UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

ESTRATEGIAS DE PREVENCIÓN FRENTE A LOS CIBERATAQUES EN LA UNIDAD EDUCATIVA FISCAL LUIS ALFREDO NOBOA ICAZA

Trabajo de titulación previo a la obtención del
Título de Ingeniero en Ciencias de la Computación

AUTOR: DENISSE AYELEN VILLAMAR ARELLANO

TUTOR: JOE FRAND LLERENA IZQUIERDO

Guayaquil – Ecuador

2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Denisse Ayelen Villamar Arellano con documento de identificación N° 0952496784 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 29 de julio del año 2022

Atentamente,

Denisse Ayelen Villamar Arellano
0952496784

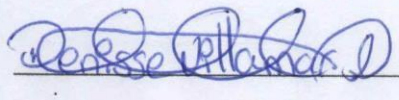
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Denisse Ayelen Villamar Arellano con documento de identificación No. 0952496784, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor(a) del Artículo Académico: "Estrategias de prevención frente a los ciberataques en la Unidad Educativa Fiscal Luis Alfredo Noboa Icaza", el cual ha sido desarrollado para optar por el título de: Ingeniero en Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 29 de julio del año 2022

Atentamente,



Denisse Ayelen Villamar Arellano
0952496784

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: Estrategias de prevención frente a los ciberataques en la Unidad Educativa Fiscal Luis Alfredo Noboa Icaza, realizado por Denisse Ayelen Villamar Arellano con documento de identificación N° 0952496784, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 29 de julio del año 2022

Atentamente,

Joe Frand Llerena Izquierdo
0914884879

DEDICATORIA

Dedico este trabajo a toda mi familia, en especial a mis padres que han sido mi apoyo incondicional a lo largo de mi carrera universitaria, a mi mamita y a mis abuelos que no están presentes ahora, pero sé que espiritualmente ellos se encuentran conmigo y están orgullosos de mí.

AGRADECIMIENTO

Agradezco a Dios en primer lugar, por permitirme culminar mi Carrera con mucho éxito, a mis padres por ayudarme en todo momento y por no dejarme rendirme en los momentos más difíciles y a toda mi familia por su apoyo incondicional; en especial a mis hermanos Luis, Xiomara y Ámbar que me han ayudado siempre en los momentos que los he necesitado.

También agradezco a mi Tutor Ing. Joe Llerena por haber aceptado ser mi guía en este artículo y ayudarme incondicionalmente por el apoyo de este trabajo culminado.

RESUMEN

Las amenazas en ciberseguridad se encuentran latentes a nivel mundial y los ataques informáticos son el resultado de la existencia de vulnerabilidades en software, hardware y sus entornos informáticos. El objetivo de este estudio es desarrollar un conjunto de estrategias de prevención en ciberseguridad para su aplicabilidad en la Unidad Educativa Fiscal Luis Alfredo Noboa Icaza mediante el uso de herramientas que permitan el registro de soluciones frente a la inseguridad informática. Se utiliza una metodología de investigación empírico-analítica de corte cuantitativo y enfoque cualitativo. Se utiliza la técnica de la encuesta, para recoger datos, a través de la tecnología de Google Forms, plataforma virtual que permite hacer encuestas online y tabula los datos al finalizar. Se aplicó una encuesta a una muestra aleatoria de 360 personas que pertenecen a la unidad educativa, entre los cuales se encuentran docentes, representantes (padres de familia) y estudiantes utilizando la escala de Likert variada. Esta herramienta permitió analizar las opciones acerca de los ítems planteados en las encuestas. Los resultados indicaron que es posible desarrollar y aplicar un conjunto de estrategias que permitan mejorar la seguridad informática en la comunidad educativa y, que es necesario concientizar acerca de la importancia de utilizar estas acciones en beneficio de la institución.

Palabras claves: Ciberseguridad, Ransomware, Troyano, Estrategias De Prevención, Malware, Ataques Informáticos.

ABSTRACT

Cybersecurity threats are latent worldwide and computer attacks are the result of the existence of vulnerabilities in software, hardware and their computing environments. The objective of this study is to develop a set of prevention strategies in cybersecurity for its applicability in the Luis Alfredo Noboa Icaza Public Education Unit through the use of tools that allow the registration of solutions to computer insecurity. An empirical-analytical research methodology of quantitative cut and qualitative approach is used. The survey technique was used to collect data through Google Forms technology, a virtual platform that allows online surveys and tabulates the data at the end. A survey was applied to a random sample of 360 people belonging to the educational unit, including teachers, representatives (parents) and students using the varied Likert scale. This tool made it possible to analyze the options regarding the items raised in the surveys. The results indicated that it is possible to develop and apply a set of strategies to improve computer security in the educational community and that it is necessary to raise awareness of the importance of using these actions for the benefit of the institution.

Keywords: Cybersecurity, Ransomware, Trojan, Prevention Strategies, Malware, Computer Attacks.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

La investigación sobre las amenazas a la ciberseguridad se centra en los hogares, ignorando en gran medida una de las labores más débiles del sistema, es decir, los dispositivos en red utilizados en el hogar. Los ataques informáticos incluyen el uso de determinadas debilidades o defectos que son las vulnerabilidades en software, hardware e incluso entornos informáticos (Pérez González, 2021)(Andrade Medina, 2021); para obtener beneficios que suelen ser de carácter económico, tendrán un impacto negativo en la seguridad del sistema y de forma directa afectar los activos de la comunidad educativa, una de las formas más directas que utilizan los ciberdelincuentes para ganar dinero son los ataques dirigidos a los clientes bancarios (Rosero Tejada, 2021), los atacantes suelen utilizar la creatividad para engañar a las víctimas para que revelen su información personal o instalen programas maliciosos para recopilar información personal como las contraseñas, las víctimas utilizan eso para acceder a sus cuentas bancarias (Toala Indio, 2021)(Orozco Bonilla, 2021).

Para minimizar el impacto negativo de un ataque, existen algunos procedimientos y mejores prácticas que pueden facilitar la lucha contra las actividades delictivas y reducir significativamente el alcance del ataque (Morán Maldonado, 2021), uno de los pasos más importantes en seguridad es la educación y comprender cuáles son las vulnerabilidades más comunes que pueden explotarse y cuáles son sus riesgos asociados que nos permitirá comprender cómo se atacan los sistemas informáticos, ayudar a identificar debilidades y riesgos; luego implementar de manera inteligente estrategia de seguridad efectivas (Sánchez Guzmán, 2021).

El malware es también una de las principales amenazas a la seguridad de cualquier población, aunque pueda parecer un problema trivial, suele ser la causa de importantes pérdidas económicas, esta amenaza se refiere a provocar algún tipo de daño o anomalía (Muñoz Campuzano, 2021), esta categoría incluye múltiples amenazas de seguridad digital como en malware infeccioso, oculto y para obtener beneficios económicos directos y estos grupos son los gusanos, spyware, adware, troyano, virus y ransomware (Escalante Quimis, 2021)(Aguirre Sánchez, 2021).

Evidentemente, el malware es un tema muy importante en el entorno digital, ya que, en la actualidad, algunos ataques de códigos dañinos en los equipos se llevan a cabo a través de programas maliciosos, que ingresan al sistema de manera completamente secreta activando el

virus (Ponce Larreategui, 2021), ya que hoy en día, se considera la amenaza de seguridad número uno y continúa prosperando en el entorno de Internet, a medida que se vuelve cada vez más importante en nuestro estilo de vida, también ha aumentado el número y la intensidad de las amenazas de malware lanzadas contra nosotros, una de las razones por las que obviamente no podemos eliminar o reducir las amenazas relacionadas con el malware puede ser la debilidad de las defensas que implementamos (Miranda Jiménez, 2021).

