UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

CARRERA: COMPUTACIÓN MENCIÓN EN SEGURIDAD INFORMÁTICA

TEMA:

"CIBERSEGURIDAD Y EDUCACIÓN ONLINE: UN ESTUDIO EMPÍRICO SOBRE LOS RIESGOS Y LAS MEDIDAS DE PREVENCIÓN DE LA VULNERACIÓN DE LA PRIVACIDAD DE LOS ESTUDIANTES EN EL ENTORNO DIGITAL"

Trabajo de titulación previo a la obtención del título de Magíster en

Computación con mención en Seguridad Informática

Línea de investigación: Desarrollo, aplicación de software y cibersecurity (seguridad cibernética)

AUTOR(A):

ARIZAGA MONTENEGRO JHON MANUEL

DIRECTOR(A):

GUEVARA VEGA VICENTE ALEXANDER

Ibarra, octubre 2025

UNIVERSIDAD TÉCNICA DEL NORTE
DIRECCIÓN DE BIBLIOTECA

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1002733945		
APELLIDOS Y NOMBRES:	ARIZAGA MONTENEGRO JHON MANUEL		
DIRECCIÓN:	Ambato 945 – Isla Fernandina		
EMAIL:	Jhonarizaga2@gmail.com		
TELÉFONO FIJO:	062545197	**TELÉFONO MÓVIL:**	0993657397

DATOS DE LA OBRA	
TÍTULO:	CIBERSEGURIDAD Y EDUCACIÓN ONLINE: UN ESTUDIO EMPÍRICO SOBRE LOS RIESGOS Y LAS MEDIDAS DE PREVENCIÓN DE LA VULNERACIÓN DE LA PRIVACIDAD DE LOS ESTUDIANTES EN EL ENTORNO DIGITAL
AUTOR (ES):	ARIZAGA MONTENEGRO JHON MANUEL
FECHA: DD/MM/AAAA	17/10/2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **GRADO** ■ **POSGRADO**
TITULO POR EL QUE OPTA:	Magíster en Computación con mención en Seguridad Informática
ASESOR /DIRECTOR:	GUEVARA VEGA VICENTE ALEXANDER

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 17 días del mes de octubre de 2025

EL AUTOR: Firmado electrónicamente por: JHON MANUEL ARIZAGA MONTENEGRO. Validar únicamente con FirmaEC

Nombre: ARIZAGA MONTENEGRO JHON MANUEL

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 17 de octubre de 2025

Vicente Alexander Guevara Vega

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

(f) .....

Vicente Alexander Guevara Vega

C.C.: 1002334827

Ibarra, 19 de noviembre de 2024

Dra.
Lucía Yépez
DECANA FACULTAD DE POSGRADO

ASUNTO: Conformidad con el documento final

Señora Decana:

Nos permitimos informar a usted que, revisado el Trabajo final de Grado "CIBERSEGURIDAD Y EDUCACIÓN ONLINE: UN ESTUDIO EMPÍRICO SOBRE LOS RIESGOS Y LAS MEDIDAS DE PREVENCIÓN DE LA VULNERACIÓN DE LA PRIVACIDAD DE LOS ESTUDIANTES EN EL ENTORNO DIGITAL", del maestrante ARIZAGA MONTENEGRO JHON MANUEL, de la Maestría en Computación mención Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	Firma
Director	MSc. Alexander Guevara Vega	
Asesor	Ph.D. Yoo Sang Guun	

INDICE DE CONTENIDOS

INDICE DE TABLAS

GLOSARIO

- Ciberseguridad: Conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas, redes y datos frente a ataques o accesos no autorizados.
- Educación Online: Modalidad de enseñanza y aprendizaje que se lleva a cabo a través de internet y plataformas digitales.
- Ley Orgánica de Protección de Datos Personales: Normativa ecuatoriana que regula el tratamiento y protección de los datos personales de los ciudadanos.
- Política Nacional de Ciberseguridad: Estrategia del Estado para garantizar la seguridad de la información en infraestructuras críticas y servicios digitales.
- MAGERIT: Metodología de Análisis y Gestión de Riesgos en Sistemas de Información, utilizada para identificar amenazas, evaluar riesgos y proponer medidas de mitigación.
- Phishing: Técnica de suplantación de identidad utilizada para engañar a usuarios y obtener información personal, como contraseñas y datos bancarios.
- Malware: Software malicioso diseñado para dañar o infiltrarse en sistemas informáticos sin el consentimiento del usuario.
- Autenticación Multifactor: Método de verificación que requiere más de un factor de autenticación para acceder a un sistema o plataforma, como una combinación de contraseña y código enviado al móvil.
- Cifrado de Datos: Proceso que convierte la información en un formato ilegible para protegerla de accesos no autorizados.
- Gestor de Contraseñas: Herramienta que permite almacenar y gestionar de manera segura múltiples contraseñas.

RESUMEN

La presente investigación analiza la importancia de la ciberseguridad en el entorno educativo digital, con el objetivo de identificar riesgos y proponer medidas para proteger los datos personales de los estudiantes secundarios en Ecuador. Se fundamenta en la Ley Orgánica de Protección de Datos Personales y la Política Nacional de Ciberseguridad, utilizando la metodología MAGERIT para evaluar amenazas como phishing, malware y accesos no autorizados. El estudio demuestra que la capacitación en ciberseguridad mejora en un 20-30% la adopción de prácticas seguras, como el uso de contraseñas robustas y autenticación multifactor. Se concluye que una formación continua y la implementación de políticas de seguridad digital fortalecen significativamente la protección de la información en plataformas educativas.

Palabras clave: Ciberseguridad, Educación Online, Protección de Datos, MAGERIT, Phishing, Autenticación Multifactor, Riesgos Digitales.

ABSTRACT

This research analyzes the importance of cybersecurity in the digital educational environment, aiming to identify risks and propose measures to protect the personal data of secondary school students in Ecuador. It is based on the Organic Law on Personal Data Protection and the National Cybersecurity Policy, using the MAGERIT methodology to assess threats such as phishing, malware, and unauthorized access. The study shows that cybersecurity training improves the adoption of safe practices by 20-30%, such as the use of strong passwords and multi-factor authentication. It concludes that continuous training and the implementation of digital security policies significantly strengthen information protection in educational platforms.

Keywords: Cybersecurity, Online Education, Data Protection, MAGERIT, Phishing, Multi-Factor Authentication

CAPITULO I

EL PROBLEMA

1.1. Problema de investigación

En Ecuador, la rápida adopción de la educación online debido a la pandemia de COVID-19 ha expuesto a los estudiantes de educación secundaria a múltiples riesgos de ciberseguridad. Según el informe de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL, 2021), los incidentes cibernéticos en instituciones educativas ecuatorianas aumentaron en un 45% durante el 2020. Estos incidentes incluyen ataques informáticos, robo de identidad, suplantación y ciberacoso, afectando directamente a la integridad y confidencialidad de los datos personales de los estudiantes.

La Ley Orgánica de Protección de Datos Personales, promulgada en 2021, busca abordar estos desafíos; sin embargo, muchas instituciones educativas aún carecen de políticas y medidas adecuadas para proteger a sus estudiantes. Por lo tanto, es imperativo analizar y proponer buenas prácticas que permitan prevenir y gestionar estos riesgos, contribuyendo al desarrollo de una cultura de ciberseguridad en el ámbito educativo ecuatoriano (Loja y Cuenca, 2020).

1.2. Interrogantes de la investigación

- ¿Cuál es el nivel de conocimiento y conciencia que tienen los estudiantes de educación secundaria en Ecuador sobre la ciberseguridad y la protección de datos personales en la educación online?
- ¿Cuáles son las principales amenazas y vulnerabilidades que enfrentan estos estudiantes en las plataformas de educación online en términos de estafas en línea y robo de identidad?
- ¿En qué medida las instituciones educativas ecuatorianas cumplen con la normativa legal vigente sobre ciberseguridad y protección de datos personales?
- ¿Qué buenas prácticas se pueden recomendar para mejorar la ciberseguridad y la protección de datos personales de los estudiantes de educación secundaria en la educación online?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Evaluar los riesgos de ciberseguridad y sugerir buenas prácticas en el ámbito de la educación online, con especial atención a la protección de los datos personales, estafas en línea y robo de identidad que sufren los estudiantes de educación secundaria en el Ecuador.

1.3.2 Objetivos específicos

Identificar y analizar las principales amenazas y vulnerabilidades específicas que enfrentan los estudiantes de educación secundaria en Ecuador en las plataformas de educación online, enfocándose en estafas en línea y robo de identidad.

Evaluar el grado de cumplimiento de las instituciones educativas ecuatorianas con la Ley Orgánica de Protección de Datos Personales y otras normativas relacionadas, en el contexto de la educación online.

Diseñar y proponer un conjunto de buenas prácticas y medidas de prevención que las instituciones educativas y los estudiantes puedan implementar para mejorar la ciberseguridad y proteger los datos personales en la educación online.

1.4. Justificación

La importancia de esta investigación radica en que, según el Informe de Ciberseguridad en América Latina y el Caribe del BID (2020), Ecuador se encuentra en una posición vulnerable en cuanto a ciberseguridad, ocupando el puesto 12 en la región (BID, 2020). Además, estudios realizados por la Universidad Técnica de Ambato (2021) indican que un 60% de los estudiantes de educación secundaria en el país no reciben formación adecuada en temas de ciberseguridad y protección de datos personales.

Estos datos evidencian la necesidad de abordar el problema de manera integral, ya que afecta directamente al bienestar y desarrollo académico de los estudiantes. Al contribuir con recomendaciones y buenas prácticas, esta investigación no solo aporta al campo académico, sino que también tiene un impacto social al promover un entorno educativo más seguro y confiable (Andrade, 2023).

La educación online se ha convertido en una modalidad educativa cada vez más relevante y demandada en el mundo, especialmente a raíz de la pandemia de COVID-19, que ha obligado a millones de estudiantes y docentes a adaptarse a esta forma de enseñanza y aprendizaje. Sin embargo, la educación online también implica una serie de riesgos y desafíos relacionados con la ciberseguridad y la protección de datos personales, que pueden afectar tanto a la calidad y la confianza de los procesos educativos, como a los derechos y la privacidad de los participantes. Por ello, es necesario realizar un análisis riguroso y actualizado de estos aspectos, desde una perspectiva integral y multidisciplinaria, que abarque los ámbitos técnico, legal, ético y pedagógico (Díaz, 2021).

Este proyecto tiene como objetivo contribuir al conocimiento científico sobre la ciberseguridad y la protección de datos personales en la educación online, así como ofrecer recomendaciones y buenas prácticas para mejorar estos aspectos en el contexto ecuatoriano. Para ello, se propone realizar una revisión bibliográfica exhaustiva sobre el tema, así como una encuesta a una muestra representativa de estudiantes que participan en esta modalidad educativa, para conocer su nivel de conocimiento, conciencia y comportamiento respecto a la ciberseguridad y la protección de datos personales. Asimismo, se pretende analizar las medidas técnicas y normativas que se aplican en las plataformas y recursos utilizados para la educación online, así como las estrategias y recursos pedagógicos que se emplean para fomentar la cultura de ciberseguridad y protección de datos personales entre los actores involucrados (Paredes y Chicaiza, 2021).

Este proyecto es relevante e innovador porque aborda un tema de gran actualidad e interés social, que tiene implicaciones para el desarrollo educativo, tecnológico y jurídico del país. Además, se basa en una metodología rigurosa y adecuada al objeto de estudio, que combina fuentes secundarias y primarias de información. Finalmente, se espera que este proyecto genere resultados útiles y aplicables para mejorar la ciberseguridad y la protección de datos personales en la educación online, así como para promover la calidad, la equidad y la inclusión de esta modalidad educativa (Fernández & Sussi de Oliveira, 2021)

CAPITULO II

MARCO REFERENCIAL

2.1 Introducción

En este capítulo se presenta el marco referencial que sustenta la investigación, el cual se divide en tres secciones principales: el marco teórico, donde se abordan los conceptos clave relacionados con la ciberseguridad, la protección de datos personales y la educación online; el marco legal, que analiza la normativa vigente en Ecuador y su aplicación en el contexto educativo; y el estado del arte, que revisa estudios previos y experiencias relacionadas con el tema de investigación (Pérez y Gómez, 2020).

Esta revisión bibliográfica permite contextualizar el problema, identificar brechas de conocimiento y fundamentar teóricamente las propuestas que se desarrollarán en los siguientes capítulos.

3.1 Análisis de Riesgos en la Educación Online

Pueden tener graves consecuencias. Los ataques cibernéticos, el ciberfraude y el robo de identidad son algunos de los problemas de seguridad que no deben pasar por alto1. Además, la educación en pandemia ha expuesto a los usuarios a distintos peligros presentes en la red (Pacheco *et al*, 2021)

4.1 Protección de Datos Personales de los Estudiantes

La protección de datos personales es un aspecto crucial en la educación online. Es imprescindible conocer buenas prácticas en protección de datos personales para realizar una adecuada recogida y un correcto uso de los datos. La Delegación de Protección de Datos ha elaborado un Decálogo de buenas prácticas para la protección de los datos personales en el ámbito educativo (Corozo, 2023).

5.1 Buenas Prácticas para la Protección de Datos Personales

Existen varias recomendaciones y buenas prácticas para asegurar que los datos personales sean recopilados, usados y protegidos de manera que se tenga en consideración la privacidad del individuo y cualquier riesgo que pueda ocurrir por no proteger adecuadamente sus datos (Galvá, 2018).

