UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE COMPUTACIÓN

Evaluación de las buenas prácticas de ciberseguridad en los estudiantes universitarios: un estudio en la Universidad Politécnica Salesiana sede Guayaquil

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

AUTOR: Jóshua David Torres Chávez y Joel Aarón Mata Pazmiño

TUTOR: Ing. Dario Fernando Huilcapi Subía, Msc.

Guayaquil – Ecuador

2024

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, Jóshua David Torres Chávez con documento de identificación N° 0953015617 y Joel Aarón Mata Pazmiño con documento de identificación N° 0951201557; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos 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, 05 de febrero del año 2024

Atentamente,

Jóshua David Torres Chávez

0953015617

Joel Aarón Mata Pazmiño

0951201557

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

Nosotros, Jóshua David Torres Chávez con documento de identificación No. 0953015617 y Joel Aarón Mata Pazmiño con documento de identificación No. 0951201557, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Artículo Académico: "Evaluación de las buenas prácticas de ciberseguridad en los estudiantes universitarios: un estudio en la Universidad Politécnica Salesiana sede Guayaquil", el cual ha sido desarrollado para optar por el título de: Ingeniero de en ciencias de la 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, 05 de febrero del año 2024

Atentamente,

Jóshua David Torres Chávez

0953015617

Joel Aarón Mata Pazmiño

0951201557

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Dario Fernando Huilcapi Subía con documento de identificación N° 0920375177, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: Evaluación de las buenas prácticas de ciberseguridad en los estudiantes universitarios: un estudio en la Universidad Politécnica Salesiana sede Guayaquil, realizado por Jóshua David Torres Chávez con documento de identificación No. 0953015617 y Joel Aarón Mata Pazmiño con documento de identificación No. 0951201557, 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, 05 de febrero del año 2024

Atentamente,

Ing. Dario Fernando Huilcapi Subía, Msc.
0920375177

DEDICATORIA

Este artículo está dedicado con todo mi amor y gratitud a mi familia, quienes han sido mi mayor apoyo y motivación en cada paso de mi vida. A mis padres, por su amor incondicional, sabiduría y sacrificio para brindarme las mejores oportunidades. A mis hermanas, por su compañía, risas y apoyo incondicional.

Jóshua David Torres Chávez

Dedico este trabajo y años de esfuerzo primeramente a mi Dios, quien me guio con sabiduría, conocimiento y entendimiento a lo largo de este camino, a mi madre Leonor Pazmiño Alvarado y a mi padre Luis Mata Morales, quienes son mis pilares, cuyo amor y sacrificio lograron que cumpliera esta meta guiándome por el buen camino.

A mis hermanos y familiares, que siempre creyeron en mí y como última mención, a mi pareja Rosario Valverde Suárez, que me acompañó en todo momento y que, gracias a su ayuda, pude seguir adelante superando cada obstáculo.

Proverbios 16:3

Joel Aarón Mata Pazmiño

AGRADECIMIENTO

Quisiera expresar mi más sincero agradecimiento a todas las personas que han hecho posible la realización de este artículo; En primer lugar, a mis padres, por su amor incondicional, apoyo constante y sacrificio para brindarme la oportunidad de seguir mis sueños; A mis hermanas, por su aliento y comprensión en cada etapa de este proceso; A mi familia, por su inquebrantable respaldo y motivación. Así mismo, deseo agradecer a mis docentes, cuya orientación y conocimientos han sido fundamentales en mi formación académica y en la elaboración de este trabajo; A mi tutor, por su guía experta, paciencia y dedicación en el desarrollo de este artículo. Sus contribuciones han sido invaluables y me siento profundamente agradecido por contar con su apoyo en este proyecto.

Jóshua David Torres Chávez

Agradezo a mis padres, quienes me ayudaron en todo lo que puedieran con tal de cumplir mi meta, me enseñaron de valores y que todo en la vida se puede lograr, si te lo propones. A todas las personas que estuvieron a lo largo de este camino, a mi pareja que me tuvo mucha paciencia y me daba motivación para seguir adelante, a las amistades de mi madre, a la Msc. Carmen López, la Lcda. Mariuxi Riofrio y la Msc. Maryuri Cortez, personas que creyeron en mí, a la Dra. Yanina Pincay, que siempre me brindo su ayuda y a mi tutor, por las enseñanzas y conocimientos brindados para lograr este trabajo.

Muchas gracias a todos.

Joel Aarón Mata Pazmiño

RESUMEN

Las buenas prácticas de ciberseguridad son esenciales en los entornos universitarios, por lo que se realizó una evaluación del nivel de conocimiento y de las buenas prácticas en ciberseguridad entre los estudiantes universitarios de la Universidad Politécnica Salesiana sede Guayaquil. Se empleó una metodología mixta, la cual combina técnicas cuantitativas y técnicas cualitativas para la recopilación de datos respecto a las buenas prácticas en la ciberseguridad, ataques más comunes en entornos universitarios, además, se realizó una revisión bibliográfica a través de la aplicación del método prisma, donde se analizó cerca de 22 artículos de las bases de datos más importantes, se logró identificar cuáles son las amenazas más comunes en los entornos universitarios (como el Phishing, Malware, etc…), cuáles son las buenas prácticas que se pueden emplear ante dichas amenazas, por ello fue necesario desarrollar una encuestas, con la que se recopilaron datos que revelaron la necesidad de promover estas prácticas entre los estudiantes, aunque un alto porcentaje de encuestados tiene conocimiento de las buenas prácticas, existe un grupo significativo que carece de este conocimiento, además, se sugiere recomendaciones específicas para mejorar la educación y la conciencia sobre ciberseguridad en la Universidad Politécnica Salesiana sede Guayaquil.

Palabras claves: Ciberseguridad, Ataques Cibernéticos, Buenas prácticas, Phishing, Malware.

ABSTRACT

Good cybersecurity practices are essential in university environments, so an evaluation of the level of knowledge and good practices in cybersecurity was carried out among university students at the Salesian Polytechnic University in Guayaquil. A mixed methodology was used, which combines quantitative and qualitative techniques for the collection of data regarding good practices in cybersecurity, the most common attacks in university environments, in addition, a bibliographic review was carried out through the application of the prism method, where about 22 articles from the most important databases were analyzed. It was possible to identify which are the most common threats in university environments (such as Phishing, Malware, etc...), what are the good practices that can be used in the face of these threats, so it was necessary to develop a survey, with which data were collected that revealed the need to promote these practices among students, although a high percentage of respondents are aware of good practices, There is a significant group that lacks this knowledge, in addition, specific recommendations are suggested to improve education and awareness about cybersecurity at the Salesian Polytechnic University in Guayaquil.

Key words: Cybersecurity, Cyber Attacks, Good Practices, Phishing, Malware.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

La seguridad cibernética es un aspecto crucial en el entorno universitario, donde la integridad de la información personal y académica enfrenta constantes amenazas, en la cual los estudiantes reciben correos electrónicos maliciosos, con el afán de obtener información confidencial y/o personal, ante esta situación se plantea las siguientes interrogantes de gran relevancia respecto al nivel de conocimiento y las buenas prácticas en la ciberseguridad por parte de los estudiantes de la Universidad Politécnica Salesiana sede Guayaquil.

Los estudiantes en la actualidad utilizan el internet y la tecnología para fines estudiantiles y para la comunicación entre familiares. Los estudiantes son los futuros líderes de nuestra sociedad. Su comportamiento seguro afectara significativamente la forma como vivimos y trabajamos (Peker et al., 2018).

Trabajar en un entorno cibernético se ha vuelvo indispensable para todos los estudiantes, dado que es esencial para sus labores y tareas. Utilizar estos recursos a aumentado el riesgo de seguridad en sus datos personales. Los ciberdelincuentes están implementando nuevas herramientas y tecnologías para lograr dichos ataques cibernéticos (Sharma et al., 2023).

El objetivo general es evaluar los conocimientos y buenas prácticas en el campo de la ciberseguridad en los estudiantes de la Universidad Politécnica Salesiana sede Guayaquil, para poder lograr este propósito, nos planteamos objetivos específicos, tales como realizar una revisión bibliográfica de las amenazas cibernéticas más comunes que enfrentan los estudiantes universitarios, evaluar el estado actual de los conocimientos y buenas prácticas de ciberseguridad de los estudiantes, y proponer un marco de acción referencial que permita fortalecer la seguridad cibernética a través del desarrollo y la propuesta de un plan de acción.

2. REVISIÓN DE LITERATURA

2.1. Buenas prácticas en la ciberseguridad

2.1.1. Implementación de la Autenticación de Dos Factores (2FA)

El artículo presentado por (Ellahi et al., 2022) indica que la autenticación de contraseña proporciona un nivel básico de seguridad. La falta de conocimiento en la seguridad y la reutilización a la hora de generar una contraseña empeora la situación. El phishing es uno de los ataques más comunes de robar credenciales de usuarios, e incluso los profesionales de TI son víctimas. La autenticación de dos factores (2FA) es un servicio diseñado para resguardar a los usuarios de posibles robos de contraseñas, brindan seguridad en forma de aplicaciones móviles o de tokens de hardware. Normalmente la 2FA proporciona dos de los siguientes tipos:

1. Información que el usuario conoce (normalmente una frase o contraseña).
2. Algo que poseen (token de hardware o teléfono).
3. Algo que tienen (es decir, datos biométricos como la huella digital).

La autenticación de dos factores (2FA) es muy fiable, pero al mismo tiempo también tienes dos grandes desventajas importantes. Primero, aumenta el coste de operación del sistema, ya que enviar mensajes de textos es costosos y segundo, al ingresar su contraseña, aumenta la demora al iniciar sesión (Pappu et al., 2021).

