ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

Aplicación de la técnica de esteganografía para el mejoramiento de la integridad de la información en sistemas académicos basados en la web, caso práctico https://sisepec.espoch.edu.ec, 2021

JUAN DIEGO VINTIMILLA CORONEL

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA - ECUADOR

ENERO 2023

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado Aplicación de la técnica de esteganografía para el mejoramiento de la integridad de la información en sistemas académicos basados en la web, caso práctico https://sisepec.espoch.edu.ec, 2021, de responsabilidad del señor Juan Diego Vintimilla Coronel, ha sido prolijamente revisado y se autoriza su presentación.

Ing. Oswaldo Geovanny Martínez Guashima, M. Sc.
PRESIDENTE

OSWALDO GEOVANNY MARTINEZ GUASHIMA

Ing. Diego Bernardo Palacios Campana, Mag.
DIRECTOR

DIEGO BERNARDO PALACIOS CAMPANA

Ing. Diego Francisco Caisaguano Villa, Mag.
MIEMBRO

Diego Francisco Caisaguano Villa

Firmado digitalmente por Diego Francisco Caisaguano Villa
Nombre de reconocimiento (DN): cn=Diego Francisco Caisaguano Villa, o=IPEC, ou=ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO, email=dfranci@hotmail.com, c=ES
Fecha: 2023.01.18 13:42:21 -05'00'

Ing. Bladimir Enrique Urgiles Rodríguez, Mag.
MIEMBRO

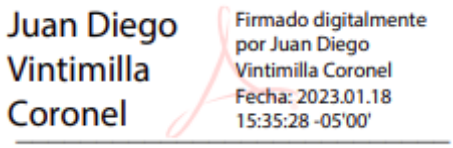
BLADIMIR ENRIQUE URGILES RODRIGUEZ

Ing. Oswaldo Geovanny Martínez Guashima, M. Sc.
PRESIDENTE

Riobamba, enero 2023

DERECHOS INTELECTUALES

Yo, Juan Diego Vintimilla Coronel, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.



Juan Diego Vintimilla Coronel
0301226031

DECLARACIÓN DE AUTENTICIDAD

Yo, Juan Diego Vintimilla Coronel, declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo,** es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Juan Diego Vintimilla Coronel
Firmado digitalmente por Juan Diego Vintimilla Coronel
Fecha: 2023.01.18 15:35:28 -05'00'

Juan Diego Vintimilla Coronel
0301226031

TABLA DE CONTENIDO

ÌNDICE DE FIGURAS

RESUMEN

El objetivo fue mejorar la integridad de los sistemas académicos basados en la web, mediante la aplicación de la esteganografía, caso práctico https://sisepec.espoch.edu.ec. 2021. Se utilizó la esteganografía como un método para mitigar la vulnerabilidad de clonación de sitios web, en la cual se esconde el código que valida el dominio del sitio web, desencadenando varios métodos de autenticación y anunciando al usuario que se encuentra navegando por un sitio web verídico. Del mismo modo, en caso de que el sitio web haya sido clonado y levantado en otro dominio, el código oculto ejecuta un script que anuncia al administrador que existe una vulnerabilidad detectada por medio de un correo electrónico. La metodología utilizada durante un ataque de tipo phishing para sustraer información sensible, a la vez que se realiza un análisis comparativo de un sitio web académico, demostrando que es posible mejorar uno de los pilares fundamentales de la seguridad de la información como es la integridad, por medio de la esteganografía; se realizó luego de la clonación del sitio web, la implementación de doble autenticación y finalmente la inclusión del código esteganográfico. Durante la comparativa realizada del ambiente actual vs el escenario plasmado con la técnica de esteganografía, se puede evidenciar una mejora significativa con respecto a la integridad del sitio web y la mitigación de la vulnerabilidad presentada en las páginas de inicio de sesión. La investigación concluye con recomendaciones que refieren a la implementación de la técnica esteganográfica, así como la versión del código usado en el desarrollo de las páginas de inicio de sesión.

Palabras Clave: ATAQUE, ESTEGANOGRAFÍA, CIBERNÉTICO, INFORMACIÓN, PHISHING, RANSOMWARE

SUMARY

The objective was to improve the integrity of web-based academic systems, through the application of steganography, practical case https://sisepec.espoch.edu.ec. 2021. Steganography was used as a method to mitigate website cloning vulnerability, in which code that validates the website's domain is hidden, triggering various authentication methods and announcing to the user that they are browsing a site true website. In the same way, in case the website has been cloned and built on another domain, the hidden code executes a script that announces to the administrator that there is a vulnerability detected by means of an email. The methodology used during a phishing attack to steal sensitive information, while performing a comparative analysis of an academic website, demonstrating that it is possible to improve one of the fundamental pillars of information security such as integrity, through steganography; it was carried out after the cloning of the website, the implementation of double authentication and finally the inclusion of the steganographic code. During the comparison made of the current environment vs. the scenario embodied with the steganography technique, a significant improvement can be seen with respect to the integrity of the website and the mitigation of the vulnerability presented in the login pages. The investigation concludes with recommendations that refer to the implementation of the steganographic technique, as well as the version of the code used in the development of the login pages.

Keywords: ATTACK, STEGANOGRAPHY, CYBER, INFORMATION, PHISHING, RANSOMWARE

CAPÍTULO I

1- INTRODUCCIÓN

1.1.- Planteamiento del problema

1.1.1 Situación problemática

La absurda evolución de la tecnología en los últimos años ha permitido que los procesos cotidianos puedan ser automatizados, facilitando las relaciones financieras, comerciales, educativas e interpersonales y convirtiéndolos en eficaces y constantes gestiones de datos. Pero esta evolución no solo ha resultado en cosas buenas, sino que también ha permitido que las amenazas informáticas tomen una activa participación en estos procesos, poniendo en riesgo los avances positivos antes mencionados (Posada, 2017).

"Su mayor riesgo podría ser la gente en la que más confía" (Institute T. P., 2018).

De forma errónea y guiados por películas y ciencia ficción, se cree que las amenazas externas son más peligrosas que las internas. Este pensamiento no puede estar más alejado de la realidad, ya que los ataques desde el exterior dependen en gran medida de la explotación de vulnerabilidades conocidas en software, lo que supone un impedimento extra de parte del atacante para cumplir su objetivo. Al contrario, las amenazas internas pueden ocurrir incluso cuando la seguridad de una organización está implementada y orientada en marcos de referencia (ISO, MAGERIT) y son más difíciles de controlar, siendo unas de las mayores amenazas de seguridad.

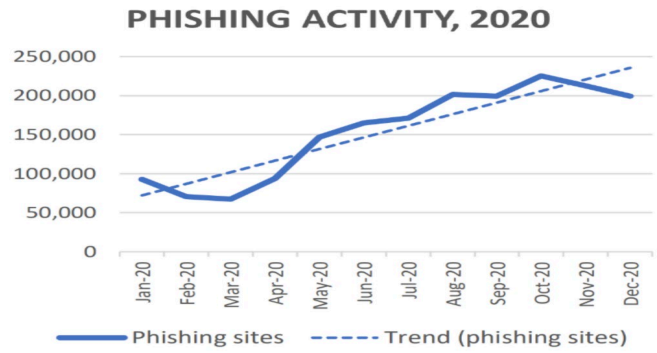


Figura 1-1 Ataques Phishing en el 2020. Fuente (APWG, 2021)

Según APWG (APWG, 2021) la cantidad de ataques phishing (técnica de la pesca) crece continuamente, llegando a su punto más alto en octubre del 2020 con 225.304 ataques exitosos. Entre los principales datos referentes a la amenaza phishing a nivel mundial, se pueden apreciar las siguientes cifras:

Un total del 84% de los profesionales estadounidenses, han confirmado haber sufrido un tipo de amenaza de seguridad, colocando al phishing y ransomware entre los principales ataques con mayor ocurrencia (Cuadernos de Seguridad, 2021). En el informe final manifiesta que los ataques más comunes son los ransomware (secuestro de información) con un 53% y el phishing con un 49% de efectividad.

Figura 1-2 Tipos de amenazas

- En Latinoamérica se ha registrado cerca del 31% de empresas que han sido posible blancos de los ciberataques en el 2020, como consecuencia de la pandemia generada por la COVID-19, siendo la principal amenaza los ataques relacionados al phishing (Microsoft, 2021).

Figura 1-3 Estado del Riesgo Cibernético en Latinoamérica en Tiempos del COVID-19, Fuente: (Microsoft, 2021)

- De acuerdo con las amenazas cibernéticas, relacionadas con la COVID-19, afectaron a unos países en mayor medida que otros. De acuerdo con el informe presentado respecto a la primera mitad del año 2021 manifiesta:

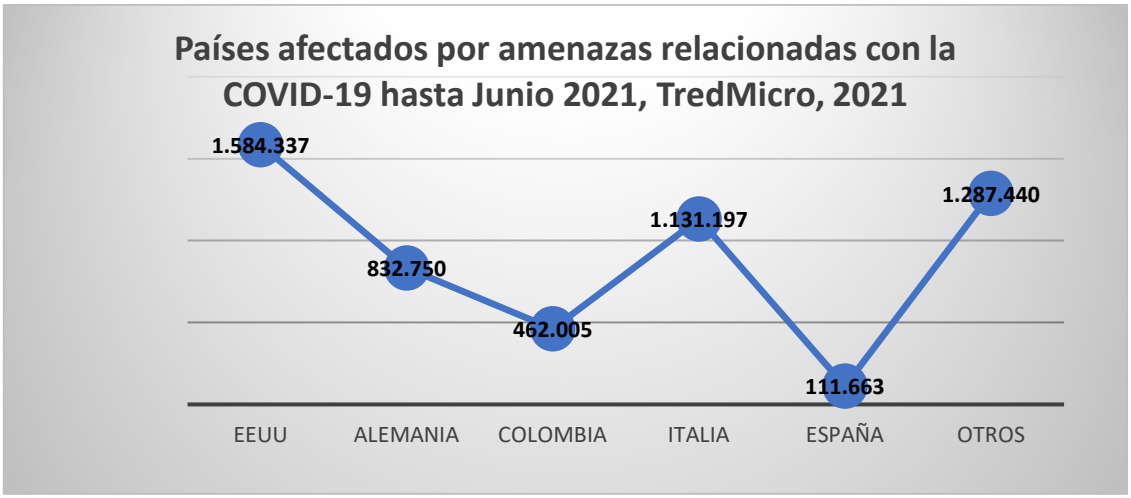


Figura 1-4 Países afectados por amenazas relacionadas con la COVID-19 primera mitad 2021, TrendMIcro, 2021

- Kaspersky, en su informe Panorama de Amenazas en América Latina, ha alertado sobre el incremento del 24% de ataques cibernéticos en los primeros 8 meses del año 2021, a comparación con el año 2020. Entre los países más vulnerables a los ciberataques, se encuentra liderando Ecuador con un 75% de incremento, seguido por Perú, Panamá, Guatemala y Venezuela.

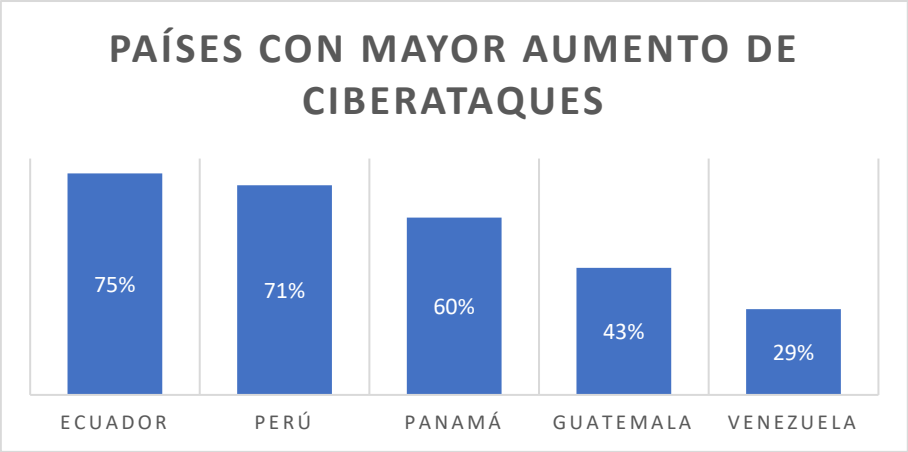


Figura 1-5 Países con mayor aumento de ciberataques. Fuente: (Diazgranados, 2021)

- Durante el año 2020, los sistemas de detección de phishing neutralizaron 434,898.635 amenazas; sin embargo, este valor es menor a la cantidad de phishing detectados en el año 2019 (Diazgranados, 2021).