6.1 Descripción del área de estudio / Descripción del grupo de estudio

En el campo de la ciberseguridad, se analizan los riesgos asociados con el uso de tecnologías de la información y comunicación en el ámbito educativo. Esto incluye el

estudio de amenazas potenciales, como ataques cibernéticos, fraudes, robos de identidad, entre otros. También se consideran las medidas preventivas y correctivas que se pueden implementar para mitigar estos riesgos (Paredes y Chicaiza, 2021).

En cuanto a la educación online, se examina cómo las plataformas digitales y las tecnologías emergentes están transformando la forma en que se imparte la educación. Se consideran aspectos como la accesibilidad, la eficacia del aprendizaje online, así como los desafíos y oportunidades que presenta este formato de enseñanza (Galvá, 2018).

El grupo de estudio que se ocupa de este tema está compuesto por profesionales y académicos de diversas disciplinas, incluyendo expertos en ciberseguridad, educadores, psicólogos, sociólogos y expertos en tecnología educativa. Estos profesionales trabajan juntos para investigar y desarrollar estrategias efectivas para proteger los datos personales de los estudiantes en un entorno online (Beltrán Muñoz, 2024)

2.2 Marco teórico

La ciberseguridad es el conjunto de medidas, técnicas y procesos que tienen como objetivo proteger la información, los sistemas y las redes informáticas de posibles ataques, intrusiones o amenazas que puedan comprometer su integridad, disponibilidad o confidencialidad. La ciberseguridad es un aspecto clave para garantizar la seguridad nacional, la competitividad económica y el bienestar social en el contexto de la sociedad digital (Muñoz Castillo, 2024)

La educación online es una modalidad de enseñanza y aprendizaje que utiliza las tecnologías de la información y la comunicación (TIC) para facilitar el acceso, la interacción y la colaboración entre los actores educativos (estudiantes, docentes, tutores, etc.) sin limitaciones de tiempo o espacio. La educación online ofrece ventajas como la flexibilidad, la personalización, la diversidad y la innovación pedagógica, pero también implica desafíos como la calidad, la equidad, la motivación y la evaluación (Díaz, 2021).

El análisis de riesgos es un proceso sistemático que permite identificar, evaluar y gestionar los riesgos asociados a una actividad, un proyecto o un sistema. El análisis de riesgos en la ciberseguridad implica considerar los factores tecnológicos, empresariales, regulatorios y humanos que pueden afectar a la seguridad de la información y las infraestructuras críticas. El análisis de riesgos en la ciberseguridad debe ser transversal

(entre sectores) y transdisciplinar (entre áreas de conocimiento) para abordar la complejidad y la dinamicidad del entorno cibernético (Salazar Mata *et al*, 2021)

Las buenas prácticas son aquellas acciones, procedimientos o recomendaciones que se consideran adecuadas o eficaces para lograr un objetivo o resolver un problema. Las buenas prácticas en la ciberseguridad son aquellas que contribuyen a prevenir, detectar o mitigar los incidentes o ataques que puedan afectar a la seguridad de la información y las redes informáticas. Las buenas prácticas en la ciberseguridad deben ser aplicadas por todos los actores involucrados en el uso, el desarrollo o la gestión de las TIC (Corozo, 2023).

La protección de datos personales es el derecho que tienen las personas a controlar el uso que se hace de su información personal por parte de terceros, ya sean públicos o privados. La protección de datos personales implica garantizar el respeto a los principios de licitud, lealtad, transparencia, limitación de la finalidad, minimización de los datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad. La protección de datos personales es un aspecto fundamental para preservar la privacidad, la dignidad y los derechos fundamentales de las personas en el ámbito digital (Paredes y Chicaiza, 2021).

La relación entre estos conceptos se puede establecer de la siguiente manera: La ciberseguridad y la educación online son dos fenómenos emergentes que tienen un gran impacto en el desarrollo social y económico. Ambos requieren de un análisis de riesgos adecuado que permita identificar y gestionar las amenazas y vulnerabilidades que pueden afectar a sus objetivos y funcionamiento. Asimismo, ambos deben aplicar buenas prácticas que contribuyan a mejorar su calidad, eficiencia y seguridad. Por último, tanto la ciberseguridad como la educación online deben respetar y garantizar la protección de datos personales de los usuarios, especialmente de los estudiantes, que son los principales beneficiarios y protagonistas del proceso educativo (Suárez *et al*, 2023)

2.3 Marco legal

La Constitución de la República del Ecuador1, que reconoce y garantiza el derecho a la protección de datos personales y el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual, así como el deber del Estado de garantizar el

efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales.

La Ley Orgánica de Protección de Datos Personales2, que regula los principios, derechos, obligaciones, procedimientos y sanciones relacionados con el tratamiento de datos personales, tanto por parte del sector público como del sector privado, con el fin de garantizar el respeto a la privacidad, la dignidad y los derechos fundamentales de las personas en el ámbito digital (Herrero *et al*, 2022).

El Acuerdo Ministerial 006-20213, que establece la Política Nacional de Ciberseguridad, que tiene como objetivo definir los lineamientos estratégicos para fortalecer la seguridad de la información y las infraestructuras críticas del país, así como promover una cultura de ciberseguridad entre los actores públicos y privados, mediante la coordinación, cooperación y articulación interinstitucional (Medina *et al*, 2023)

CAPITULO III
MARCO METODOLÓGICO

3.1.Descripción del área de estudio / Descripción del grupo de estudio

Tipo y diseño de la investigación: Se trata de una investigación mixta, que combina el enfoque cualitativo y el cuantitativo, con un diseño exploratorio-descriptivo. El enfoque cualitativo permite comprender los significados, las percepciones y las experiencias de los actores involucrados en la educación online, así como profundizar en los aspectos contextuales y subjetivos del fenómeno. El enfoque cuantitativo permite medir, comparar y contrastar los datos obtenidos, así como generalizar y validar los resultados. El diseño exploratorio-descriptivo permite indagar sobre un tema poco estudiado o novedoso, así como describir sus características, dimensiones y variables.

Población y muestra: La población de la investigación está conformada por las instituciones educativas que ofrecen educación online en Ecuador, así como por los estudiantes que participan en dicha modalidad. La muestra se seleccionará mediante un muestreo no probabilístico por conveniencia, teniendo en cuenta los criterios de accesibilidad, disponibilidad y colaboración. Se estima que la muestra estará compuesta por unas 5 instituciones educativas y unos 200 estudiantes, lo que representa un 10% de la población aproximada.

Técnicas e instrumentos de recolección de datos: Las técnicas e instrumentos que se utilizarán para recolectar los datos son los siguientes:

Análisis documental: Se revisarán los documentos oficiales, normativos y académicos relacionados con la ciberseguridad y la protección de datos personales en la educación online, tanto a nivel nacional como internacional. El instrumento que se utilizará será una ficha de análisis documental, que permitirá registrar los datos bibliográficos, el resumen, las palabras clave, las citas relevantes y el análisis crítico de cada documento.

Encuesta: Se aplicará un cuestionario a los estudiantes que participan en la educación online, con el fin de obtener información sobre sus características sociodemográficas, sus hábitos y actitudes frente a la ciberseguridad y la protección de datos personales, así como su nivel de satisfacción y confianza con la modalidad. El

cuestionario será autoadministrado mediante una plataforma online, previo consentimiento informado. El cuestionario tendrá una estructura mixta, con preguntas cerradas (tipo Likert, dicotómicas, múltiple opción) y abiertas (de opinión o sugerencia). El cuestionario tendrá una duración aproximada de 15 minutos y se validará mediante una prueba piloto.

Entrevista: Se realizarán entrevistas semiestructuradas a los representantes o responsables de las instituciones educativas que ofrecen educación online, con el fin de obtener información sobre sus políticas, normas y prácticas de ciberseguridad y protección de datos personales, así como sobre los riesgos y desafíos que enfrentan en dicha modalidad. Las entrevistas serán individuales, presenciales o virtuales, previa cita y consentimiento informado. Las entrevistas tendrán una duración aproximada de 30 minutos y se grabarán con autorización. El instrumento que se utilizará será una guía de entrevista, que contendrá las preguntas generales y específicas que se formularán a los entrevistados, así como los aspectos a observar durante la entrevista.

Técnicas e instrumentos de análisis de datos: Las técnicas e instrumentos que se utilizarán para analizar los datos son los siguientes:

Análisis de contenido: Se aplicará al material documental y a las entrevistas, con el fin de identificar, clasificar y categorizar las unidades de sentido o significado que emergen del discurso. El instrumento que se utilizará será un sistema de categorías, que permitirá organizar y codificar los datos según los objetivos y las variables de la investigación. El sistema de categorías se elaborará de forma inductiva, a partir de los datos, o deductiva, a partir de la teoría, o mixta, combinando ambos criterios.

Análisis estadístico: Se aplicará a los datos cuantitativos obtenidos mediante el cuestionario, con el fin de describir, comparar y contrastar las variables numéricas o categóricas que se han medido. El instrumento que se utilizará será un software estadístico, que permitirá realizar los cálculos, las tablas, los gráficos y las pruebas necesarias para el análisis. El software estadístico que se utilizará será el SPSS (Statistical Package for the Social Sciences), que es uno de los más utilizados y reconocidos en el ámbito académico y profesional.

3.2.Enfoque y tipo de investigación

El enfoque es mixto, lo que significa que se combina el uso de métodos cualitativos y cuantitativos para obtener una visión más completa y profunda del fenómeno a estudiar. El enfoque mixto permite integrar diferentes fuentes, tipos y niveles de datos, así como contrastar, complementar o corroborar los resultados obtenidos.

El tipo de investigación es exploratorio-descriptivo, lo que implica que se busca indagar sobre un tema poco conocido o novedoso, así como describir sus características, dimensiones y variables. El tipo exploratorio-descriptivo permite generar preguntas, hipótesis o categorías de análisis, así como establecer relaciones o diferencias entre los elementos del estudio.

3.3.Procedimiento de investigación

- **Planteamiento del problema:** Consiste en definir claramente el tema, el objetivo, las preguntas y las hipótesis de la investigación, así como la justificación y la delimitación del estudio.
- **Revisión de la literatura:** Consiste en buscar, seleccionar, analizar y sintetizar la información existente sobre el tema de investigación, tanto en fuentes primarias como secundarias, con el fin de establecer el estado del arte y el marco teórico del estudio.
- **Diseño de la investigación:** Consiste en determinar la metodología que se utilizará para recoger y analizar los datos, es decir, el tipo y el nivel de la investigación, las variables e indicadores, la población y la muestra, las técnicas e instrumentos de recolección y análisis de datos, y los aspectos éticos y legales del estudio.
- **Recolección de datos:** Consiste en aplicar las técnicas e instrumentos seleccionados para obtener la información necesaria para responder a las preguntas e hipótesis de la investigación, ya sea mediante encuestas, entrevistas, observaciones, experimentos u otras fuentes.
- **Análisis de datos:** Consiste en procesar, organizar, sintetizar e interpretar los datos obtenidos mediante técnicas estadísticas, cualitativas o mixtas, con el fin de extraer conclusiones y responder a las preguntas e hipótesis de la investigación.

3.4.Presentación de resultados:

Consiste en comunicar los hallazgos y las conclusiones de la investigación mediante un informe escrito en modelo “Artículo Científico” y una exposición oral, siguiendo las normas académicas y científicas correspondientes.

CAPITULO IV
MARCO ADMINISTRATIVO

4.1.Recursos

4.1.1. Humano

Tabla 1

Recurso Humano

Recurso	**Institución**
Investigador	UTN
Director de Tesis	UTN
Autoridades de Varias Instituciones	IBARRA

4.1.2. Materiales

Tabla 2

Recurso Materiales

Recurso	**Valor**
Internet	160
Laptops	900,00
Impresora	350
Tintas	65
Resmas de Papel	40
TOTAL	**1515,00**

4.1.3. Financieros

Tabla 3

Recurso Financiero

Recurso	**Valor**

Presupuesto General	200
Gastos Operativos	200
Contingencia	500
TOTAL	**3000,00**

4.2.Cronograma de actividades

Tabla 4

Cronograma de Actividades

Actividad	**Mes 1**	**Mes 2**	**Mes 3**	**Mes 4**	**Mes 5**
Revisión bibliográfica	X	X	X		
Diseño del cuestionario	X	X			
Prueba piloto del cuestionario		X			
Aplicación del cuestionario			X	X	
Diseño de la guía de entrevista	X	X			
Realización de las entrevistas			X	X	
Análisis de los datos documentales	X	X	X	X	X
Análisis de los datos cuantitativos				X	X
Análisis de los datos cualitativos				X	X
Redacción del informe final		X	X	X	X

CAPITULO V

DESARROLLO

5. Recopilación de datos

5.1.Evaluación de estudiantes

En este apartado, se identificaron las necesidades críticas de formación en ciberseguridad y protección de datos personales entre los estudiantes y docentes involucrados en la educación online. Se realizó un análisis del conocimiento general y la conciencia de los estudiantes sobre la ciberseguridad y los riesgos relacionados, previo a la implementación de un programa de formación enfocado en mejorar las prácticas de seguridad digital en entornos educativos.

5.2. Nivel de conocimiento pre-implementación

Para determinar el nivel de conocimiento antes de la implementación del programa, se utilizaron dos técnicas de investigación: la encuesta y la observación. La encuesta fue elaborada utilizando Google Forms, y contenía preguntas enfocadas en los siguientes temas: aspectos básicos de ciberseguridad, protección de datos personales, estafas en línea, robo de identidad, phishing, gestión de contraseñas, políticas de privacidad en plataformas de educación online, y buenas prácticas de seguridad.

