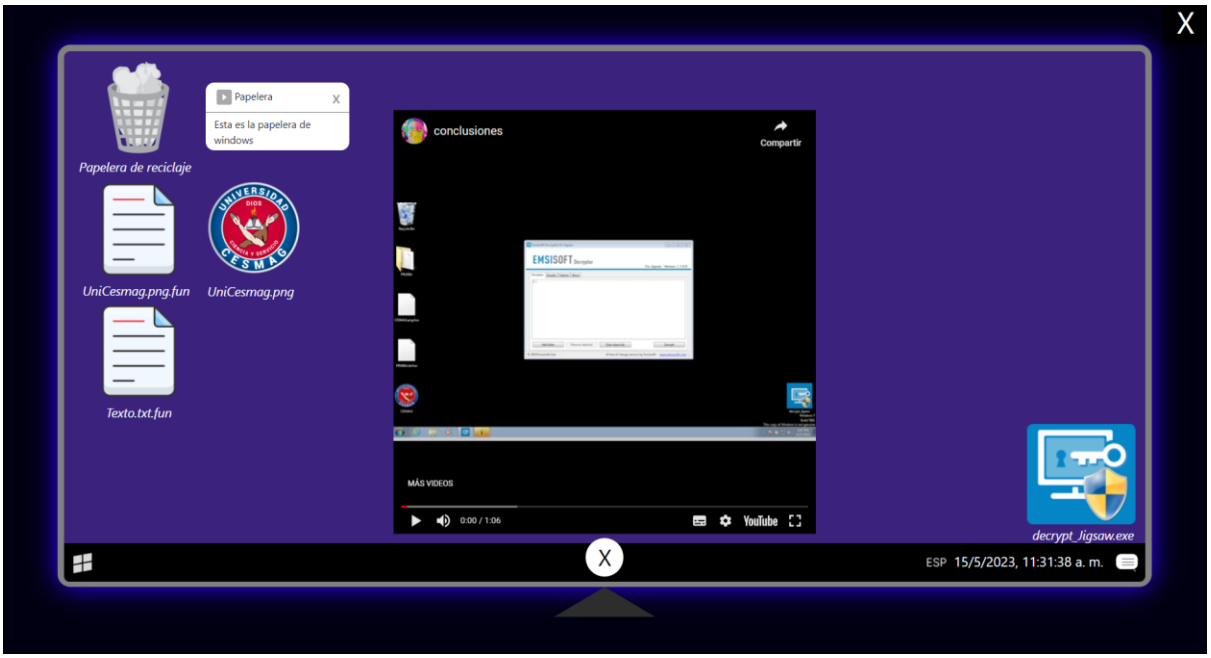
En la siguiente figura se puede observar con mayor detalle la ejecución de la herramienta de desencriptado, mostrando todas sus funciones disponibles para restaurar los archivos de manera segura y eficiente. Es importante destacar que esta herramienta representa una valiosa ayuda en casos de infección por ransomware, brindando a los usuarios una opción confiable para recuperar su información de manera exitosa.



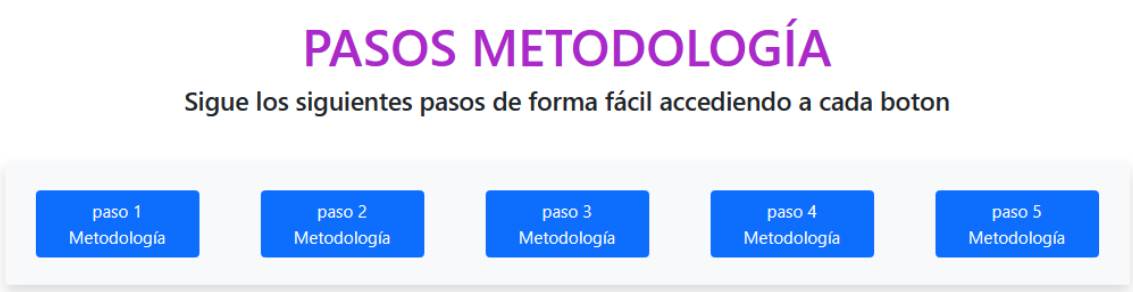
En la figura se puede apreciar el proceso de ejecución de la herramienta de desencriptado en acción. Se observa cómo la herramienta trabaja diligentemente para descifrar los archivos afectados por el ransomware. Cada paso del proceso se muestra de manera clara y detallada, brindando al usuario una visión completa de la restauración de sus datos.



En la siguiente figura se puede apreciar el resultado exitoso de la ejecución de la herramienta de desencriptado. El escritorio del sistema se muestra completamente descifrado, con todos los archivos y carpetas restaurados a su estado original.