2.1.2. Seguridad del dispositivo

La seguridad cada día se está convirtiendo en una problemática muy preocupante, una de las razones principales es la creación de programas maliciosos los cuales buscan como objetivo el daño permanente de tus archivos. Los virus pueden provocar varios problemas graves en la red al transmitir datos confidenciales, archivos, contraseñas, a entidades externas no autorizadas. Una contramedida ante estos programas maliciosos es el software de antivirus. Este software se instala en tu dispositivo con el objetivo de proteger tu información, detectando la aparición de virus y otros ataques externos, evitando ser infectados y eliminándolos en el mayor de los casos (Chavan et al., 2021).

2.1.3. Contraseñas con caracteres especiales

La autentificación de usuario es uno de los métodos que se utilizan para la confirmación de identidad de la persona que desea acceder a recursos en la red. Actualmente las contraseñas son las más implementadas para la verificación del usuario para las aplicaciones o sitios web. Es de suma importancia saber que parámetros se deben llevar a cabo para la creación de una contraseña segura, se establece características como letras mayúsculas y minúsculas, que vengan acompañadas de números y caracteres especiales. Estas contraseñas son bastantes seguras para evadir ataques de fuerza bruta, lo que las convierte en un problema para los atacantes (Adamu et al., 2022).

2.2. Malware

Es un término amplio que incluye virus, troyanos, spyware y otros códigos integrados que son comunes en la actualidad. La investigación de malware es un proceso de varios pasos que revela el diseño y la eficacia del malware e impulsa el desarrollo de tratamientos (Mira, 2021).

El malware ha existido desde los principios de la informática. Gran parte de las organizaciones de todo el mundo emplean software antivirus que detectan y reducen el tamaño de inconvenientes que pueden aparecer debido al malware. Entre estos riesgos se encuentra la filtración de datos personales, denegación de servicios y manipulación de recursos informáticos de los usuarios en beneficio del atacante (Or-Meir et al., 2021).

2.2.1. Phishing

El ciberataque que más utilizan es el phishing y, cada vez más, el Spear-phishing, este es un tipo de phishing orientado a objetivos específicos, debido a que estos ataques utilizan las llamadas técnicas de persuasión para atraer a sus víctimas, presumiblemente plantea la mayor amenaza a la integridad de la información de las agencias del sector público, varios estudios proporciona información sobre el impacto potencial de los efectos de la exposición constante al phishing y muestra que el grado de especificidad de dominio de los ataques afecta la susceptibilidad de las víctimas. (Koddebusch, 2022).

El phishing es un tipo de delito cibernético que consiste en enredar al usuario para que revele información personal/confidencial y detalles de la sesión. Los atacantes utilizan varias técnicas para lograr esto, como el robo de identidad, la creación de sitios web fraudulentos y el remitir

correos electrónicos o mensajes de texto fraudulentos. Por ejemplo, un atacante podría enviar un correo electrónico que parezca de parte de la institución a la que pertenece el receptor del correo, advirtiéndole que su contraseña está por caducar y que debe realizar el cambio lo antes posible ingresando al enlace que le proporciona el mismo atacante mediante el correo (Patil & Dhage, 2019).

La palabra “phishing” es similar a la palabra “pesca”, indicando que el atacante prepara un señuelo en forma de correo electrónico que proporciona información falsa, el cual tiene como objetivo atraer a la víctima. Si la víctima cae en el anzuelo, el pescador logrará robar su información pudiendo divulgar sus datos personales (Leonov et al., 2021).

La importancia de comprender el papel de los factores humanos respecto a la efectividad de los ataques de phishing, así como las tácticas para mitigar estos riesgos, se exploran temas como la conciencia del usuario, la educación en seguridad, el diseño de interfaces y las técnicas de ingeniería social, también se identifican áreas de investigación futuras para mejorar la comprensión y la prevención de los ataques de phishing (Desolda et al., 2021).

Los ataques de phishing están diseñados a usuarios que han sido analizados determinadamente por el atacante, por ejemplo, información recolectada sobre las acciones tomadas anteriormente o posibles decisiones que serán tomadas por la víctima que pueden ser utilizadas como ayuda para el atacante (Allodi et al., 2020).

El phishing es uno de los ataques más comunes que usan la ingeniería social, este tipo de ataque son los que se enfrentan las organizaciones, los gobiernos y el público en general, la amenaza que suponen los correos electrónicos clonados ha aumentado drásticamente en estos últimos años (Shakya et al., 2023).

.

2.2.2. Smishing

Estos ataques se dan mediante correos electrónicos u otros medios digitales de comunicación que logran confundir a las víctimas ya sea una sola persona, organizaciones o empresas. La victima puede sufrir un intento de robo de datos por medio de la instalación de malware de parte del ciberdelincuente. El smishing es enviar correos a través de fuente confiable la cual la información como tal es la que está falsificada direccionándote a un lugar infectado de malware (Baig et al., 2021)

El smishing se ha vuelto significativamente más complejo gracias a la incorporación de troyanos y virus, que permiten a los intrusos de la informática explotar las vulnerabilidades de los sistemas, dichos troyanos se propagan mediante técnicas de ingeniería social, estos se descargan como archivos adjuntos al correo electrónico y operan en la computadora de un usuario para robar sus ID o contraseñas, o para proporcionar datos de monitoreo informático a otros sitios web, en la actualidad se han desarrollado métodos para llevar a los usuarios a un sitio de phishing al conectarse a un sitio web favorito a través del celular. Esto ocurre después de que un archivo host de usuario ha sido modificado para establecer una ruta de transferencia usando un virus, de tal modo que, el usuario y la contraseña que ha iniciado sesión en un sitio web confiable sean recopilados y proporcionados al atacante (Blancaflor et al., 2023).

Los ciberdelincuentes crean varias formas de comunicación, mediante SMS, correos electrónicos, entre otros métodos, estableciendo como problemática una urgencia influyendo miedo en los destinatarios y/o usuarios, lo cual atrae a la víctima para que realice la acción requerida por el ciberdelincuente (Guaña-Moya et al., 2022).

2.2.3. Ransomware

Es un malware o código malicioso que se encarga de cifrar los archivos de la víctima o bloqueo del dispositivo, el atacante toma el control total de los datos o dispositivo con el objetivo de solicitar quitar las restricciones a cambio de pagos (Shehata et al., 2023).

El ransomware es una amenaza muy alarmante para cualquier dispositivo conectado a la red. Es cada vez más peligroso para muchas organizaciones o usuarios individuales, ya que son utilizados para fines económicos o políticos (Cheon et al., 2023).

2.2.4. Spyware

Es un software malicioso espía que trabaja en secreto, recopilando la información como historial de navegación, registro de actividades y datos confidenciales del dispositivo infectado siendo enviada la información a los servidores del atacante (Shehata et al., 2023).

Los ataques de spyware son realizados en su mayoría fácilmente en teléfonos móviles, ya que este dispositivo es utilizado comúnmente en el día a día, en donde el usuario instala ciertas aplicaciones ya sea desde Google Play Store, App Store o fuentes desconocidas, lo que conlleva a que el atacante piratee el sistema del usuario (Kumari & Sharma, 2023b).

2.2.5. Adware

Es un tipo de malware que se encarga de llenarte de anuncios maliciosos y archivos no deseados en un dispositivo infectado, lo que a menudo causa fallas y otros problemas en el sistema del usuario (Shehata et al., 2023).

El adware se da a conocer en una descarga falsa, ventanas emergentes o integrado en un programa gratuito patrocino por anuncios, al desarrollador se le genera pagos cada vez que el usuario da clic en un anuncio mostrado por un adware, ciertos AdWare evitan la navegación limpia ya que te envían a sitios web peligrosos (Kumari & Sharma, 2023).

2.3. Población y muestra

En el libro de (Condori Ojeda, 2020) nos indica que el universo o población objetivo es un conjunto de elemento (personas, objetos, programas, etc) de una población, es decir, son los elementos accesibles o unidades de análisis que pertenece a un área particular, en donde, se realizará el estudio respectivo y la muestra en la porción representativa de la población.

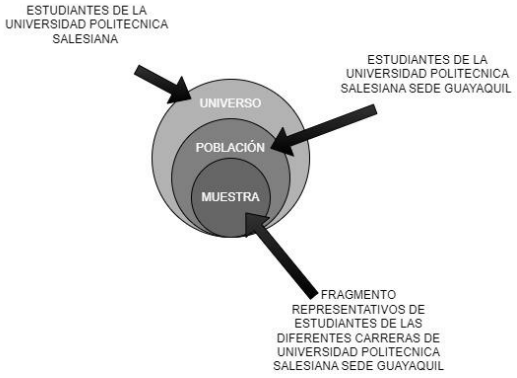

Figura 1. Modelo Universo, población y muestra

En la revista de Intervalos de confianza de (Ventura-León & Valencia, 2020) nos explican que Los Intervalos de Confianza (IC) se definen como un rango de valores que sigue una distribución normal, en la que existe la probabilidad de encontrar el verdadero valor de la población. Más, sin embargo, en ciertos casos, la distribución es desconocida, por lo que se pueden utilizar técnicas de muestreo para calcular los IC, uno de los problemas principales de los IC es la interpretación errónea, ya que a menudo se asume que el intervalo resultante incluye

el verdadero valor poblacional, cuando la realidad de este procedimiento nos revela que el intervalo resultante es solo 1 de 95 intervalos posibles.