Los atacantes suelen combinar caballos de troya con otros tipos de códigos maliciosos (Moncayo Ronquillo, 2021). Por ejemplo, cuando, acceden a través de caballos de troya, colocarán otros códigos maliciosos en el sistema, como rootkits, que pueden ocultar los rastros que deja el atacante en la computadora y volver a ingresar al sistema cuando lo crea necesario, todo de forma remota y en la mayoría de los casos, el administrador de la red no notará la actividad (Melendrez-Caicedo & Llerena-Izquierdo, 2022)(Guaigua Bucheli, 2021).

2. REVISIÓN DE LITERATURA

2.1. Código malicioso y sus tipos de ciberataques

El malware es un conjunto de instrucciones que es un software que se utiliza para el acceso no autorizado (Makandar & Patrot, 2017). Es una amenaza que aumenta rápidamente para la informática moderna (Roseline et al., 2020)(Chévez Morán, 2021). Distinguir y clasificar diferentes tipos de malware es importante para comprender mejor cómo pueden infectar computadoras y dispositivos, el nivel de amenaza que representan y cómo protegerse contra ellos (Kebede TM, Djaneye-Boundjou O, Narayanan BN, Ralescu A, 2017). La clasificación de malware es el proceso de asignar una muestra de malware a una familia de malware específica (Alsulami & Mancoridis, 2019). Recientemente, la cantidad de malware aumenta día a día y genera muchas víctimas (Kim et al., 2018)(Alvarado Ronquillo, 2021).

Es un software malicioso que intenta invadir o dañar ordenadores, aunque no pueda dañar el hardware del equipo, puede robar, invadir o cifrar las funciones básicas del ordenador y espiar sin el permiso del usuario, dentro del grupo de malware se identifica los gusanos, virus, spyware, troyano, adware y ransomware (Terán Terranova, 2021)(Guaman Villalta, 2021).

Los programas malignos se pueden presentar mediante diferentes métodos, estos a su vez generan ciberataques que afectan de modos variados a la comunidad educativa de la Unidad

Educativa Fiscal "Luis Alfredo Noboa Icaza", algunas de estos se los ejemplifica a continuación:

Tabla 1. Tipos de ciberataques

Tipos	Repercusiones
Gusano	Se puede ejecutar de manera independiente, normalmente un gusano toma el control de un equipo y lo usa como punto de partida para controlar otros sistemas vulnerables (Andrade Valdez & Galarza Zurita, 2019). Causando el daño a las computadoras y las redes, dificultando el trabajo de los usuarios.
Spyware	Espía el dispositivo de manera silenciosa, en vez de permitir el acceso a él, pero puede robar información bancaria como los números de tarjeta de crédito y cualquier otra información personal y confidencia, que esté almacenada o sea accesible desde el equipo (Mariam & Morgado, 2021). Conduce a un rendimiento lento de la computadora, retrasos y fallas frecuentes del sistema e incluso una sobrecarga de la computadora
Ransomware	Es un tipo de malware con el fin de extorsionar víctimas, exigiendo pagos para deshacer los cambios realizados en los archivos infectados (Andrade Valdez & Galarza Zurita, 2019), provocando un secuestro mediante el cifrado de los archivos de la computadora infectada, para así exigir un rescate y en la mayoría de estos ataques hay una fecha límite, si no paga, podría perder el acceso de los archivos o afectando el bloqueo de su computadora.
Virus	Un programa que está usualmente oculto dentro de otro programa aparentemente inocuo y que produce copias de sí mismo e inserta otros programas y usualmente realiza una acción maliciosa (como destruir datos)(Lezama, 2016), afectando a los programas que lo controlan o causan daños al utilizar recursos escasos como el espacio en disco duro, memoria, fallas del sistema, eliminación de archivos, mal comportamiento de la pantalla, desorden en datos del disco.
Adware	Su único objetivo es entrar en un dispositivo y comenzar a mostrar todo ese spam, ya sea en forma de popup, es decir, una ventana emergente en momentos aleatorios, mientras se navega por Internet o durante la ejecución de un programa (Mariam & Morgado, 2021), afectando significativamente la funcionalidad del equipo, haciéndolo más lento, recopilando datos y mostrando anuncios.
Troyano	Software que obtiene información de una persona u organización sin su conocimiento y que puede enviar tal información a otra entidad sin el consentimiento del cliente, o que impone el control sobre una computadora sin el conocimiento del cliente (Lezama, 2016), es decir causa daños de privacidad

como el uso no autorizado de la cámara web, modificar lista de contactos, realizar llamadas y enviar mensajes de texto, incluso ubicar usuarios a través de GPS, interrumpir el funcionamiento de la computadora y capturar texto ingresado mediante el teclado o registrar contraseñas introducidas por el usuario.

2.2. Estrategias de prevención contra los ataques informáticos

Los ciberataques han sido una gran problemática a lo largo de los años y se han venido incrementando conforme al crecimiento en el uso de la tecnología con múltiples plataformas tecnológicas que soportan multiplicidad de servicios (Florez & Pinzon, 2017)(Llerena Izquierdo et al., 2018)(Llerena Izquierdo et al., 2009). La mejora de la sociedad como contramedida para eliminar los factores delictivos que provocan una actitud positiva o neutral hacia los delitos cibernéticos debe orientarse hacia una vida mejor, ya que cuanto más alto es el estándar, menor es el nivel de delitos cibernéticos (Veresha, 2018). En la mayoría de los casos, pasan desapercibidos y se utilizan para lanzar programas de espionaje y rescate (Rao et al., 2022). Los productos antivirus (AV) son algunos de los sistemas de protección de seguridad más utilizados (Mylnikov et al., 2022)(Holguín Mendoza, 2021).

Un ciberataque se refiere a un individuo u organización que deliberadamente intenta dañar el sistema de información de un usuario, la complejidad y diversos de los ataques cibernéticos están aumentando y existen diferentes tipos de ataques para cada propósito malicioso. Aunque las precauciones de seguridad de la red para cada tipo de ataque son diferentes, las buenas prácticas de seguridad de la red para cada tipo de ataque y la seguridad de TI generalmente mitigan bien estos ataques, ya que la higiene de TI identifica los riesgos y vulnerabilidades (Ayala Carabajo & Llerena Izquierdo, 2017).

Además de implementar buenas prácticas de seguridad cibernética, la organización también debe implementar prácticas de codificación seguras para mantener actualizados los sistemas de seguridad y el software (Ayala Carabajo & Llerena Izquierdo, 2014)(de la Nube Toral Sarmiento et al., 2018).

Las estrategias principales para mitigar los ataques cibernéticos, que cumplen con diversidad de características dependiendo de la implementación y fuente de ejecución, cada una tendrá beneficios y prejuicios en concordancia del contexto expuesto anteriormente, estas se exponen del siguiente modo:

Tabla 2. Estrategias para ataques cibernéticos

Estrategias	Beneficios	Prejuicios
Usar firewalls y solución de administración de amenazas (García Monge, 2017)**.**	Es una aplicación o programa diseñado para garantizar la seguridad de las conexiones a internet, éste realiza monitoreo a las comunicaciones entrantes y salientes de un sistema informático y bloquea las entradas o salidas de información sin autorización (García Monge, 2017), protegiendo la red al monitorear el tráfico que ingresa a la computadora y es responsable de inspeccionar cada paquete, y si detecta un paquete dañino, lo bloquea de inmediato, lo que ayuda a mantener un alto nivel de privacidad al brindar protección contra elementos dañinos.	El firewall tiene sus limitantes determinado por sus propias características, donde se puede presentar un ciberataque si este proviene de un tráfico permitido, como el uso de puertos TCP, así mismo no puede proteger de ataques cuyo tráfico no pase por él, así como de amenazas provocadas por ataques internos o usuarios negligentes(Freire López, 2017), teniendo el riesgo de un ciberataque.
Instalar software de antivirus (García Monge, 2017)**.**	Se recomienda instalar uno en los sistemas informáticos y éste debe configurarse para que revise todo el sistema periódicamente; también es necesario verificar con frecuencia que está activo (los antivirus pueden desactivarse por error del usuario o por un virus)(García Monge, 2017). Detectando cualquier malware malicioso en nuestra computadora, mantiene el rendimiento del dispositivo y bloquea cualquier spam o publicidad.	Debido a que día a día aparecen nuevos virus (García Monge, 2017), teniendo el factor de dañar archivos, fallos frecuentes de la computadora, perdida de datos y haciendo lenta la computadora si es que ingresa algún malware y no se encuentra instalado ningún software de antivirus.
Mantener un respaldo en la nube (Chilán, 2021)**.**	Crear un programa periódico de respaldo del sistema para garantizar que sus datos sean recuperables en caso de que algo le suceda a su computadora (Chilán, 2021). En caso de datos de recuperación dañados o pérdidas, la copia de seguridad se puede restaurar si es	Las amenazas a la seguridad informática son posibles peligros que pueden obstaculizar el funcionamiento normal de su computadora (Chilán, 2021). Por eso debemos mantenernos con una

	necesario, con mayor capacidad de almacenamiento del computador.	copia de respaldo por la falta de seguridad y privacidad.
Mantener contraseñas seguras (Chilán, 2021)**.**	Las contraseñas seguras son vitales para una buena seguridad en línea. Haga que su contraseña sea difícil de adivinar (Chilán, 2021).Ingresando una combinación entre mayúsculas y minúsculas, números y símbolos, entre 8 a 12 caracteres y cambiándolo regularmente.	Las amenazas a la seguridad informática se están volviendo implacablemente inventivas en estos días (Chilán, 2021).Teniendo el factor de correr riesgo de pérdida de datos y no tener una buena protección, pudiendo, ser accedido indebidamente por usuarios no autorizados en la computadora.
Proteger los correos electrónicos (García Monge, 2017)**.**	Antes de abrir los correos electrónicos recibidos, desconfíe de los mensajes de remitentes desconocidos con adjuntos o vínculos dudosos (García Monge, 2017). Protegiendo así contra cualquier malware que quiera adquirir cualquier información personal del usuario.	Hacen llegar a los usuarios el virus en forma de archivo adjunto de un correo, normalmente, estos mensajes suplantan la información del remitente con el objetivo de generar confianza y que los receptores ejecuten el virus (García Monge, 2017). Los correos masivos de spams, es donde más peligro encontramos.

2.3. Uso incorrecto de la tecnología

En la actualidad, el uso de la tecnología es característico de todas las poblaciones a nivel local, nacional e internacional; específicamente el manejo de las redes sociales en línea son parte del diario vivir de muchas personas y, en especial, de la niñez y la adolescencia costarricense (Astorga-Aguilar & Schmidt-Fonseca, 2019)(Recalde Monar, 2021). Internet es uno de los aspectos importantes en nuestra vida, nos proporciona acceso a información del mundo real en cualquier lugar donde la red esté disponible (Abdullah et al., 2019)(Tacuri López, 2021).

Proteger los sistemas informáticos y las redes de los ataques digitales es una preocupación creciente en los últimos años (Martins et al., 2020)(Rodríguez Pesantes, 2021). Los ataques cibernéticos basados en malware tienen como objetivo principal obtener datos confidenciales, robo de propiedad intelectual, denegación de servicios y datos críticos y ganancias financieras

(Finder et al., 2022). Los delitos cibernéticos modernos han crecido exponencialmente durante la última década (Javed Butt et al., 2019).

Según un Informe de inteligencia de seguridad reciente de Microsoft (Terán Terranova, 2021)(Guaranda Lara, 2021)(Llerena-Izquierdo & Ayala-Carabajo, 2022), en promedio, una de cada cuatro computadoras no tiene un software antivirus actualizado (Carvajal Nagua & Solano Cedeño, 2021). Además, indica que los equipos tienen 5,5 veces más probabilidades de ser infectados con software malicioso (o malware) sin la protección del software antivirus (Chen & Liang, 2019)(Narváez Picón, 2021).

La tecnología actual es nuestro buen vivir, debemos tener en cuenta que se ha convertido en un entorno crítico, cuyas consecuencias no se pueden observar, y debemos tomar precauciones para evitar que los datos de los usuarios sean manipulados o robados (Guaigua Bucheli, 2021)(Reinoso Ordóñez, 2021). Hay que empezar a reflexionar sobre la tecnología y su mal uso, en cuanto a las consecuencias del avance tecnológico, la navegación por Internet y las redes sociales es inevitable, ya que favorecen la interacción y participación de diferentes virus (Pérez González, 2021)(Falconi Tamayo, 2021).

El uso inadecuado de estos servicios puede crear una serie de riesgos que deben ser atendidos para evitar que ocurran (Muñoz Campuzano, 2021). Dejar a los adolescentes navegar durante horas puede llegar a consecuencias negativas, ya que en ocasiones aceptamos spam, buscamos páginas no deseadas, etc. (Escalante Quimis, 2021). Por lo tanto, le damos acceso a los posibles virus más conocidos, como malware o software malicioso (Holguín Mendoza, 2021).

La tecnología utilizada correctamente puede mejorar la calidad de vida de las personas, pero el mal uso de esta puede causar un gran daño a las personas y a la sociedad, como el uso de la tecnología por ataques de malware. En el mal uso de la tecnología tenemos las siguientes desventajas, menor seguridad y más vulnerabilidades (Coello Ochoa, 2021).

3. METODOLOGÍA

Se utiliza una metodología de investigación empírico-analítica de corte cuantitativo y cualitativo. El marco metodológico se elaboró con el fin de contestar a los objetivos de la presente investigación los cuales se sustentan en la teoría. Estos procesos ayudaron a la

investigación a conseguir los resultados, mediante el uso de proceso, métodos y técnicas aplicados en el desarrollo de este trabajo.

Se aplica un método no experimental donde las variables motivo de estudio no serán manipuladas, solo se procederá a visualizar y analizar los hechos en su entorno habitual. Teniendo en cuenta que la población de estudio es la comunidad de la Unidad Educativa Fiscal "Luis Alfredo Noboa Icaza", se procederá a realizar una encuesta como técnica de recogida de datos, para identificar los tipos de ciberataques más frecuentes, dar a conocer los posibles riesgos y así obtener soluciones. Esta investigación tiene un enfoque cualitativo, debido a las características en el diseño del estudio para el planteamiento de las posibles soluciones que permitan obtener respuestas frente a las situaciones encontradas en la institución educativa, además, la participación de los miembros de la comunidad educativa será un factor determinante en la transmisión de conocimientos y opiniones que permitan dar una posible resolución al problema.

El enfoque cualitativo, nos facilita analizar los datos obtenidos y, de ser factible brindar una posible respuesta de los fenómenos observados. La población de estudio está conformada por 5.500 en su totalidad, haciendo el respectivo desglose contamos con 2.800 estudiantes y 2.700 padres de familia de la Unidad Educativa "Luis Alfredo Noboa Icaza", los cuales nos aportarán la información necesaria. La muestra, obtenida a través de la población, cuyos miembros comparten una o varias características nos permitirá obtener determinadamente conclusiones a partir de la información que nos puedan brindar para así conseguir conclusiones que puedan ser dirigidas hacia el cumplimiento del objetivo de la investigación. Por lo tanto, se considera el universo finito, según la determinación del tamaño de la población. En la fórmula que se aplicará para obtener la muestra, esta da como resultado 360 personas, siendo esta una muestra estratificada (dividida en docentes, estudiantes y padres).