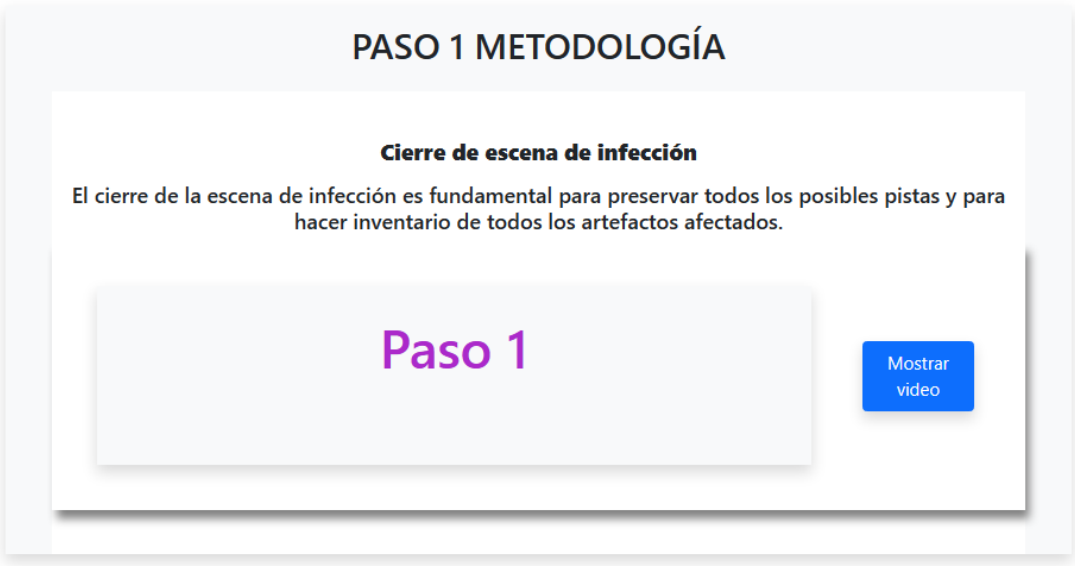


PASOS METODOLOGÍA



La figura muestra la barra de navegación que contiene los 5 botones de los pasos de la metodología creada. Accediendo a cada botón pasamos a las siguientes vistas.

Fig. Paso 1

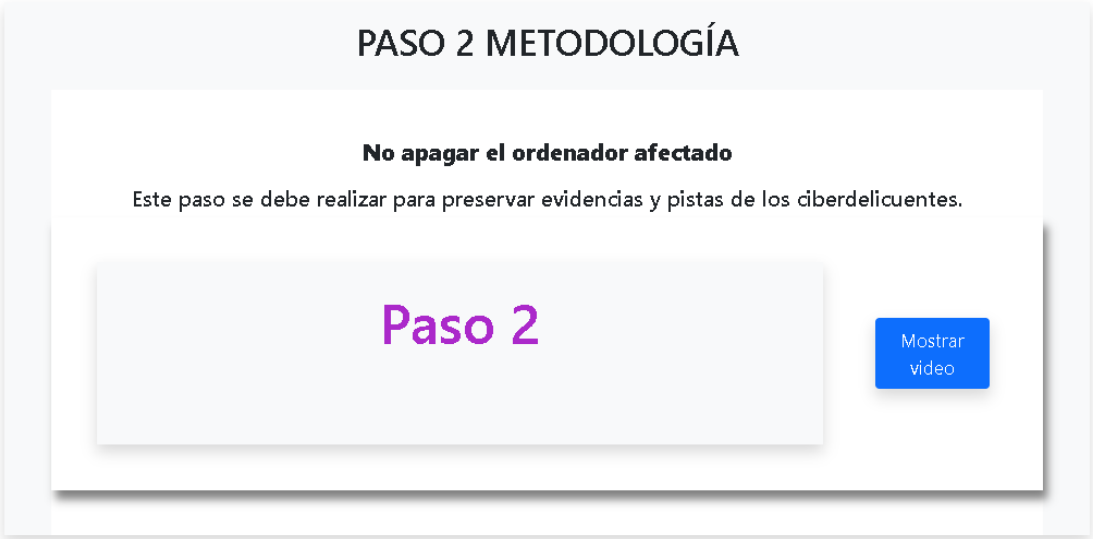


La figura muestra el paso 1 de la metodología, Haciendo click en MOSTRAR VIDEO accede a un video explicativo que te capacita sobre el paso cierre de escena de infección.

Fig. Video paso 1

La figura muestra el video explicativo sobre el primer paso de la metodología al finalizar haz click en la X para cerrar y continuar con los siguientes pasos.

Fig. Paso 2 Metodología

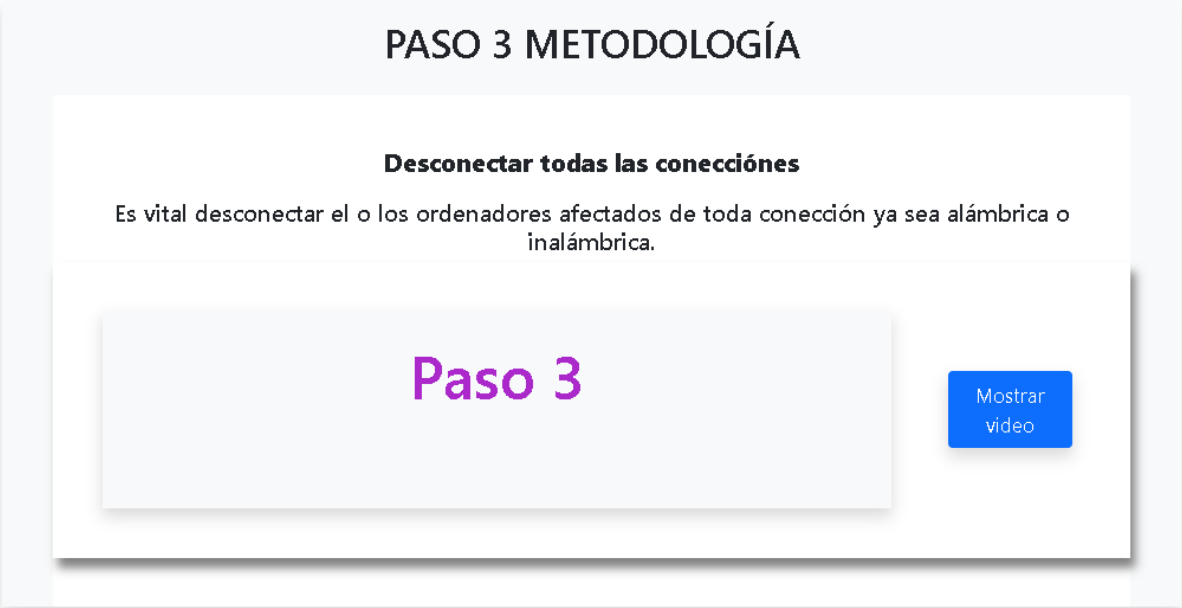


La figura muestra el banner de ingreso al paso 2 de la metodología. Haciendo clic en MOSTRAR VIDEO accede a un video explicativo sobre no apagar el ordenador afectado.

Fig. Video paso 2

La figura muestra el video explicativo sobre el paso 2 de la metodología. Al finalizar el video haz click en la X para cerrarlo y pasar a los siguientes pasos.