1.1.2.- Formulación del problema

¿La aplicación de la esteganografía puede mejorar la integridad de los sistemas académicos basados en la web, caso práctico https://sisepec.espoch.edu.ec, 2022?

1.1.3.- Sistematización del problema

¿El uso de la tecnología de la información y comunicación (TIC) se incrementó desde la pandemia provocada por la COVID-19?

¿Los usuarios se convirtieron en potenciales víctimas de los ciberataques?

¿La amenaza de ser víctima de Phishing sigue latente en sitios web académicos?

¿Los sitios web son vulnerables ante programas de clonación?

1.2 Justificación de la investigación

En el ámbito de la seguridad de la información, se han realizado modelos y marcos de referencia para evitar los ataques cibernéticos que puedan violentar la integridad, disponibilidad y confiabilidad de la información de una empresa; pero a pesar de ello, estos marcos tienden a

indicar la realidad, el nivel de seguridad de la información será directamente proporcional a la concientización al usuario. Se le considera el mayor riesgo de seguridad al usuario, puesto que los malos hábitos y la falta de buenas prácticas, provocan un incremento en el riesgo para que un ataque se consolide.

Entre las principales estrategias usadas para el primer acercamiento con la víctima es la conocida "Ingeniería Social", conceptualizada como el arte de engañar al usuario, para que éste le entregue información sensible sin ser descubierto. Actualmente en la sociedad, no existe una sola persona que no haya experimentado o haya sido víctima de esta técnica sin siquiera conocerla, solo por el afán de conocer información de otra persona.

Muchos lo realizan al observar notificaciones en los teléfonos de sus amigos, o escuchar la llamada porque el volumen está muy alto, o simplemente por observar fotografías posteadas en las redes sociales.

Este actuar es un claro ejemplo de la necesidad por conocer lo que sucede en la vida de sus semejantes. Entre las principales herramientas que utilizan los hackers para robar la identidad de un usuario, está la conocida técnica del phishing. El uso de esta técnica casi se a convertido en una rutina para ciertos conocedores del hacking, a tal punto que se han desarrollado diversos sitios, aplicaciones y técnicas que guían a un usuario a realizar la clonación de sitios web con el objetivo de generar ataques phishing. Las instituciones de educación superior no son la excepción en cuanto a ataques se refieren, ya que también han sido víctimas de hackers que han logrado vulnerar la seguridad de sus escuelas virtuales desde el "eslabón más débil", el usuario.

Simultáneamente que incrementa el nivel de conocimiento de los hackers, al mismo tiempo incrementan las técnicas de defensa para los sitios web. La defensa contra los hackers radica en no descubrimiento de contraseñas o, demorar el mayor tiempo posible de averiguar la contraseña de acceso, a tal punto que la información que esta guardaba simplemente sea inútil. Esta segunda

opción de seguridad, cada día se convierte en algo muy difícil de cumplir, ya que la velocidad de procesamiento de las últimas tecnologías ha empezado a realizar los ataques en menor tiempo, lo que implica que el tiempo ya no es un factor en el que se pueda confiar como una medida de seguridad.

1.3 Objetivos de la investigación

1.3.1.- Objetivo General

Mejorar la integridad de los sistemas académicos basados en la web, mediante la aplicación de la esteganografía, caso práctico https://sisepec.espoch.edu.ec. 2021.

1.3.2.- Objetivos Específicos

- Realizar la clonación del sitio web usado como caso práctico por medio de herramientas open source.
- Analizar el método de cifrado de información LSB en imágenes de diferentes tamaños por pixeles.
- Implementación de código esteganográfico en imagen en ambiente de desarrollo del sitio web clonado.
- Comparar el nivel de integridad del sitio web https://sisepec.espoch.edu.ec, 2021 antes y después de la aplicación de la técnica esteganográfica.

1.4.- Hipótesis

La aplicación de la esteganografía en sistemas académicos basados en la web, SI mejora la integridad de la información, caso práctico https://sisepec.espoch.edu.ec.

CAPÍTULO II

2.- MARCO TEÓRICO

2.1.- Antecedentes del problema

Para el desarrollo de la presente investigación, se toma como referencia el análisis realizado por trabajos anteriores en los que intervienen la esteganografía como un método de autenticidad (Jaimes Iguavita, 2018) para el inicio de sesión a plataformas de e-learning, tales como Moodle, Chamilo, Open edX, etc., así como el uso de la técnica para ocultar información dentro de multimedia que valide la originalidad del medio desde el cual se está reproduciendo.

El uso de credenciales que permitan la autenticidad del usuario es una forma muy común de inicio de sesión a las plataformas, dando como resultado la responsabilidad entera al usuario, para la generación de claves seguras. La cultura de seguridad de la información en los usuarios es muy escasa, a tal punto que no tienen conocimiento de los parámetros generales que permiten tener una contraseña segura, por el contrario, usan información personal como cumpleaños, fechas de nacimiento, aniversarios, nombres de hijos o mascotas, siendo vulnerables a ataques de diccionario o comúnmente llamados fuerza bruta.

Las contraseñas cumplen el objetivo de preservar la información evitando el conocimiento y acceso a personas no autorizadas, tomando como principio el tiempo de validez de esta. Esta práctica ha sido eficiente hasta los últimos años, pues la velocidad de procesamiento de los computadores para realizar ataques de diccionario era relativamente lenta, llegando a descubrir una clave luego de que la información ya no era válida. Sin embargo, el avance de la tecnología ha permitido que los procesadores sean tan rápidos como los llamados procesadores quantum de generaciones anteriores, haciendo que la técnica del uso de contraseñas seguras sea poco eficientes y más vulnerables a ataques cibernéticos.

Otra técnica usada por los atacantes cibernéticos, son los conocidos phishing, donde el atacante se aproveche del desconocimiento del usuario en el ámbito de la informática, haciendo llegar un correo electrónico el cual le indica que existe un problema en su perfil (información referente a calificaciones, servicios contratados, compras realizadas con su cuenta, etc.) y que necesita ser resuelto lo antes posible.

Le entrega un enlace el cual le direcciona al sitio web (clonado - fraudulento) específicamente al de inicio de sesión. El usuario sin percatarse de que está siendo víctima de un ataque cibernético, por no tener los conocimientos necesarios a reconocimiento de una página fraudulenta, simplemente ingresa sus credenciales y espera hasta que esta página le muestre su perfil para revisar los inconvenientes indicados en el correo electrónico recibido, sin percatarse que envió sus credenciales correctas de inicio de sesión al atacante mediante la página fraudulenta. (Belcic, 2020)

Esta práctica ha sido realizada por muchos hackers a nivel mundial, enviando correos electrónicos (spam) a empresas e instituciones con el objetivo de que usuarios caigan en su red y envíen información personal que les permitirán realizar un ataque phishing de acuerdo con un pequeño estudio (ingeniera social) aplicado.

La mayoría de las técnicas y procesos que se implementan en un sitio web, tienen como objetivo mejorar la disponibilidad o la confidencialidad de esta, quedando el tercer pilar fundamental de la seguridad de la información (integridad), completamente vulnerable y sin un mayor esfuerzo de evitar que sea afectada.

La facilidad de clonar una página web y permitirle levantar a un servidor en cuestión de horas, ha facilitado mucho a los atacantes el desarrollo de realizar phishing; por no considerar una seguridad más eficiente contra esta gran vulnerabilidad latente en todas las páginas de internet.

En la actualidad, existe poca aplicabilidad de la técnica de esteganografía en los sitios web, siendo un campo muy poco explotado de la seguridad como medida de prevención ante ataques cibernéticos, pero muy utilizada por ciberdelincuentes como herramienta para cumplimiento de sus fines.

2.2.- Bases Teóricas

2.2.1.- Seguridad de la Información

De acuerdo con (Pacheco, 2016), "La información es el activo más preciado que tienen las organizaciones". La palabra "Seguridad" quiere decir ausencia de peligro o de riesgo. En el mundo de las ISO, seguridad de la información significa preservación de la integridad disponibilidad y confidencialidad de la información. ("Seguridad de la información, vulnerabilidades y riesgos ... - Isbel") ("Seguridad de la información, vulnerabilidades y riesgos ... - Isbel").

Figura 2-1 Pilares de la seguridad de la información (Castro, 2019)

Hoy en día la información corporativa es uno de los activos más importantes que maneja una empresa, las cuales han empezado a optar técnicas, procesos y sistemas que permitan garantizar la seguridad contra ataques cibernéticos. La Seguridad de la información se fundamenta en la necesidad de los usuarios para obtener, disponer o compartir la información de una manera eficiente, con integridad en los datos y con la certeza de que solo los usuarios autorizados la puedan conocer (Castro, 2019).

Si bien es cierto, en la actualidad existen tecnologías que permiten la detección de phishing, por medio de análisis realizado a los datos recibidos, los dominios desde donde se reciben los correos y el uso de listas negras. El aprendizaje automático ha evolucionado en gran medida, analizando rasgos determinantes en el reconocimiento de un ataque cibernético, reconociendo el mismo y aplicando protocolos que impidan el progreso del robo, suplantación de identidad, secuestro o modificación de información sensible. Los rasgos, sin importar en el ambiente en que se desarrollen, pueden llegar a ser extraídos de fuentes diversas como la URL, contenido compartido mediante correo electrónico o una red social, el certificado digital, etc. (Hernández Dominguez, 2021). Principales mecanismos para el enfrentamiento al phishing en las redes de datos). (“Principales mecanismos para el enfrentamiento al phishing en las redes ...”) (“Principales mecanismos para el enfrentamiento al phishing en las redes ...”)

A continuación, detallo más a fondo sobre los tres pilares de la seguridad de la información.

2.2.1.1 Confidencialidad. Este pilar tiene como finalidad asegurar que exclusivamente el usuario autorizado tenga acceso a la información de acuerdo con su rol o perfil. De esta manera se garantiza que los funcionarios hagan un buen uso de esta información y la puedan procesar mediante sus actividades diarias, sin entorpecer a otras áreas de la empresa o compañía ni arriesgando a que la información sea mal utilizada por usuarios no autorizados. (Romero, y otros, 2018).

Para mantener la confidencialidad de los datos, se optan medidas como:

- Autenticación de usuarios para conocer la actividad realizada por un usuario sobre la información a la cual tiene acceso.
- El cifrado de información agrega un nivel de seguridad al acceso de esta, de tal manera que únicamente el usuario con el perfil adecuado pueda tener acceso a los datos luego de un proceso de descifrado mediante el uso de llaves públicas y privadas, mensajes ocultos o contraseñas en los ficheros (Romero, y otros, 2018).

2.2.1.2 Disponibilidad. Este pilar de la seguridad, como su nombre lo indica, hace referencia a que la información debe estar al alcance del usuario cada que éste lo requiera. Al igual que los servicios, la información es de vital importancia para tomar decisiones que puedan afectar los procesos del negocio, por lo tanto, esta debe estar al alcance en el tiempo requerido y que su acceso sea de forma fácil para el usuario y siempre bajo la normativa de seguridad, respetando las políticas que refieran el uso de esta. (ISOTools, 2021)

La disponibilidad de la información no solo hace referencia a la data en la que exista un proceso de modificación o que en ese momento se encuentre en producción, sino que también hace referencia a la disponibilidad de los medios de almacenamiento, así como los respaldos que se pudieran realizar a través del tiempo. Se debe entonces, tomar en cuenta lo siguiente:

- Mantener una información disponible en líneas de tiempo.
- Preocuparse por el levantamiento de la información en canales alternos para respetar el principio de alta disponibilidad.
- Preparar técnicas, adquirir hardware o implementar servicios que permitan proteger esta información de ataques cibernéticos.

2.2.1.3 Integridad. Quizás, el pilar más vulnerable en la actualidad y medio por el cual, se puede derrumbar la seguridad de la información. La integridad se refiere a la presentación de la información sin que esta se haya visto afectada en su forma o fondo.