El cuestionario se configuró con preguntas cerradas para evaluar el nivel de conciencia y conocimiento sobre los riesgos cibernéticos que enfrentan los estudiantes de secundaria en Ecuador. Un total de 150 estudiantes de cinco instituciones educativas participaron en la encuesta. Es importante resaltar que el programa estaba dirigido a estudiantes sin conocimientos técnicos avanzados en tecnología, lo que permitió obtener una visión precisa sobre las necesidades formativas en este ámbito.

Grafico 1

¿Utiliza conexiones seguras (HTTPS) y cifra sus archivos sensibles para proteger su información?

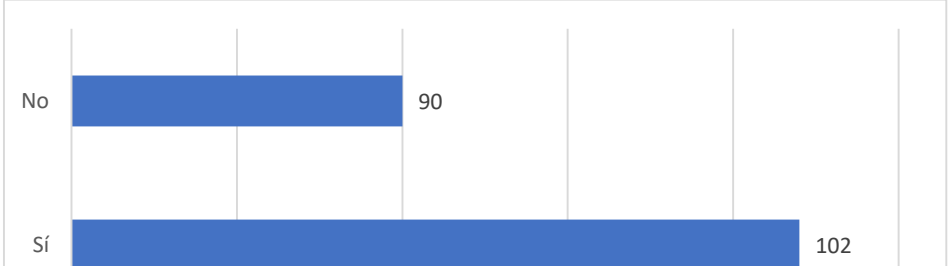


Grafico 2

¿Asegura que su sistema operativo y software estén siempre actualizados con las últimas correcciones de seguridad?

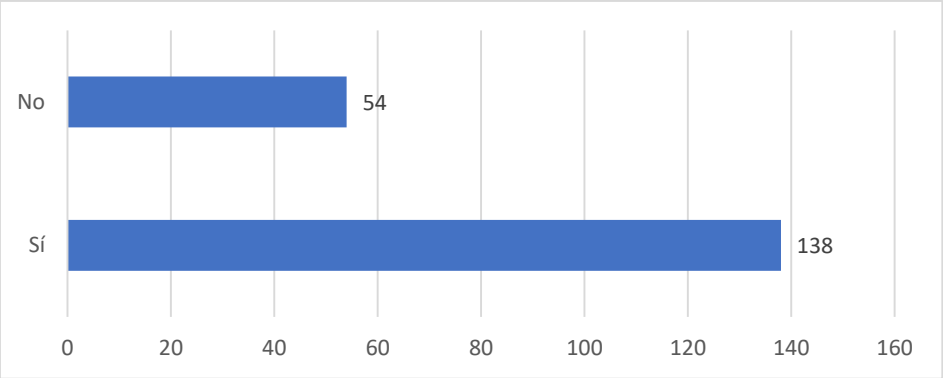


Grafico 3

¿Utiliza contraseñas robustas y únicas para sus cuentas en línea, evitando contraseñas simples como "123456"?

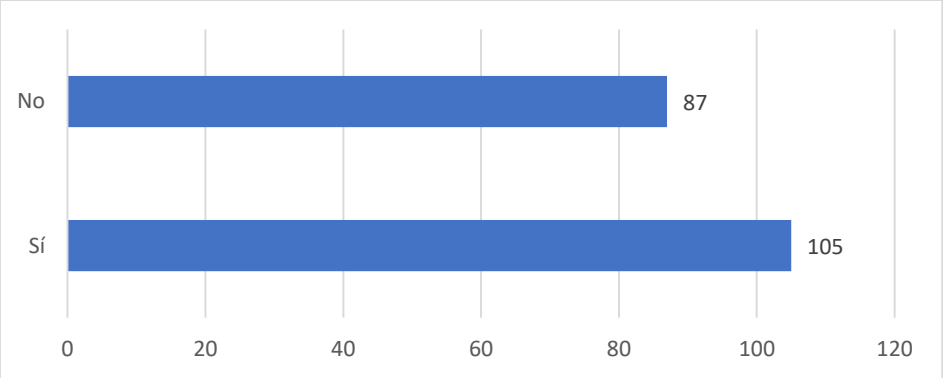


Grafico 4

¿Implementa la autenticación de dos factores siempre que sea posible para añadir una capa adicional de seguridad?

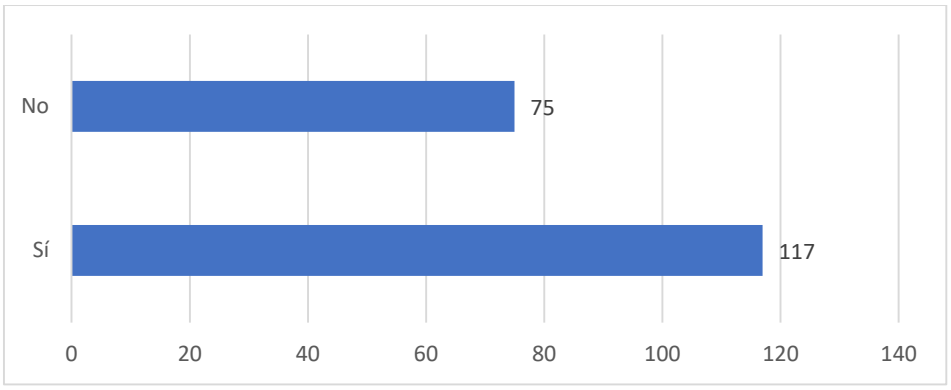


Grafico 5

¿Está al tanto de las amenazas de seguridad cibernética, como el phishing, el malware y las estafas en línea?

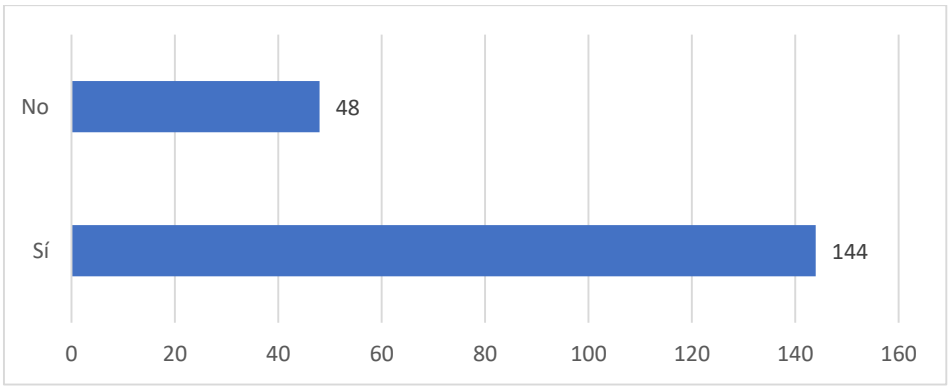


Grafico 6

¿Realiza copias de seguridad periódicas de sus datos importantes y los almacena de forma segura?

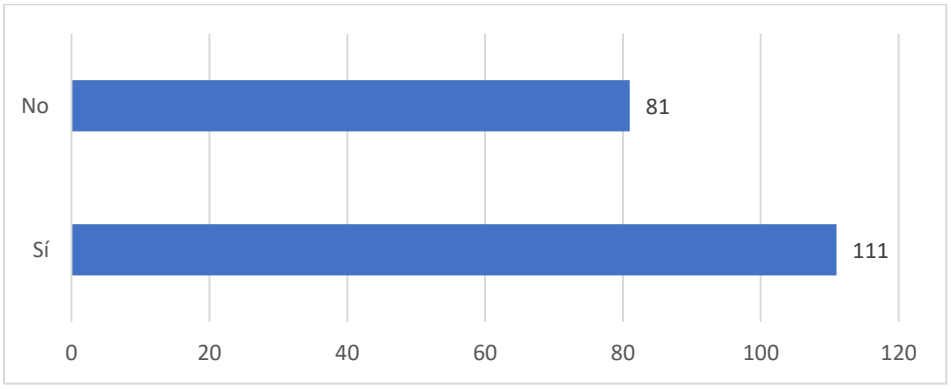


Grafico 7

¿Protege su red Wi-Fi con una contraseña sólida y evita conectarse a redes públicas no seguras o desconocidas?

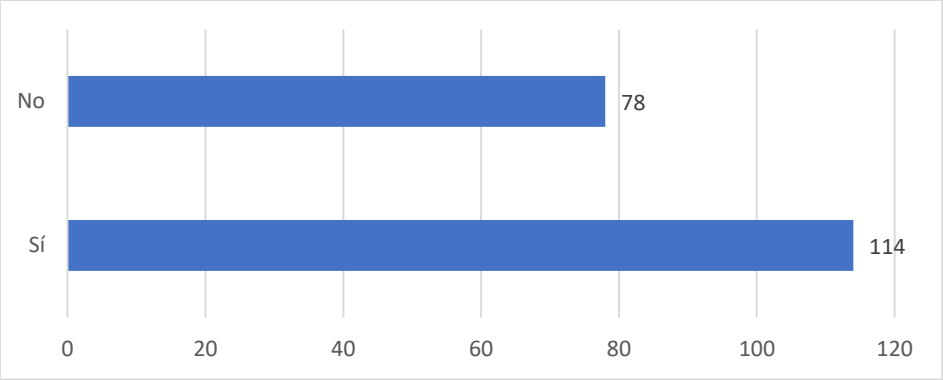


Grafico 8

¿Utiliza software de seguridad confiable como antivirus y mantiene sus configuraciones actualizadas?

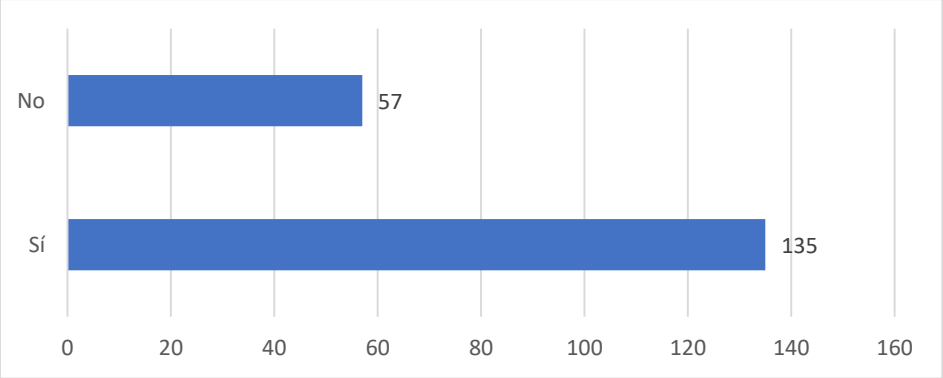


Grafico 9

¿Limita el acceso a su dispositivo y datos solo a personas autorizadas?

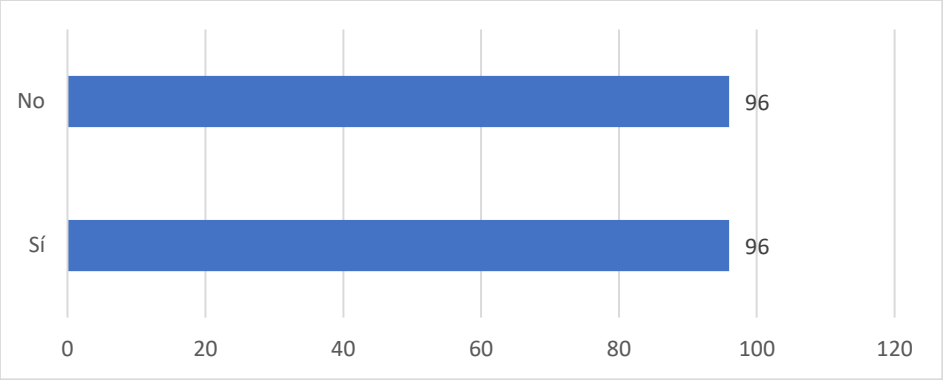


Grafico 10

¿Define un período para retener datos personales y elimina información que ya no sea necesaria?

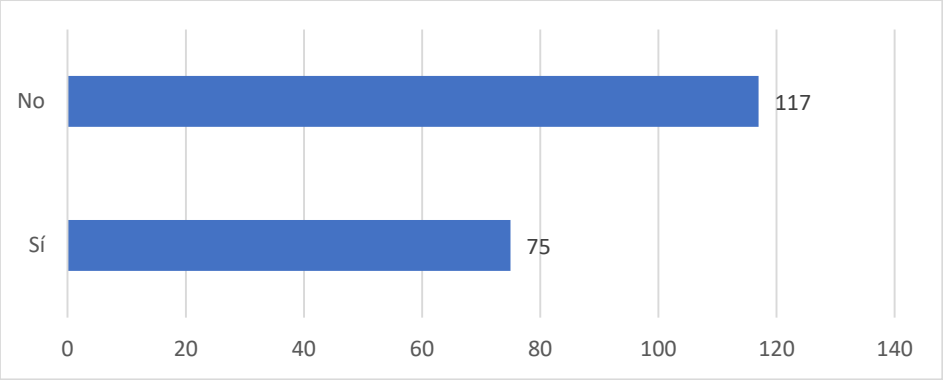


Grafico 11

¿Dispone de una política de privacidad clara si maneja datos de terceros y cumple con las regulaciones?