Fig. Paso 3 Metodología

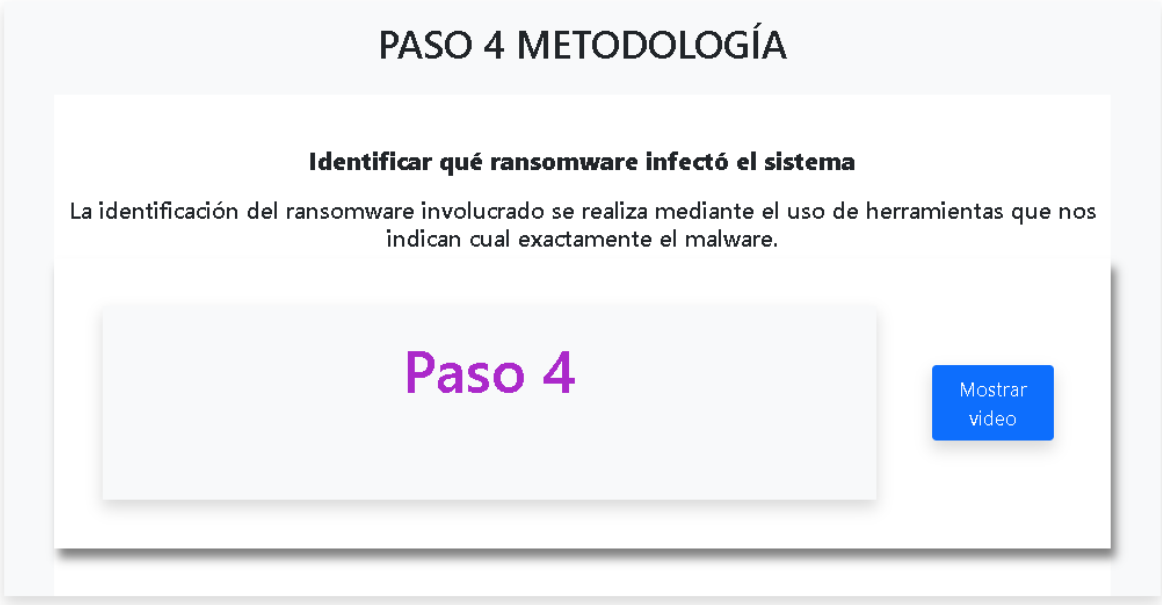


La figura muestra el paso 3 de la metodología. Haciendo Click en MOSTRAR VIDEO accede al video explicativo sobre desconectar todas las conexiones.

Fig. Video paso 3

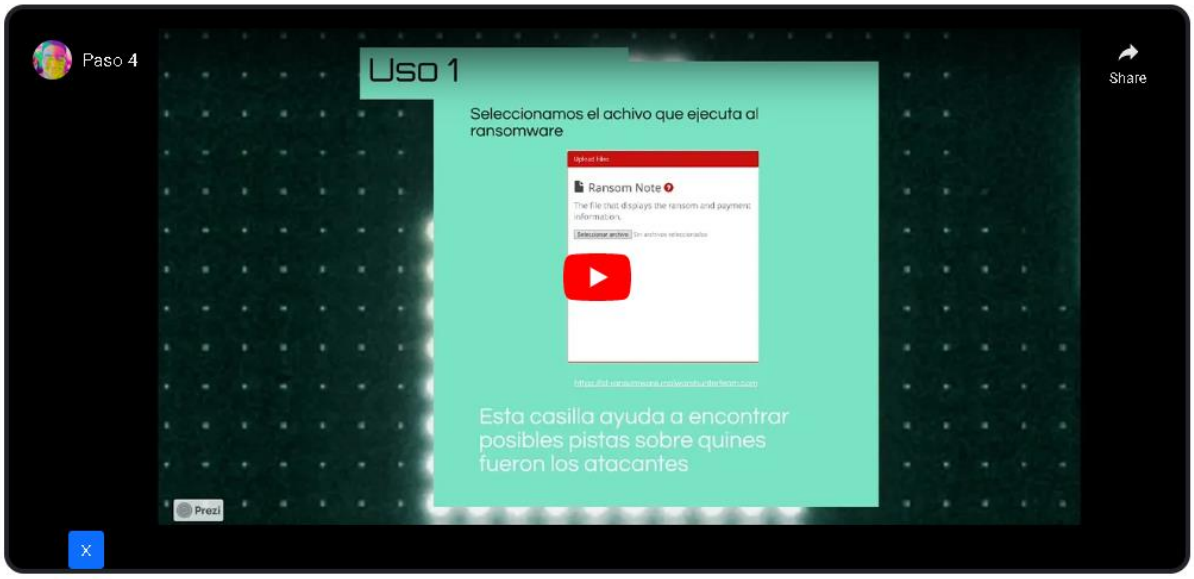
La figura muestra el video del paso 3 de la metodología. Al finalizar haz click en la X para cerrarlo y pasar a los siguientes pasos.