3.1. Métodos y técnicas de Recopilación de datos empleadas

La técnica de recolección que vamos a utilizar en la presente investigación será la encuesta, para lo cual, a través de respuestas múltiples, el encuestado seleccionará la más pertinente, corroborando con información para el cumplimiento de los objetivos que se están investigando.

El instrumento de recolección de datos será una encuesta diseñada con preguntas cerradas a seleccionarse bajo la escala de Likert como instrumento de medición para analizar el uso que

se da a la tecnología y si esta es seguro o no. En este instrumento se contará con diferentes alternativas las cuales podrán ser elegidas según sea su apreciación, entre ellas, con base a estas alternativas contestarán los estudiantes, según sea su apreciación, *nunca, regularmente, siempre*, mientras que, en otras escalas, se utilizará, *alto, medio, bajo*; *sí, no*; entre otras.

3.2. Métodos y técnicas de Análisis de datos

Se aplicará el método de muestreo probabilístico de forma aleatoria simple, en donde todos los elementos que forman parte del universo finito pueden ser escogidos. Esto será realizado a los docentes, padres de familias y estudiantes, los cuales colaboraran con el objetivo de estudio, y así poder denotar a profundidad el uso que se da a la tecnología, y las causas que provocan los ciberataques.

Para la aplicación de la escala, se califica cada ítem de acuerdo con la perspectiva de entendimiento de la persona que lo conteste y así codificar la información para sacar conclusiones y darles un puntaje justo a las alternativas. Para llevar a cabo la tabulación de los datos, que se obtendrán a través de las respuestas de los estudiantes y familiares a los que se les aplicó, se utilizará el programa Google Forms, plataformas virtuales que permiten hacer encuestas online y tabular los datos al finalizar.

4. RESULTADOS

Los resultados estadísticos para cada ítem determinan distintos aspectos, estableciendo datos importantes ante el análisis de la situación de los estudiantes de la Unidad Educativa Fiscal "Luis Alfredo Noboa Icaza" entre ellas se escogió, las preguntas con mayor índice de relevancia. En la figura 1 se indica el tipo rol dentro de la Unidad Educativa.

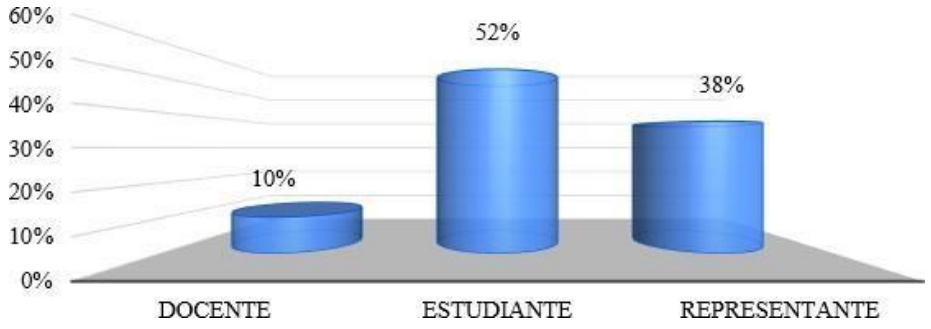


Figura 1. Porcentaje de participantes en el estudio de acuerdo con su rol

Se observa que un 10% de participación en este estudio corresponde al personal docente, un 52% de participación corresponde a los estudiantes y un 38% de participación corresponde al representante del estudiante (ver Fig. 1).

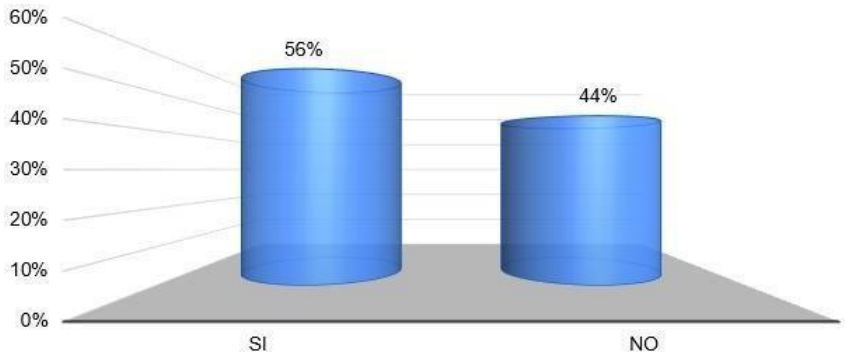


Figura 2. Porcentaje de participantes que indican conocer un ciberataque

A los participantes se les consultó sobre si conoce o no qué es un ciberataque, obteniendo que un 56% indica que sí y un 44% indica que no conoce. Con esto se evidencia que existe un porcentaje todavía de personas que no conocen qué es un ciberataque (ver Fig. 2).

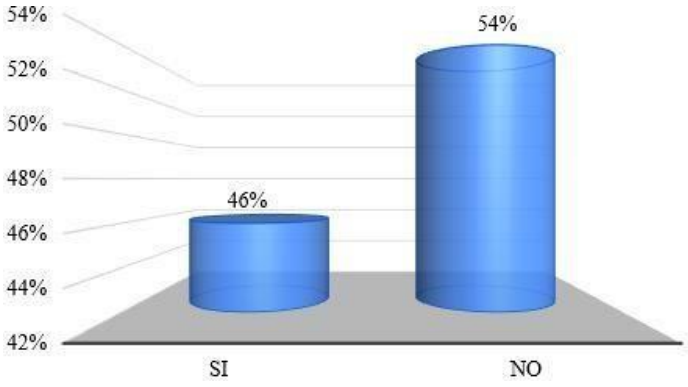


Figura 3. Porcentaje de participantes que indican conocer los tipos de ataques electrónicos

A los participantes se les consultó sobre si conocen los distintos tipos de ataques electrónicos desde internet, obteniendo que un 46% indica que sí y un 54% indican que no conoce. Con esto se evidencia que existe un porcentaje al de personas que no tienen conocimientos sobre los distintos tipos de ataques electrónicos (ver Fig.3).

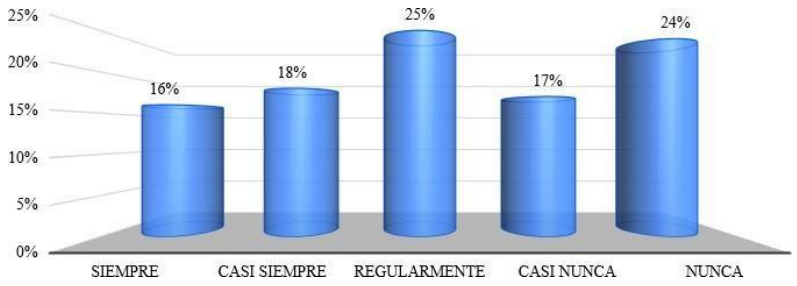


Figura 4. Porcentaje de participantes que realizan respaldo de información

A los participantes se les consultó si realizan algún respaldo de información de su computadora en algún medio digital o repositorio en internet, obteniendo que un 16% indican que siempre han realizado respaldo de información en su computador, un 18% indican que casi siempre, un 25% indican que regularmente, un 17% indican que casi nunca y un 24% indican que nunca han realizado respaldo de información (ver Fig. 4).