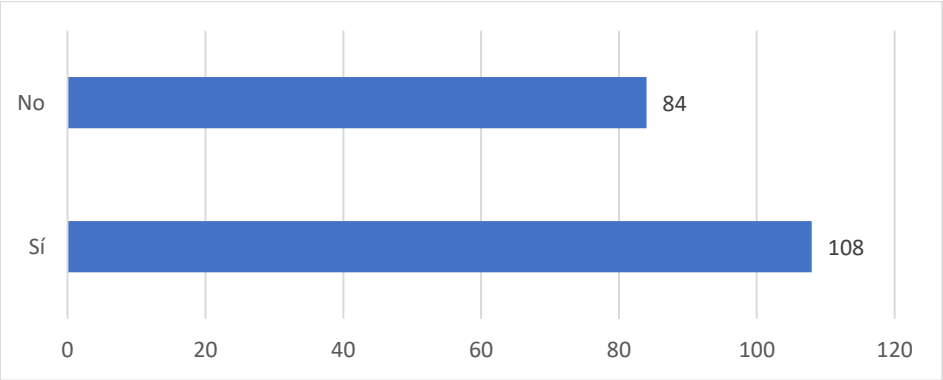


Grafico 12

¿Realiza evaluaciones periódicas de seguridad para identificar posibles vulnerabilidades?

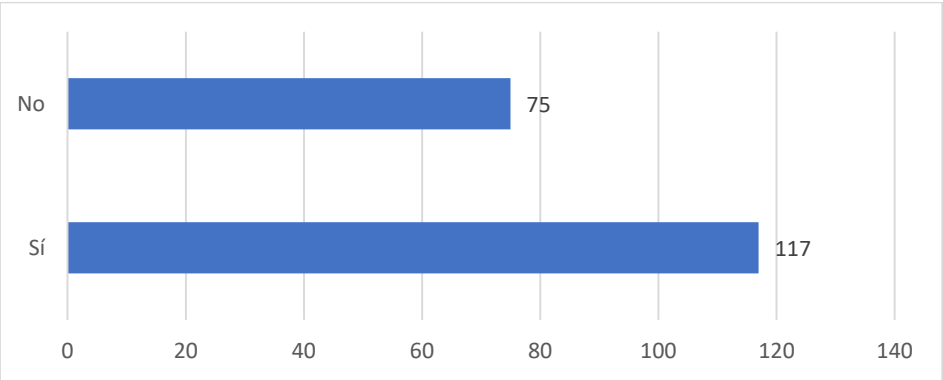


Grafico 13

¿Cuenta con sistemas de registro y monitorización para detectar actividad inusual en su dispositivo?

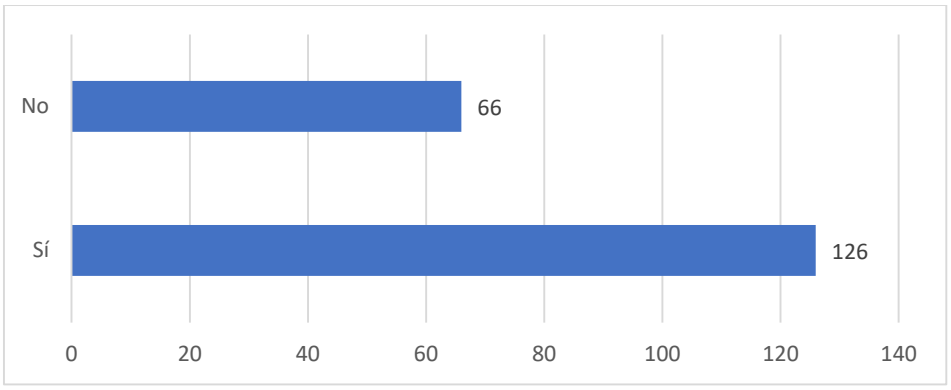


Grafico 14

¿Dispone de un plan de respuesta a incidentes informáticos para abordar problemas de seguridad?

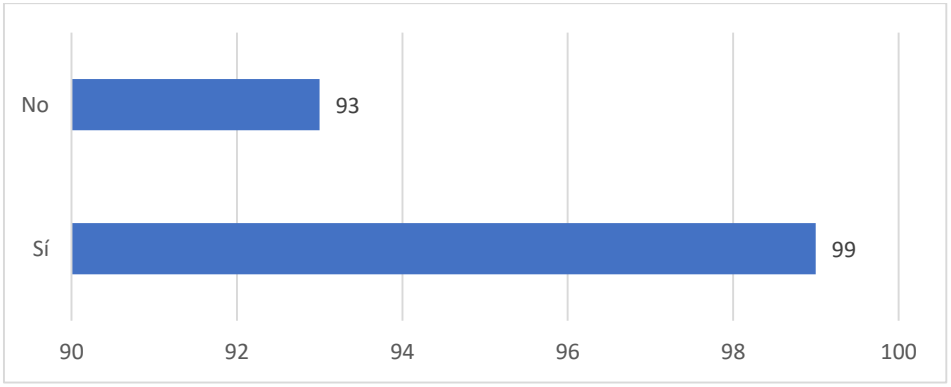


Grafico 15

¿Mantiene su sistema y aplicaciones siempre actualizados con los últimos parches de seguridad?

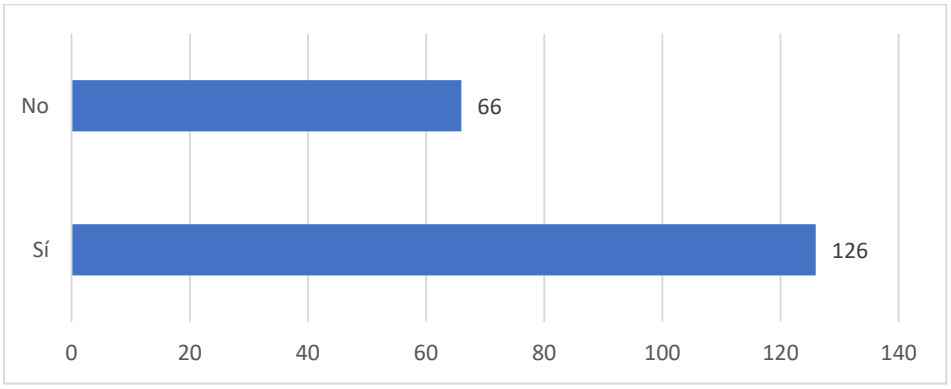


Grafico 16

¿Sigue una política propia de contraseñas que promueve contraseñas seguras y cambios regulares?

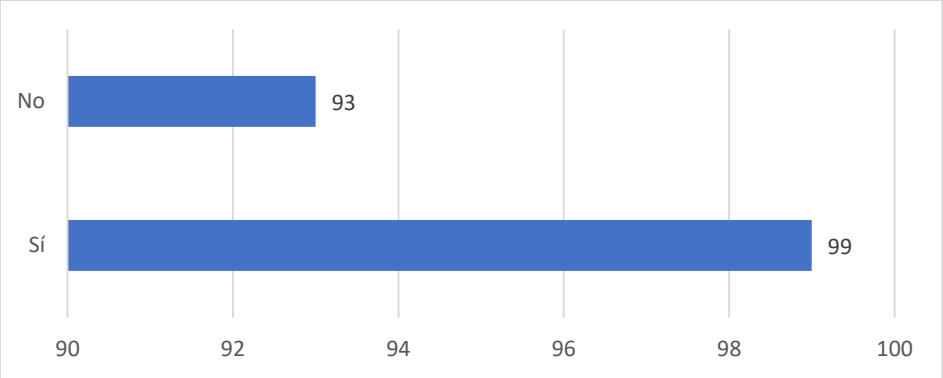


Grafico 17

¿Se mantiene informado sobre prácticas seguras de seguridad cibernética y privacidad?

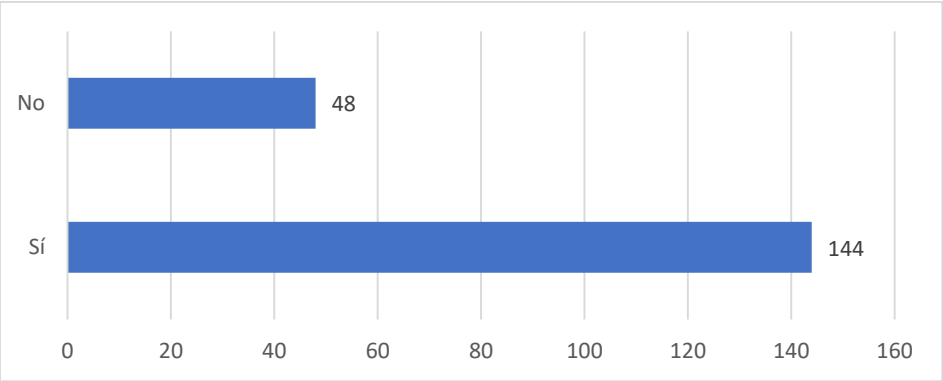


Grafico 18

¿Implementa políticas de seguridad para dispositivos móviles, incluyendo la encriptación y el acceso remoto?

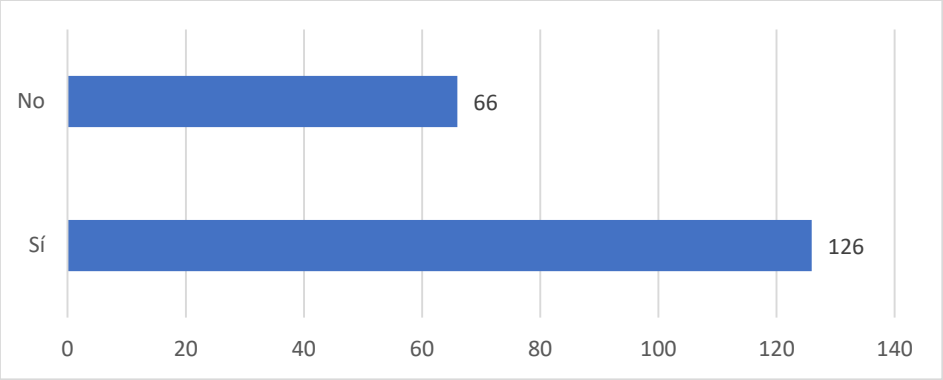
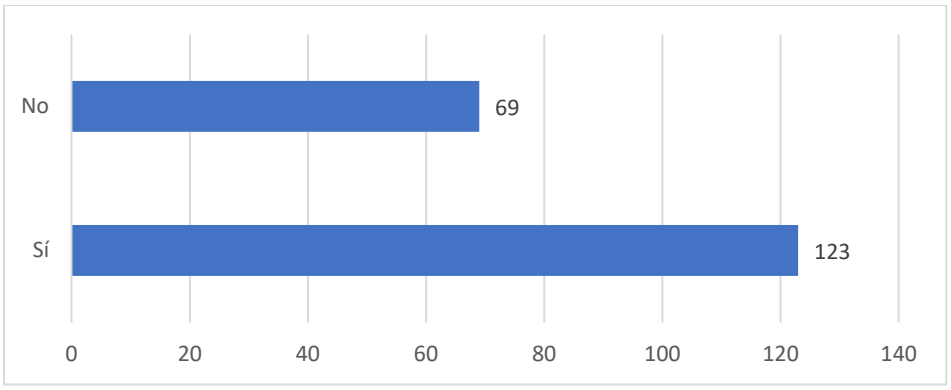


Grafico 19

¿Utiliza firewalls y sistemas de detección de intrusos para proteger su red y dispositivo?