De tal manera, la responsabilidad de este pilar fundamental de la información, sobre ella, es presentar la información sin modificación o alteración, bien sea voluntaria o involuntaria. (ISOTools, 2021)

Mientras los desarrolladores, generan códigos para facilitar el uso de la tecnología y realizar procesos en menor tiempo, la delincuencia cibernética se aprovecha de estos códigos para proceder con sus intenciones maliciosas y con fines lucrativas.

2.2.2 Riesgo Informático:

"El riesgo se puede definir como un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se cuentan expuestos, así como su probabilidad de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo." (Pilar, 2018)

Figura 2-2 Riesgo Informático. Fuente: (INCIBE, 2017)

Para tener un mejor entendimiento de lo que es un Riesgo Informático, se debe conocer el significado de 2 pilares que lo conforman.

2.2.2.1.- Vulnerabilidad. Se le otorga el nombre de vulnerabilidad a la debilidad o defecto conocido, que se pueda prestar como una puerta para que un atacante cumpla su propósito. Cuando en la actualidad, los dispositivos como tabletas, portátiles, celulares inteligentes aparatos electrónicos deben mantener una comunicación constante entre sí, es casi imposible que una aplicación sea desarrollada con un 100% de efectividad y que no disponga de vulnerabilidades. (PMG, 2015)

2.2.2.1.1.- Tipos de vulnerabilidades. Cuando hablamos de ciberseguridad siempre escuchamos de las técnicas para explotar vulnerabilidades, sin embargo, pocas veces se escucha un análisis de que son las vulnerabilidades y por qué existen.

Formalmente existen 3 tipos de vulnerabilidades, por diseño, por implementación y por configuración:

- Las vulnerabilidades por diseño, como su nombre lo indica, aparecen en la etapa del diseño de un sistema, software o producto en general. Dicho producto no es inseguro porque el desarrollador se equivocó, o porque los componentes están errados, simplemente fue el diseño para hacer lo incorrecto, hablando desde un enfoque de seguridad. Generalmente el problema empieza desde los requerimientos, que son una lista de objetivos que un producto debe cumplir, sin embargo, muchos de ellos son pensados para las necesidades manifestadas, invalidar otros posibles enfoques o usos que un cliente podría dar. Por suponer un escenario, surge la necesidad de que un usuario levante sus credenciales a un sitio web para acceder a un servicio, pero si el texto viaja en texto plano, entonces surge una vulnerabilidad por diseño. (PMG, 2015)
- Las vulnerabilidades por implementación surgen debido a que la persona que recibe el diseño para implementar dicho producto, lo hace a través de malas prácticas. Por ejemplo, si en el requerimiento es que el usuario ingrese su nombre, pero la persona que lo implementa no valida una cantidad de caracteres para ese campo, o el tipo de caracteres que el usuario pueda ingresar, esto podría ocasionar una vulnerabilidad por implementación. (PMG, 2015)
- Finalmente, las vulnerabilidades por configuración surgen por una mala configuración del producto. El más común es dejar las contraseñas predefinidas. Por diseño el producto es seguro, pero la persona que implemento dicho diseño lo hizo siguiendo las mejores prácticas, pero cuando se adquiere el producto y no se cambia las credenciales de fábrica, automáticamente el riesgo de que un atacante acceda a dicho producto usando las credenciales predefinidas, incrementan. (PMG, 2015)

2.2.2.2 Amenaza. Una amenaza es todo elemento o acción, capaz de afectar, dañar o atentar en contra de la seguridad. Estas pueden surgir desde cualquier lado, momento o circunstancia, pero algo que se sabe algo siempre, es que para que una amenaza existe, antes debió existir una vulnerabilidad. (PMG, 2015)

Una definición menos teórica puede ser, la posibilidad de que suceda una acción o evento y que este pueda producir un daño o un comportamiento no esperado. Algo importante de las amenazas es siempre clasificarlas. Aunque exciten clasificaciones generales, la mayoría se hacen dependiendo de la industria o del giro de la empresa y puede haber ciertos cambios. No todas las empresas tienen los mismos empleados, departamentos, métodos de pago, procesos de inicio de sesión o métodos de registro. Estos son solo algunos de los factores que hacen que las clasificaciones sean diferentes por empresa.

Una clasificación general de amenazas es la de los tipos. Existen los tipos intencionales y no intencionales. Esta clasificación es la más genérica y permite separar de una forma sencilla e importante, el tipo de amenaza a la que nos podemos encontrar.

- **Intencionales:** Es cuando la intención quiere producir un daño, este tipo de daño puede ser de varias formas: conocimiento, eliminación o modificación de información que permitan accesos no autorizados o dar privilegios a perfiles a quienes no deben.

- **No intencionales:** Es cuando por circunstancias: omisiones, falta de conocimiento o preparación, pueden producir un daño. Uno de los tipos no intencionales más famosos son los daños por fenómenos naturales, ya que no existe una intención, pero la circunstancia ha provocado la pérdida parcial o total de la información almacenada en un computador que estuvo presente en el fenómeno natural.

2.2.3 Criptografía.

Se puede considerar la criptografía como una rama de la matemática, y en la actualidad de la informática y telemática, ya que hace uso de métodos y técnicas con el objetivo principal de cifrar y, por lo tanto, proteger, un mensaje o archivo por medio de un algoritmo usando una o varias claves. Esto da lugar a diferentes tipos de cifrados denominados criptosistemas que nos permiten asegurar, al menos, 3 de los 4 aspectos básicos de la seguridad informática. (Henry González, 2018)

La confidencialidad que es asegurar que la comunicación sea visible solo para el emisor y el receptor, la integridad asegura que el mensaje no haya sido modificado por terceras personas durante el transito; y, el no repudio que es evitar que la persona que envía el mensaje niegue haberlo hecho.

Los objetivos fundamentales de un sistema criptográfico son: Garantizar el secreto en la comunicación entre las partes, asegurar que la información que se envía es auténtica en un doble sentido, impedir que el contenido del mensaje enviado sea modificado en el tránsito de esta.

Aunque la definición de criptografía en la Real Academia es: el arte de escribir con clave secreta o de un modo enigmático; en el ámbito informático se conoce a la palabra criptografía, proveniente del griego krytpos (oculto) y gráphein (escribir), como el estudio de los principios y mecanismos necesarios para establecer procesos de cifrado y descifrado y generación de claves necesarios para ellos. (Española, 2019)

La criptografía permite almacenar información sensible o transmitirla a través de redes inseguras (internet), de modo que nadie pueda acceder a ella sin ser autorizado. Un concepto muy relacionado es el criptoanálisis, que proviene del griego kryptos (oculto) y analyén (desatar). Es el estudio de los principios y mecanismos necesarios para descifrar mensajes sin conocer las claves utilizadas al momento del cifrado.

Durante las guerras del imperio Romano, César utilizaba un cifrado en sus mensajes para protegerlos de caer en manos enemigas y que éstos conozcan sus planes de batallas. Su método fue trasladar cada letra del alfabeto 13 espacios en el mismo, dando lugar a un método de cifrado básico pero eficiente.

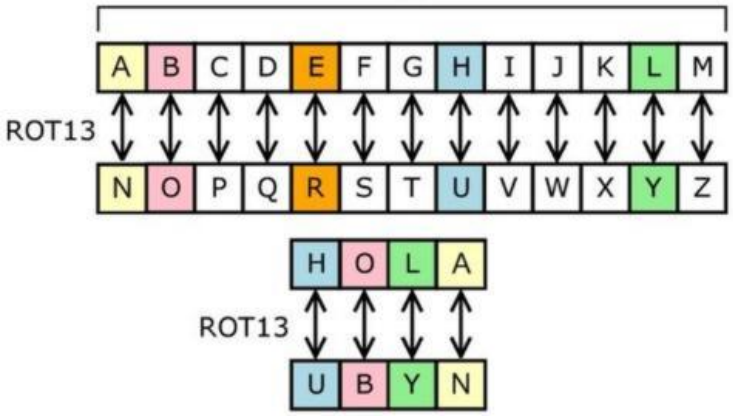


Figura 2-3 Cifrado Cesar. Fuente: (NEOTEO, 2010)

2.2.4 Tipos de cifrado

Cuando navegamos por internet, es común ver un pequeño candado que acompaña al nombre del sitio web en la barra de navegación del explorador, este pequeño candado indica que la página dispone de un método de cifrado de información y que es una página segura. Esta tecnología también se puede evidenciar en los diferentes aplicativos de mensajería instantánea como WhatsApp, Telegram, Messenger, entre otros.

Se puede explicar el cifrado como guardar la información en una libreta que contenga un candado o cerradura y que solo puede ser abierto por la persona que dispone de la llave. Del mismo modo funciona el cifrado de información en la tecnología, en donde el computador solicitante envía la información de lo que requiere y ésta se encuentra cifrada, de tal manera que únicamente el computador que dispone de la llave puede entender el mensaje en claro, dejando de lado a cualquier atacante que se puede pasar por servidor o cliente en una red enlazada.

Aunque esta información no sea nueva para la mayoría de los usuarios, es verdad que no conocen los tipos de cifrado que existen en la actualidad, como son los simétricos y los asimétricos.

2.2.4.1.- Cifrado Simétrico. "Es un tipo de cifrado en el que solo se utiliza una clave simétrica secreta para cifrar el texto sin formato y descifrar el texto cifrado." (“¿Qué es el cifrado? Definición de cifrado de datos | IBM”) (“¿Qué es el cifrado? Definición de cifrado de datos | IBM”)

Los métodos más comunes de cifrado simétrico son:

- Estándares de cifrado de datos (DES). Es un algoritmo de cifrado de bloques de cifrado de bajo nivel que convierte texto sin formato en bloques de 64 bits y los convierte en texto cifrado utilizando claves de 48 bits. (“¿Qué es el cifrado? Definición de cifrado de datos | IBM”) (“¿Qué es el cifrado? Definición de cifrado de datos | IBM”) (IBM, 2019)
- Blowfish. Este algoritmo consta de un bloque de código con un tamaño de 64 bits y claves de longitud variable, superiores a los 448 bits. (““Esteganografía” - Deloitte Argentina”) (““Esteganografía” - Deloitte Argentina”) Es utilizado en una gran cantidad de paquetes software incluyendo Nautilus y PGPfone.
- IDEA. Es un algoritmo que utiliza una clave de 128 bits, es considerado un algoritmo seguro y es uno de los mejores de conocimiento público. (““Esteganografía” - Deloitte Argentina”) (““Esteganografía” - Deloitte Argentina”) (IBM, 2019)

2.2.4.2.- Cifrado Asimétrico. "También conocido como criptografía de clave pública, cifra y descifra los datos utilizando dos claves asimétricas criptográficas independientes." (“¿Qué es el cifrado? Definición de cifrado de datos | IBM”) (“¿Qué es el cifrado? Definición de cifrado de datos | IBM”) Estas dos claves se conocen como “llave pública” y “llave privada”

Los métodos más comunes de cifrado asimétrico son:

- RSA. Que lleva el nombre de los científicos informáticos Ron Rivest, Adi Shamir y Leonard Adleman, es un algoritmo popular que se utiliza para cifrar datos con una llave

pública y descifrarlos con una llave privada para una transmisión segura de datos. (“¿Qué es el cifrado? Definición de cifrado de datos | IBM”) (“¿Qué es el cifrado? Definición de cifrado de datos | IBM”) (IBM, 2019)

- Diffie-Hellman. Es un algoritmo de clave pública utilizado generalmente para realizar intercambios de claves. "Es considerado seguro ya que utiliza claves largas y generadores propios." (““Esteganografía” - Deloitte Argentina”) (““Esteganografía” - Deloitte Argentina”) (IBM, 2019)
- Criptosistemas de clave pública de curva elíptica. Es una especialidad que está surgiendo en la actualidad. Son de ejecución lenta, pero pueden ser ejecutados por computadoras modernas. Son considerados suficientemente seguros, pero no fueron examinados de la misma manera que por ejemplo el algoritmo RSA. (IBM, 2019)

2.2.5 Phishing

El phishing ha manifestado un incremento significativo en el mundo del ciberdelito, tomando como reseña histórica, en 1987 en la conferencia INTEREX, un documento presentado por Jerry Felix y Chris Hauck, titulado “Seguridad del sistema: la perspectiva de un hacker” hubo una discusión de un método para que un tercer individuo cibernético imite un servicio confiable. En ese momento se generaba lo que hoy se conoce como el ataque MITM (man in the middle) o el hombre del medio, el cual consiste en utilizar un dispositivo que permita interactuar con el servidor haciéndose pasar como el cliente que emite el requerimiento de información; y al mismo tiempo, interactuando como servidor con el cliente original y entregando la información requerida luego de haber sido analizada. (Castillo, 2021).