Fig. Paso 4 metodología



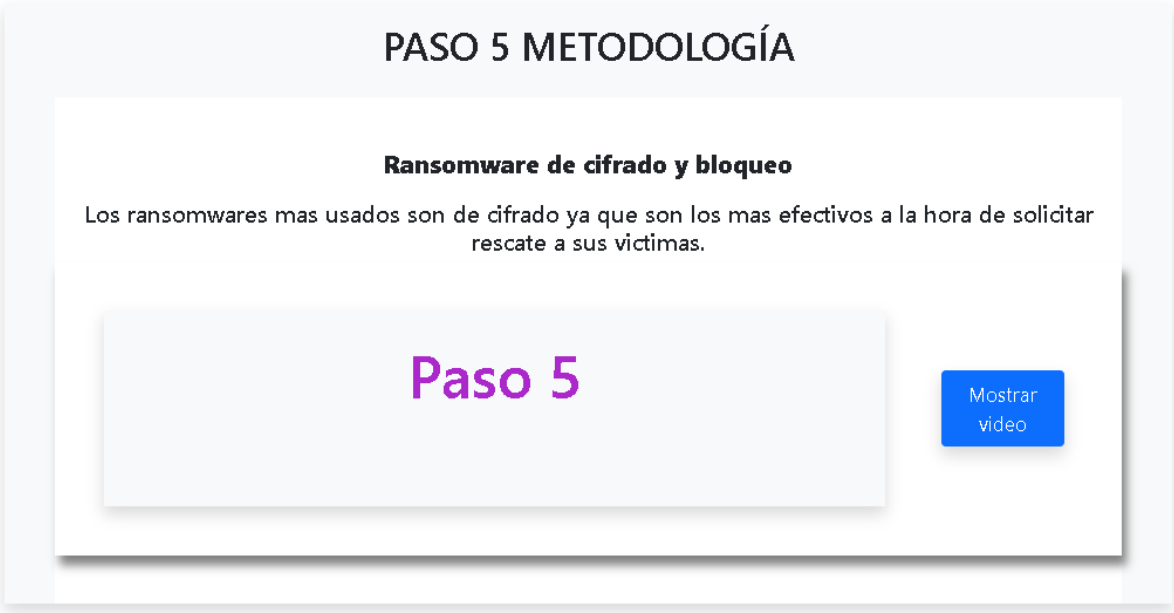
La imagen muestra el banner del paso 4 de la metodología. Haciendo click en el botón MOSTRAR VIDEO accede al video del paso e identifica que ransomware infecto el sistema.

Fig. Video paso 4



La figura muestra el video del paso 4 de la metodología. Al finalizar el video haz clic en la X para continuar con los pasos.

Fig. Paso 5 Metodología.



La imagen muestra el banner para acceder al video explicativo sobre el paso 5 de la metodología. Haciendo click en el botón MOSTRAR VIDEO accede al video explicativo.

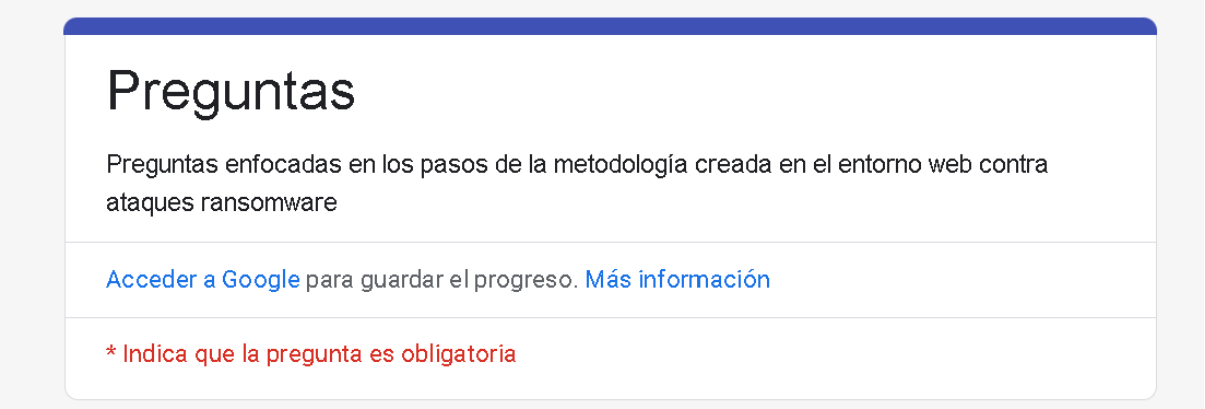
Fig. Video paso 5

La figura muestra el video 5 de la metodología.

Fig. Encuesta Validación Metodología Ransomware

La figura muestra el banner de acceso al link de la encuesta de validación de la metodología. Haciendo click en en botón ENCUESTA VALIDACIÓN PASO A PASO METODOLOGÍA accede a la encuesta en Google forms.

Fig. Encuesta Validación.

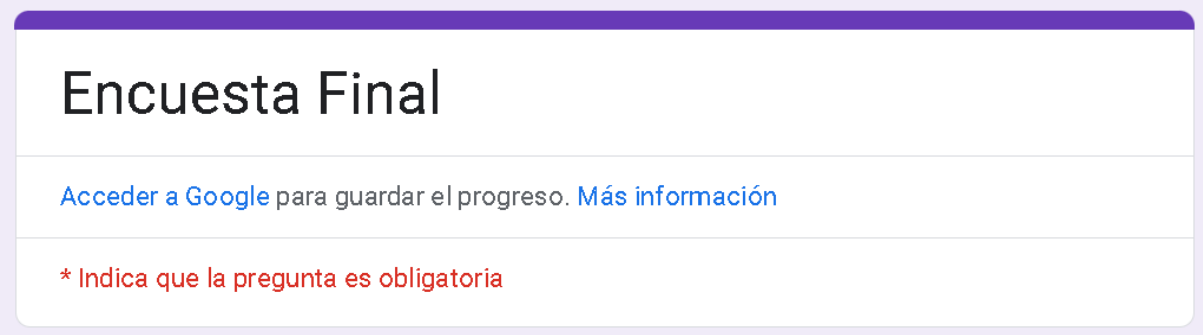


La figura muestra el inicio de la encuesta.

Fig. Encuesta Evaluación de satisfacción

La imagen muestra el banner de la encuesta final de evaluación de satisfacción de usuario. haciendo click en el botón ENCUESTA EVALUACIÓN para acceder a la encuesta en Google forms.