Tabla 1. Nivel de confianza de Z alfa

Nivel de Confianza	**Z alfa**
99,70%	3
99%	2,58
98%	2,33
96%	2,05
95%	1,96
90%	1,645
80%	1,28
50%	0,674

3. METODOLOGÍA

Es necesario conocer y comprender cuales son las amenazas más comunes a los que se enfrentan los estudiantes universitarios, además de identificar las amenazas de mayor impacto, por ellos es necesario realizar una revisión bibliográfica en las bases de datos de artículos científicos que nos den pautas acerca de los riesgos y buenas prácticas vigentes aplicables al estudio.

Se utilizará una metodología de investigación cualitativa y método PRISMA debido a que es necesario analizar datos cualitativos y cuantitativos acerca del conocimiento y buenas prácticas aplicadas por los estudiantes de la Universidad Politécnica Salesiana Sede Guayaquil.

3.1. Métodos y técnicas de investigación

Se aplicarán técnicas de investigación Cualitativa, se realizará revisión exhaustiva de la literatura existente sobre seguridad cibernética, incluyendo estudios previos referentes a la ciberseguridad, a los Ciber-ataques más comunes, a las buenas prácticas en los estudiantes universitarios, también se empleará el método PRISMA para identificar y analizar trabajos científicos sobre las buenas prácticas aplicadas ante las amenazas más comunes en los entornos universitarios.

3.2. Métodos y técnicas para recopilación de información

Para la revisión bibliográfica se utilizará el método PRISMA, esta es una herramienta que nos servirá para la revisión sistemática de la literatura científica, la cual, nos ayuda a identificar, seleccionar y evaluar artículos relevantes para el estudio de la evaluación del nivel de conocimiento y las buenas prácticas en la ciberseguridad entre los estudiantes universitarios.

Para la investigación mixta, se utilizarán encuestas y análisis estadísticos, con los que se identificará patrones, tendencias y brechas en el conocimiento y las prácticas de seguridad cibernética entre los estudiantes universitarios.

Se eligió Microsoft Forms como la principal herramienta para el desarrollo del cuestionario por su facilidad de uso y versatilidad, su interfaz amigable permite a los usuarios crear formularios de manera eficiente, basándose en los artículos previamente revisados durante la revisión bibliográfica, se desarrolló un total de 17 preguntas enfocadas para evaluar el nivel de conocimiento, ataques más comunes y percepción del estudiantes dentro de la Universidad politécnica Salesiana Sede Guayaquil, estás preguntas estarán divididas por tres fases:

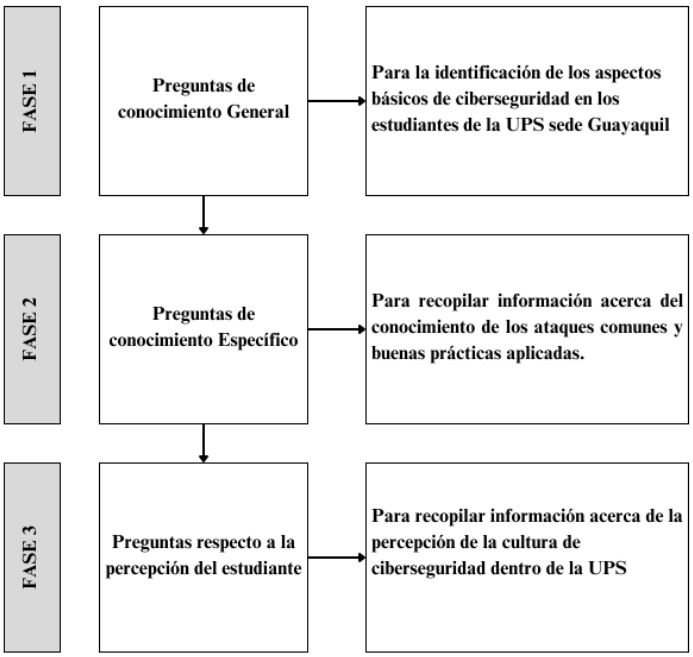

Figura 2. Fases del desarrollo de preguntas para la encuesta

Con el desarrollo del cuestionario se busca recopilar información valiosa referente al conocimiento básico de las buenas prácticas en la ciberseguridad, en el conocimiento especifico en los diferentes tipos de ataques cibernéticos como lo es el Phishing, también se busca saber cuál es la percepción del estudiante respecto a la ciberseguridad de la Universidad Politécnica Salesiana sede Guayaquil, esto nos ayudará con la recolección de datos, logrando identificar los diferentes patrones, tendencias y correlaciones que presentan los estudiantes de la Universidad Politécnica Salesiana ante los ataques cibernéticos más comunes en la ciberseguridad. El cuestonario está validado por los Msc. Dario Huilcapi. & Msc. Guillermo Pizarro.

3.3. Definición de la población y espacio muestral

Se obtuvo un total de 7.251 en general de la población conocida (finita) que está conformada por estudiantes universitarios de varias carreras de la Universidad Politécnica Salesiana Sede Guayaquil con sus respectivos campus.

Tabla 2. Población de estudiantes del campus Centenario.

Carreras del campus Centenario	**N° de estudiantes**
Administración de empresas	552
Biomedicina	160
Computación e ingeniería en sistemas	571
Comunicación	123
Contabilidad y Auditoria	424
Electricidad e ingeniería Eléctrica	494
Electrónica y Automatización	342
Ingeniería Automotriz	543
Ingeniería Industrial	794
Mecánica Industrial [Tecnología]	20
Mecatrónica	594
Telecomunicaciones	202
Total, de estudiantes:	**4819**

Tabla 3. Población de estudiantes del campus María Auxiliadora

Carreras del campus María Auxiliadora	**N° de estudiantes**
Administración de empresas	103
Arquitectura	147
Biotecnología	290
Derecho	291
Diseño Multimedia	93
Economía	92
Educación básica	49
Educación Inicial	101
Ingeniería Ambiental	92
Ingeniería Civil	311
Negocios Digitales	29
Odontología	256
Psicología	547
Psicología Clínica [Psicología Clínico]	31
Total, de estudiantes:	**2432**

Tabla 4. Población de estudiantes de los campus de la UPS sede Guayaquil.

Campus de la Ups sede Guayaquil	**N° de estudiantes**
Campus Centenario	4819
Campus María Auxiliadora	2432
Total, de estudiantes:	**7251**

Con la población previamente obtenida nos enfocaremos en obtener el porcentaje y el número de encuestas a realizar mediante el uso de la fórmula de la muestra de la población en estudiantes de la Universidad politécnica salesiana:

$$n = \frac{N * Z_{\propto}^2 * P * Q}{e^2 * (N-1) + Z_{\propto}^2 * P * Q}$$

Figura 3. Formula de la muestra de una población conocida (finita).

La relación entre los parámetros que componen la fórmula para conseguir la muestra de una población finita:

n **=** Es el tamaño de muestra que deseamos obtener, es decir, la cantidad de encuestas a realizar.

N **=** Representa el tamaño de la población, es decir, el número total de estudiantes en ambos campus.

Zα **=** Este parámetro estadístico se relaciona con el nivel de confianza que buscamos al estimar un valor utilizando una muestra previamente recolectada, el nivel de confianza (NC) representa la certeza o probabilidad expresada en porcentaje con la que realizamos esta estimación.

P **=** Es la probabilidad de que la muestra finita de estudiantes participe en la encuesta.

Q **=** Es la probabilidad de que la muestra finita de estudiantes no participe en la encuesta.

Dado que no se conoce la probabilidad exacta (**P**), se le asigna el mismo peso que (**Q**). es decir, ambos parámetros se establecen en un 50%.

e **=** Representa la cantidad de error de muestreo aleatorio, este valor también será determinado por los investigadores y estará relacionado con el nivel de certeza que deseas en un estudio.

Tabla 5. Formula aplicada de la muestra finita a la población del campus Centenario y María Auxiliadora.

Campus Centenario	**Campus María Auxiliadora**
$n = \frac{4819 * 3_{\propto}^{2} * 50 * 50}{6^{2} * (4819 - 1) + 3_{\propto}^{2} * 50 * 50}$	$n = \frac{2432 * 3_{\propto}^{2} * 50 * 50}{6^{2} * (2432 - 1) + 3_{\propto}^{2} * 50 * 50}$
$n = \frac{108427500}{195948}$	$n = \frac{54720000}{110016}$
$n = 554$	$n = 498$

Se obtiene un tamaño de muestra diferente por cada campus de la UPS sede Guayaquil, con estos resultados se procederá a obtener el porcentaje adecuado de acuerdo con los estudiantes que representan a cada carrera.

Después de obtener las muestras, se procedió a la distribución de la encuesta, debido a la gran cantidad de estudiantes de los campus, se estimaba poder cumplir con las 1052 encuestas en los campus, dicha encuesta se sobrepasó el total de la muestra ya definida, llegando a las 1340 encuestas de los diferentes tipos de carreras y campus.