En los años 90 se registraron los primeros ataques phishing, concretamente hablado del caso AOL (América Online), los atacantes utilizaron la función Instant Messenger de AOL para enviar mensajes a los usuarios indicando irregularidades en sus cuentas, por supuesto haciéndose pasar como parte del equipo técnico de AOL. Una vez establecido el contacto con la víctima, usaban

frases como “verificando cuenta” o “confirmando información de factura” con el objetivo de hacerse de información privilegiada (Wesner, 2020).

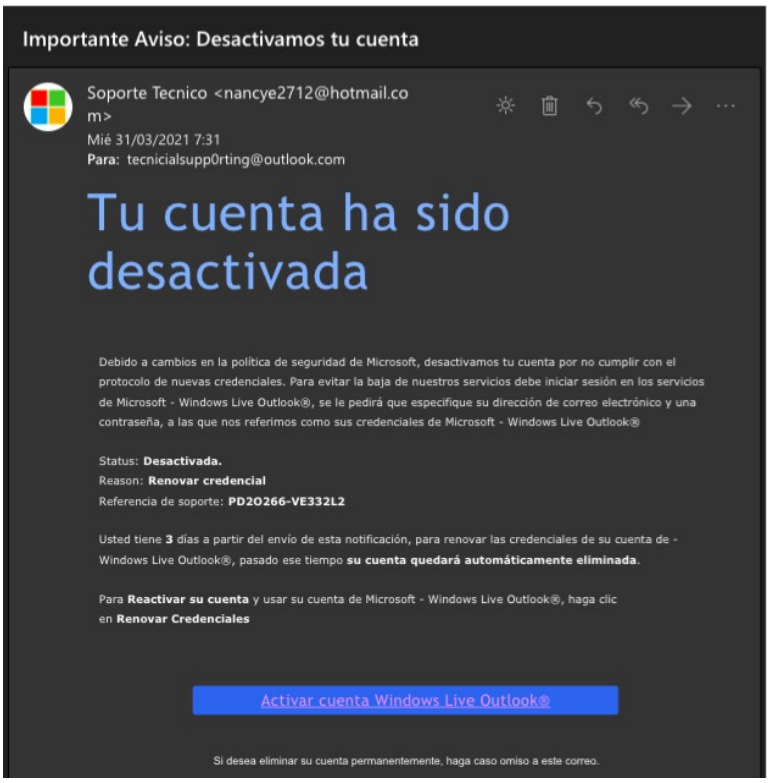
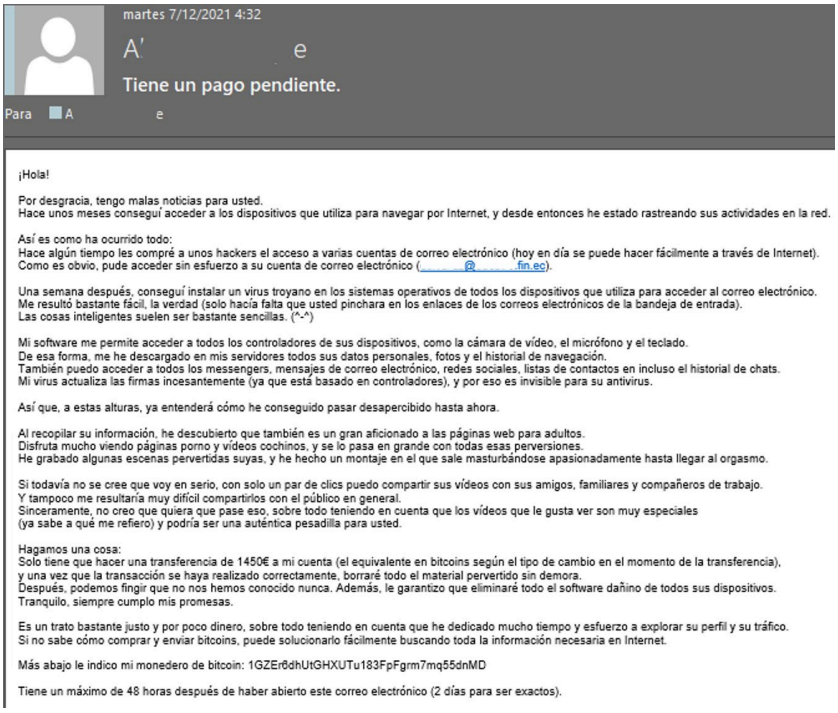


Figura 2-4 Ataque Phishing AOL (Castillo, 2021).

Desde luego, estos primeros pasos de ciberdelincuencia darían lugar a una oleada de ideas para obtener información de usuarios y utilizarlos a conveniencia, desde la creación de dominios de nombre similar, hasta la creación de sitios web con gran similitud a los originales para que el usuario no advirtiera que es víctima de un ataque cibernético y que conllevaría a grandes pérdidas económicas para las víctimas, pues los ataques se enfocarían hacia cuentas bancarias internacionales, cuando la seguridad era mínima en las entidades bancarias que ofertaban estos servicios.

En la actualidad, los delincuentes utilizan la extorsión como un método para cumplir el phishing, generalmente haciendo alusión a actos obscenos que puedan deteriorar la imagen de la víctima ante la sociedad, o culpándolo de crímenes no cometidos. Estos medios de extorsión siempre han estado latentes en la sociedad, pero ahora han sido llevados al mundo tecnológico como una herramienta adicional para incrementar las posibilidades de éxito de los ataques.

A continuación, detallo un ataque phishing a una entidad financiera reconocida a nivel nacional y con fecha actualizada. En la imagen se puede apreciar como el hacker intenta persuadir al usuario indicando que se ha ingresado en cada uno de los dispositivos que utiliza y que lleva un control de la actividad que realiza en cada uno de ellos. El atacante mantiene una presión sobre el usuario haciendo alusión a que ha utilizado la cámara de su dispositivo móvil para grabarlo mientras este, realizaba actos obscenos y que puede llegar a causarle una mala reputación entre sus amigos y familiares, si es que se llegaran a enterar. Al final, le solicita que realice una transferencia de un valor elevado mediante criptomonedas, pues como es de conocimiento mundial, las criptomonedas no pueden ser rastreadas al ser un tipo de valor monetario que solo sirve en el ciberespacio, pero que puede ser cambiado por dinero real en cualquier denominación.


martes 7/12/2021 4:32

A' e

Tiene un pago pendiente.

Para A e

¡Hola!

Por desgracia, tengo malas noticias para usted.
Hace unos meses conseguí acceder a los dispositivos que utiliza para navegar por Internet, y desde entonces he estado rastreando sus actividades en la red.

Así es como ha ocurrido todo:
Hace algún tiempo les compré a unos hackers el acceso a varias cuentas de correo electrónico (hoy en día se puede hacer fácilmente a través de Internet).
Como es obvio, pude acceder sin esfuerzo a su cuenta de correo electrónico (@ .fin.ec).

Una semana después, conseguí instalar un virus troyano en los sistemas operativos de todos los dispositivos que utiliza para acceder al correo electrónico.
Me resultó bastante fácil, la verdad (solo hacía falta que usted pinchara en los enlaces de los correos electrónicos de la bandeja de entrada).
Las cosas inteligentes suelen ser bastante sencillas. (^-^)

Mi software me permite acceder a todos los controladores de sus dispositivos, como la cámara de vídeo, el micrófono y el teclado.
De esa forma, me he descargado en mis servidores todos sus datos personales, fotos y el historial de navegación.
También puedo acceder a todos los messengers, mensajes de correo electrónico, redes sociales, listas de contactos en incluso el historial de chats.
Mi virus actualiza las firmas incesantemente (ya que está basado en controladores), y por eso es invisible para su antivirus.

Así que, a estas alturas, ya entenderá cómo he conseguido pasar desapercibido hasta ahora.

Al recopilar su información, he descubierto que también es un gran aficionado a las páginas web para adultos.
Disfruta mucho viendo páginas porno y vídeos cochinos, y se lo pasa en grande con todas esas perversiones.
He grabado algunas escenas pervertidas suyas, y he hecho un montaje en el que sale masturbándose apasionadamente hasta llegar al orgasmo.

Si todavía no se cree que voy en serio, con solo un par de clics puedo compartir sus vídeos con sus amigos, familiares y compañeros de trabajo.
Y tampoco me resultaría muy difícil compartirlos con el público en general.
Sinceramente, no creo que quiera que pase eso, sobre todo teniendo en cuenta que los vídeos que le gusta ver son muy especiales
(ya sabe a qué me refiero) y podría ser una auténtica pesadilla para usted.

Hagamos una cosa:
Solo tiene que hacer una transferencia de 1450€ a mi cuenta (el equivalente en bitcoins según el tipo de cambio en el momento de la transferencia),
y una vez que la transacción se haya realizado correctamente, borraré todo el material pervertido sin demora.
Después, podemos fingir que no nos hemos conocido nunca. Además, le garantizo que eliminaré todo el software dañino de todos sus dispositivos.
Tranquilo, siempre cumplo mis promesas.

Es un trato bastante justo y por poco dinero, sobre todo teniendo en cuenta que he dedicado mucho tiempo y esfuerzo a explorar su perfil y su tráfico.
Si no sabe cómo comprar y enviar bitcoins, puede solucionarlo fácilmente buscando toda la información necesaria en Internet.

Más abajo le indico mi monedero de bitcoin: 1GZEr6dhUtGHXUTu183FpFgrm7mq55dnMD

Tiene un máximo de 48 horas después de haber abierto este correo electrónico (2 días para ser exactos).

Figura 2-5 Ataque Phishing (Propio, 2021)

Las legislaciones estatales, a nivel mundial, también han tenido que evolucionar en conjunto con la tecnología para mantener bajo control y normar las actividades que se realicen en el ciberespacio. De esta manera, a nivel mundial han empezado a reconocer a los actos delictivos cometidos por medios tecnológicos, como parte activa de su derecho penal, y otorgando el nombre de ciberdelito o ciberfraude. “El ciberfraude sigue siendo el crimen prevalente en el ciberespacio,

especialmente si tenemos en cuenta que otros ciberataques como el hacking, el envío de spam, o las infecciones de programa maligno suele realizarse instrumentalmente para la posterior defraudación (Miró, 2015). (“LA RESPUESTA PENAL AL CIBERFRAUDE”) (“LA RESPUESTA PENAL AL CIBERFRAUDE”)

2.2.6 Esteganografía

Según la compañía de seguridad Kaspersky, una de las más reconocidas a nivel mundial por sus soluciones contra ciberataques a empresas y equipos personales, conceptualiza a la esteganografía como “técnica a través de la cual el autor de un mensaje oculta la información secreta en algo que parece inocente a simple vista” (Diazgranados, 2021).

La palabra esteganografía, proviene del griego Steganos (oculto) graphos (escritura) es decir escritura oculta. La esteganografía es una disciplina que se basa en el estudio de las técnicas que tienen como fin la ocultación de información. El objetivo principal es que la información se transmita de forma inadvertida para terceros mediante el uso de fotografías, audios y textos que hace las funciones de tapadera, portada o cubierta, conocida como estegomedio y se comporta como un canal subliminal.

El proceso esteganográfico más común basado es la normalización de los datos de una imagen. Mediante un proceso de reducción de un bit por píxel y normalizando a 3 bits por pixel, la representación de binario de 8 bits por carácter del mensaje se convierte en el método de cifrado para el mensaje, aplicando la idea inversa de que cada valor par de R, G o B es 0 y 1 impar (Stylesuxx & Victor, 2021).

2.2.6.1.- Tipos de Esteganografía.

Entre los tipos de esteganografía encontramos de 3 tipos:

Pura: Basado en la confidencialidad y dependencia de los usuarios que mantienen el conocimiento de la comunicación, este tipo no requiere el intercambio de un cifrado como un

stego-key. Este tipo de esteganografía no es utilizada hoy en día, por la facilidad que implica adquirir la información que se encuentre oculta gracias a herramientas desarrolladas en pro de la seguridad de la información, pero que son utilizadas con otros propósitos. (ayudaley, 2021)

De clave secreta: En esta clasificación, la llave secreta es intercambiada antes, de tal manera que el mensaje es oculto en otro mensaje por medio de la llave. Sólo las partes que disponen de la llave o palabra secreta, puede revertir el proceso y leer el mensaje en claro. (ayudaley, 2021)

De clave pública: En este caso, se utilizan 2 llaves por cada usuario, una llave pública la cual se utiliza para cifrar el mensaje y una llave privada la cual es utilizada por el destinatario del mensaje para descifrar el mismo y acceder a la información oculta. (ayudaley, 2021)

2.2.6.2.- Técnicas esteganográficas.