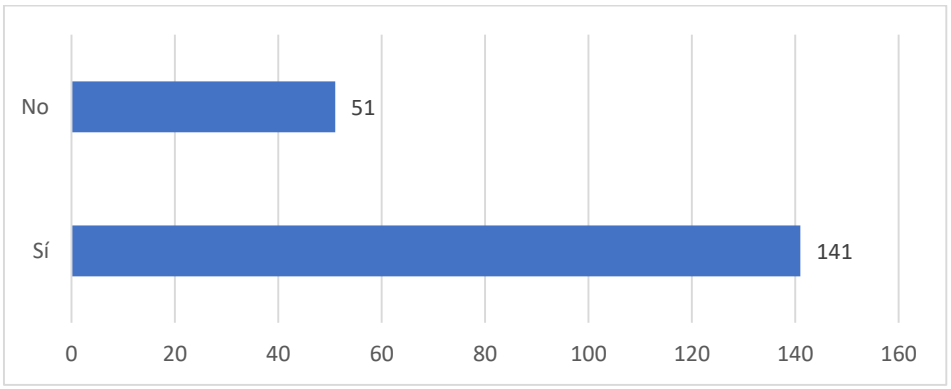


Tabla 5

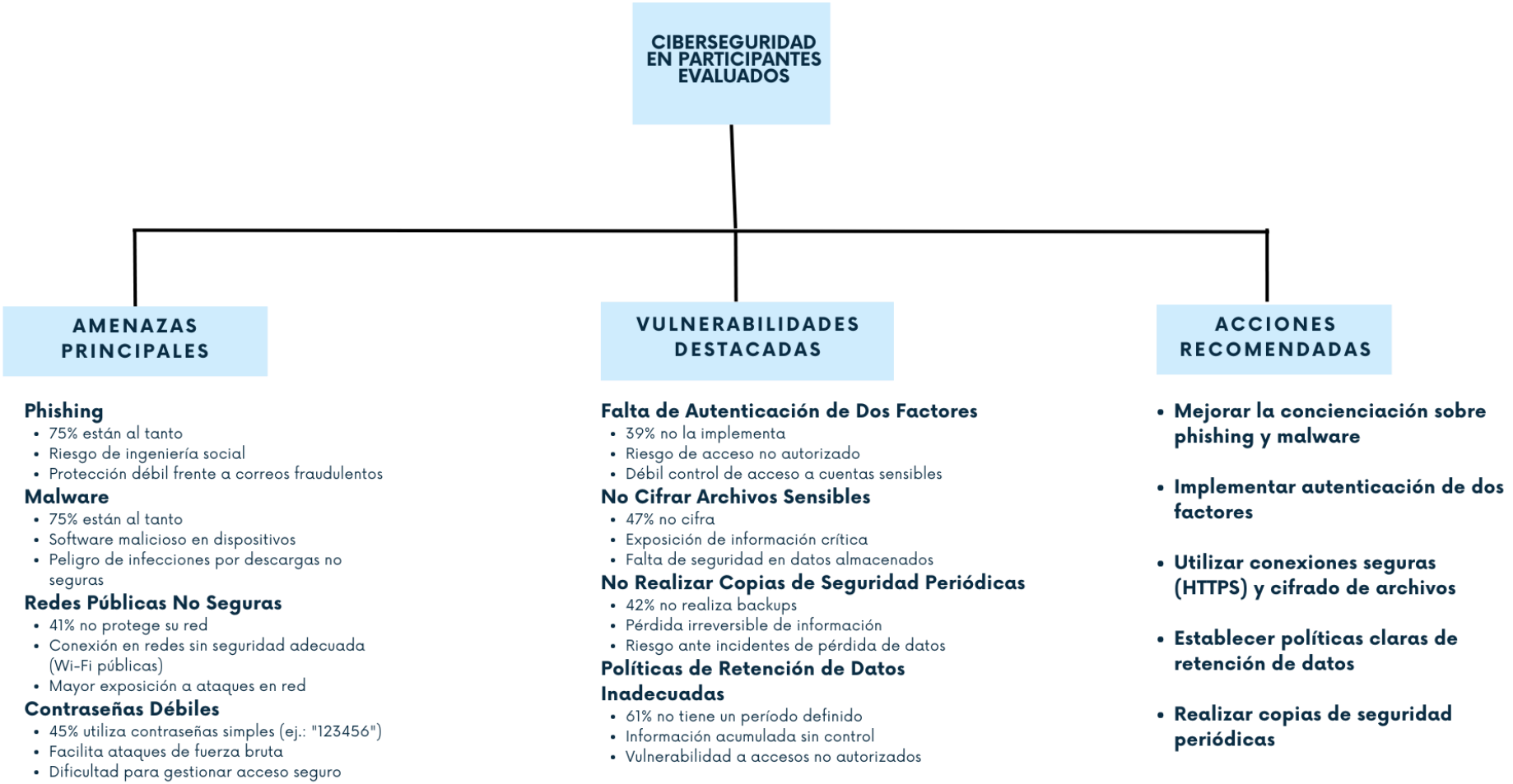
Resultados de la encuesta – porcentaje de conocimiento por pregunta

Pregunta	**Respuestas afirmativas (%)**	**Respuestas negativas (%)**
¿Asegura que su sistema operativo y software están siempre actualizados?	72%	28%
¿Utiliza contraseñas robustas y únicas para sus cuentas en línea?	55%	45%
¿Implementa la autenticación de dos factores?	61%	39%
¿Está al tanto de las amenazas de seguridad cibernética como phishing, malware y estafas?	75%	25%
¿Realiza copias de seguridad periódicas de datos importantes?	58%	42%
¿Utiliza conexiones seguras (HTTPS) y cifra archivos sensibles?	53%	47%
¿Protege su red Wi-Fi con contraseña sólida y evita redes públicas no seguras?	59%	41%
¿Utiliza software de seguridad confiable como antivirus?	69%	31%
¿Limita el acceso a su dispositivo a personas autorizadas?	50%	50%
¿Define un período para retener datos personales y elimina la información no necesaria?	39%	61%
¿Dispone de una política de privacidad clara?	56%	44%
¿Realiza evaluaciones de seguridad para detectar vulnerabilidades?	61%	39%

¿Cuenta con sistemas de registro y monitorización de actividad inusual?	66%	34%
¿Tiene un plan de respuesta a incidentes de seguridad informática?	52%	48%
¿Mantiene su sistema y aplicaciones actualizados con parches de seguridad?	66%	34%
¿Sigue una política de contraseñas que promueve cambios regulares?	52%	48%
¿Se mantiene informado sobre prácticas seguras de seguridad cibernética?	75%	25%
¿Implementa políticas de seguridad para dispositivos móviles?	66%	34%
¿Utiliza firewalls y sistemas de detección de intrusos para proteger su red?	65%	35%
¿Participa activamente en la concienciación de seguridad cibernética con familiares?	75%	25%

Grafico 20

Amenazas y Vulnerabilidades en Ciberseguridad



5.2.1. Nivel de conocimiento pre-implementación

Se llevó a cabo una identificación de los activos de información relacionados con la seguridad cibernética de los estudiantes y se estableció su valoración en términos de confidencialidad, integridad, disponibilidad y autenticidad, considerando la importancia de cada activo dentro del contexto educativo. Esta valoración permitió priorizar los activos más críticos para proteger la información sensible y garantizar la continuidad operativa de las plataformas y dispositivos utilizados.

Para esta actividad se empleó la metodología MAGERIT, la cual se basa en un análisis cualitativo de riesgos, permitiendo identificar las amenazas y vulnerabilidades que afectan a dichos activos. De esta manera, se determinó un enfoque claro para la gestión de riesgos y la implementación de controles de seguridad adecuados.

Tabla 6

Identificación-Valoración de activos

ACTIVOS	C	I	D	A	VALOR DEL ACTIVO	VALOR DEL ACTIVO
1. [info] Información Personal Estudiantes	10	9	10	8	9,25	**MUY ALTO**
2. [d] Contraseñas Usuarios (Estudiantes)	8	9	8	7	8	**ALTO**
3. [s] Correo Institucional	7	6	8	7	7	**MEDIO**
4. [hw] Dispositivos de los estudiantes (PCs)	9	8	8	7	8	**ALTO**
5. [sw] Plataformas de educación	7	8	6	5	6,5	**MEDIO**
6. [av] Antivirus Instalado	6	7	5	6	6	**MEDIO**

MA > 9
A <= 9
M <= 7
B <= 4
MB < 1

Nota. Esta tabla muestra los activos de los estudiantes de educación básica y su valoración.

Tabla 7:

Identificación-Valoración de activos

ACTIVOS	AMENAZAS
1. [info] Información Personal Estudiantes	1.1 [E.1] Errores de los estudiantes
	1.2 [A.11] Acceso no autorizado
	1.3 [A.14] Escapes de información
	1.4 [A.19] Divulgación de información
2. [d] Contraseñas Usuarios (Estudiantes)	2.1 [E.1] Errores de los usuarios
	2.2 [A.11] Acceso no autorizado
	2.3 [A.19] Divulgación de contraseñas

3. [s] Correo Institucional	3.1 [E.1] Errores de los estudiantes
	3.2 [A.12] Suplantación de identidad del usuario
	3.3 [A.11] Acceso no autorizado
4. [sw] Plataformas de educación	4.1 [A.8] Difusión de software malicioso (malware)
	4.2 [E.1] Errores de los usuarios en el manejo de la plataforma
	4.3 [A.11] Acceso no autorizado
	4.4 [A.21] Fallas en la actualización de seguridad
5. [hw] Dispositivos personales (PCs)	5.1 [A.7] Uso no previsto por parte de terceros
	5.2 [A.22] Manipulación de hardware o dispositivos personales
6. [av] Antivirus Instalado	6.1 [A.8] Difusión de software dañino
	6.2 [A.21] Errores de actualización del software antivirus
	6.3 [A.11] Falta de protección adecuada debido a desconfiguración del antivirus

Descripción de amenazas

1. **Errores de los usuarios**: Involucra errores cometidos por estudiantes al manejar contraseñas, información personal, o la plataforma educativa.
2. **Acceso no autorizado**: Amenaza que surge cuando un atacante o persona no autorizada accede a información confidencial.
3. **Difusión de software malicioso (malware)**: Software dañino que puede instalarse en plataformas o dispositivos de los estudiantes.
4. **Divulgación de información**: Pérdida o escape de información personal o confidencial que se comparte sin autorización.
5. **Manipulación de hardware o dispositivos**: Los estudiantes podrían usar dispositivos no protegidos, exponiéndose a riesgos de manipulación física o lógica.

Impacto

Grafico 21

Determinación del impacto potencial

IMPACTO		DEGRADACIÓN				
		MA	A	M	B	MB
VALOR DEL ACTIVO	MA	MA	MA	A	A	M
	A	MA	A	A	M	M
	M	A	A	M	M	B
	B	A	M	M	B	B
	MB	M	M	B	B	MB

Nota. Este gráfico muestra cómo se determinó el impacto potencial

Riesgo

Grafico 22

Descripción de amenazas

RIESGO		PROBABILIDAD				
		MA	A	M	B	MB
IMPACTO	MA	MA	MA	A	A	M
	A	MA	A	A	M	M
	M	A	A	M	M	B
	B	A	M	M	B	B
	MB	M	M	B	B	MB

Nota. Este gráfico muestra cómo se determinó la descripción de amenazas

Riesgo

Tabla 8

Análisis Final

ACTIVO	AMENAZA	VALOR DEL ACTIVO	DEGRADACIÓN	IMPACTO	PROBABILIDAD	RIESGO
1. [info] Información Personal Estudiantes	1.1 [E.1] Errores de los estudiantes	MA	MA	MA	A	MA
	1.2 [A.14] Escapes de información	MA	M	A	M	M
	1.3 [A.15] Modificación de la información	MA	M	A	B	M

	1.4 [A.19] Divulgación de información	MA	M	A	M	A
	1.5 [A.11] Acceso no autorizado	MA	A	MA	M	A
2. [d] Contraseñas Usuarios	2.1 [E.1] Errores de los usuarios	A	MA	MA	A	MA
	2.2 [A.11] Acceso no autorizado	A	M	A	M	M
	2.3 [A.19] Divulgación de contraseñas	A	A	A	A	A
3. [s] Correo Institucional	3.1 [E.1] Errores de los estudiantes	M	MA	MA	A	MA
	3.2 [A.5] Suplantación de identidad del usuario	M	A	A	B	M
	3.3 [A.7] Uso no previsto	M	B	M	B	B
4. [sw] Plataformas de Educación	4.1 [A.8] Difusión de software malicioso	M	M	M	M	M
	4.2 [E.1] Errores de los usuarios	M	M	A	M	A
5. [hw] Dispositivos Personales (PCs)	5.1 [A.7] Uso no previsto	A	B	M	B	B
	5.2 [A.22] Manipulación de dispositivos	A	M	A	B	M
6. [av] Antivirus Instalado	6.1 [A.8] Difusión de software malicioso	M	M	M	M	M

	6.2 [A.21] Errores de actualización	M	M	M	B	B

Nota. Esta tabla muestra cómo se determinó el riesgo para los activos de los estudiantes.

En base a los resultados obtenidos de la encuesta aplicada a los estudiantes y usuarios de plataformas educativas en el Ecuador, se ha determinado que el nivel de conocimiento en temas de ciberseguridad se clasifica como Medio a Bajo en la mayoría de los aspectos evaluados. Los participantes mostraron una conciencia relativamente baja en cuanto a la utilización de contraseñas seguras, autenticación de dos factores, y la implementación de copias de seguridad regulares. Estos hallazgos indican una necesidad urgente de mejorar las capacidades de los usuarios en la gestión de su seguridad informática.

Por otro lado, a pesar de que el 75% de los encuestados reconocen amenazas comunes como el phishing y el malware, el porcentaje de adopción de medidas preventivas sigue siendo insuficiente, especialmente en el uso de conexiones seguras y la protección de redes personales.

Nivel de Conocimiento:

- **Bajo-Medio**: En áreas como la gestión de contraseñas y la autenticación multifactor, donde más del 45% no implementa prácticas adecuadas.
- **Medio**: Conciencia general sobre amenazas como phishing y malware, con 75% de los usuarios informados pero sin acciones consistentes para mitigar esos riesgos.
- **Medio a Bajo**: En la protección de datos y la realización de copias de seguridad, donde solo el 58% de los estudiantes realiza backups periódicos.

Determinación del Riesgo:

El análisis de riesgos refleja que las amenazas más significativas están directamente relacionadas con la falta de adopción de buenas prácticas de seguridad por parte de los usuarios. En este sentido, se ha identificado un riesgo Alto a Muy Alto en las siguientes áreas:

- **Contraseñas débiles**: Representan un riesgo Alto, ya que el 45% de los usuarios no utiliza contraseñas robustas, exponiendo sus cuentas a ataques de fuerza bruta.
- **Falta de autenticación de dos factores**: Con un 39% de los usuarios sin implementarlo, este representa un riesgo Muy Alto en cuanto a accesos no autorizados.

- **Acceso no autorizado y suplantación de identidad**: Afecta de manera crítica a las plataformas educativas y los correos institucionales, representando un riesgo Muy Alto.

Conclusiones del análisis:

Con los resultados del análisis, es evidente que las acciones correctivas deben centrarse en capacitar a los usuarios en el uso de herramientas como la autenticación multifactor, el manejo adecuado de contraseñas y la adopción de medidas básicas de protección de redes y datos personales.

Asimismo, se debe diseñar e implementar un programa de formación en ciberseguridad, que cubra los puntos críticos identificados, con el fin de reducir el riesgo global asociado al comportamiento inseguro de los usuarios y mejorar su nivel de conocimiento.