Tabla 6. Población, muestra, porcentaje y numero de encuestas a realizar por carreras de la UPS campus Centenario

Población Finita del campus Centenario			**4819**
Muestra del campus Centenario			**554**
Carreras del campus Centenario	**N° de estudiantes**	**Porcentaje**	**N° de encuestas a realizar**
Administración de empresas	552	11,5%	63
Biomedicina	160	3,3%	18
Computación e ingeniería en sistemas	571	11,8%	66
Comunicación	123	2,6%	14
Contabilidad y Auditoria	424	8,8%	49
Electricidad e ingeniería Eléctrica	494	10,3%	57
Electrónica y Automatización	342	7,1%	39
Ingeniería Automotriz	543	11,3%	62
Ingeniería Industrial	794	16,5%	91
Mecánica Industrial [Tecnología]	20	0,4%	2
Mecatrónica	594	12,3%	68
Telecomunicaciones	202	4,2%	23
Total, de estudiantes:	**4819**	**100%**	**554**

Tabla 7. Población, muestra, porcentaje y número de encuestas a realizar por carreras de la UPS campus María Auxiliadora

Población Finita del campus Centenario			**2432**
Muestra del campus Centenario			**498**
Carreras del campus Centenario	**N° de estudiantes**	**Porcentaje**	**N° de encuestas a realizar**
Administración de empresas	103	4,2%	21
Arquitectura	147	6,0%	30
Biotecnología	290	11,9%	59
Derecho	291	12,0%	60
Diseño Multimedia	93	3,8%	19
Economía	92	3,8%	19
Educación básica	49	2,0%	10
Educación Inicial	101	4,2%	21
Ingeniería Ambiental	92	3,8%	19
Ingeniería Civil	311	12,8%	64
Negocios Digitales	29	1,2%	6
Odontología	256	105%	52
Psicología	547	22,5%	112
Psicología Clínica [Psicología Clínico]	31	1,3%	6
Total, de estudiantes:	**4819**	**100%**	**498**

4. RESULTADOS

4.1. Análisis de riesgos y buenas prácticas en trabajos literarios y científicos previos

De un total de 143 artículos, se discriminó debido a duplicidad de resultados y se realizó el primer filtro a través de la exclusión de acuerdo con el título considerando la afinidad con el tema de investigación, dando como resultado un total de 48 artículos, posteriormente, se consideraron 20 artículos y 2 revistas relevantes para esta investigación de acuerdo con la pertinencia en función de la revisión de los abstract. Los artículos provienen principalmente de otras regiones y se encontraron mediante la búsqueda de palabras clave en diversas bases de datos. Se aplicaron filtros relacionados con el tipo de artículo, la fecha, la fuente, el idioma y otros parámetros permitidos por las bases de datos. El método PRISMA se utilizó siguiendo sus respectivas fases: identificación, examinación y final. Al analizar el contenido de los 20 artículos científicos, junto a las 2 revistas, se pudo determinar que abordan diferentes temas, como las buenas prácticas de la ciberseguridad en entornos universitarios, las amenazas más comunes en entornos universitarios, El Phishing y sus variables, etc.

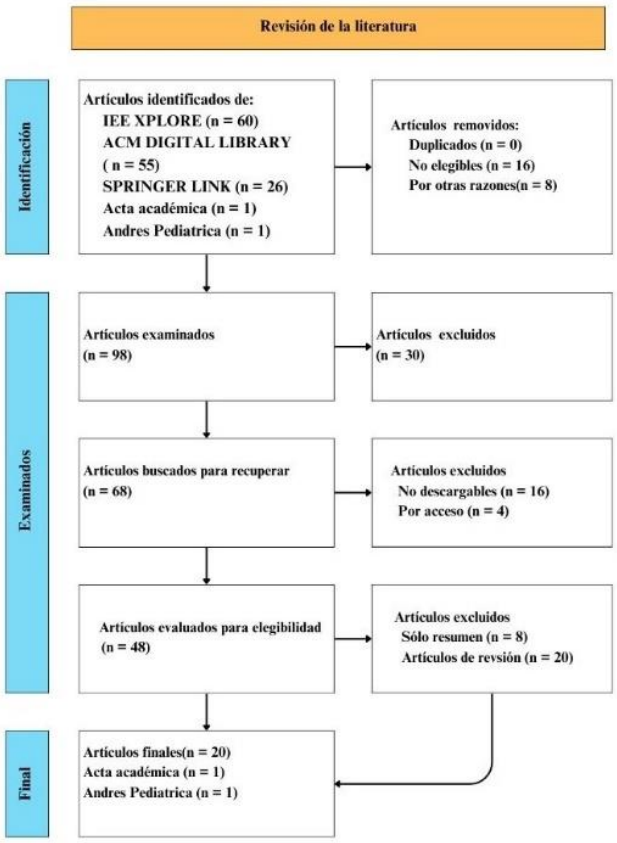

Figura 4. Modelo PRISMA

4.2. Revisión Literaria

La tabla 8 muestra los 22 artículos y 2 revistas agrupados por bibliotecas virtuales IEEE Xplore, ACM, SPRINGER LINK, Acta Académica y Andrés Pediátrica, seleccionados según los criterios de inclusión/exclusión, estos artículos y revistas nos muestra que los autores basan sus propuestas en: la detección de phishing junto con una forma de construir un marco antiphishing, la detección de correos electrónicos fraudulentos, tipos de malware (phishing, spear phishing, clones-phishing, smishing, ransomware, spyware y adware), la forma correcta para formula de la muestra de población, entre muchas cosas más.

Tabla 8. Artículos y revistas seleccionados

	Artículo y revista por año de producción	**Cantidad**
IEE	(Cheon et al., 2023), (Sharma et al., 2023), (Patil & Dhage, 2019), (Mira, 2021), (Adamu et al., 2022), (Shehata et al., 2023), (Chavan et al., 2021), (Peker et al., 2018), (Or-Meir et al., 2021), (Guaña-Moya et al., 2022), (Kumari & Sharma, 2023a), (Ellahi et al., 2022), (Pappu et al., 2021), (Baig et al., 2021), (Leonov et al., 2021), (Allodi et al., 2020), (Kumari & Sharma, 2023b)	17
ACM	(Blancaflor et al., 2023), (Desolda et al., 2021)	2
SPRINGER LINK	(Shakya et al., 2023)	1
Acta Académica	(Condori Ojeda, 2020)	1
Andrés Pediátrica	(Ventura-León & Valencia, 2020)	1
		22

Fuente: Realizado por autor.

4.3. Resultado del cuestionario

P1. ¿A qué campus pertenece?

De acuerdo con los datos recopilados, la mayoría de los encuestados (61%) pertenecen al campus Centenario, mientras que un 39% pertenece al campus María Auxiliadora.

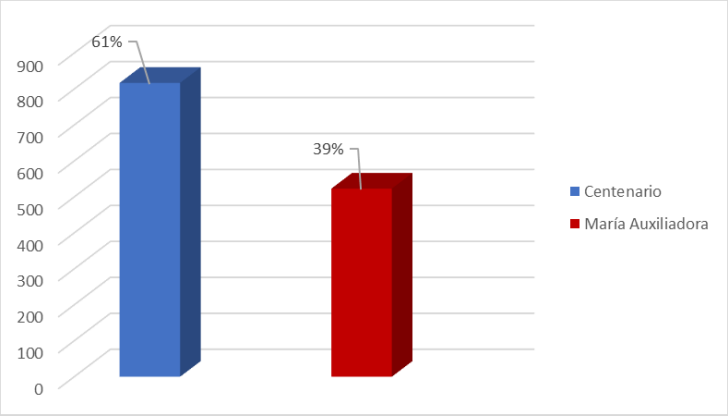

Figura 5. Pregunta 1 -. ¿A qué campus pertenece?

P2. ¿Indique a que carrera pertenece?

De acuerdo con los resultados recopilados, los estudiantes de las carreras de Computación e Ingeniería de Sistemas (201 encuestados) y Administración (127 encuestados), son los que más han contribuido con la encuesta, esto demuestra su participación en el proceso de recopilación de datos, por otro lado, se logró cumplir con la cantidad de encuestas a realizar por carreras en ambos campus.

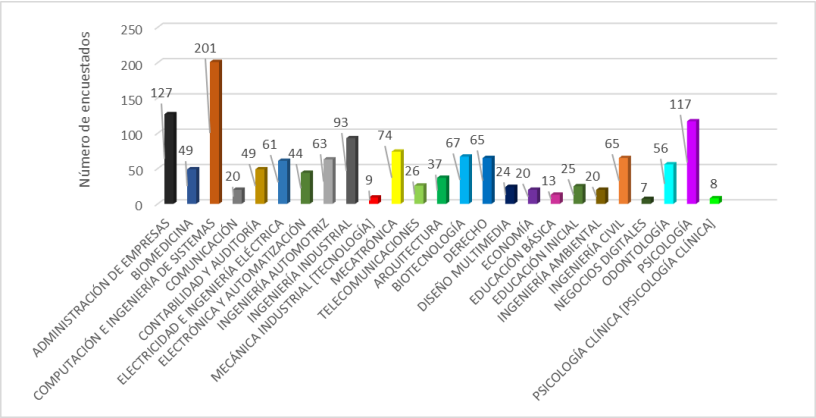

Figura 6. Pregunta 2 - ¿Indique a que carrera pertenece?

P3. ¿Tiene conocimiento de las buenas prácticas respecto a la ciberseguridad?

Entre los resultados recopilados, 1118 encuestados (83%) tienen conocimiento de las buenas prácticas respecto a la ciberseguridad, mientras que 222 encuestados (17%) no cuentan con dicho conocimiento, es importante que las personas estén informadas y apliquen medidas de seguridad para protegerse en el entorno digital.