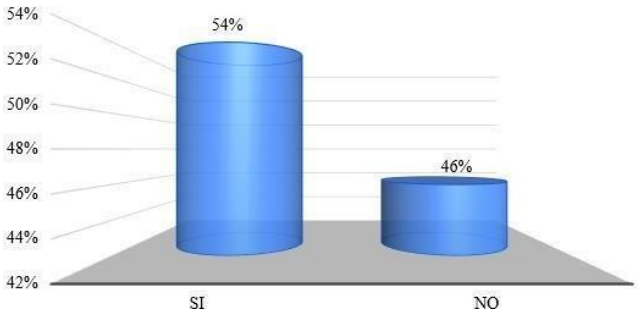


Figura 5. Porcentaje de participantes que utiliza algún software de antivirus

A los participantes se les consultó sobre si es que utilizan algún software como antivirus en su equipo, obteniendo que un 54% indica que sí y un 46% indican que no utilizan software de antivirus. Con esto se evidencia que existe un porcentaje todavía de personas que si utilizan un software de antivirus en su equipo (ver Fig. 5).

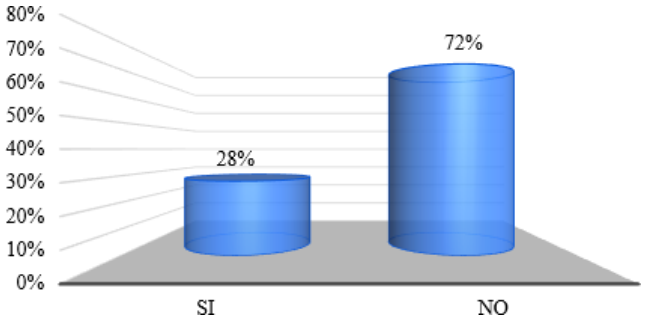


Figura 6. Porcentaje de participantes que creen que las contraseñas de los sitios webs son seguras

A los participantes se les consultó sobre que, si creen que las contraseñas de los sitios webs que utilizan constantemente son seguras, obteniendo que un 28% indica que sí y un 72% indica que no son seguras las contraseñas. Con esto se evidencia que existe un porcentaje todavía al de personas que no creen que las contraseñas que utilizan constantemente son seguras (ver Fig. 6).

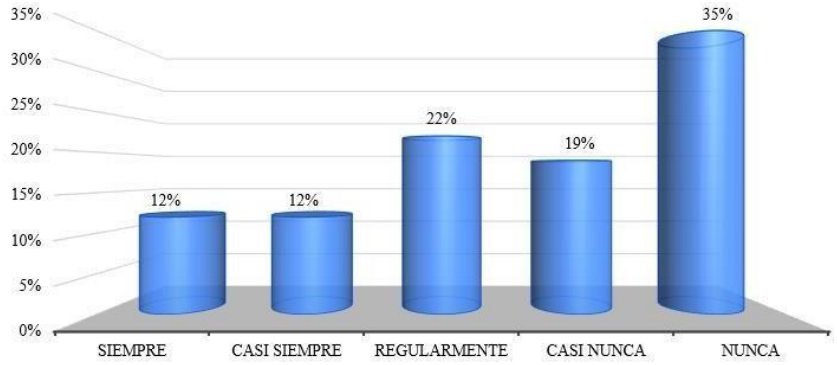


Figura 7. Porcentaje de participantes que utilizan dispositivos de almacenamiento

A los participantes se les consultó si utilizan dispositivos de almacenamiento secundarios como USB, disco duro u otros para realizar actividades académicas en la Unidad Educativa, obteniendo que un 12% indican que siempre han utilizado dispositivos de almacenamiento, un 12% indican que casi siempre, un 22% indican que regularmente, un 19% indican que casi nunca y un 35% indican que nunca han utilizado dispositivos de almacenamiento para realizar sus actividades académicas. Con esto se evidencia que existe un porcentaje todavía al de personas que nunca han utilizado dispositivos de almacenamientos secundarios (ver Fig. 7).

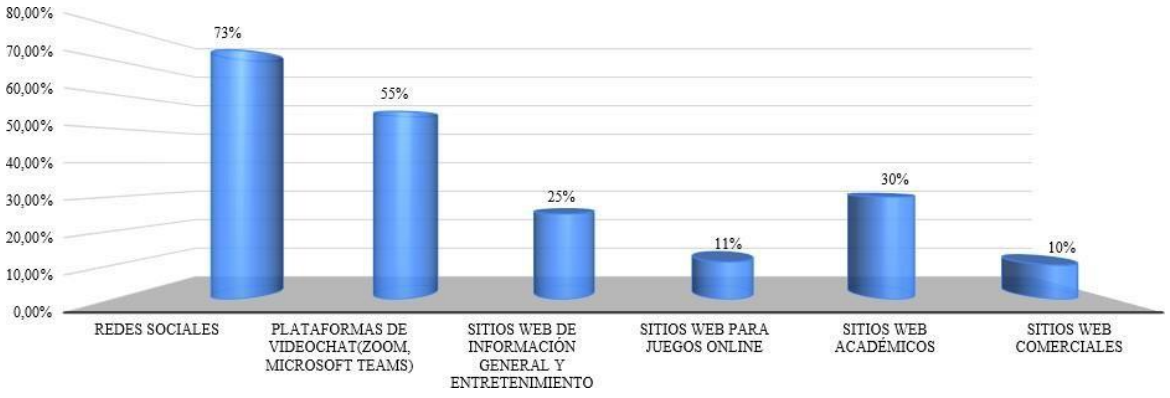


Figura 8. Porcentaje de participantes que acceden a servicios de internet con frecuencia

A los participantes se les consultó cuáles son los siguientes servicios de internet que accede con frecuencia, obteniendo que un 73% indican que ingresan en las redes sociales, el 55% indican que ingresan a las plataformas de video chat (Zoom, Microsoft teams, etc.), un 25% ingresan a sitios web de información general y de entretenimiento, el 11% ingresan a sitios web para juegos online, el 30% ingresan a sitios web académicos y con un 10% ingresan a sitios webs comerciales. Con esto se evidencia que existe un porcentaje todavía al de personas que acceden a las redes sociales con frecuencia (ver Fig. 8).

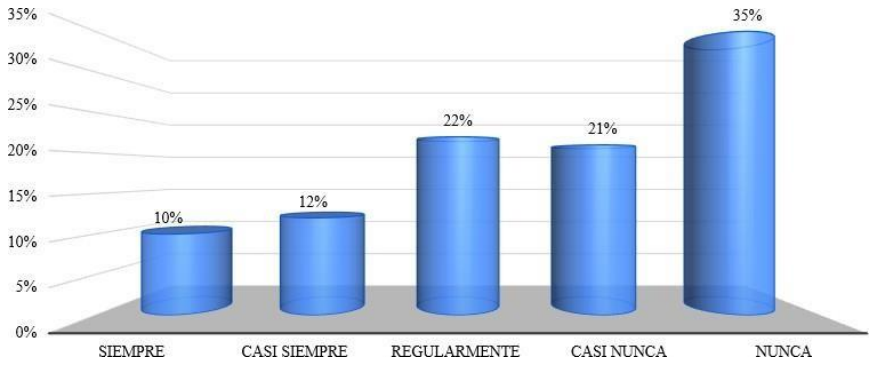


Figura 9. Porcentaje de participantes que conectan dispositivos de almacenamiento en su computador

A los participantes se les consultó si conectan algún dispositivo de almacenamiento masivo a su computador, obteniendo que un 10% indican que siempre conectan dispositivos de almacenamiento en su computador, el 12% indican que casi siempre, que el 22% regularmente, el 21% casi nunca y que el 35% nunca han conectado dispositivos de almacenamiento masivos en su computador. Con esto se evidencia que existe un porcentaje todavía al de personas que nunca han conectado dispositivos de almacenamiento en su computador (ver Fig. 9).