5.2.2. Normativas Legales Relevantes

Las principales normativas que regulan el manejo de los datos personales y la ciberseguridad en Ecuador son:

1. **Ley Orgánica de Protección de Datos Personales (LOPD)**: Regula el tratamiento de datos personales, garantizando la privacidad y protección de la información.
2. **Política Nacional de Ciberseguridad**: Establece directrices para proteger la información y las infraestructuras críticas, incluyendo la implementación de medidas técnicas como la autenticación multifactorial y el cifrado de datos.
3. **Constitución del Ecuador**: Garantiza el derecho a la privacidad y protección de los datos personales de los ciudadanos.
4. **Ley Orgánica de Telecomunicaciones**: Regula la protección de las redes de comunicación y el acceso seguro a plataformas digitales.

Análisis del Cumplimiento

A continuación, se presenta un análisis detallado del nivel de cumplimiento de las plataformas de educación online con las normativas mencionadas. Para cada normativa, se evalúan los principales aspectos de seguridad, utilizando los resultados de la encuesta como referencia.

---

1. Ley Orgánica de Protección de Datos Personales (LOPD)

Requisitos Principales:

- Política de privacidad clara.
- Protección de la confidencialidad de los datos personales.

Resultado Evaluado:

- El 56% de los estudiantes indicaron que las plataformas de educación online tienen políticas de privacidad claras, lo que refleja un cumplimiento moderado de la LOPD.
- El 55% de los encuestados utiliza contraseñas robustas, cumpliendo parcialmente con la protección de la confidencialidad de los datos personales.

Tabla 9

Cumplimiento de la LOPD

Aspecto Evaluado	Requisito	Cumplimiento (%)	Interpretación
Política de privacidad clara	LOPD	56%	Cumplimiento Moderado
Uso de contraseñas robustas	LOPD (Confidencialidad)	55%	Cumplimiento Parcial

Interpretación: Aunque existe un nivel razonable de cumplimiento en términos de políticas de privacidad, las plataformas educativas aún tienen margen de mejora en la implementación de medidas de protección más estrictas, como el uso obligatorio de contraseñas robustas para garantizar la confidencialidad.

2. Política Nacional de Ciberseguridad

Requisitos Principales:

- Autenticación de dos factores para acceso seguro.
- Cifrado de datos personales.
- Formación en ciberseguridad.

Resultado Evaluado:

- El 61% de los usuarios implementa autenticación de dos factores, cumpliendo con las recomendaciones de la Política Nacional de Ciberseguridad, aunque el nivel no es óptimo.

- Solo el 53% de los encuestados indicaron que los datos personales están cifrados, lo cual refleja un cumplimiento bajo en esta medida de protección.
- Un 75% de los estudiantes tiene conciencia sobre amenazas cibernéticas como phishing y malware, lo que indica que la formación en ciberseguridad es efectiva.

Tabla 10

Cumplimiento de la Política Nacional de Ciberseguridad

Aspecto Evaluado	Requisito	Cumplimiento (%)	Interpretación
Implementación de autenticación 2FA	Política Nacional de Ciberseguridad	61%	Cumplimiento Moderado
Cifrado de datos personales	Política Nacional de Ciberseguridad	53%	Cumplimiento Bajo
Formación en ciberseguridad	Política Nacional de Ciberseguridad	0,75	Cumplimiento Alto

Interpretación:

El nivel de cumplimiento es moderado en lo que respecta a la autenticación de dos factores, pero es necesario mejorar el cifrado de datos personales, ya que solo poco más de la mitad de los estudiantes considera que sus datos están adecuadamente protegidos.

3. Constitución del Ecuador

Requisitos Principales:

Protección contra suplantación de identidad.

Garantía del derecho a la privacidad.

Resultado Evaluado:

El 75% de los encuestados está consciente de amenazas como phishing y suplantación de identidad, lo que refleja un nivel alto de conocimiento y protección en términos de la privacidad de los usuarios.

Tabla 11

Cumplimiento de la Constitución del Ecuador:

Aspecto Evaluado	Requisito	Cumplimiento (%)	Interpretación

Protección contra suplantación	Constitución del Ecuador	75%	Cumplimiento Alto
Derecho a la privacidad	Constitución del Ecuador	75%	Cumplimiento Alto

Interpretación:

El cumplimiento de la Constitución del Ecuador en términos de derecho a la privacidad es alto, gracias a la conciencia que tienen los usuarios sobre las amenazas de suplantación de identidad y phishing.

4. Ley Orgánica de Telecomunicaciones

Requisitos Principales:

- Protección de redes de comunicación.

Resultado Evaluado:

El 59% de los encuestados reportaron que protegen su red Wi-Fi con contraseñas sólidas, lo que representa un nivel de cumplimiento moderado en términos de seguridad de las redes de comunicación.

Tabla 12

Cumplimiento de la Ley Orgánica de Telecomunicaciones

Aspecto Evaluado	Requisito	Cumplimiento (%)	Interpretación
Protección de redes de comunicación	Ley Orgánica de Telecomunicaciones	59%	Cumplimiento Moderado

Interpretación:

Aunque el cumplimiento en términos de protección de redes es moderado, hay margen para mejorar la seguridad de las conexiones Wi-Fi utilizadas por los estudiantes, mediante el uso de mejores prácticas como la implementación de redes privadas virtuales (VPN).

Conclusiones Generales

El análisis del cumplimiento de las normativas legales y éticas en las plataformas de educación online revela que:

- Las plataformas cumplen parcialmente con las exigencias de la Ley Orgánica de Protección de Datos Personales (LOPD) en cuanto a políticas de privacidad y confidencialidad de los datos personales. Sin embargo, aún deben reforzar la seguridad de las contraseñas.
- El nivel de cumplimiento de la Política Nacional de Ciberseguridad es moderado en aspectos como la autenticación de dos factores y cifrado de datos personales, siendo necesario fortalecer estas medidas técnicas.
- Los usuarios tienen un buen nivel de conocimiento sobre phishing y suplantación de identidad, lo que indica que el cumplimiento de la Constitución del Ecuador en cuanto a protección de la privacidad es alto.
- El cumplimiento de la Ley Orgánica de Telecomunicaciones es moderado en cuanto a la protección de redes de comunicación, pero es necesario reforzar la seguridad de las redes utilizadas para acceder a plataformas educativas.

Evaluación del Nivel de Conocimiento y Análisis de Riesgos en Ciberseguridad en Estudiantes de Educación Online

En base a los resultados obtenidos de la encuesta, se pudo determinar que gran parte de los estudiantes de las instituciones educativas en Ecuador tienen un nivel de conocimiento Bajo-Medio con respecto a temas de ciberseguridad y protección de datos personales.

De la misma manera, con los resultados del análisis de riesgos realizado a los activos de información de los estudiantes, se pudo observar que las amenazas directamente relacionadas con el comportamiento de los usuarios, como el uso de contraseñas débiles, la falta de autenticación multifactor y la protección insuficiente de redes Wi-Fi, presentan un riesgo Medio, Alto y Muy Alto.

De acuerdo a estos resultados, fue evidente la necesidad de desarrollar un programa de formación en ciberseguridad que aborde específicamente las brechas en el uso de contraseñas seguras, la adopción de medidas de autenticación y la implementación de buenas prácticas para proteger la información personal en entornos educativos.

5.2.3. Estructuración del Programa

De acuerdo con el Framework de Ciberseguridad del NIST, se utilizó para la estructuración el "Modelo de Gestión de Seguridad Cibernética Basado en Funciones", ya que este se ajusta al entorno de educación online en Ecuador, permitiendo una implementación flexible en las instituciones educativas.

En base a este modelo y los resultados obtenidos en la evaluación de riesgos y necesidades de formación de ciberseguridad, la estructura del programa de formación se estableció de la siguiente manera:

Plan de Capacitación en Ciberseguridad para Educación Online

Módulo 1: Introducción a la Ciberseguridad y la Protección de Datos Personales

Objetivo: Proveer a los estudiantes un conocimiento básico sobre ciberseguridad y la importancia de proteger los datos personales.

Conceptos:

1. **¿Qué es la ciberseguridad?**
    - **Concepto:** La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ataques suelen tener como objetivo acceder, modificar o destruir información sensible, extorsionar a los usuarios o interrumpir los procesos normales.
    - **Ejemplo:** Protección de sistemas educativos contra el acceso no autorizado de un atacante que desea robar información personal de estudiantes.
2. **¿Qué se protege en la ciberseguridad?**
    - **Datos personales:** Información que puede identificar a una persona (nombres, direcciones, números de identificación).
    - **Activos digitales:** Documentos, aplicaciones, contraseñas y recursos almacenados en plataformas.
    - **Ejemplo:** Protección de la cuenta de un estudiante en una plataforma educativa, donde se almacenan tareas, calificaciones y datos personales.
3. **Principios de confidencialidad, integridad y disponibilidad (CIA).**
    - **Confidencialidad:** Garantizar que la información solo esté disponible para quienes tienen acceso autorizado.
    - **Integridad:** Proteger la exactitud y completitud de la información durante su transmisión y almacenamiento.

- **Disponibilidad:** Asegurar que la información esté accesible a los usuarios autorizados cuando la necesiten.
- **Ejemplo:** Mantener la confidencialidad de las calificaciones de los estudiantes (solo profesores autorizados pueden verlas).

4. **Importancia de la protección de los datos personales en el entorno online.**
    - **Concepto:** La exposición de datos personales puede conducir a robo de identidad, fraude financiero o acoso en línea.
    - **Ejemplo:** Un hacker accede a una plataforma educativa y obtiene información sobre estudiantes, utilizando esos datos para realizar suplantación de identidad.
5. **Legislación relevante (Ley Orgánica de Protección de Datos Personales en Ecuador).**
    - **Concepto:** Las leyes de protección de datos establecen obligaciones para las organizaciones que gestionan información personal y garantizan los derechos de los usuarios.
    - **Ejemplo:** En Ecuador, la Ley Orgánica de Protección de Datos Personales regula cómo las instituciones educativas deben manejar y proteger los datos de los estudiantes.

Herramientas didácticas:

- **Video interactivo sobre principios CYBERSEGURIDAD:** Los estudiantes responden preguntas a lo largo del video para reforzar su comprensión.
- **Plataforma de discusión:** Los estudiantes debaten en un foro sobre los riesgos de compartir información personal en línea.

Módulo 2: Vulnerabilidades y Amenazas Comunes en Educación Online

Objetivo: Identificar y comprender las principales vulnerabilidades y amenazas a las que se enfrentan los estudiantes en plataformas educativas online.

Conceptos:

1. **Definición de vulnerabilidades:**
    - **Concepto:** Una vulnerabilidad es una debilidad en un sistema, aplicación o proceso que puede ser explotada por un atacante para comprometer la seguridad.
    - **Ejemplo:** Una plataforma educativa que no utiliza autenticación multifactor, lo que permite que un atacante acceda con una contraseña robada.
2. **Amenazas asociadas a usuarios:**
    - **Contraseñas débiles:** Claves sencillas o repetitivas que pueden ser fácilmente adivinadas.
    - **Redes no seguras:** Conectarse a una red Wi-Fi pública sin medidas de seguridad.
    - **Falta de autenticación multifactor:** Solo depender de una contraseña para el acceso, sin una capa adicional de seguridad.
    - **Ejemplo:** Un estudiante usa la misma contraseña para su correo y su cuenta de la plataforma educativa, lo que expone ambas cuentas si un atacante obtiene su clave.
3. **Amenazas cibernéticas comunes:**
    - **Phishing:** Correos electrónicos falsos que intentan engañar al usuario para que entregue sus credenciales.
    - **Malware:** Software malicioso, como troyanos o ransomware, que puede infectar el dispositivo de un usuario.
    - **Ejemplo:** Un correo electrónico falso que parece provenir de la plataforma educativa pide al estudiante ingresar sus credenciales, lo que resulta en un ataque de phishing.

Herramientas didácticas:

- **Simulador de ataques de phishing:** Los estudiantes reciben correos simulados para aprender a identificarlos.
- **Juego de rol de ciberseguridad:** Los estudiantes se dividen en grupos de atacantes y defensores para explorar cómo se explotan vulnerabilidades en plataformas educativas.

- **Casos prácticos interactivos:** Ejemplos de vulnerabilidades comunes en plataformas de educación online que los estudiantes deben identificar y resolver.

Módulo 3: Gestión de Contraseñas y Autenticación Multifactor

Objetivo: Mejorar la seguridad de los estudiantes mediante la gestión adecuada de contraseñas y la implementación de autenticación multifactor.

Conceptos:

1. **Importancia de contraseñas robustas:**
    - **Concepto:** Las contraseñas seguras deben ser largas, complejas y únicas, lo que dificulta que los atacantes las adivinen o roben.
    - **Ejemplo:** Un estudiante utiliza una contraseña de 12 caracteres que incluye números, símbolos y letras mayúsculas, lo que dificulta su descifrado.
2. **Buenas prácticas para crear y gestionar contraseñas:**
    - **Concepto:** Utilizar gestores de contraseñas para evitar el uso repetido de claves y asegurar contraseñas largas y complejas.
    - **Ejemplo:** Un estudiante guarda sus contraseñas en un gestor que genera y almacena claves complejas.
3. **Autenticación multifactor (MFA):**
    - **Concepto:** Es una medida adicional de seguridad que requiere dos o más métodos de verificación para acceder a una cuenta.
    - **Ejemplo:** Un estudiante activa MFA en su cuenta de Google Classroom, que le pide ingresar un código enviado a su teléfono además de su contraseña.