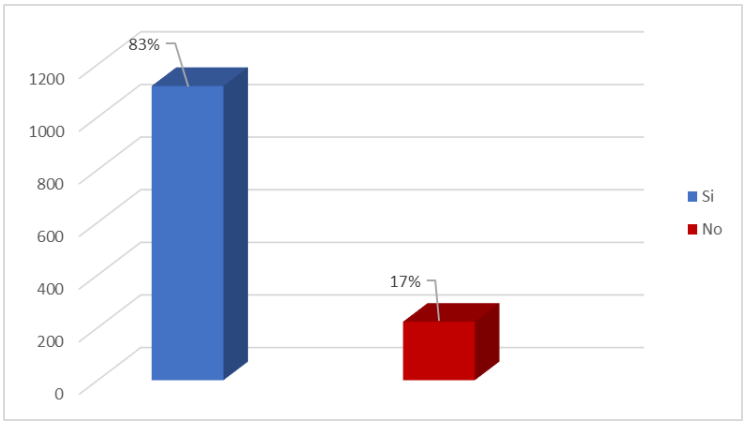

Figura 7. Pregunta 3 - ¿Tiene conocimiento de las buenas prácticas respecto a la ciberseguridad?

P4. ¿Considera importante mantener sus contraseñas seguras y únicas para cada cuenta?

Entre los resultados recopilados, se observó que 623 encuestados (aproximadamente el 46%) están “Totalmente de acuerdo” indicando que es importante mantener sus contraseñas seguras y únicas para cada cuenta, otros 603 encuestados (alrededor del 45%) están simplemente “De acuerdo”, un grupo más pequeño de 95 encuestados (aproximadamente el 7%) se mantiene en una posición neutral. Por otro lado, 13 encuestados (representando el 1.4%) están “En desacuerdo” con la importancia de mantener sus contraseñas seguras, finalmente, 6 encuestados (equivalente al 0.6%) se encuentran en la categoría de “Totalmente en desacuerdo”, esto subraya la relevancia de proteger nuestras cuentas con contraseñas sólidas y distintas para cada servicio, mantener la seguridad de nuestras contraseñas es fundamental para proteger nuestra información personal y digital.

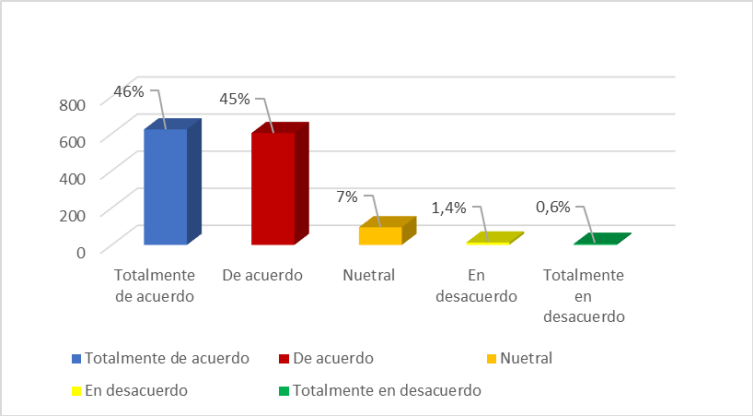

Figura 8. Pregunta 4 - ¿Considera importante mantener sus contraseñas seguras y únicas para cada cuenta?

P5. Cuál de las siguientes amenazas usted conoce:

Entre los datos recopilados, la mayoría de los estudiantes están familiarizados con algunas amenazas en la ciberseguridad. Las más comunes que conocen son “El Phishing” y “Malware”, sin embargo, también se observa que hay otros ataques menos conocidos entre los estudiantes, como “El Ransomware”, “Spyware” y el “AdWare”, por otro lado, se evidenció que hay estudiantes que no tienen conocimiento alguno de las amenazas dentro de la ciberseguridad. Es importante estar informado sobre estas amenazas para protegerse adecuadamente en línea.

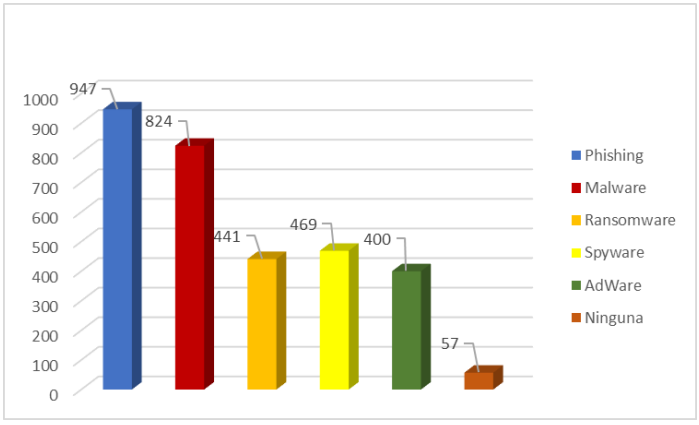

Figura 9. Pregunta 5 - Cuál de las siguientes amenazas usted conoce:

P6. ¿Ha sufrido usted alguno de los siguientes ataques cibernéticos dentro de la Universidad?

Entre los datos recopilados, se ha observado que los estudiantes en el entorno universitario han sido víctimas de varios tipos de ataques cibernéticos. Los más comunes incluyen “El Phishing” y “El Malware”, estos ataques pueden comprometer la seguridad de los datos y la privacidad de los usuarios, por otro lado, aunque suelen ser menos frecuentes, también se han registrado casos de “El Ransomware”, “El Spyware” y “El AdWare”, es importante destacar que algunos estudiantes no han experimentado ningún tipo de ataque cibernético durante su tiempo en la universidad.

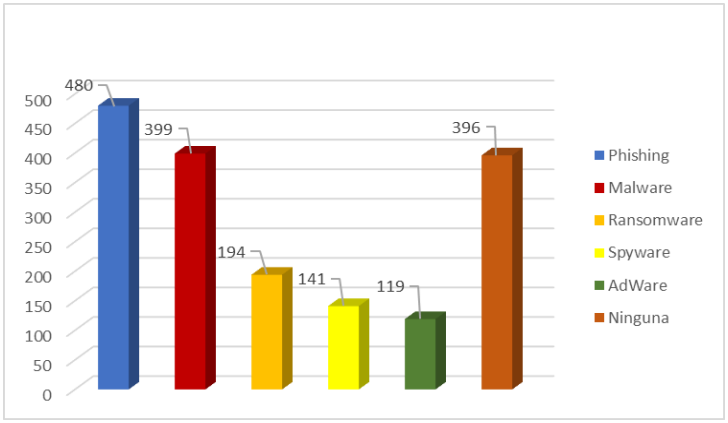

Figura 10. Pregunta 6 - ¿Ha sufrido usted alguno de los siguientes ataques cibernéticos dentro de la Universidad?

P7. ¿Conoce qué es el phishing y cómo evitarlo?

Entre los resultados recopilados, se observó 482 encuestados (aproximadamente el 36%) cuentan con un buen conocimiento respecto al “Phishing y el cómo evitarlo”, otros 362 encuestados (alrededor del 27%) cuentan con un conocimiento básico, otros 251 encuestados (aproximadamente el 19%) cuentan con un conocimiento moderado. Por otro lado, 120 encuestados (representando el 9%) cuentan con un conocimiento experto, finalmente, 125 encuestados (equivalente al 9%) No cuentan con conocimiento alguno.

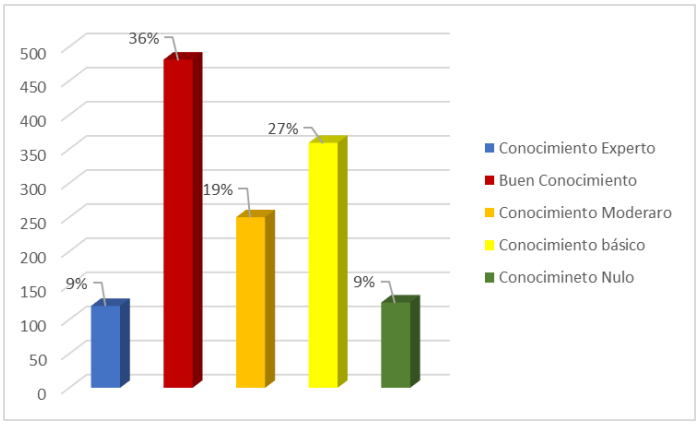

Figura 11. Pregunta 7 - ¿Conoce qué es el phishing y cómo evitarlo?

P8. ¿Cree que el uso de autenticación de dos factores es una práctica recomendada para proteger tus cuentas en línea?

Entre los resultados recopilados, se observó que 658 encuestados (aproximadamente el 49%) indican que están "De acuerdo" en el uso de autenticación de dos factores es una práctica recomendada para proteger sus cuentas en línea, otros 453 encuestados (alrededor del 34%) se encuentran "Totalmente de acuerdo", un grupo más pequeño de 154 encuestados (aproximadamente el 11%) se mantiene en una posición "Neutral". Por otro lado, 55 encuestados (representando el 4%) están "Totalmente en desacuerdo" con la autenticación de dos factores, finalmente, 20 encuestados (equivalente al 2%) se encuentran en la categoría de "En desacuerdo".

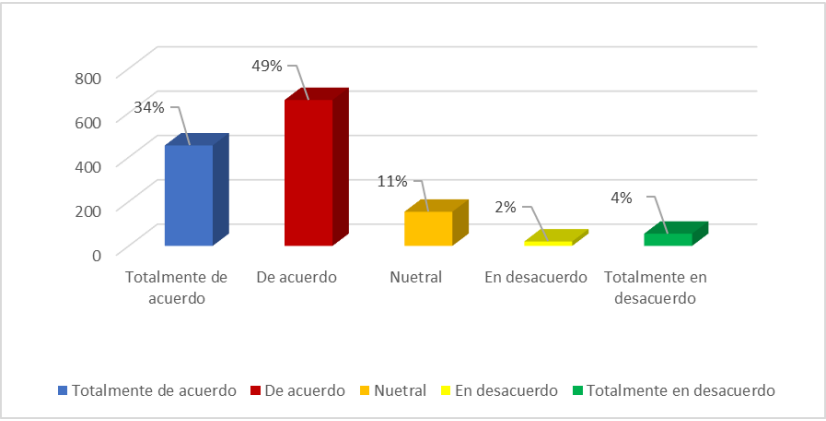

Figura 12. Pregunta 8 - ¿Cree que el uso de autenticación de dos factores es una práctica recomendada para proteger tus cuentas en línea?