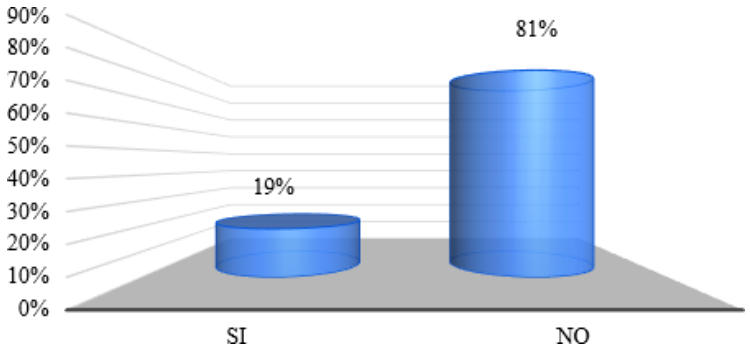


Figura 10. Porcentaje de personas que han sido víctima de robo o pérdida de información digital

A los participantes se les consultó de que, si han sido víctimas de robo o pérdida de información digital de carácter personal por virus o delincuentes informáticos, obteniendo que un 19% indica que sí y un 81% indican que no han sido víctimas de robo o perdida de información digital. Con esto se evidencia que existe un porcentaje todavía de personas que no han sido víctimas por delincuentes informáticos (ver Fig. 10).

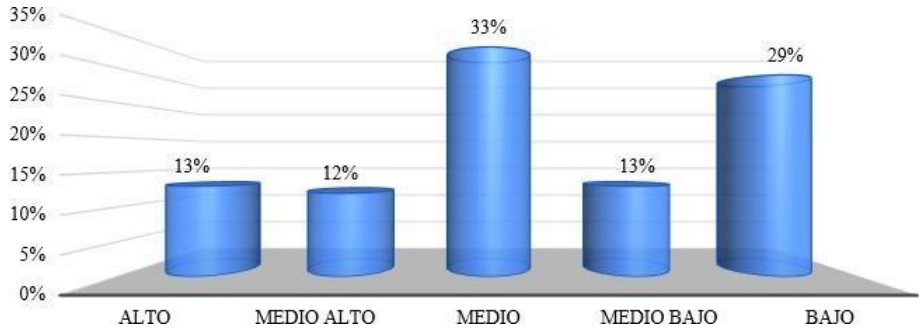


Figura 11. Porcentaje de personas sobre el conocimiento de los peligros por ciberataques

A los participantes se les consultó sobre el conocimiento que tienen acerca de los peligros que pueden producirse por ciberataques, obteniendo que un 13% indican que alto es el porcentaje del conocimiento de los peligros, un 12% medio alto, un 33% medio, un 13% medio bajo y un 29% bajo. Con esto se evidencia que existe un porcentaje todavía al de personas, que medio es el porcentaje que tienen sobre el conocimiento de los peligros que pueden producirse por ciberataques (ver Fig. 11).

5. DISCUSIÓN

Los resultados obtenidos en el presente trabajo de investigación permiten denotar que el conocimiento acerca de la prevención de ciberataques que poseen los estudiantes, padres de familia y representantes de la Unidad Educativa Fiscal “Luis Alfredo Noboa Icaza” es bajo y que se requieren acciones afirmativas para mejorar el nivel de seguridad informática con el objetivo de evitar el robo de información de tipo personal, la cual pueda ser utilizada de forma negativa (Salazar, 2018)(Montenegro Cruz, 2006)(Vera Navas, 2021).

Además, en los resultados obtenidos se puede observar que un alto porcentaje de personas no conocen acerca de los distintos tipos de ataques electrónicos que pueden ser realizados desde internet, por lo tanto, es necesario hacer énfasis en este tema, ya que puede ser considerado el punto de partida para evitar situaciones de riesgos informáticos. Adicionalmente, se debe de

crear una cultura de autoprotección ya que también es visible que muchas personas no tienden a proteger su información personal ni mucho menos la respaldan en las diferentes plataformas o recursos que se pueden utilizar (Miranda Jiménez, 2021)(Muñoz Campuzano, 2021).

Es también preocupante que un alto grado de personas, según la muestra no cuentan si quieran con un software antivirus básico que permita disminuir los riesgos informáticos que puedan suscitarse en las actividades que realizan a diario. Por otro lado, se vuelve necesario implementar una guía que permita a las personas conocer de qué forma se puede crear contraseñas más seguras, las mismas que son utilizadas diariamente en diferentes aplicaciones y sitios webs; así, disminuir la facilidad que tienen los hackers de acceder a información personal.

Es importante recalcar que un alto porcentaje de los encuestados manifiestan a acceder a servicios de internet con frecuencia, siendo los recursos más utilizados las redes sociales. Este punto es importante ya que un mundo globalizado, en el cual cada vez es más sencillo acceder a internet, las personas deben conocer con claridad los beneficios que se puede obtener de estas plataformas, pero también, los diversos peligros que pueden surgir de no utilizar adecuadamente este recurso.

Por eso debemos utilizar todos los recursos que se encuentren disponibles, que sean de fácil acceso y mayormente comprensible para las personas, en especial, para aquellas que no poseen conocimientos avanzados en el uso de las tecnologías de información y comunicación (TICs) (López & Parra, 2015)(Llerena et al., 2021). Además, generar en las personas el hábito de compartir estas estrategias hacia otros miembros cercanos y poder ampliar el alcance y aporte de este proyecto a la comunidad Educativa (López & Parra, 2015)(Álava Morán, 2021).

6. CONCLUSIÓN

En este trabajo de investigación se pudo identificar los tipos de ciberataques en el contexto de la Unidad Educativa Fiscal “Luis Alfredo Noboa Icaza”, entre ellos podemos mencionar los troyanos y ransomware ya que según las encuestas existen personas que han sido víctimas de algún tipo de robo de información de tipo digital a causa de algún virus o delincuente informático, aunque los resultados por otro lado demuestren que existe conocimiento de ciertas personas en el área de seguridad de informática, se puede entender que aún existen aspectos

que deben ser mejorados y así poder tener mejores herramientas con las cuales se pueda evitar el acceso de los hackers a la información personal de los miembros de la unidad educativa.

Se logró determinar las estrategias de prevención para mitigar los ataques informáticos, entre ellos se recomienda el uso de firewalls, los cuales podrán ser conseguidos a través del uso de softwares antivirus, y en caso de no contar con la capacidad económica para adquirir una licencia pagada, dar a conocer otras alternativas gratuitas como el Windows defender. Además, recalcar la importancia de mantener un respaldo en la nube de su información tanto personal como de cualquier otro tipo. Promover el uso de contraseñas seguras que disminuyan el riesgo de ser víctimas de ataques informáticos y la importancia de proteger los correos electrónicos.

Se pudo valorar los aspectos y beneficios de una adecuada implementación de medidas de ciberseguridad, de esta forma se puede indicar que una correcta aplicación de herramientas informáticas nos permite garantizar la seguridad de nuestra conexión a internet también la protección de las redes pudiendo actuar a tiempo antes de que los delincuentes informáticos puedan acceder a los datos de la computadora. Otro beneficio que destacar es que los programas de antivirus permiten verificar de forma periódica si existe algún software malicioso en los equipos y así proteger el rendimiento del dispositivo. Adicionalmente la restauración de los datos es un tema que debe ser enfatizado ya que la información personal, en general, es el principal objetivo de los hackers, por ello, realizar la copia de seguridad permite a las personas protegerse frente a un posible robo de datos, sin embargo, una de las desventajas es la inminente conexión a internet con la que debe contar la institución para poder funcionar.

Se puede destacar que al conocer los datos obtenidos a través de la encuesta, así como los beneficios de tener una buena seguridad informática y, además, conocer las diferentes estrategias de prevención es que estos procesos nos permiten ampliar la visión hacia uno de los problemas que más afectan a la vida digital de la unidad educativa , de esta forma el presente trabajo de investigación pretende colaborar con datos que evidencien la problemática desde su origen y que ayude a determinar qué elementos requieren de una mayor adquisición de conocimientos.