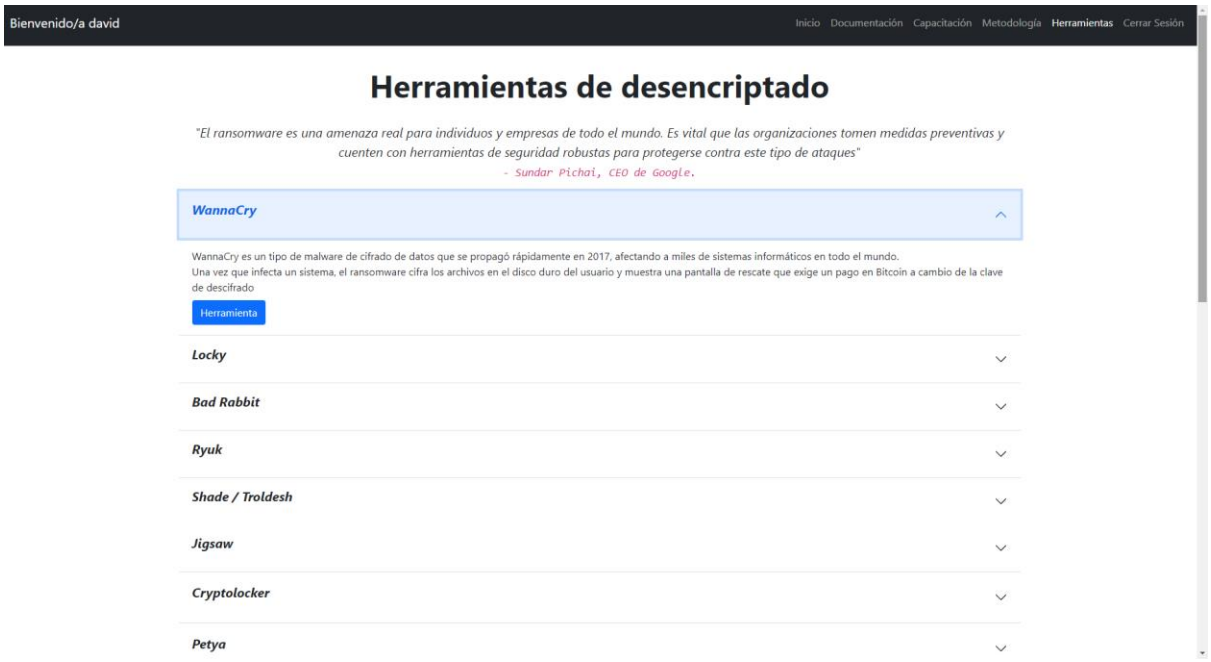
Fig. encuesta final.



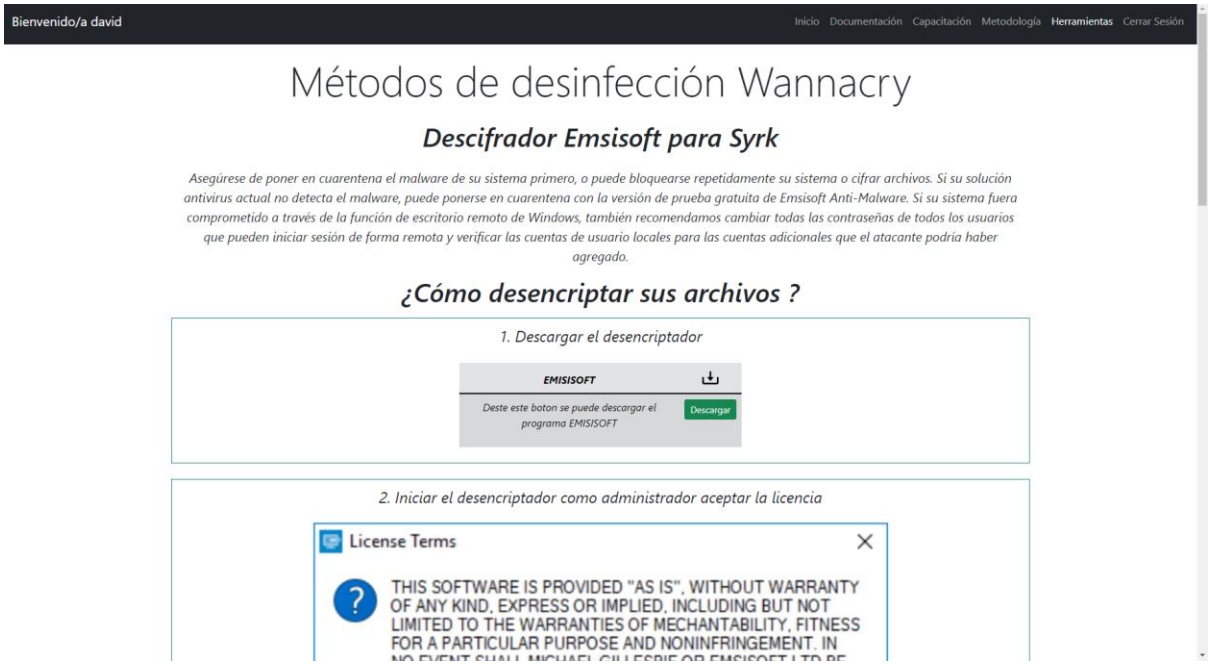
La figura muestra el inicio de la encuesta final.

Módulo de las Herramientas

En la figura siguiente se presenta el módulo de herramientas de descifrado diseñado para combatir ransomware de cifrado. En esta sección, encontrará una recopilación de las 10 variantes de ransomware más populares que se han propagado hasta la fecha, junto con sus respectivas herramientas de descifrado. Todos los usuarios tendrán acceso a este módulo, el cual proporcionará información detallada sobre el proceso paso a paso de cada herramienta, así como su documentación correspondiente.