P9. ¿Está al tanto de los riesgos asociados con hacer clic en enlaces o archivos adjuntos desconocidos en correos electrónicos?

Entre los resultados recopilados, se observó que 911 encuestados (aproximadamente el 68%) si tienen en cuenta los riesgos asociados con hacer clic en enlaces no deseados o archivos adjuntos desconocidos en correos electrónicos, otros 222 encuestados (representando el 17%) no están al tanto de los riesgos asociados. Por otro lado, 207 encuestados (aproximadamente el 15%) se encuentran en una posición de incertidumbre, manifestando un tal vez con relación a los riesgos asociados.

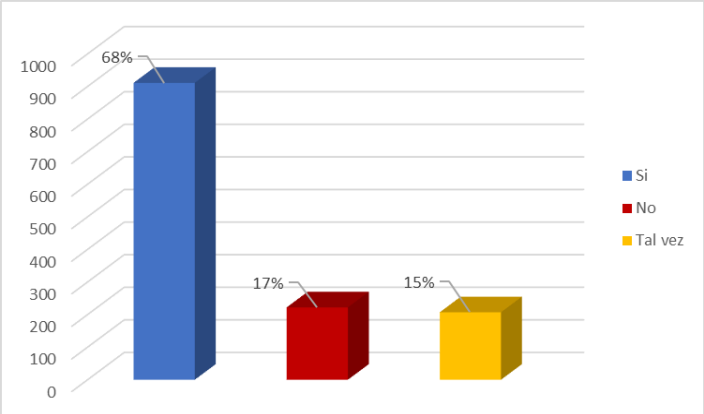

Figura 13. Pregunta 9 - ¿Está al tanto de los riesgos asociados con hacer clic en enlaces o archivos adjuntos desconocidos en correos electrónicos?

P10. ¿Puede reconocer señales típicas de un correo electrónico de phishing?

Entre los resultados recopilados, se observó que 544 encuestados (aproximadamente el 41%) si logran reconocer las señales típicas de un correo electrónico de phishing, otros 410 encuestados (representando el 30%) no logran reconocer las señales típicas. Por otro lado, 386 encuestados (aproximadamente el 29%) se encuentran en una posición de incertidumbre, manifestando un tal vez con relación al reconocimiento de señales típicas.

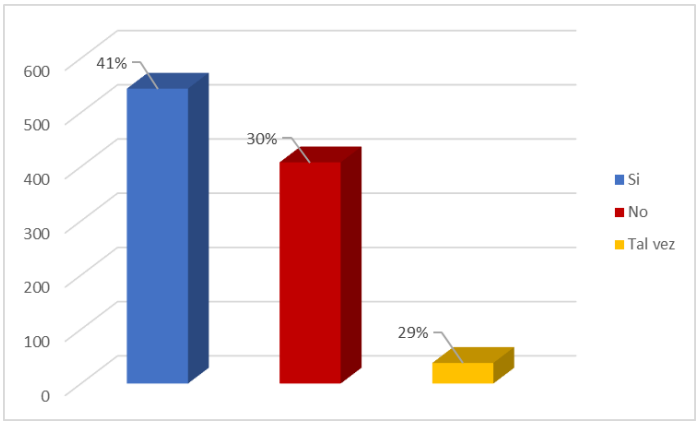

Figura 14. Pregunta 10 - ¿Puede reconocer señales típicas de un correo electrónico de phishing?

P11. ¿Cómo verifica si un correo electrónico es fraudulento?

Entre los 1340 resultados recopilados, se observó que el 46% de encuestados verifican mediante “Los enlaces", el 29% de encuestados verifica mediante “El remitente”. Por otro lado, el 19% de encuestados verifica mediante “La ortografía”. Finalmente, el 6% de encuestados no sabe identificar un correo electrónico fraudulento lo cual es muy alarmante ya que esto determina la falta de conocimiento y lo muy probable a sufrir ataques.

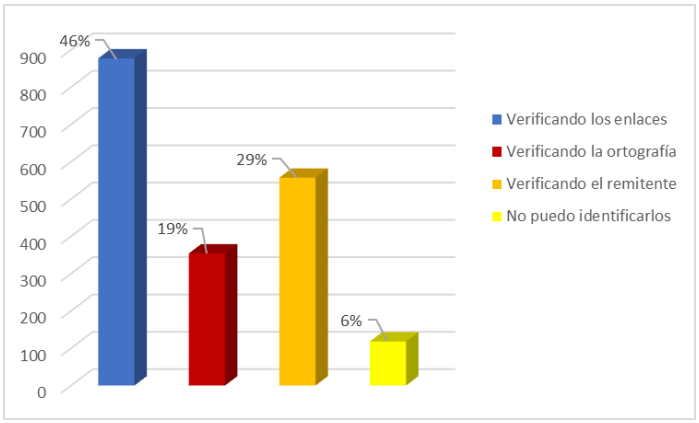

Figura 15. Pregunta 11 - ¿Cómo verifica si un correo electrónico es fraudulento?

P12. ¿Está familiarizado en la importancia de ser cauteloso al compartir información confidencial en línea, incluso en aplicaciones y sitios web aparentemente seguros?

Entre los resultados recopilados, se observó que 615 encuestados (aproximadamente el 46%) que están "De acuerdo" indicando que, si se encuentra familiarizado en la importancia de ser cauteloso al compartir información confidencial en línea, incluso en aplicaciones y sitios web, otros 476 encuestados (alrededor del 36%) se encuentran "Totalmente de acuerdo", un grupo más pequeño de 190 encuestados (aproximadamente el 14%) se mantiene en una posición "Neutral". Por otro lado, 33 encuestados (representando el 2%) se encuentran "En desacuerdo". Finalmente, 26 encuestados (equivalente al 2%) se encuentran en la categoría de "Totalmente en desacuerdo".

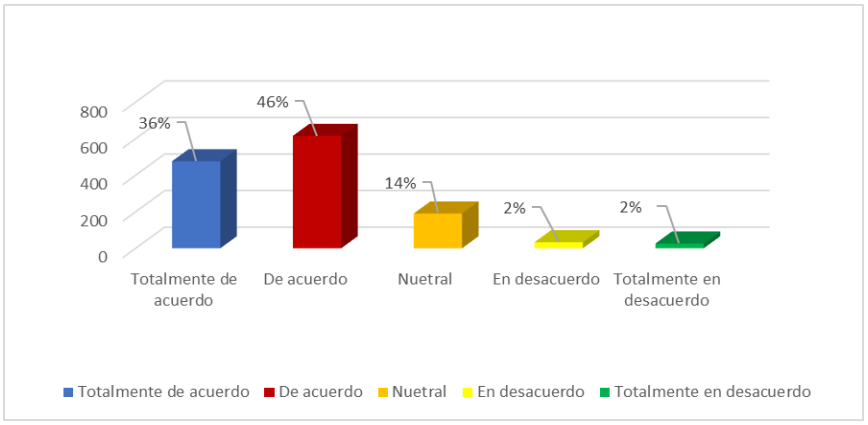

Figura 16. Pregunta 12 - ¿Está familiarizado en la importancia de ser cauteloso al compartir información confidencial en línea, incluso en aplicaciones y sitios web aparentemente seguros?

P13. ¿Considera usted que la universidad brinde alguna capacitación o charla referente a las buenas prácticas de la ciberseguridad?

Según los resultados recopilados, aproximadamente el 94% de los encuestados considera que la Universidad Politécnica Salesiana sede Guayaquil brinda capacitaciones o charlas referentes a las buenas prácticas de la ciberseguridad, sin embargo, un pequeño porcentaje (alrededor del 6%) no comparte esta opinión y no cree que la universidad ofrezca suficiente capacitación en este ámbito, determinando un punto esencial para la implementación de planes de estudios para el mejoramiento en el conocimiento de la ciberseguridad.

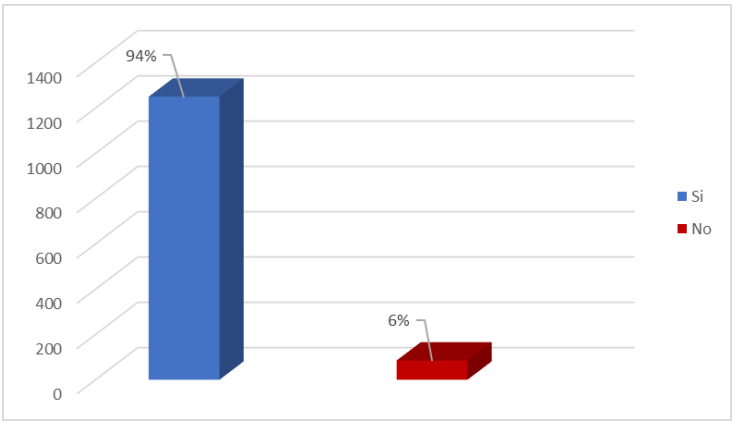

Figura 17. Pregunta 13 - ¿Considera usted que la universidad brinde alguna capacitación o charla referente a las buenas prácticas de la ciberseguridad?

P14. ¿Cómo percibe la ciberseguridad dentro de la Universidad Politécnica Salesiana sede Guayaquil?