Existen muchas técnicas para ocultar la información, pero entre las principales se destaca las siguientes:

2.2.6.2.1.- Enmascaramiento

"En este caso la información se oculta dentro de una imagen digital usando marcas de agua donde se introduce información, como el derecho de autor, la propiedad o licencias." (“Esteganografía. Definición, técnicas y usos frecuentes”) (“Esteganografía. Definición, técnicas y usos frecuentes”) El objetivo es diferente de la esteganografía tradicional, lo que se pretende es añadir un atributo a la imagen que actúa como cubierta. (“Esteganografía - EcuRed”) (“Esteganografía - EcuRed”) De este modo se amplía la cantidad de información presentada. (Ley, 2019)

2.2.6.2.2.- Algoritmos de la compresión de datos

"Esta técnica oculta datos basados en funciones matemáticas que se utilizan a menudo en algoritmos de la compresión de datos." (“Esteganografía. Definición, técnicas y usos frecuentes”) (“Esteganografía. Definición, técnicas y usos frecuentes”) "La idea de este método es ocultar el

mensaje en los bits de datos menos importantes." (“Esteganografía - Wikipedia, la enciclopedia libre”) (“Esteganografía - Wikipedia, la enciclopedia libre”) (Ley, 2019)

2.2.6.3.- Métodos de sustitución

"Una de las formas más comunes de hacer esto es alterando el bit menos significativo (LSB)." (“Esteganografía. Definición, técnicas y usos frecuentes”) (“Esteganografía. Definición, técnicas y usos frecuentes”) En archivos de imagen, audio y otros, los últimos bits de información en un byte no son necesariamente tan importantes como los iniciales. Por ejemplo, 10010010 podría ser un tono de azul. Si solo cambiamos los dos últimos bits a 10010001, podría ser un tono de azul que es casi exactamente igual. (“AF2-INV-ESTENOGRAFIA.docx - Reporte Objetivo: El objetivo...”) (“AF2-INV-ESTENOGRAFIA.docx - Reporte Objetivo: El objetivo...”) Esto significa que podemos ocultar nuestros datos secretos en los dos últimos bits de cada píxel de una imagen, sin cambiar la imagen de forma notable. Si cambiamos los primeros bits, lo alteraría significativamente. (Navas & Rodríguez Medina, 2019)

El método del LSB funciona mejor en los archivos de imágenes que tienen una alta resolución y usan gran cantidad de colores. En caso de archivos de audio, favorecen aquellos que tienen muchos y diferentes sonidos que poseen una alta tasa de bits. (“Esteganografía - Wikipedia, la enciclopedia libre”) (“Esteganografía - Wikipedia, la enciclopedia libre”)

Además, este método no altera en absoluto el tamaño del archivo portador o cubierta (por eso es «una técnica de sustitución»). (“Esteganografía - Wikipedia, la enciclopedia libre”) (“Esteganografía - Wikipedia, la enciclopedia libre”) Posee la desventaja de que el tamaño del archivo portador debe ser mayor al mensaje a embeber; se necesitan 8 bytes de imagen por cada byte de mensaje a ocultar; es decir, la capacidad máxima de una imagen para almacenar un mensaje oculto es de su 12,5%. Si se pretende emplear una mayor porción de bits de la imagen (por ejemplo, no solo el último, sino los dos últimos), puede comenzar a ser detectable al ojo humano la alteración general provocada. (“Esteganografía. Definición, técnicas y usos

frecuentes") ("Esteganografía. Definición, técnicas y usos frecuentes") (Navas & Rodríguez Medina, 2019)

2.2.6.3.- Aplicación de la Esteganografía.

La forma en que se codifican los archivos se cambian los bits de tal manera que sea imperceptibles para el sentido humano. Dependiendo de la metodología utilizada para realizar el proceso de esteganografía, se puede utilizar 1 o 2 bits de la cadena menos o más significativos que serán reemplazados por los bits del documento que se está ocultando.

Por supuesto hay programas que pueden identificar que en un archivo (texto, audio o imagen) existe información oculta, como por ejemplo Xiao Steganography, Image Steganography, CryptureCrypture, etc.: pero para llegar a esa conclusión lo primero que se debe hacer es dudar de la integridad de dicha información, lo cual daría paso a realizar pruebas con la imagen en cuestión y en búsqueda del código de cifrado que haya sido implementado.

El estegomedio es la parte fundamental para ocultar la información, pues su tamaño será el limitante para la información que se desea ocultar. Por ejemplo, en una imagen pequeña (512px * 512px) solo se podrá introducir un pequeño código de texto como una URL, no así en una imagen grande de fondo de pantalla (1800px * 2024px) se puede ocultar un código que pueda validar información ingresada como un inicio de sesión con conexión a una base de datos.

Otro claro ejemplo del uso de esta técnica fue en la época de los CD, dónde los Ingenieros encontraron la forma de proteger las obras musicales de los artistas, embebiendo un código en las canciones que eviten la copia ilegal de las mismas.

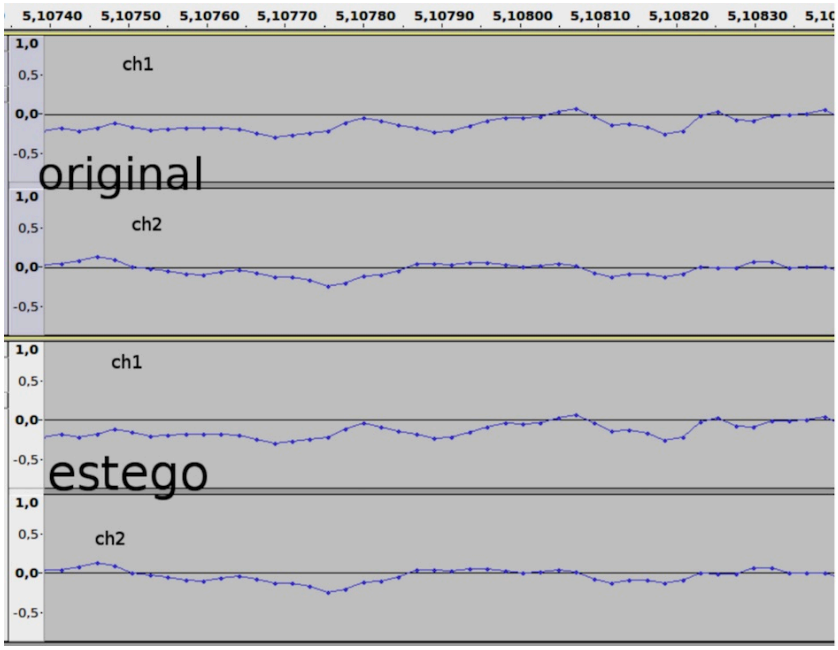


Figura 2-6 Audio aplicado esteganografía. Fuente: (Mal, 2016)

Como se puede observar en el grafico anterior, a un audio se le puede aplicar la técnica para ocultar información, siendo totalmente imperceptible, incluso con un análisis de audio, para el ser humano. Para lograr apreciar la diferencia en los bits, se debe acercar aún más el espectro de audio entre los puntos, para poder apreciar una mínima diferencia, de tal manera que el oído humano no podrá notar la diferencia entre el original y aquel audio que almacena información privilegiada o programada con un objetivo, como se puede apreciar en el siguiente gráfico.

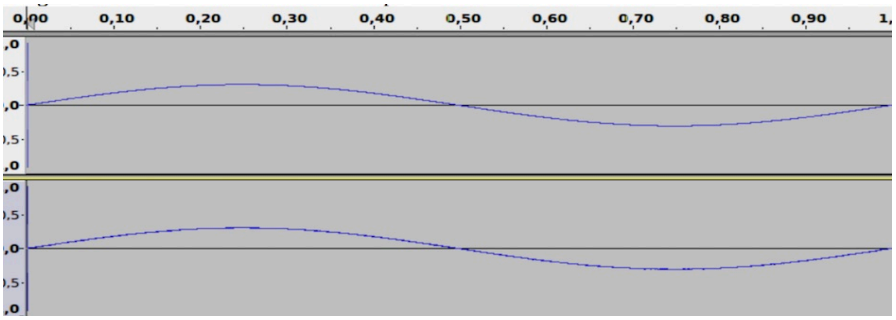


Figura 2-7 Apreciación de la técnica. Fuente: (Mal, 2016)

2.2.7 Esteganografía con gráficos.

2.2.7.1.- Archivos de imágenes.

Para la computadora, una imagen es una matriz de número que nunca representan intensidades de colores en varios pixeles. Una imagen típica es de 640 x 480 pixeles y 256 colores (u 8 bits por píxel).

Las imágenes digitales normalmente se almacenan en una calidad de 24 bits. Una imagen de 24 bits es lo ideal para esconder información, pero estas imágenes pueden llegar a ser bastante grande en tamaño.

2.2.7.2.- Compresión de archivos

Hay dos tipos de compresión de archivos: el que guarda la estructura original del archivo (por ejemplo, GIF) y el que ahorra espacio, pero no mantiene la integridad del archivo original (por ejemplo, JPEG).

Para trabajar con esteganografía es necesario que se utilice el primer tipo, el que guarda la estructura original del archivo.

2.2.7.3.- Almacenando información

Almacenar la información que va a ser escondida en una imagen, requiere de dos archivos. El primero es la imagen "inocente" que será nuestra cubierta y alojará la información que queremos esconder, este archivo se llama: imagen de cubierta. El segundo archivo es el mensaje (la información a esconder). Un mensaje puede ser texto plano, un texto encriptando, otra imagen o cualquier cosa que pueda ser llevado a bits.

2.2.7.4.- Formas de esteganografía en imágenes

Según, Friedrich (2009) existen dos formas de crear imágenes digitales, una es a través de la computadora, con herramientas de dibujo o diseño que generan diagramas, gráficos estadísticos u otros, y la otra es con los sensores que generan imágenes digitales, los cuales son el corazón de dispositivos como escáneres, cámaras y video cámaras digitales. Por tanto, afirma que este

segundo tipo de imágenes son las favoritas para la esteganografía, debido a que se las más usadas y por ende se ha desarrollado un mejor ambiente para el uso de estas.

En este caso, Hussain y Hussain (2013), clasifican a las técnicas de imagen en esteganografía en los siguientes dominios: 1) métodos de domino espacial, 2) técnica del dominio de transformación, 3) técnicas de distorsión y 4) enmascaramiento y filtrado.

Swain y Lenka (2014) aseguran que existen muchos métodos en el dominio de espacial, de los cuales se destacan los siguientes: 1) Least Significant Bit, 2) RGB based steganography, 3) Pixel Value Differencing (PVD) y 4) Mapping based steganography. Seguidamente, se presentan cada una de estas técnicas.

- **Least Significant Bit**

Con respecto a esta técnica, Kaur, Bansal y Bansal (2014), sostienen que es la más popular y simple en el trabajo con imágenes, puesto que cuenta con una baja complexidad computacional y alta capacidad de incrustación. ("Modelo Monografia Ciclo Actualizacion EPIS v2.0 | PDF | Integral") ("Modelo Monografía Ciclo Actualización EPIS v2.0 | PDF | Integral") También Swain y Lenka (2014) indican que LSB oculta los mensajes dentro de una imagen remplazando el bit menos significativo de cada pixel, es decir el bit de menor valor, por los datos a incrustar.

En particular, Singla y Juneja (2014) señalan que esta técnica no es segura, dado que la estegoimagen contiene manchas en los lugares donde se ocultan los bits, y al aplicar ataques, como el análisis de pares de muestras, análisis de histograma de imagen u otros, se puede obtener fácilmente la información. ("Análisis de técnicas de esteganografía aplicadas en archivos de audio e ...") ("Análisis de técnicas de esteganografía aplicadas en archivos de audio e ...")