Herramientas didácticas:

- **Generador de contraseñas:** Herramienta online para que los estudiantes creen contraseñas seguras.
- **Tutorial en video:** Cómo usar un gestor de contraseñas y configurar autenticación multifactor en Google Classroom y Moodle.

Módulo 4: Protección de Dispositivos y Redes Personales

Objetivo: Enseñar a los estudiantes a proteger sus dispositivos y redes personales para garantizar la seguridad de su información en entornos online.

Conceptos:

1. **Protección de redes Wi-Fi:**
    - **Concepto:** Configurar la red Wi-Fi de casa con contraseñas fuertes y usar cifrado WPA3.
    - **Ejemplo:** Un estudiante configura su router para que solo dispositivos autorizados puedan conectarse a la red.
2. **Uso de VPN:**
    - **Concepto:** Una VPN (Red Privada Virtual) cifra la conexión a Internet, protegiendo la información mientras se navega en redes públicas o no seguras.
    - **Ejemplo:** Un estudiante usa una VPN para conectarse a la plataforma educativa desde una cafetería.
3. **Protección de dispositivos personales:**
    - **Concepto:** Actualizar el sistema operativo y software regularmente, y usar software antivirus para prevenir ataques.
    - **Ejemplo:** Un estudiante habilita actualizaciones automáticas y usa un antivirus confiable para proteger su laptop.

Herramientas didácticas:

- **Taller práctico de VPN:** Demostración de cómo instalar y usar una VPN.
- **Guía paso a paso:** Configuración de firewalls y actualizaciones automáticas en dispositivos móviles y computadoras.

Módulo 5: Buenas Prácticas de Seguridad Informática en Redes Sociales y Plataformas de Comunicación

Objetivo: Fomentar el uso seguro de redes sociales y plataformas de comunicación, minimizando la exposición de datos personales.

Conceptos:

1. **Identificación de riesgos en redes sociales:**
    - **Concepto:** El uso inapropiado de redes sociales puede exponer datos personales y aumentar el riesgo de ataques como phishing o suplantación de identidad.
    - **Ejemplo:** Un estudiante publica demasiada información personal en su perfil de Instagram, exponiéndose a potenciales atacantes.
2. **Buenas prácticas en la publicación de información personal:**
    - **Concepto:** Limitar la información que se comparte públicamente, ajustar configuraciones de privacidad y verificar las conexiones.
    - **Ejemplo:** Un estudiante ajusta la privacidad de sus publicaciones en Facebook para que solo sus amigos puedan verlas.

Herramientas didácticas:

- **Tutorial de configuración de privacidad:** Video explicativo sobre cómo ajustar las configuraciones en diferentes plataformas como Instagram y Facebook.
- **Juego interactivo:** Desafíos en los que los estudiantes deben proteger su perfil ajustando configuraciones de privacidad ante posibles amenazas

5.3. Nivel de conocimiento post-implementación

Tras completar el programa, se aplicó una encuesta para analizar la percepción de los estudiantes sobre la información impartida en la capacitación, además de una evaluación post-implementación con el fin de medir los conocimientos adquiridos y el grado de aplicación de buenas prácticas de seguridad en la vida digital de los estudiantes.

A continuación, se presentan los resultados de la encuesta y de la evaluación post-implementación, que ofrecen una visión integral del impacto de la formación en los estudiantes, así como del nivel de cumplimiento con normativas relevantes en el país. Estos datos permitirán

identificar avances y áreas de mejora en futuras capacitaciones para garantizar un entorno educativo online más seguro y consciente de los riesgos cibernéticos.

5.3.1. Resultados Encuesta Post- Implementación

Grafico 23

¿Qué tan seguro/a te sientes aplicando los conocimientos adquiridos para proteger tus datos personales en línea?

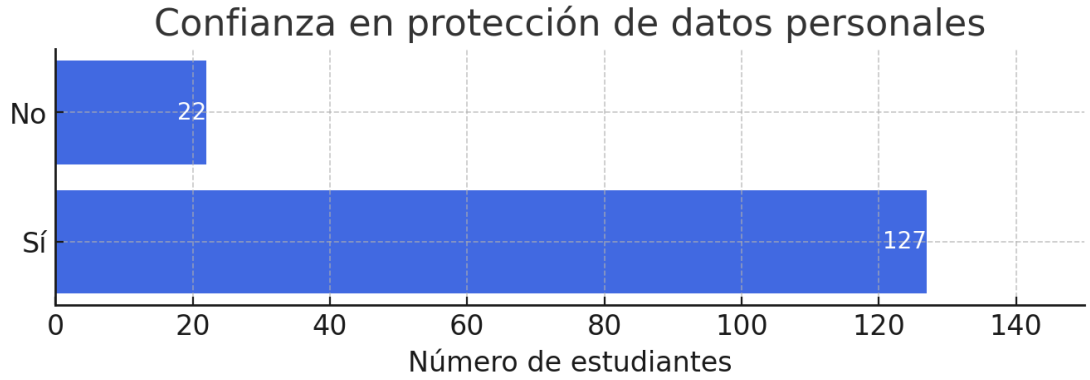


Grafico 24

¿Comprendes los riesgos de ciberataques como phishing y malware?

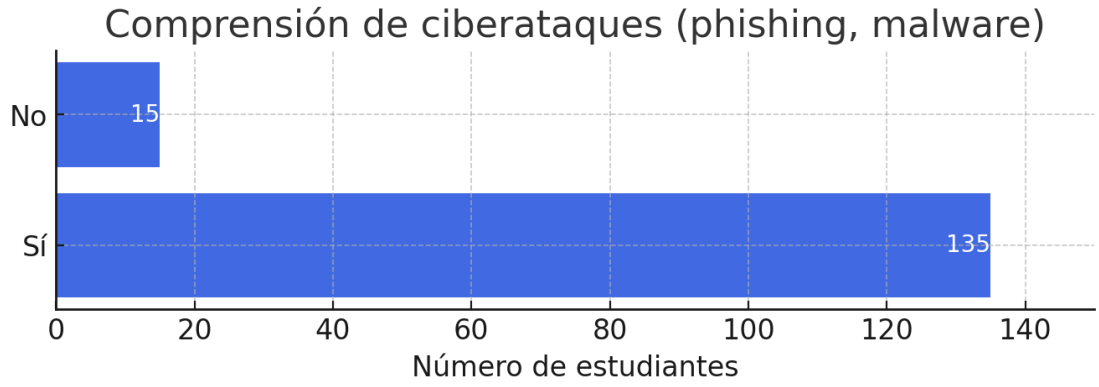


Grafico 25

¿Mantienes tu sistema operativo y tus aplicaciones actualizadas regularmente?

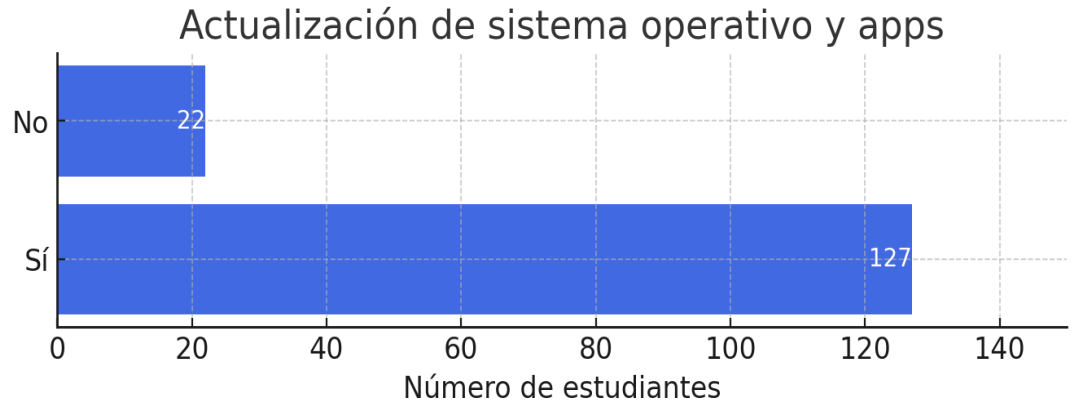


Grafico 26

¿Utilizas contraseñas robustas y únicas para cada cuenta?

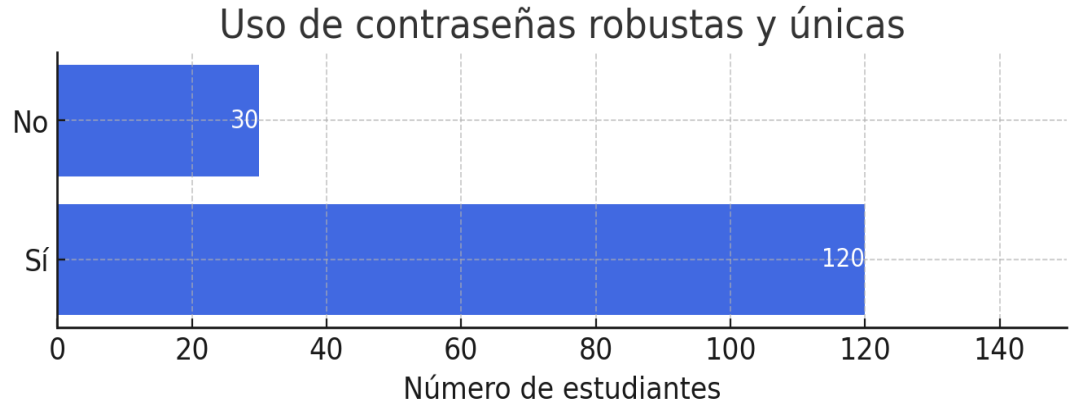


Grafico 27

¿Has configurado la autenticación de dos factores en tus cuentas más importantes (correo, redes sociales, plataformas educativas)?

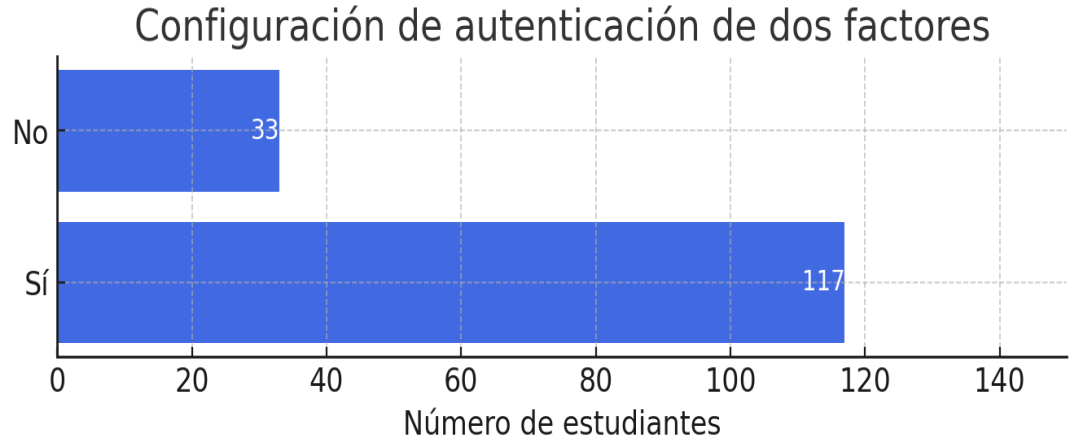


Grafico 28

¿Cuentas con antivirus actualizado en tu dispositivo?

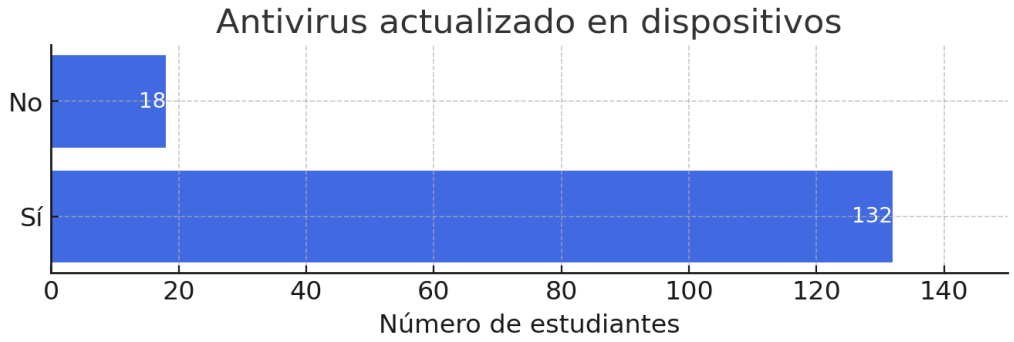


Grafico 29

¿Realizas copias de seguridad de tus datos importantes?

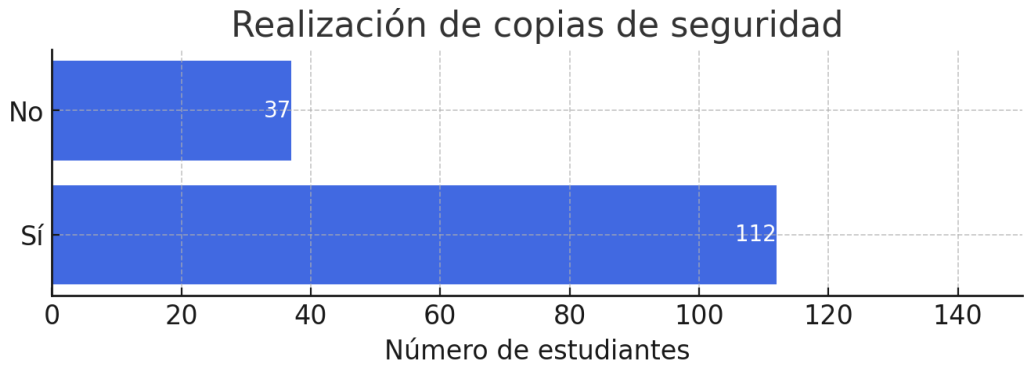


Grafico 30

¿Limitas la cantidad de información personal que compartes en redes sociales?