Entre los resultados recopilados, se observó que 818 encuestados (aproximadamente el 61%) indican que se sienten "Totalmente protegidos" respecto a la ciberseguridad en la UPS sede Guayaquil, otros 245 encuestados (alrededor del 18%) indican que se "Sienten protegidos", otros 230 encuestados (aproximadamente el 17%) se encuentran en una posición de incertidumbre, manifestando que no tienen "conocimiento alguno". Por otro lado, 32 encuestados (representando el 3%) indican que se "Sienten desprotegidos" respecto a la ciberseguridad en la UPS sede Guayaquil. Finalmente, 15 encuestados (equivalente al 1%) indican que se "Sienten totalmente desprotegidos".

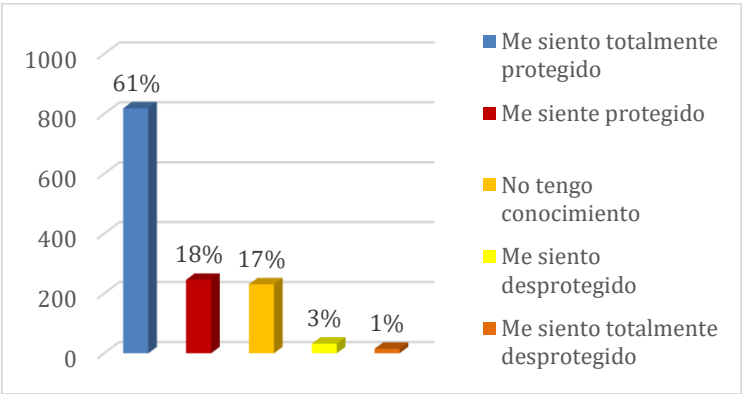

Figura 18. Pregunta 14 - ¿Cómo percibe la ciberseguridad dentro de la Universidad Politécnica Salesiana sede Guayaquil?

P15. ¿Considera que los estudiantes universitarios están suficientemente informados sobre las buenas prácticas de ciberseguridad?

Entre los resultados recopilados, aproximadamente el 48% de los encuestados están “De acuerdo” en que los estudiantes universitarios están suficientemente informados sobre las buenas prácticas de ciberseguridad, además, alrededor del 30% de los encuestados están “Totalmente de acuerdo”; Por otro lado, aproximadamente el 17% se mantiene en una posición “Neutral”; Sin embargo, hay un pequeño porcentaje, alrededor del 4% que está “En desacuerdo”, finalmente, un 1% de los encuestados se encuentra en la categoría de “Totalmente en desacuerdo”, es importante considerar estas opiniones para evaluar la efectividad de las prácticas de ciberseguridad en la institución.

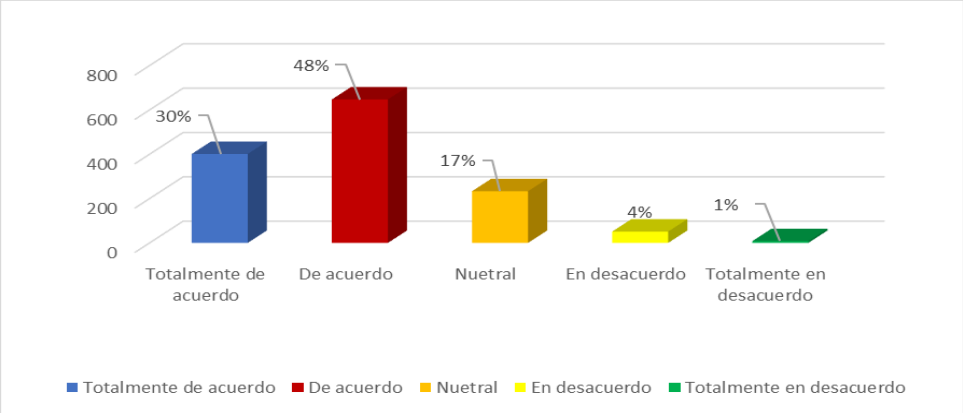

Figura 19. Pregunta 15 - ¿Considera que los estudiantes universitarios están suficientemente informados sobre las buenas prácticas de ciberseguridad?

P16. ¿Cree que la Universidad Politécnica Salesiana sede Guayaquil brinda suficiente capacitación y recursos para fomentar las buenas prácticas de ciberseguridad entre los estudiantes?

La mitad de los estudiantes encuestados considera que la Universidad Politécnica Salesiana sede Guayaquil ofrece suficiente formación y recursos en materia de ciberseguridad, a este grupo se suma un 28% que está totalmente de acuerdo con esta afirmación, sin embargo, un 17% se mantiene neutral; Detectamos que un 3% de los encuestados no está de acuerdo con la afirmación, y un 2% incluso la rechaza por completo, estas opiniones minoritarias son relevantes para evaluar la eficacia de las prácticas de ciberseguridad de la institución.

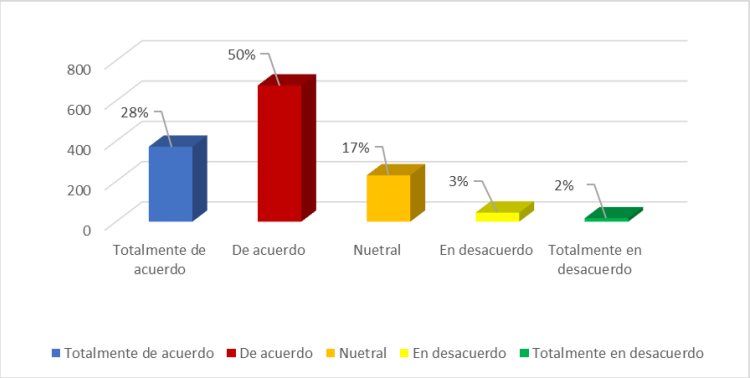

Figura 20. Pregunta 16 - ¿Cree que la Universidad Politécnica Salesiana sede Guayaquil brinda suficiente capacitación y recursos para fomentar las buenas prácticas de ciberseguridad entre los estudiantes?

P17. ¿Está de acuerdo que se debería incluir un curso obligatorio de ciberseguridad en el plan de estudios de los estudiantes universitarios para promover las buenas prácticas de seguridad?

Entre los resultados recopilados, se observó que 611 encuestados (alrededor del 46%) se encuentran "Totalmente de acuerdo", en que se debería incluir un curso obligatorio de ciberseguridad en el plan de estudios de los estudiantes universitarios para promover las buenas prácticas de seguridad, otros 620 encuestados (aproximadamente el 45%) indican que están "De acuerdo", otros 95 encuestados (aproximadamente el 7%) se mantiene en una posición "Neutral". Por otro lado, 9 encuestados (representando el 1%) se encuentran "En desacuerdo". Finalmente, 5 encuestados (equivalente al 1%) se encuentran en la categoría de "Totalmente en desacuerdo", es evidente que la mayoría reconoce la importancia de la ciberseguridad en la educación universitaria.

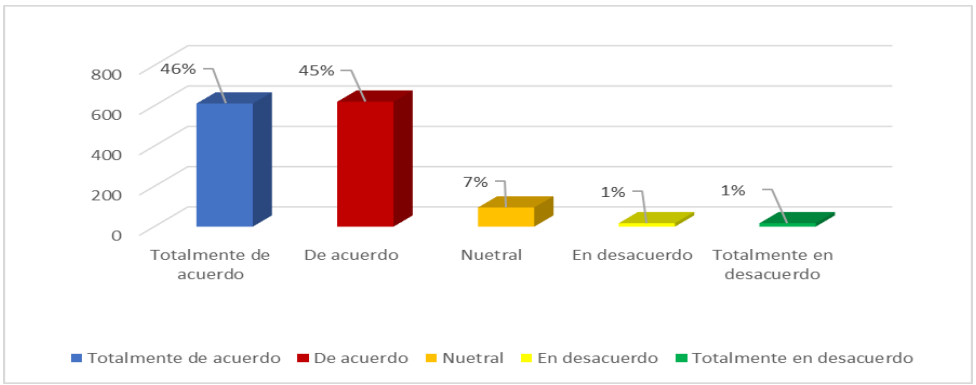

Figura 21. Pregunta 17 - ¿Está de acuerdo que se debería incluir un curso obligatorio de ciberseguridad en el plan de estudios de los estudiantes universitarios para promover las buenas prácticas de seguridad?

5. DISCUSIÓN

La revisión bibliográfica y la aplicación del método PRISMA nos permitió discernir y comprender cuales son los tipos de amenazas más comunes a las cuales están propensos los estudiantes de la Universidad Politécnica Salesiana sede Guayaquil, además de conocer que las buenas prácticas son esenciales dentro de la comunidad universitaria y en la cultura general que marcan las actividades tecnológicas en las cuales se encuentran inmersos cotidianamente, es un factor fundamental y de vital importancia transmitir este conocimiento a cada estudiante que forma parte de este centro de estudios.

Si bien la mayoría de los estudiantes de la Universidad Politécnica Salesiana sede Guayaquil, conocen de las buenas prácticas de ciberseguridad, existe un porcentaje de estudiantes que desconocen sobre el riesgo potencial para la seguridad de la información a la hora de reconocer correos maliciosos. Por ello, recomendamos implementar cursos de capacitación que aborden gran parte de las amenazas existentes que ayude a reforzar la importancia sobre el conocimiento de la ciberseguridad.

Este análisis revela que, una gran parte de los estudiantes universitarios conocen de los ataques más comunes como lo son el phishing y malware, por lo contrario, desconocen del ataque ransomware, siendo este uno de los más peligroso para los estudiantes y la institución. Esta grieta puede generar futuros problemas si no se toman las medidas adecuadas que ayuden con la detección y prevención ante esta amenaza.