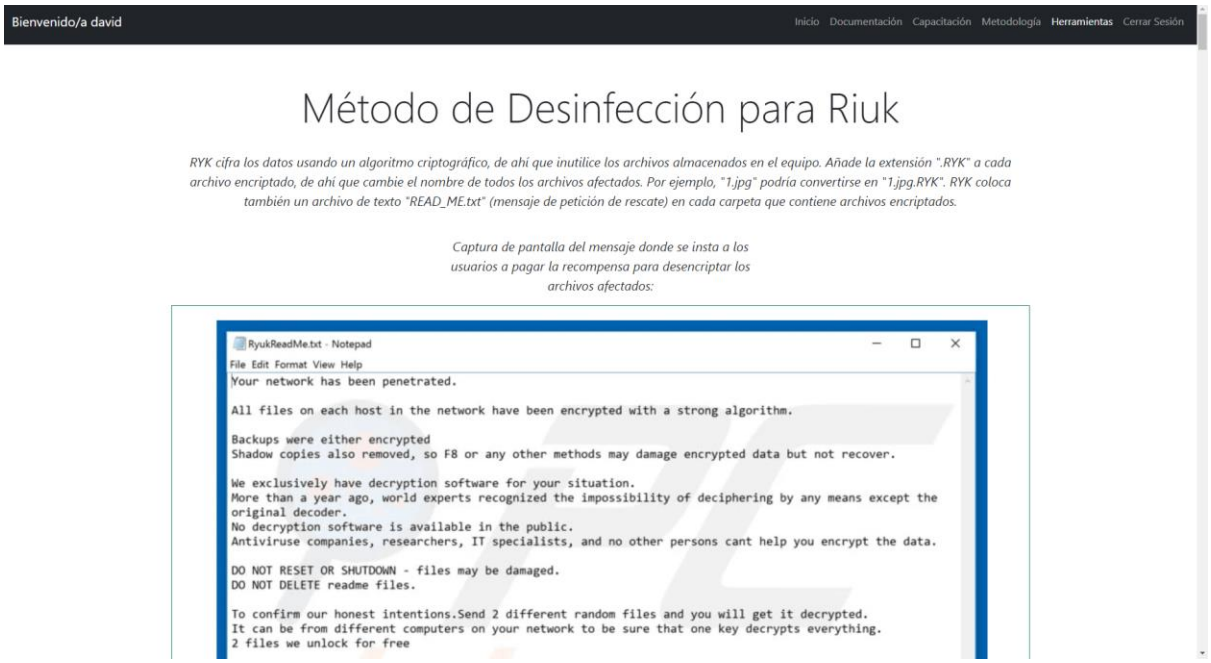
La siguiente figura muestra el método de desinfección para el ransomware Wannacry. En esta sección encontrará la herramienta correspondiente junto con las instrucciones paso a paso para su uso. Además, se proporcionará información detallada sobre cómo intentar recuperar su información en caso de que la herramienta no funcione correctamente. También se encontrará disponible un enlace de descarga para obtener la herramienta.



La figura siguiente presenta el procedimiento de desinfección para el ransomware Locky o una de sus variantes, PyLocky. En este apartado, podrá acceder a la herramienta adecuada junto con instrucciones detalladas que le guiarán en su uso. Además, se le brindará información exhaustiva sobre cómo intentar recuperar sus datos en caso de que la herramienta no logre funcionar correctamente. Asimismo, se dispondrá de un enlace de descarga para obtener la herramienta necesaria.

La siguiente ilustración muestra el método de desinfección para el ransomware Bad Rabbit. En esta sección, tendrá acceso a la herramienta correspondiente junto con instrucciones minuciosas que le orientarán en su utilización. Además, se le proporcionará información detallada sobre cómo intentar recuperar sus datos en caso de que la herramienta no tenga un rendimiento óptimo. También encontrará disponible un enlace para descargar la herramienta necesaria.

En la figura siguiente se presenta el procedimiento de desinfección para el ransomware Riuk. En este apartado, podrá acceder a la herramienta apropiada junto con instrucciones detalladas que le guiarán en su uso. Además, se le brindará información exhaustiva sobre cómo intentar recuperar sus datos en caso de que la herramienta no funcione de manera óptima. Asimismo, dispondrá de un enlace para descargar la herramienta necesaria.

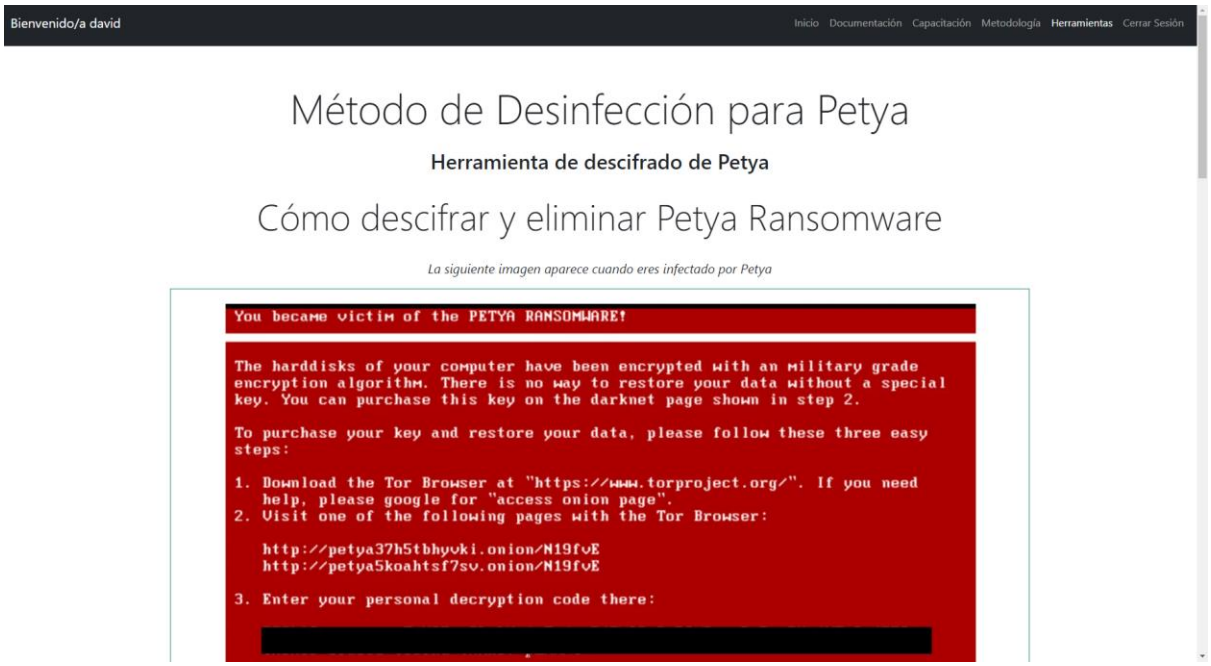


En la siguiente ilustración se muestra el método de desinfección para el ransomware Shade / Troldesh. En esta sección, podrá obtener la herramienta adecuada junto con instrucciones detalladas que le ayudarán en su utilización. Además, se le proporcionará información exhaustiva sobre cómo intentar recuperar sus datos en caso de que la herramienta no presente un rendimiento óptimo. También encontrará disponible un enlace para descargar la herramienta necesaria.