- **RGB Based Steganography**

Bairagi, Mondal y Debnath (2014) exponen que esta técnica se denomina de tal manera a causa de los tres colores primarios en inglés, Red (R), Green (G) y Blue (B), donde un valor por cada tres valores describe un pixel, es decir cada pixel es una combinación de los componentes R, G y B en un esquema de color de 24 bits. Ahora bien, Gutub (2010) propone un método usando pixeles de imagen RGB como medio de cobertura, a través del uso de un canal para la indicación de los datos secretos en los otros canales, en el que el canal de indicación cambia de un pixel a otro con valores aleatorios naturales que dependen de los píxeles de la imagen. ("Análisis de técnicas de esteganografía aplicadas en archivos de audio e ...") ("Análisis de técnicas de esteganografía aplicadas en archivos de audio e ...")

En el caso del estudio de Gutub (2010), las comparaciones, realizadas entre esta técnica basa en RGB y otras técnicas de LSB, demuestran que tiene más capacidad con el mismo de nivel de seguridad.

- **Pixel Value Differencing**

Respecto a PVD, Wu y Tsai (2003) refieren que este método facilita la incorporación de mensajes secretos en una imagen, sin que se produzca grandes cambios en el archivo original, puesto que su mecanismo se basa en incrustar los datos secretos en una imagen de cobertura, mediante la sustitución de los valores de la diferencia de los bloques de dos píxeles de dicha imagen, con otros similares donde se incluyen bits de datos incrustados. De la misma manera, estos autores señalan que una de sus características es el aprovechamiento a la sensibilidad de la vista humana para las variaciones de valores grises.

Otros autores, como Shen y Huang (2014), destacan que PVD puede incrustar más datos en parejas de píxeles con más grandes diferencias. "Sin embargo, en estos casos, PVD provoca una distorsión considerable que conlleva a la degradación de la calidad de la imagen." ("Modelo Monografia Ciclo Actualizacion EPIS v2.0 | PDF | Integral") ("Modelo Monografía Ciclo Actualización EPIS v2.0 | PDF | Integral")

- **Mapping Based Steganography**

Según, Bhattacharyya, et al. (2011), esta técnica se la puede llamar Pixel Mapping Method (PMM), y puede ocultar datos dentro de cualquier imagen con escala de grises. Esto lo hace, seleccionando los pixeles de incrustación por medio de funciones matemáticas dependiendo de la intensidad del valor del pixel semilla. Antes de la incrustación, se realiza un chequeo que define si los pixeles seleccionados o sus vecinos se encuentran dentro de los límites de la imagen o no, y luego la incrustación de datos se efectúa con un mapeo de cada dos o cuatro bits del mensaje secreto en cada pixel vecino. Dentro de la tabla 1 se aprecia este mapeo de la información para incrustación de dos bits.

2.2.8 Clonación de sitios web.

En la actualidad existen muchas aplicaciones y servicios gratuitos que permiten a un usuario realizar la clonación de un sitio web, como por ejemplo el httrack, Getleft, WebSutcion, etc.; de una forma muy fugaz y simplemente copiando los archivos enlazados como imágenes, textos, audios, complementos y todo el material utilizado para subir el sitio web.

Sin embargo, cada vez son menos las técnicas aplicadas para impedir que este proceso se lleve a cabo, dejando en completa vulnerabilidad ante una amenaza de clonación, usando sus páginas de inicio de sesión como parte de un proyecto de hacking.

CAPÍTULO III

3.- METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Integridad del Sitio Web Practico https://sisepec.espoch.edu.ec

La aplicación de la esteganografía se puede realizar en un sitio web sin importar el servicio que brinde o la información que muestre. Con esta primicia se manifiesta que la presente implementación se realizó en un ambiente preparado, tomando como punto de partida el sitio web https://sisepec.espoch.edu.ec, el cual fue desarrollado por la misma Institución con el objetivo de brindar información referente a los estudios ofertados de 4to nivel; y también siendo una plataforma completa de aula virtual, en el cual los estudiantes desarrollan y entregan las diferentes actividades académicas.

Como primer punto para mejorar la integridad de un sitio web, se debe analizar las vulnerabilidades que tiene frente a la probabilidad de un ataque cibernético. Como ya se conoce, la mayoría de los sitios web pueden ser copiados parcial o totalmente, representando la vulnerabilidad más grande para una Institución. Para medir el alcance de la vulnerabilidad del sitio, se procedió a realizar una simulación de ataque, realizando una copia exacta de todo el sitio web con 2 aplicaciones ejecutadas en 2 sistemas operativos diferentes. Las aplicaciones utilizadas para este proceso son HTTRACK en MacOS; y, Web Copy bajo sistema operativo Windows.

Hay que tomar en consideración que el aplicativo HTTRACK, es multiplataforma, lo cual permite la ejecución bajo cualquier sistema operativo (Windows, Linux o MacOS). Para este ejemplo, se realizará en los 2 sistemas operativos y en 2 ambientes diferentes; en MacOS bajo líneas de comando y con Windows mediante el uso del entorno gráfico.

3.2. Clonación de Sitio Web

Cuando se procedió a realizar la clonación del sitio web, mediante el uso del HTTRACK, este se realizó de una forma mucho más rápida cuando se usa la línea de comandos, que cuando se usó la interfaz gráfica, pero con la desventaja que no muestra una barra de progreso o un porcentaje mientras realiza el procedimiento de clonación. Mientras que el aplicativo bajo sistema operativo Windows, y con interfaz gráfica, muestra el avance mediante el uso de una barra progresiva, que permite al usuario el tiempo estimado de clonación. También indica muy velozmente, el archivo que se encuentra copiando y almacenando en la carpeta del proyecto, haciendo que la clonación se realice con menor velocidad que el anterior.

Una vez finalizada la clonación del sitio, se muestra la carpeta resultante, la cual se puede utilizar para realizar los ajustes necesarios, a nivel de programación, para que la víctima ingrese las credenciales de acceso, y estas se almacenen en una base de datos.

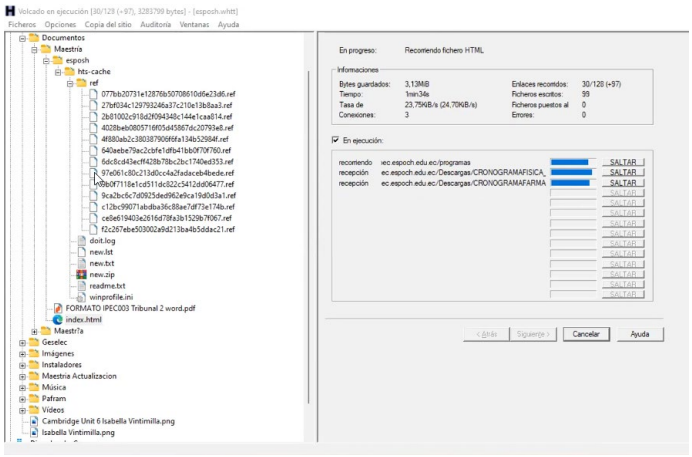


Figura 3-1 Ejecución de HTTRACK en Windows. Fuente: (Propio,2022)

Figura 3-2 Ejecución de HTTRACK en MacOS. Fuente: (Propio,2022)

Este último procedimiento es el más utilizado por los hackers al momento de generar un medio para ataques phishing, pues la facilidad con la que se puede realizar este proceso, el tiempo que requiere y la autenticidad de usar las mismas fuentes, formatos, colores e imágenes, hacen que sea la metodología perfecta para la implementación de la carnada.

Como resultado de esta operación se obtuvo el sitio web completo en ambas plataformas y con el mismo tamaño de archivo resultante, lo que implica que cualquier aplicativo puede ser utilizado para explotar esta vulnerabilidad.

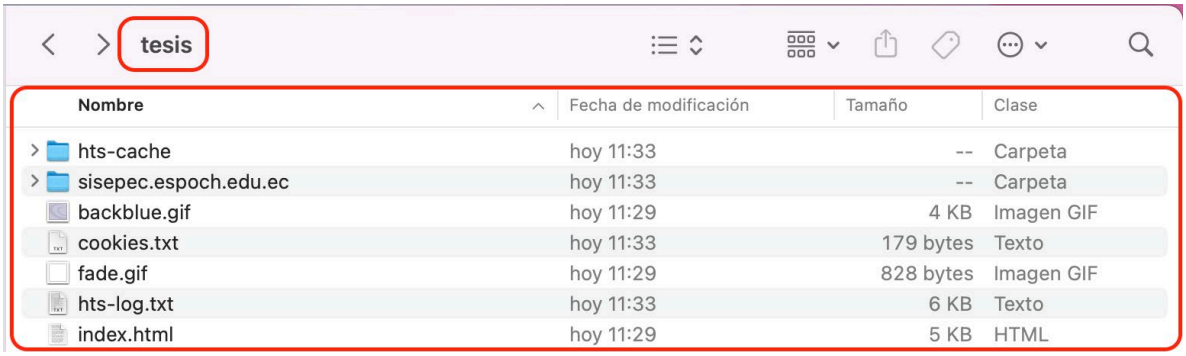


Figura 3-3 Carpeta resultante de clonación. Fuente: (Propio,2022)

3.3. Código de programación para aplicar esteganografía

Para la implementación de un código esteganográfico, se plantean 3 escenarios, entre los cuales se estudian las diversas técnicas existentes de la esteganografía, con el objetivo de analizar la factibilidad, compatibilidad y nivel de seguridad a nivel del sitio web de la sisepec.

Una vez definido el primer escenario que es la situación actual del sistema web, se procedió con la investigación de un código ya realizado que proceda con la aplicación de la esteganografía y que podía ser utilizado como parte fundamental de este proyecto. Luego de varias búsquedas en conjunto con un desarrollador, encontré un pequeño proyecto que cumplía con los requisitos necesarios para implementarlo en el proyecto, el cual contenía el código que realiza el cifrado y otro para descifrado de la información, bajo el lenguaje de programación de php y HTML. Este proyecto diseñado por Chris (Chris, 2021) utiliza el método LSB (Less Significant Bit) o bit menos significativo, para esconder el texto en una imagen acorde al tamaño de la información que se requiere esconder.

Se midió la factibilidad de implementación de acuerdo con el tipo de lenguaje de programación el cual está basado y, la funcionalidad de este con imágenes de diferentes tamaños. Para las primeras pruebas con el presente código, se utilizó texto con diferentes números de caracteres (361) y con diferentes tamaños de imágenes, con el objetivo de revisar si la lógica de cifrado no variaba entre cada prueba, dando como resultado que las imágenes de tamaño pequeño (hasta 550kb), incrementaba el tamaño resultante (730 kb) al momento de aplicar el cifrado de información.

Este resultado manifiesta que el incremento no es muy significativo, ayudando a que no se levante sospechas de la parte atacante que la imagen utilizada puede ser de un tamaño adecuado, desde el punto de vista de la programación.

3.4. Aplicando el código en el sitio web

Al tener la limitante de no poder trabajar bajo el servidor de producción de SISEPEC por temas de seguridad y disponibilidad de los servicios, realicé la implementación de un servidor contratado el cual fue adaptado un dominio con similitud de nombre al original (https://esposh.digital) y un subdominio para que hiciera de dominio atacante (https://demostack.esposh.digital). De esta manera se obtuvo el ambiente de desarrollo y posteriores pruebas para continuar con la aplicación de la técnica esteganográfica.

Por cuestiones estéticas y para mayor comprensión de la implementación de la técnica, realicé la captura de una imagen que está acorde al inicio de sesión y en la cual se aplicó el código oculto que notificará al usuario si está navegando por un sitio seguro.

Figura 3-4 Imagen con código esteganográfico. Fuente: (Freepik)

3.4.1. Agregando funcionalidad a la técnica.

Analizando el mecanismo de defensa adecuado para alertar al usuario de navegación de una página web fraudulenta y, notificando al administrador del sitio web original cuando este fuere levantado en un dominio o ip diferente, concluí que la mejor manera de mitigar la vulnerabilidad que atenta contra la integridad del sitio web es mediante la doble autenticación. Procedí a incluir un código el cual valide la dirección URL en la cual se encuentre almacenada el sitio web, de

esta manera, el momento en que identifique que se encuentra en un dominio diferente, el código esteganográfico se activa y advierte al usuario que está navegando sobre un sitio web fraudulento; y, al mismo tiempo, notificaría al administrador del sitio que su web está levantada en un dominio diferente al real, permitiendo realizar una actualización al mismo y proceder con los correctivos necesarios para evitar el hackeo de sus usuarios.