Aunque la mayoría de los estudiantes confían en la seguridad digital que brinda la universidad, existe un segmento significativo que necesitan mayor información sobre las seguridades disponibles que ofrece la universidad y poder cambiar su perspectiva en consencuencia.

Además, los resultados determinan que los estudiantes sufren más de ataques phishing y malware por una falta de familiaridad con los aspectos de la ciberseguridad, especialmente las carreras de contabilidad, arquitectura, odontología y psicología. En contraste, estudiantes de computación e ingeniería de sistemas y telecomunicaciones demuestran ser más hábiles al detectar correos maliciosos. Esta discrepancia puede afectar la forma en que detectamos y comprendemos las amenazas en el ámbito digital, resaltando la necesidad de desarrollar cursos de ciberseguridad que se adapten a las necesidades de las diferentes carreras de la universidad y garantice una protección uniforme en toda la universidad.

6. CONCLUSIÓN

Los resultados de la investigación revelan una diferencia significativa respecto a la cantidad de estudiantes entre los campus Centenario y María Auxiliadora de la Universidad Politécnica Salesiana, en el Campus Centenario, las carreras técnicas predominan, mientras que en el campus María Auxiliadora, las carreras relacionadas con ciencias de la vida y educación son más comunes, específicamente, se destaca la "Ingeniería Industrial" en el campus Centenario y "Psicología" en el campus María Auxiliadora como las carreras con mayor matrícula en sus respectivos campus, en relación con la ciberseguridad, se observa que la mayoría de los estudiantes manifiestan poseer conocimientos básicos sobre buenas prácticas en este ámbito, esto es un indicador positivo, ya que la conciencia y la capacitación en ciberseguridad son fundamentales en la actualidad.

Además, los datos recopilados revelan una carencia en la gestión de contraseñas, especialmente en el contexto del correo institucional, un porcentaje significativo de estudiantes muestra desconocimiento en prácticas de ciberseguridad relacionadas con la administración de contraseñas. Por lo tanto, se recomienda implementar programas de capacitación específicos para fortalecer la seguridad en el acceso a plataformas y servicios digitales.

Por otro lado, se ha evidenciado una brecha de conocimiento en conocimiento a las buenas prácticas en la ciberseguridad, como lo son la identificación de correos fraudulentos, principalmente del tipo Phishing y el reconocimiento de amenazas como el ransomware (que representa el Ciber-ataque más peligroso para el estudiante y para la institución). Aunque la mayoría de los estudiantes no ha reportado incidentes de ciberseguridad dentro de la institución, existe una cantidad significativa de estudiantes que pueden ser engañada por enlaces maliciosos, por lo que se resalta la importancia de ampliar el conocimiento y la conciencia en las buenas prácticas de la ciberseguridad para mitigar esto riesgos.

Por lo tanto, se recomienda la implementación de estrategias de educación y sensibilización en ciberseguridad, enfocadas en fortalecer la cultura de seguridad digital entre la comunidad estudiantil de la Universidad Politécnica Salesiana, dichas estrategias deben incluir componentes prácticos, como simulacros de ataques cibernéticos en entornos controlados, cursos de capacitaciones interactivas, con el propósito de promover una comprensión más profunda de las amenazas y fomentar las buenas prácticas en la ciberseguridad.

7. REFERENCIAS BIBLIOGRÁFICAS

Adamu, H., Mohammed, A. D., Adepoju, S. A., & Aderiike, A. O. (2022). A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication. *Proceedings of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development, NIGERCON 2022*. https://doi.org/10.1109/NIGERCON54645.2022.9803122

Allodi, L., Chotza, T., Panina, E., & Zannone, N. (2020). The Need for New Antiphishing Measures against Spear-Phishing Attacks. *IEEE Security and Privacy*, *18*(2), 23–34. https://doi.org/10.1109/MSEC.2019.2940952

Baig, M. S., Ahmed, F., & Memon, A. M. (2021). Spear-Phishing campaigns: Link Vulnerability leads to phishing attacks, Spear-Phishing electronic/UAV communication-scam targeted. *Proceedings - 2021 IEEE 4th International Conference on Computing and Information Sciences, ICCIS 2021*. https://doi.org/10.1109/ICCIS54243.2021.9676394

Blancaflor, E., Romero, M. A., Nacu, I., & Golosinda, D. R. (2023). A Case Study on Smishing: An Assessment of Threats against Mobile Devices. *ACM International Conference Proceeding Series*, 172–178. https://doi.org/10.1145/3605423.3605446

Chavan, A., Kerakalamatti, K., & Srivastva, S. (2021). Implementation of Portable Antivirus System using Signature-based Detection and Heuristic Analysis. *Proceedings of the 5th International Conference on Trends in Electronics and Informatics, ICOEI 2021*, 1481–1486. https://doi.org/10.1109/ICOEI51242.2021.9452909

Cheon, S. B., Choi, G. Y., & Kim, D. Y. (2023). A Cheating Attack on a Whitelist-based Anti-Ransomware Solution and its Countermeasure. *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, *2023-January*. https://doi.org/10.1109/ICCE56470.2023.10043480

Condori Ojeda, P. (2020). *Universo, población y muestra*. https://www.aacademica.org/cporfirio/18

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys (CSUR)*, *54*(8). https://doi.org/10.1145/3469886

Ellahi, O., Umer, M., Raza, A., & Rehman, K. (2022). Analyzing 2FA Phishing Attacks and Their Prevention Techniques. *SIST 2022 - 2022 International Conference on Smart Information Systems and Technologies, Proceedings*. https://doi.org/10.1109/SIST54437.2022.9945766

Guaña-Moya, J., Chiluisa-Chiluisa, M. A., Jaramillo-Flores, P. del C., Naranjo-Villota, D., Mora-Zambrano, E. R., & Larrea-Torres, L. G. (2022). Phishing attacks and how to prevent them. *Iberian Conference on Information Systems and Technologies, CISTI*, *2022-June*. https://doi.org/10.23919/CISTI54924.2022.9820161

Kumari, A., & Sharma, I. (2023a). SafeDroid: Safeguarding Android Mobile Phones from Adware and Banking Maldroid Attacks. *International Conference on Sustainable Communication Networks and Application, ICSCNA 2023 - Proceedings*, 98–103. https://doi.org/10.1109/ICSCNA58489.2023.10370154

Kumari, A., & Sharma, I. (2023b). Towards Securing Mobile Communication from Spyware Attacks with Artificial Intelligence Techniques. *2023 IEEE International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering, RMKMATE 2023*. https://doi.org/10.1109/RMKMATE59243.2023.10369812

Leonov, P. Y., Vorobyev, A. V., Ezhova, A. A., Kotelyanets, O. S., Zavalishina, A. K., & Morozov, N. V. (2021). The main social engineering techniques aimed at hacking information systems. *Proceedings - 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT 2021*, 471–473. https://doi.org/10.1109/USBEREIT51232.2021.9455031

Mira, F. (2021). A systematic literature review on malware analysis. *2021 IEEE International IOT, Electronics and Mechatronics Conference, IEMTRONICS 2021 - Proceedings*. https://doi.org/10.1109/IEMTRONICS52119.2021.9422537

Or-Meir, O., Cohen, A., Elovici, Y., Rokach, L., & Nissim, N. (2021). Pay Attention: Improving Classification of PE Malware Using Attention Mechanisms Based on System

Call Analysis. *Proceedings of the International Joint Conference on Neural Networks, 2021-July*. https://doi.org/10.1109/IJCNN52387.2021.9533481

Pappu, S., Kangane, D., Shah, V., & Mandwiwala, J. (2021). AI-Assisted Risk Based Two Factor Authentication Method (AIA-RB-2FA). *Proceedings of the 2021 IEEE International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems, ICSES 2021*. https://doi.org/10.1109/ICSES52305.2021.9633937

Patil, S., & Dhage, S. (2019). A Methodical Overview on Phishing Detection along with an Organized Way to Construct an Anti-Phishing Framework. *2019 5th International Conference on Advanced Computing and Communication Systems, ICACCS 2019*, 588–593. https://doi.org/10.1109/ICACCS.2019.8728356

Peker, Y. K., Ray, L., & Da Silva, S. (2018). Online cybersecurity awareness modules for college and high school students. *Proceedings - 2018 National Cyber Summit Research Track, NCS 2018*, 24–33. https://doi.org/10.1109/NCS.2018.00009

Shakya, S., Papakostas, G., & Kamel, K. A. (2023). *Mobile Computing and Sustainable Informatics Proceedings of ICMCSI 2023*. https://doi.org/10.1007/978-981-99-0835-6

Sharma, A. K., Galav, R. K., & Sharma, B. (2023). A Comprehensive Survey of various Cyber Attacks. *2023 6th International Conference on Information Systems and Computer Networks, ISCON 2023*. https://doi.org/10.1109/ISCON57294.2023.10111998

Shehata, S. M., Hegazy, I., & El-Horbaty, E.-S. M. (2023). Android Cloud Antivirus Based on Static Analysis. *2023 Eleventh International Conference on Intelligent Computing and Information Systems (ICICIS)*, 219–224. https://doi.org/10.1109/ICICIS58388.2023.10391148

Ventura-León, J., & Valencia, P. D. (2020). Confidence intervals: Clarifications and interpretations in the field of health. In *Revista Chilena de Pediatria* (Vol. 91, Issue 6, pp. 991–992). Sociedad Chilena de Pediatria. https://doi.org/10.32641/RCHPED.V91I6.2972