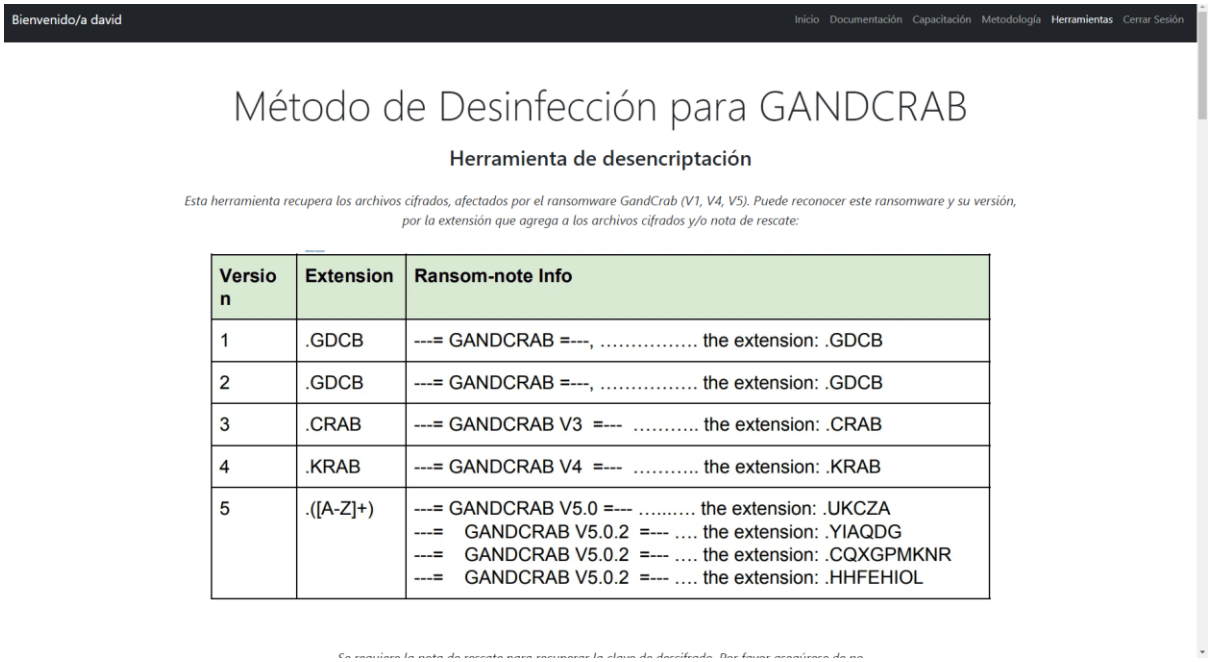
En la figura que se presenta a continuación, se exhibe el procedimiento de desinfección para el ransomware Jigsaw. En este apartado, usted podrá adquirir la herramienta apropiada, acompañada de instrucciones detalladas que le serán de utilidad al momento de utilizarla. Asimismo, se le brindará una amplia información sobre cómo intentar recuperar sus datos en caso de que la herramienta no funcione de manera óptima. Adicionalmente, encontrará un enlace disponible para descargar la herramienta necesaria.

En la siguiente ilustración, se muestra el proceso de desinfección para el ransomware Cryptolocker. En esta sección, podrá obtener la herramienta adecuada, junto con instrucciones detalladas que le serán útiles al momento de usarla. Además, se le proporcionará una amplia información sobre cómo intentar recuperar sus datos en caso de que la herramienta no funcione de manera óptima. También dispondrá de un enlace para descargar la herramienta necesaria.

En la figura siguiente, se visualiza el método de desinfección para el ransomware Perya. Dentro de esta sección, tendrá acceso a la herramienta adecuada, así como a instrucciones detalladas que resultan útiles durante su utilización. Además, se le brindará una amplia variedad de información sobre cómo intentar recuperar sus datos en caso de que la herramienta no presente un rendimiento óptimo. También encontrará disponible un enlace para descargar la herramienta necesaria.



La ilustración que sigue muestra el proceso de desinfección para el ransomware GandCrab. En esta sección, podrá obtener la herramienta apropiada junto con instrucciones detalladas que serán de utilidad durante su uso. Además, se proporcionará una amplia gama de información sobre cómo intentar recuperar sus datos en caso de que la herramienta no funcione de manera óptima. También encontrará a su disposición un enlace para descargar la herramienta necesaria.



La siguiente ilustración muestra el procedimiento de desinfección para el ransomware GoldenEye. En esta sección, podrá acceder a la herramienta apropiada, así como a instrucciones detalladas que serán de utilidad durante su aplicación. Además, se proporcionará una amplia gama de información sobre cómo intentar recuperar sus datos en caso de que la herramienta no funcione de manera óptima. Asimismo, encontrará a su disposición un enlace para descargar la herramienta necesaria.

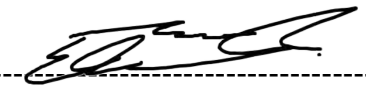
San Juan de Pasto, 22/06/2023

Biblioteca
REMIGIO FIORE FORTEZZA OFM. CAP.
Universidad CESMAG
Pasto

Saludo de paz y bien.