3.4.2. Inclusión del código de programación mediante esteganografía.

Mientras realizaba la implementación del código en la imagen y se iban realizando las pruebas pertinentes de funcionamiento, se presentaron inconvenientes que debían ser subsanados para la buena implementación de la técnica y que los procesos se lleven a cabo satisfactoriamente. Entre los todos los inconvenientes, hubo uno que destacó sobre manera: el código encontrado para proceder con el envío de los correos electrónicos se encontraba diseñado en un lenguaje más actualizado que el que usa la página de SISEPEC, dando como resultado una incompatibilidad de versiones del lenguaje de programación.

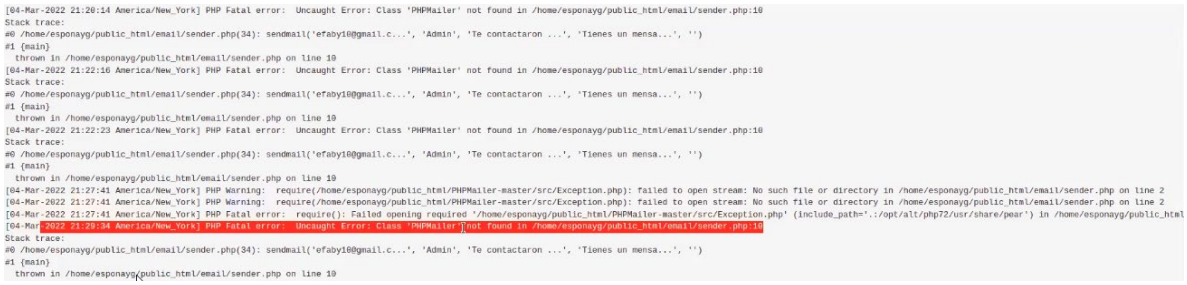


Figura 3-5 Problema - Implementación de código Mailer. Fuente: (Propio,2022)

Para dar una solución definitiva al código que permita enviar el mail por medio de código php, realicé una búsqueda de posibles soluciones para esa incompatibilidad de versiones del lenguaje de programación, llegando a la solución indicada por un grupo de programadores que distribuyeron su conocimiento mediante la plataforma GitHub (Bointon, Jagielski, Andy, & Matzele, 2020).

Una vez superado los obstáculos impuestos al momento de implementar los procesos de programación, y, con varias pruebas exitosas, se da por terminada la implementación del código

de esteganografía como una técnica para ayudar a mitigar la vulnerabilidad que amenazaba la integridad del sitio web.

3.4.3. Prueba final de implementación.

Con las pruebas satisfactoriamente realizadas y con un ambiente de pruebas debidamente controlado y revisado, se realiza la prueba final de implementación, en el que se vuelve a clonar el sitio web (https://esposh.digital) y levantamiento en el dominio preparado para phishing (https://demostack.esposh.digital), se observa que el código esteganográfico se activa y realiza el llamado a los procedimientos indicados, el cual me indica que estoy navegando por un sitio web fraudulento, y del mismo modo, un correo electrónico llega mi mail manifestando la amenaza de seguridad de la integridad.

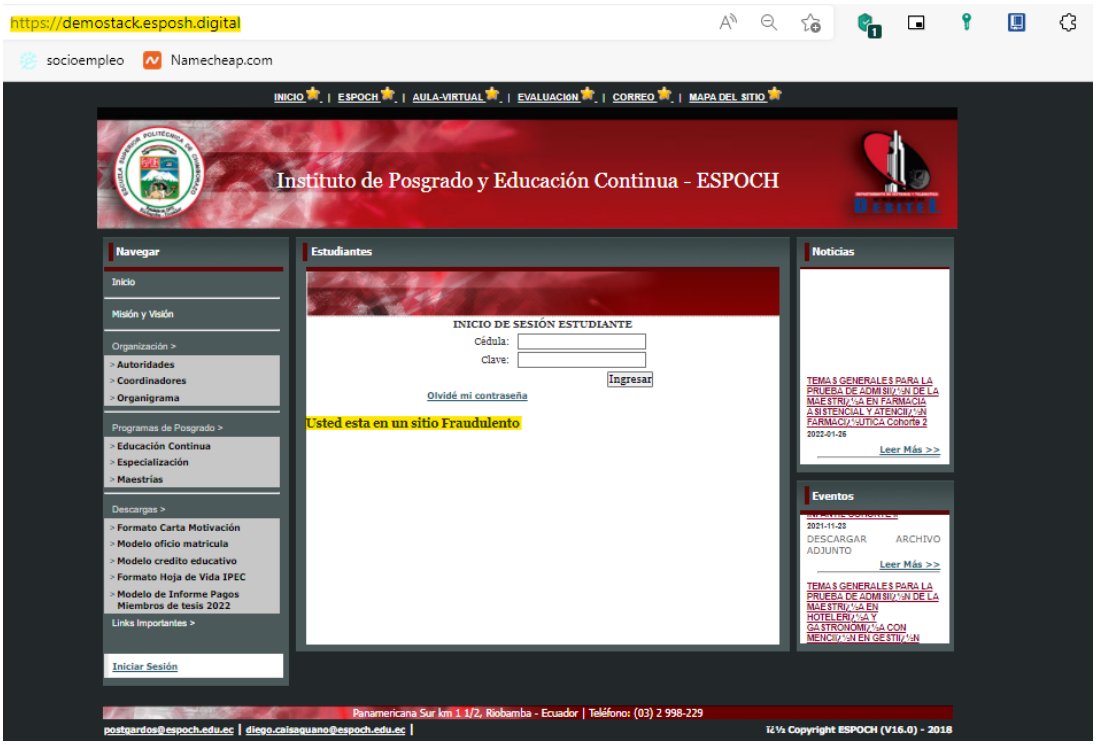


Figura 3-6 Página web resultante. Fuente: (Propio,2022)

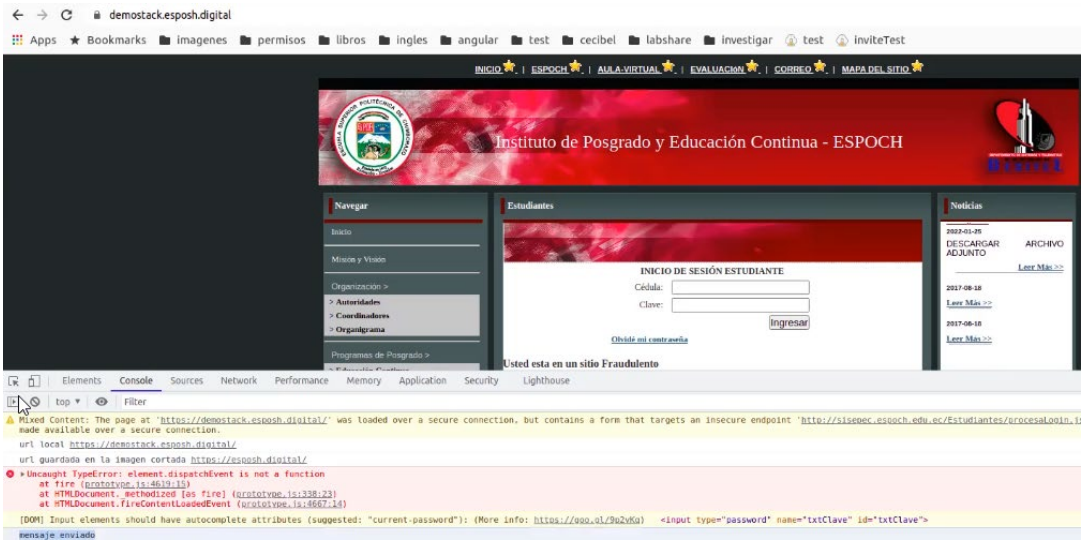


Figura 3-7 Demostración de mensaje enviado por consola. Fuente: (Propio,2022)

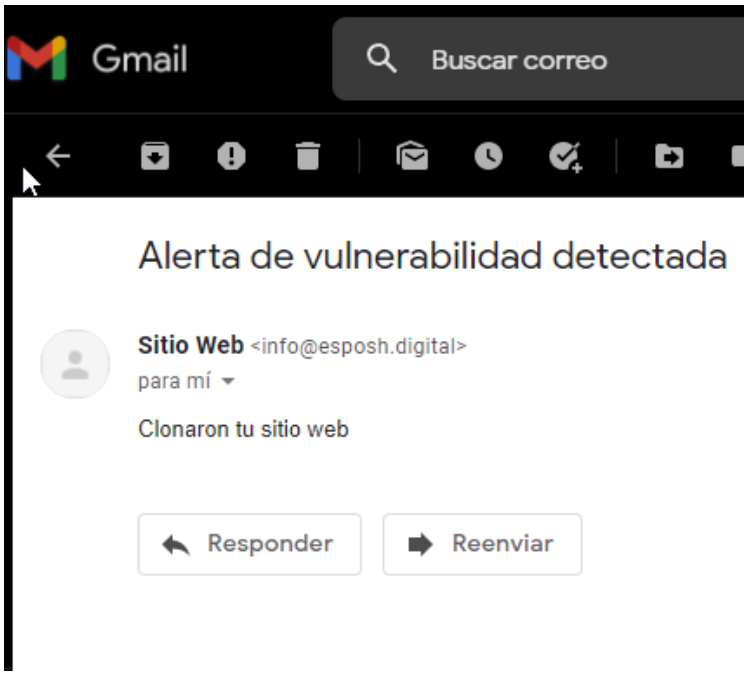


Figura 3-8 Llegada de correo electrónico con alerta de vulnerabilidad. Fuente: (Propio,2022)

CAPÍTULO IV

4.- RESULTADOS

4.1 Análisis Final

Hipótesis:	La aplicación de la esteganografía en sistemas académicos basados en la web, si mejora la integridad de la información, caso práctico https://sisepec.espoch.edu.ec.		
Página WEB	**Control de página web**	**Susceptible a clonación**	**Doble Autenticación**
http://sisipecevaluacion.espoch.edu.ec/index.jsp?accion=LOGIN-ESTUDIANTE	☒Contraseña ☐Esteganografía	☒Si ☐No	☐Implementado ☒No implementado
http://sisipecevaluacion.espoch.edu.ec/index.jsp?accion=LOGIN-DOCENTE	☒Contraseña ☐Esteganografía	☒Si ☐No	☐Implementado ☒No implementado
http://sisipecevaluacion.espoch.edu.ec/index.jsp?accion=LOGIN-USUARIO	☒Contraseña ☐Esteganografía	☒Si ☐No	☐Implementado ☒No implementado

Tabla 1 Checkpoint de seguridad previa aplicación de la técnica esteganográfica

Durante el desarrollo del presente trabajo de investigación se pudo apreciar que las páginas de inicio de sesión tienen una alta posibilidad de ser vulneradas y utilizadas como un medio para ataques de tipo phishing. Esta vulnerabilidad representa un riesgo para la información almacenada por los estudiantes, al igual que los servicios que la institución brinda a través del sitio web mencionado.

El uso de programas y aplicativos gratuitos que permitan la clonación del sitio web, han sido de vital importancia para determinar el nivel de seguridad que presenta el sitio web, en el ámbito de la seguridad de la información. Este resultado, siendo un nivel 0 de acuerdo con los controles ISO 27002, determinan un potencial riesgo para la información que el sitio web almacena, entre los cuales se pueden evidenciar las credenciales de acceso de los usuarios.

La implementación de la esteganográfica, por medio de la técnica de sustitución, ha demostrado ser la más efectiva y simple al momento de implementarla, por la capacidad de código que pueda

almacenar una imagen de acuerdo con su tamaño y el uso de código cifrado que permita la carga de aplicativos o compilación de código que realice validación del dominio, información o validación de credenciales para el ingreso a un sitio web.