REFERENCIAS

Abdullah, M. S., Zainal, A., Maarof, M. A., & Nizam Kassim, M. (2019). Cyber-Attack Features for Detecting Cyber Threat Incidents from Online News. *Proceedings of the 2018 Cyber Resilience Conference, CRC 2018*, 2–5. https://doi.org/10.1109/CR.2018.8626866

Aguirre Sánchez, M. J. (2021). *Tecnologías de Seguridad en Bases de Datos: Revisión Sistemática* . http://dspace.ups.edu.ec/handle/123456789/20566

Álava Morán, N. S. (2021). *Metodologías y técnicas analíticas de aprendizaje en la educación superior: un mapeo sistemático*.

Alsulami, B., & Mancoridis, S. (2019). Behavioral Malware Classification using Convolutional Recurrent Neural Networks. *MALWARE 2018 - Proceedings of the 2018 13th International Conference on Malicious and Unwanted Software*, 103–111. https://doi.org/10.1109/MALWARE.2018.8659358

Alvarado Ronquillo, M. L. (2021). *Analysis for the adoption of security standards to improve the management of securities in public organizations*. https://dspace.ups.edu.ec/handle/123456789/19760

Andrade Medina, A. V. (2021). *Gestión Informática Educativa: Un mapeo sistemático*. https://dspace.ups.edu.ec/handle/123456789/20841

Andrade Valdez, J. A., & Galarza Zurita, G. P. (2019). *Elaboración de recomendaciones de buenas prácticas a partir del estudio de los principales tipos de malware Ransomware que han atacado en Ecuador a las estaciones de trabajo con sistema operativo Windows mediante análisis dinámico y estático*. 215.

Astorga-Aguilar, C., & Schmidt-Fonseca, I. (2019). Social nerworks dangers: How to educate our childs in cibersecurity. *Revista Electronica Educare*, *23*(3), 1–24. https://doi.org/10.15359/ree.23-3.17

Ayala Carabajo, R., & Llerena Izquierdo, J. (2014). *Primer Congreso Salesiano de Ciencia, Tecnología e Innovación para la Sociedad. Memoria Académica*. http://dspace.ups.edu.ec/handle/123456789/9506

Ayala Carabajo, R., & Llerena Izquierdo, J. (2017). *Tercer Congreso Internacional de Ciencia, Tecnología e Innovación para la Sociedad*. https://dspace.ups.edu.ec/handle/123456789/14450

Carvajal Nagua, K. A., & Solano Cedeño, C. S. (2021). *Desarrollo de una Aplicación Web para el Control de citas y manejo de historial médico en la Unidad Médica Family care de la ciudad de Guayaquil*. https://dspace.ups.edu.ec/handle/123456789/20905

Chen, D. Q., & Liang, H. (2019). Wishful Thinking and IT Threat Avoidance: An Extension to the Technology Threat Avoidance Theory. *IEEE Transactions on Engineering Management*, *66*(4), 552–567. https://doi.org/10.1109/TEM.2018.2835461

Chévez Morán, M. J. (2021). *Estudio de los patrones de seguridad para la atenuación de las irregularidades, las debilidades y amenazas en empresas de servicios de telecomunicaciones*. http://dspace.ups.edu.ec/handle/123456789/20568

Chilán, G. (2021). *Medidas de seguridad informática para la implementación de repositorio de almacenamiento de documentos en la carrrera de tecnología de la información, Universidad Estatal del Sur de Manabí*.

Coello Ochoa, I. N. (2021). *Análisis de ciberataques en organizaciones públicas del Ecuador y sus impactos administrativos*. http://dspace.ups.edu.ec/handle/123456789/20738

de la Nube Toral Sarmiento, A., Loaiza Martínez, M. de L., Llerena Izquierdo, J., Ayala Carabajo, R., Torres Toukoumidis, A., Romero-Rodríguez, L. M., Aguaded, I., Vega Ureta, N. T., Fuentes Espinoza, P. G., Peñafiel Caicedo, J. A., & others. (2018). *4to. Congreso Internacionalde Ciencia, Tecnología e Innovación para la Sociedad. Memoria académica*. https://dspace.ups.edu.ec/handle/123456789/16318

Escalante Quimis, O. A. (2021). *Prototipo de sistema de seguridad de base de datos en organizaciones públicas para mitigar ataques cibernéticos en Latinoamérica*. http://dspace.ups.edu.ec/handle/123456789/20576

Falconi Tamayo, L. F. (2021). *Desarrollo e implementación de una aplicación Web para la Gestión de Boletería de Vilaró Microteatro Restaurante*.https://dspace.ups.edu.ec/handle/123456789/20292

Finder, I., Sheetrit, E., & Nissim, N. (2022). Time-interval temporal patterns can beat and explain the malware. *Knowledge-Based Systems*, *241*, 108266. https://doi.org/10.1016/j.knosys.2022.108266

Florez, C. A. G., & Pinzon, C. A. A. (2017). Protocolos Para La Mitigacion De Ciberataques En El Hogar. *Universidad Catolica De Colombia*, 79.

Freire López, K. B. (2017). *Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad*. 119.

García Monge, A. R. (2017). *Seguridad Informáticay el Malware*. 1–11.

Guaigua Bucheli, C. J. (2021). *Algoritmos de seguridad para mitigar riesgos de datos en la nube: un mapeo sistemático*. https://dspace.ups.edu.ec/handle/123456789/20319

Guaman Villalta, M. G. (2021). *Hyperledger Blockchain para la seguridad en bases de datos un mapeo sistemático*. https://dspace.ups.edu.ec/handle/123456789/20320

Guaranda Lara, S. N. (2021). *Modelo de gestión para el alineamiento de estrategias corporativas en pymes mediante las tecnologías de la información y comunicación*. http://dspace.ups.edu.ec/handle/123456789/20911

Holguín Mendoza, J. D. (2021). *Categorización de protocolos de seguridad en criptomonedas para mitigar ataques informáticos: una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20915

Javed Butt, U., Abbod, M., Lors, A., Jahankhani, H., Jamal, A., & Kumar, A. (2019). Ransomware Threat and its Impact on SCADA. *Proceedings of 12th International Conference on Global Security, Safety and Sustainability, ICGS3 2019*. https://doi.org/10.1109/ICGS3.2019.8688327

Kebede TM, Djaneye-Boundjou O, Narayanan BN, Ralescu A, K. D. (2017). *Classification of malware programs using autoencoders based deep learning architecture and its application to the microsoft malware classification challenge (BIG 2015) dataset.* 70-75.

Kim, H. M., Song, H. M., Seo, J. W., & Kim, H. K. (2018). Andro-Simnet: Android Malware Family Classification using Social Network Analysis. *2018 16th Annual Conference on Privacy, Security and Trust, PST 2018*. https://doi.org/10.1109/PST.2018.8514216

Lezama, A. La. (2016). Advances in Natural Language Processing and Computational Linguistics. *Research in Computing Science*, *115*.

Llerena-Izquierdo, J., & Ayala-Carabajo, R. (2022). Inventory of ICTs for learning in engineering for emergency virtual teaching by COVID-19. *2022 IEEE World Engineering Education Conference (EDUNINE)*, 1–6. https://doi.org/10.1109/EDUNINE53672.2022.9782389

Llerena Izquierdo, J., Naranjo Sánchez, R., Zambrano Santos, M., & Espol. (2018, July 5). *Sistema de*

información geográfico socioeconómico y del medio ambiente. Espol. http://www.dspace.espol.edu.ec/handle/123456789/43942

Llerena Izquierdo, J., Ortiz Rojas, J. G., Mora Saltos, N. S., & Freire, L. (2009, February 20). *Sistema de Gestión de Asistencia Institucional, SIGAI*. https://www.dspace.espol.edu.ec/handle/123456789/767

Llerena, J., Alava-Moran, N., & Zamora-Galindo, J. (2021). Learning analytics for student academic tracking, a comparison between Analytics Graphs and Edwiser Reports. *2021 Second International Conference on Information Systems and Software Technologies (ICI2ST)*, 101–107. https://doi.org/10.1109/ICI2ST51859.2021.00022

López, C., & Parra, A. (2015). *Análisis técnico de los recursos disponibles de la UEFS Santa María Mazzarello de Guayaquil para el diseño e implementación de un escenario de arquitectura*. 143. http://dspace.ups.edu.ec/handle/123456789/10286

Makandar, A., & Patrot, A. (2017). *Malware class recognition using image processing techniques*. 2017 International Conference on Data Management, Analytics and Innovation, ICDMAI 2017. https://doi.org/10.1109/ICDMAI.2017.8073489

Mariam, M., & Morgado, C. (2021). *El malware y las redes sociales*.