Por medio de la presente se hace entrega del Trabajo de Grado / Trabajo de Aplicación denominado desarrollo de una metodología como respuesta a incidentes de infección por ransomware, presentado por el (los) autor(es) Juan David Rojas Rosero y Freyder Alejandro Urbano Rosales del Programa Académico Ingeniería de sistemas al correo electrónico biblioteca.trabajosdegrado@unicesmag.edu.co. Manifiesto como asesor(a), que su contenido, resumen, anexos y formato PDF cumple con las especificaciones de calidad, guía de presentación de Trabajos de Grado o de Aplicación, establecidos por la Universidad CESMAG, por lo tanto, se solicita el paz y salvo respectivo.

Atentamente,



MSc. Edgar Rodrigo Enríquez Rosero
98395427
Ingeniería de Sistemas
311 3548203
erenriquez@unicesmag.edu.co

INFORMACIÓN DEL (LOS) AUTOR(ES)	
Nombres y apellidos del autor: Juan David Rojas Rosero	**Documento de identidad:** 1085343758
Correo electrónico: juanrojas043@gmail.com	**Número de contacto:** 3164890183
Nombres y apellidos del autor: Freyder Alejandro Urbano Rosales	**Documento de identidad:** 87062458
Correo electrónico: freurbano@gmail.com	**Número de contacto:** 3113389976
Nombres y apellidos del asesor: Edgar Rodrigo Enríquez Rosero	**Documento de identidad:** 98395427
Correo electrónico: erenriquez@unicesmag.edu.co	**Número de contacto:** 3113548203
Título del trabajo de grado: Desarrollo de una metodología como respuestas a incidentes de infección por ransomware	
Facultad y Programa Académico: Ingeniería de Sistemas	

En mi (nuestra) calidad de autor(es) y/o titular (es) del derecho de autor del Trabajo de Grado o de Aplicación señalado en el encabezado, confiero (conferimos) a la Universidad CESMAG una licencia no exclusiva, limitada y gratuita, para la inclusión del trabajo de grado en el repositorio institucional. Por consiguiente, el alcance de la licencia que se otorga a través del presente documento, abarca las siguientes características:

a) La autorización se otorga desde la fecha de suscripción del presente documento y durante todo el término en el que el (los) firmante(s) del presente documento conserve (mos) la titularidad de los derechos patrimoniales de autor. En el evento en el que deje (mos) de tener la titularidad de los derechos patrimoniales sobre el Trabajo de Grado o de Aplicación, me (nos) comprometo (comprometemos) a informar de manera inmediata sobre dicha situación a la Universidad CESMAG. Por consiguiente, hasta que no exista comunicación escrita de mi(nuestra) parte informando sobre dicha situación, la Universidad CESMAG se encontrará debidamente habilitada para continuar con la publicación del Trabajo de Grado o de Aplicación dentro del repositorio institucional. Conozco(conocemos) que esta autorización podrá revocarse en cualquier momento, siempre y cuando se eleve la solicitud por escrito para dicho fin ante la Universidad CESMAG. En estos eventos, la Universidad CESMAG cuenta con el plazo de un mes después de recibida la petición, para desmarcar la visualización del Trabajo de Grado o de Aplicación del repositorio institucional.
b) Se autoriza a la Universidad CESMAG para publicar el Trabajo de Grado o de Aplicación en formato digital y teniendo en cuenta que uno de los medios de publicación del repositorio institucional es el internet, acepto(amos) que el Trabajo de Grado o de Aplicación circulará con un alcance mundial.
c) Acepto (aceptamos) que la autorización que se otorga a través del presente documento se realiza a título gratuito, por lo tanto, renuncio(amos) a recibir emolumento alguno por la publicación, distribución, comunicación pública y/o cualquier otro uso que se haga en los términos de la presente autorización y de la licencia o programa a través del cual sea publicado el Trabajo de grado o de Aplicación.
d) Manifiesto (manifestamos) que el Trabajo de Grado o de Aplicación es original realizado sin violar o usurpar derechos de autor de terceros y que ostento(amos) los derechos patrimoniales de autor

Powered by CamScanner

sobre la misma. Por consiguiente, asumo(asumimos) toda la responsabilidad sobre su contenido ante la Universidad CESMAG y frente a terceros, manteniéndose indemne de cualquier reclamación que surja en virtud de la misma. En todo caso, la Universidad CESMAG se compromete a indicar siempre la autoría del escrito incluyendo nombre de(los) autor(es) y la fecha de publicación.

e) Autorizo(autorizamos) a la Universidad CESMAG para incluir el Trabajo de Grado o de Aplicación en los índices y buscadores que se estimen necesarios para promover su difusión. Así mismo autorizo (autorizamos) a la Universidad CESMAG para que pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

NOTA: En los eventos en los que el trabajo de grado o de aplicación haya sido trabajado con el apoyo o patrocinio de una agencia, organización o cualquier otra entidad diferente a la Universidad CESMAG. Como autor(es) garantizo(amos) que he(hemos) cumplido con los derechos y obligaciones asumidos con dicha entidad y como consecuencia de ello dejo(dejamos) constancia que la autorización que se concede a través del presente escrito no interfiere ni transgrede derechos de terceros.

Como consecuencia de lo anterior, autorizo(autorizamos) la publicación, difusión, consulta y uso del Trabajo de Grado o de Aplicación por parte de la Universidad CESMAG y sus usuarios así:

- Permito(permitimos) que mi(nuestro) Trabajo de Grado o de Aplicación haga parte del catálogo de colección del repositorio digital de la Universidad CESMAG por lo tanto, su contenido será de acceso abierto donde podrá ser consultado, descargado y compartido con otras personas, siempre que se reconozca su autoría o reconocimiento con fines no comerciales.

En señal de conformidad, se suscribe este documento en San Juan de Pasto a los 22 días del mes de junio del año 2023.

Nombre del autor: Juan David Rojas Rosero	Nombre del autor: Freyder Alejandro Urbano Rosales
Nombre del asesor: Edgar Rodrigo Enríquez Rosero	

Powered by CamScanner