Hipótesis:	La aplicación de la esteganografía en sistemas académicos basados en la web, si mejora la integridad de la información, caso práctico https://sisepec.espoch.edu.ec.		
Página WEB	**Control de página web**	**Susceptible a clonación**	**Doble Autenticación**
http://sisipecevaluacion.espoch.edu.ec/index.jsp?accion=LOGIN-ESTUDIANTE	☒Contraseña ☒Esteganografía	☐Si ☒No	☒Implementado ☐No implementado
http://sisipecevaluacion.espoch.edu.ec/index.jsp?accion=LOGIN-DOCENTE	☒Contraseña ☒Esteganografía	☐Si ☒No	☒Implementado ☐No implementado
http://sisipecevaluacion.espoch.edu.ec/index.jsp?accion=LOGIN-USUARIO	☒Contraseña ☐Esteganografía	☒Si ☐No	☐Implementado ☒No implementado

Tabla 2Tabla 2 Checkpoint de seguridad posterior aplicación de la técnica esteganográfica

Una vez finalizada la implementación de la esteganografía, se puede apreciar una mejora significativa en la página web de inicio de sesión para los estudiantes del SISEPEC, la cual brinda una seguridad al usuario de que se encuentra navegando por la página oficial y que cualquier notificación que pueda ser enviada con enlaces a la presente página, serán enviados bajo el mismo dominio de la Escuela Superior Politécnica de Chimborazo.

El uso de la esteganografía, por medio del presente trabajo de investigación, ha demostrado ser una técnica aplicable en cualquier sitio web, basándose en el principio de ocultación de información, como un medio de autenticidad que brinda mayor seguridad a los pilares de la seguridad de la información.

CONCLUSIONES

Una vez finalizada la demostración de la aplicabilidad de la esteganografía, como medida de seguridad para mitigar la vulnerabilidad de clonación de los sitios web, concluyo:

1. La técnica de la esteganografía puede ser aplicada como una medida de seguridad para cualquier sitio web, sin importar los servicios que brinde o la información que sea publicada.
2. Los métodos de cifrado que utiliza la esteganografía están orientados, en su mayoría, a la aplicación de esta en imágenes, las cuales pueden ser fácilmente determinantes por un hacker con conocimientos básicos de seguridad.
3. El método de cifrado LSB es el más eficiente al momento de aplicar la técnica esteganográfica como medida de seguridad en los sitios web académicos, por la versatilidad de implementación en diferentes tipos de archivos que pueden ser indispensables al momento de presentar los sitios web.
4. El nivel de integridad del sitio web https://sisepec.espoch.edu.ec puede llegar a incrementar en un nivel de seguridad 1, al aplicar la técnica de esteganografía como un medio para mitigar la vulnerabilidad de la clonación web, como se ha demostrado en el presente trabajo de investigación.

RECOMENDACIONES

1. Implementar la esteganografía, en los sitios web de la Escuela Superior Politécnica de Chimborazo, como medida de seguridad para mitigar la clonación y que puedan ser usados como parte de un ataque informático a los usuarios.

2. Realizar una actualización del sitio web https://sisepec.espoch.edu.ec a la última versión del lenguaje de programación.
3. Utilizar el método de cifrado LSB con los 2 dígitos menos significativos al momento de implementar la técnica de esteganografía para brindar un mayor nivel de seguridad y, que no sea fácilmente rastreable por los programas de análisis de esteganografía.
4. Mitigar la amenaza de clonación en las páginas de inicio de sesión del sitio web https://sisepec.espoch.edu.ec mediante la doble autenticación.
5. Aplicar la técnica esteganográfica a imágenes que sean de autoría de la ESPOCH, de tal manera que sean indispensables al momento de realizar una copia de la página y que el código esteganográfico esté inmiscuido.

GLOSARIO

A

ataques de fuerza bruta
Proceso dónde el atacante utiliza diccionario de datos para comparar una por una las palabras del diccionario como posibles contraseñas de acceso a sistemas informáticos. · vi

C

ciberdelincuencia
delitos cometidos a través de la red informática y que afecta a la seguridad y confidencialidad · vi
delitos cometidos a través de la red informática y que afecta a la seguridad y confidencialidad · vi
delitos cometidos a través de la red informática y que afecta a la seguridad y confidencialidad · vi
delitos cometidos a través de la red informática y que afecta a la seguridad y confidencialidad · vi
delitos cometidos a través de la red informática y que afecta a la seguridad y confidencialidad · 26
ciberespacio
"el conjunto de interconexiones electrónicas dispuestas en red, que constituye un espacio de relación integrado por componentes de naturaleza material de base tecnológica, de naturaleza inmaterial sustentada en la información y el conocimiento, a través del lenguaje, y de naturaleza antropológica fundamentada en la sociabilidad del ser humano, que ha devenido en medio y procedimiento para prestar servicios, y ha generado un nuevo marco espacio cultural con efectos económicos, políticos, jurídicos, sociales, culturales y de seguridad · vi, 27
clonación
Realizar una copia de la forma de una página web de un sitio web, comunmente utilizado para realizar ataques de pesca. · vi, 10, 11, 12, 13, 36, 38, 39, 45, 46, 47, 48

D

doble autenticación
Uso de software que valida el inicio de sesión a una cuenta, mediante la aprobación del usuario. · vi, 41, 48

E

e-learning
Uso de tecnología como método de enseñanza - aprendizaje utilizado en instituciones Educativas de nivel medio y superior. · 14
esteganografía · vi
Arte de ocultar información dentro de imágenes, texto o sonido · vi

H

hackers
Delincuentes cibernéticos con altos conocimientos de Informática, Redes y Programación, que realizan ataques a usuarios (personas o empresas) con un objetivo personal malicioso. · 12, 15, 39

I

Ingeniería Social

P

R

S

T

V

BIBLIOGRAFÍA

APWG. (31 de Diciembre de 2021). *APWG*. Obtenido de APWG: https://apwg.org/trendsreports/

ayudaley. (17 de 03 de 2021). *ayudaley*. Obtenido de ayudaley: https://ayudaleyprotecciondatos.es/2021/03/17/esteganografia/

Belcic, I. (05 de 02 de 2020). *avast*. Obtenido de avast: https://www.avast.com/es-es/c-phishing#topic-1

Bointon, M., Jagielski, J., Andy, P., & Matzele, B. (01 de Enero de 2020). *PHPMailer*. Obtenido de PHPMailer: https://github.com/PHPMailer/PHPMailer/blob/master/src/PHPMailer.php

Castillo, O. (N/A de N/A de 2021). *Uniersidad Externado de Colombia.* (U. E. Colombia, Ed.) Obtenido de Uniersidad Externado de Colombia: https://bdigital.uexternado.edu.co/handle/001/4353

Castro, M. R. (N/A de N/A de 2019). *StuDocu*. Obtenido de StuDocu: https://www.studocu.com/es-mx/document/universidad-tecnologica-de-mexico/seguridad-y-salud-en-el-trabajo/introduccion-a-la-seguridad-informatica-y-el-analisis-de-vulnerabilidades/8251059

Chris. (30 de 05 de 2021). *stylesuxx / steganography*. Obtenido de github: https://github.com/stylesuxx/steganography

Diazgranados, H. (31 de Agosto de 2021). *Kaspersky Latinoamerica*. Obtenido de Kaspersky Latinoamerica: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

Española, R. A. (01 de 01 de 2019). *Real Academia Española*. Obtenido de Real Academia Española: https://dle.rae.es/criptograf%C3%ADa

Freepik. (s.f.). *Login.*

Henry González, W. B. (24 de 05 de 2018). *Ecured*. Obtenido de Criptografía en Ciberseguridad: https://www.ecured.cu/Criptograf%C3%ADa_en_Ciberseguridad#Introducci.C3.B3n

Hernández Dominguez, A. &. (2021). IV Conferencia Científica Internacional UCIENCIA 2021. *IV Conferencia Científica Internacional* (págs. 2-5). La Habana: Futuro. Obtenido de https://repositorio.uci.cu/jspui/bitstream/123456789/9692/1/UCIENCIA_2021_paper_458.pdf

IBM. (12 de 08 de 2019). *IBM*. Obtenido de IBM: https://www.ibm.com/es-es/topics/encryption

INCIBE. (20 de Marzo de 2017). *INCIBE*. Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Institute, P. (25 de 05 de 2018). *Ponemon*. Obtenido de Ponemon: https://www.ponemon.org/userfiles/filemanager/nvqfztft3qtufvi5gl60/

Institute, T. P. (24 de 04 de 2018). *proofpoint*. Obtenido de proofpoint: https://www.proofpoint.com/us/blog/insider-threat-management/new-ponemon-institute-study-insider-threats-lead-big-losses-and

ISOTools. (01 de 01 de 2021). *Normas ISO de seguridad de la información*. Obtenido de Normas ISO de seguridad de la información: https://www.isotools.org/2022/02/10/normas-iso-de-seguridad-de-la-informacion-conociendo-la-iso-27001/

Jaimes Iguavita, N. &. (N/A de N/A de 2018). *Repositorio Institucional.* Obtenido de Repositorio Institucional: https://repository.udistrital.edu.co/bitstream/handle/11349/14198/JaimesIguavitaNathaly2018.pdf?sequence=1&isAllowed=y

Ley, A. d. (17 de 08 de 2019). *ayudadeley*. Obtenido de ayudadeley: https://ayudaleyprotecciondatos.es/2021/03/17/esteganografia/#Tipo_de_esteganografia

Mal, U. I. (24 de Mayo de 2016). *El Lado del Mal*. (C. Alonso, Editor) Obtenido de El Lado del Mal: https://www.elladodelmal.com/2016/05/esteganografia-con-ficheros-de-audio.html

Micro, T., & Fuentes, I. (17 de Agosto de 2021). *Cuadernos de Seguridad*. (T. Micro, Productor) Obtenido de Cuadernos de Seguridad: https://cuadernosdeseguridad.com/2021/08/el-84-de-las-organizaciones-sufre-amenazas-de-phishing-y-ransomware/

Microsoft. (02 de Marzo de 2021). *News Center Microsoft Latinoamérica*. Obtenido de News Center Microsoft Latinoamérica: https://news.microsoft.com/es-xl/marsh-y-microsoft-ingenieria-social-o-phishing-es-el-ciberataque-que-mas-aumento-en-latinoamerica-a-raiz-de-la-pandemia/

Miró, F. (N/A de N/A de 2015). *Torrossa.* (Dykinson, Ed.) Obtenido de Torrossa: https://www.torrossa.com/en/resources/an/3052068

Navas, G. S., & Rodríguez Medina, C. G. (02 de 01 de 2019). *Sistema Nacional de Repositorios Digitales*. Obtenido de Sistema Nacional de Repositorios Digitales: https://repositoriosdigitales.mincyt.gob.ar/vufind/Record/SEDICI_3add0647cfd63930cc554750ee71e8c7

NEOTEO. (2010). *El cifrado de César.* España: NeoTeo. Obtenido de https://www.abc.es/ciencia/cifrado-cesar-201007050000_noticia.html

Pacheco, J. C. (22 de 09 de 2016). *Unirioja*. Obtenido de Unirioja: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUK

Ewj60-i9-tX6AhXLTDABHYy0AegQFnoECA4QAQ&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F6080426.pdf&usg=AOvVaw1Z3g-ANeIQvXZQRncC_LC8

Pilar. (01 de 01 de 2018). *Pilar*. Obtenido de Pilar: https://pilar.ccn-cert.cni.es/index.php/analisis-de-riesgos/analisis-de-riesgos-pilar#:~:text=El%20an%C3%A1lisis%20de%20riesgos%20inform%C3%A1ticos,adecuados%20para%20aceptar%2C%20disminuir%2C%20transferir

PMG. (06 de 04 de 2015). *ISO 27001: Amenazas y vulnerabilidades*. Obtenido de ISO 27001: Amenazas y vulnerabilidades: https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

Posada, R. (2017). *Los Cibercrímenes: Un nuevo paradigma de Criminalidad.* Bogotá, Colombia: Ibañez.

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., . . . Castillo, M. (2018). Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. *3ciencias*, 26. doi:http://dx.doi.org/10.17993/IngyTec.2018.46

Salcedo, M. (N/A de 10 de 2010). *Repositorio Institucional UIGV.* Obtenido de Repositorio Institucional UIGV: http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/967/COMTEL-2010-54-65.pdf?sequence=1&isAllowed=y

Stylesuxx, C., & Victor, B. (30 de Mayo de 2021). *Github*. Obtenido de Github: https://github.com/stylesuxx/steganography

Wesner, F. (N/A de N/A de 2020). *Universidad de Buenos Aires.* Obtenido de Universidad de Buenos Aires: http://bibliotecadigital.econ.uba.ar/econ/collection/tpos/document/1502-1712_WesnerFB?p.s=TextQuery