Martins, N., Cruz, J. M., Cruz, T., & Henriques Abreu, P. (2020). Adversarial Machine Learning Applied to Intrusion and Malware Scenarios: A Systematic Review. *IEEE Access*, *8*, 35403–35419. https://doi.org/10.1109/ACCESS.2020.2974752

Melendrez-Caicedo, G., & Llerena-Izquierdo, J. (2022). Secure Data Model for the Healthcare Industry in Ecuador Using Blockchain Technology. *Smart Innovation, Systems and Technologies*, *252*, 479–489. https://doi.org/10.1007/978-981-16-4126-8_43

Miranda Jiménez, J. N. (2021). *Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos*. http://dspace.ups.edu.ec/handle/123456789/20966

Moncayo Ronquillo, K. C. (2021). *Seguridades de la información bases de datos distribuidas: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/21701

Montenegro Cruz, A. (2006). *Diseño e implementación de un software educativo para niños discapacitados de SERLI en la ciudad de Guayaquil*. http://dspace.ups.edu.ec/handle/123456789/3185

Morán Maldonado, N. M. (2021). *Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática*. http://dspace.ups.edu.ec/handle/123456789/20243

Muñoz Campuzano, P. S. (2021). *Modelos de seguridad para prevenir riesgos de ataques Informáticos: Una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20932

Mylnikov, V. A., Bezzateev, S. V, & Mylnikov, N. V. (2022). Modeling the Security System of the Cloud IoT Platform of an Smart Supermarket. *2022 Wave Electronics and Its Application in Information and Telecommunication Systems (WECONF)*, 1–4. https://doi.org/10.1109/WECONF55058.2022.9803415

Narváez Picón, E. A. (2021). *Las tecnologías de la información y comunicación orientadas a la calidad del servicio en la gestión empresarial: una revisión sistemática*. https://dspace.ups.edu.ec/handle/123456789/20929

Orozco Bonilla, C. A. (2021). *Estrategias algorítmicas orientadas a la ciberseguridad: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/20933

Pérez González, R. F. (2021). *Softwares de penetración utilizados por los piratas informáticos: Una revisión sistemática (2015-2020)*.

Ponce Larreategui, J. G. (2021). *Indicadores de compromiso (IOC) para detección de amenazas en la seguridad informática con enfoque en el código malicioso*. http://dspace.ups.edu.ec/handle/123456789/20937

Rao, V. V., Marshal, R., & Gobinath, K. (2022). *The IoT Supply Chain Attack Trends-Vulnerabilities and Preventive Measures*. 1–4. https://doi.org/10.1109/isea-isap54304.2021.9689704

Recalde Monar, J. A. (2021). *El ciberacoso por redes sociales en el Ecuador*. http://dspace.ups.edu.ec/handle/123456789/20945

Reinoso Ordóñez, L. A. (2021). *Desarrollo de sistema informático para la gestión de pagos de cuotas de los residentes de la Urbanización Belo Horizonte*. https://dspace.ups.edu.ec/handle/123456789/20332

Rodríguez Pesantes, R. P. (2021). *Seguridad en dispositivos IOT en Organizaciones de América Latina*. http://dspace.ups.edu.ec/handle/123456789/20970

Roseline, S. A., Geetha, S., Kadry, S., & Nam, Y. (2020). Intelligent Vision-Based Malware Detection and Classification Using Deep Random Forest Paradigm. *IEEE Access*, *8*, 206303–206324. https://doi.org/10.1109/ACCESS.2020.3036491

Rosero Tejada, L. F. (2021). *El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/21699

Salazar, L. (2018). *Implementación de sistema de matriculación y carnetización en la unidad educativa Pablo Picasso.* http://dspace.ups.edu.ec/handle/123456789/16844

Sánchez Guzmán, C. O. (2021). *Modelo de red segura en un entorno distribuido para la transferencia de datos con mecanismos básicos de seguridad*. https://dspace.ups.edu.ec/handle/123456789/20321

Tacuri López, I. L. (2021). *Acoso por medio de las tecnologías en las redes sociales durante tiempos de pandemia en Ecuador, una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20242

Terán Terranova, Y. J. (2021). *Seguridad en la Gestión de la información para las organizaciones públicas desde el enfoque ISO/IEC 2700: un Mapeo Sistemático*. https://dspace.ups.edu.ec/handle/123456789/20333

Toala Indio, Y. I. (2021). *Delitos informáticos frecuentes en el Ecuador: casos de estudio*. http://dspace.ups.edu.ec/handle/123456789/20942

Vera Navas, N. A. (2021). *Modelo de seguridad informática para riesgos de robo de información por el uso de las redes sociales*. http://dspace.ups.edu.ec/handle/123456789/20949

Veresha, R. V. (2018). Preventive measures against computer related crimes: Approaching an individual. *Informatologia*, *51*(3–4), 189–199. https://doi.org/10.32914/i.51.3-4.7

ANEXO

Encuesta aplicada a los miembros de la Institución Educativa.

Indique su rol dentro de la Unidad Educativa Luis Alfredo Noboa Icaza*
Docente
Estudiante
Representante
1. ¿Sabe usted qué es un ciberataque? *
Sí
No
2. ¿Conoce usted los distintos tipos de ataques electrónicos desde Internet? *
Sí
No
3. ¿Usted realiza el respaldo de información de su computadora en algún medio digital o repositorio en Internet? *
Pueden ser servicios como OneDrive, Google drive, correo electrónico propio o de su empresa
Siempre
Casi siempre
Regularmente
Casi nunca
Nunca
4. ¿Usted utiliza algún software como antivirus en su equipo? *
Sí
No
5. En su opinión, ¿Usted cree que las contraseñas de los sitios webs que utiliza constantemente son seguras? *
Sí
No
6. ¿Utiliza dispositivos de almacenamiento secundario como USB, discos duro u otros para realizar actividades académicas en la Unidad Educativa Luis Alfredo Noboa Icaza? *
Siempre
Casi siempre
Regularmente
Casi nunca
Nunca
7. ¿Cuáles de los siguientes servicios de Internet usted accede con frecuencia? *
Redes Sociales
Plataformas de Videochat (Zoom, Google Meet, Microsoft Teams, etc.)
Sitios web de información general y entretenimiento
Sitios web para juegos online
Sitios web académicos
Sitios web comerciales

8. ¿Usted conecta dispositivos de almacenamiento masivo a su computador? * Como celulares, USBs, etc.
Siempre
Casi siempre
Regularmente
Casi nunca
Nunca
9. ¿Alguna vez has sido víctima de robo o pérdida de información digital de carácter personal por virus o delincuentes informáticos? *
Sí
No
10. ¿Cuál es el nivel de conocimiento que usted tiene acerca de los peligros que pueden producirse por ciberataques? *
Por ejemplo, de virus como: troyanos, gusanos, spyware, adwares o ransomware.
Alto
Medio alto
Medio
Medio bajo
Bajo