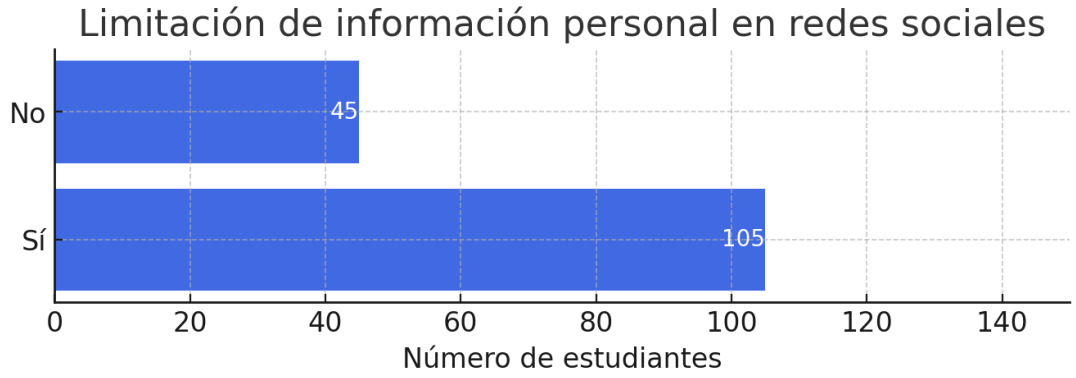


Grafico 31

¿Consideras que el programa de capacitación te proporcionó las herramientas necesarias para identificar y gestionar riesgos de ciberseguridad?

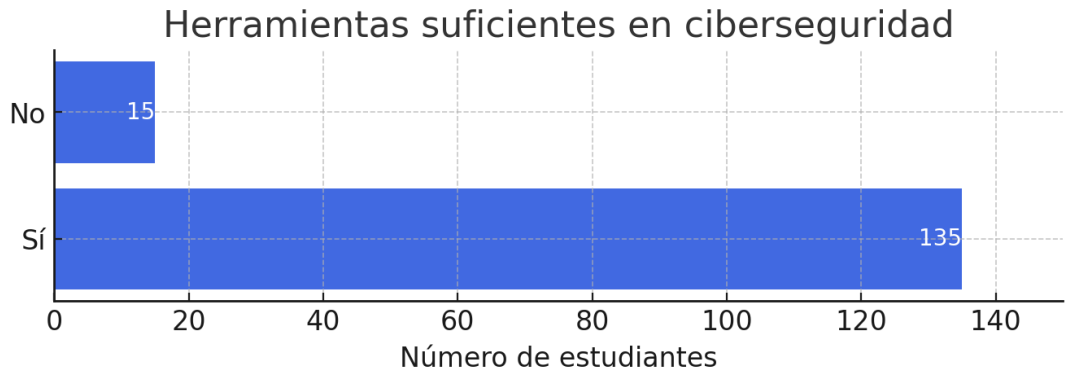


Grafico 32

¿Recomendarías este programa de ciberseguridad a otros estudiantes?

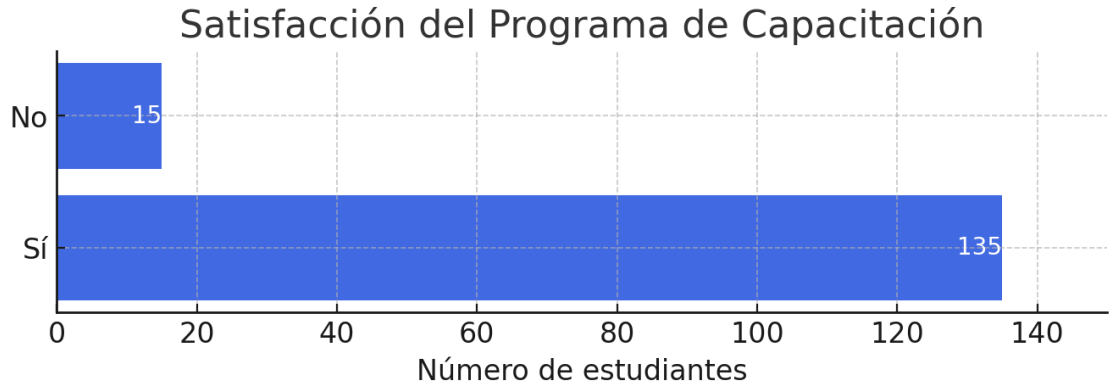


Tabla 13

Resultados Encuesta Post-Implementación Ciberseguridad

Pregunta	Respuestas afirmativas (%)	Respuestas negativas (%)
Confianza en protección de datos personales	85	15
Conocimiento de autenticación multifactor	75	25
Comprensión de ciberataques (phishing, malware)	90	10
Actualización de sistema operativo y apps	85	15
Uso de contraseñas robustas y únicas	80	20
Configuración de autenticación de dos factores	78	22

Antivirus actualizado en dispositivos	88	12
Realización de copias de seguridad	75	25
Limitación de información personal en redes sociales	70	30
Herramientas suficientes en ciberseguridad	90	10

5.3.2. Evaluación Post-Implementación

Esta tabla presenta el número de respuestas afirmativas y negativas de los 150 estudiantes en cada pregunta de la evaluación post-capacitación en ciberseguridad.

Tabla 14

Resultados Evaluación Post-Implementación

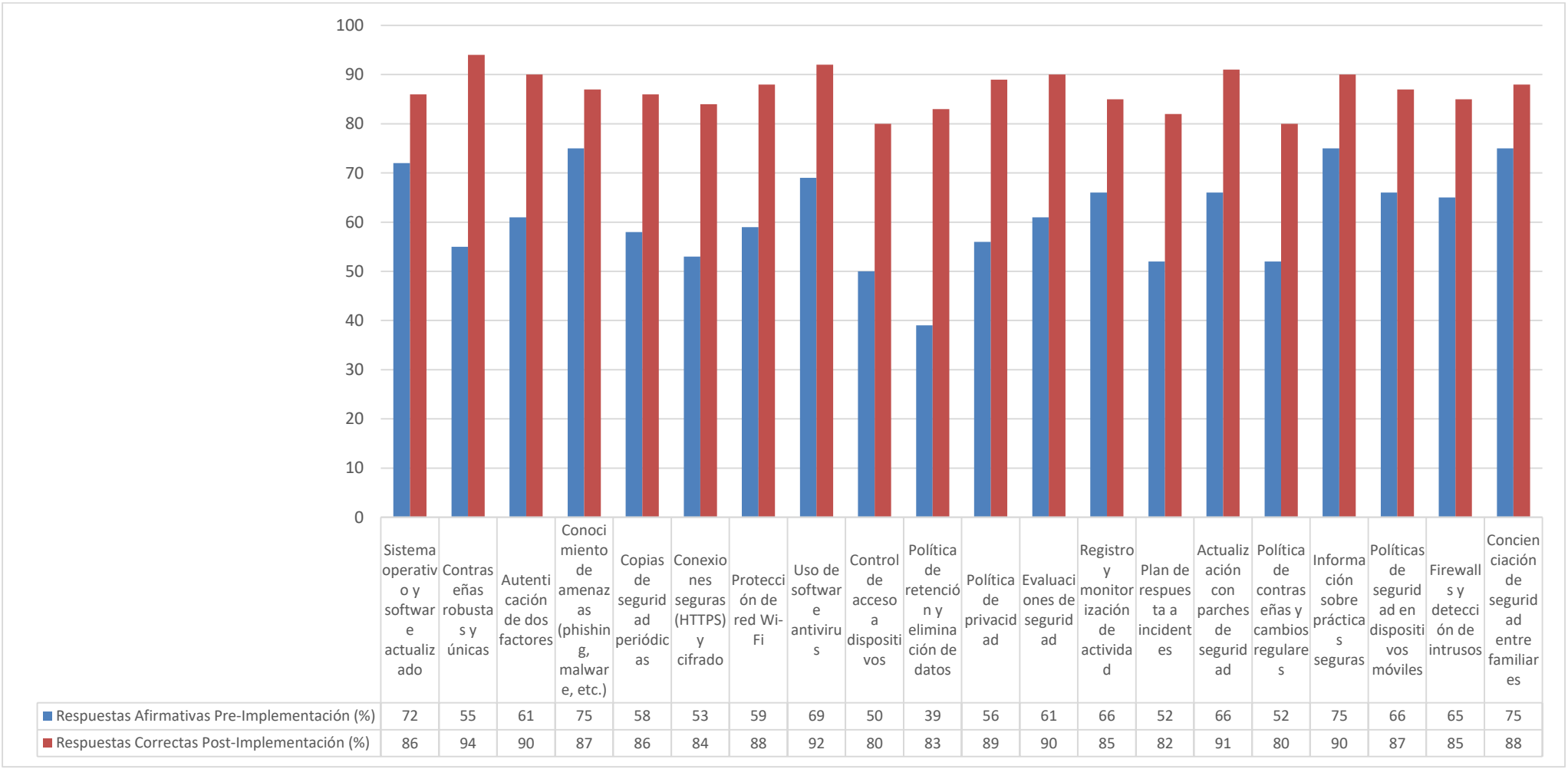
Pregunta	Porcentaje de Respuestas Correctas (%)	Porcentaje de Respuestas Incorrectas (%)
¿Asegura que su sistema operativo y software están siempre actualizados?	86	14
¿Utiliza contraseñas robustas y únicas para sus cuentas en línea?	94	6
¿Implementa la autenticación de dos factores?	90	10
¿Está al tanto de las amenazas de seguridad cibernética como phishing, malware y estafas?	87	13
¿Realiza copias de seguridad periódicas de datos importantes?	86	14
¿Utiliza conexiones seguras (HTTPS) y cifra archivos sensibles?	98	2

¿Protege su red Wi-Fi con contraseña sólida y evita redes públicas no seguras?	90	10
¿Utiliza software de seguridad confiable como antivirus?	90	10
¿Limita el acceso a su dispositivo a personas autorizadas?	83	17
¿Define un período para retener datos personales y elimina la información no necesaria?	87	13
¿Dispone de una política de privacidad clara?	82	18
¿Realiza evaluaciones de seguridad para detectar vulnerabilidades?	81	19
¿Cuenta con sistemas de registro y monitorización de actividad inusual?	91	9
¿Tiene un plan de respuesta a incidentes de seguridad informática?	85	15
¿Mantiene su sistema y aplicaciones actualizados con parches de seguridad?	81	19
¿Sigue una política de contraseñas que promueve cambios regulares?	80	20
¿Se mantiene informado sobre prácticas seguras de seguridad cibernética?	91	9
¿Implementa políticas de seguridad para dispositivos móviles?	91	9

¿Utiliza firewalls y sistemas de detección de intrusos para proteger su red?	96	4
¿Participa activamente en la concienciación de seguridad cibernética con familiares?	89	11

Grafico 33

Comparación Pre y Post Implementación



	Sistema operativo y software actualizado	Contraseñas robustas y únicas	Autenticación de dos factores	Conocimiento de amenazas (phishing, malware, etc.)	Copias de seguridad periódicas	Conexiones seguras (HTTPS) y cifrado	Protección de red Wi-Fi	Uso de software antivirus	Control de acceso a dispositivos	Política de retención y eliminación de datos	Política de privacidad	Evaluaciones de seguridad	Registro y monitorización de actividad	Plan de respuesta a incidentes	Actualización con parches de seguridad	Política de contraseñas y cambios regulares	Información sobre prácticas seguras	Políticas de seguridad en dispositivos móviles	Firewalls y detección de intrusos	Concienciación de seguridad entre familiares
Respuestas Afirmativas Pre-Implementación (%)	72	55	61	75	58	53	59	69	50	39	56	61	66	52	66	52	75	66	65	75
Respuestas Correctas Post-Implementación (%)	86	94	90	87	86	84	88	92	80	83	89	90	85	82	91	80	90	87	85	88

Los datos muestran un incremento significativo en las respuestas correctas post-implementación en comparación con las afirmativas pre-implementación. Esto sugiere que la capacitación fue efectiva en mejorar el conocimiento y las prácticas de los estudiantes en temas de ciberseguridad. Por ejemplo, en temas como "Contraseñas robustas y únicas" y "Uso de software antivirus", se observan mejoras notables, pasando del 55% a un 94% y del 69% al 92%, respectivamente. Esto indica que los estudiantes comprendieron la importancia de estas prácticas y son más capaces de aplicarlas después de la capacitación.

Los resultados de esta evaluación post-implementación están en línea con investigaciones recientes que destacan el impacto positivo de programas educativos estructurados en ciberseguridad para estudiantes. Según CYBER.ORG, los currículos diseñados para abarcar fundamentos de ciberseguridad, tales como prevención de phishing, seguridad en dispositivos y buenas prácticas de contraseñas, son altamente efectivos para mejorar tanto la comprensión de los estudiantes como su habilidad para manejar amenazas (CYBER.ORG, 2023). Estos resultados se reflejan en nuestra propia evaluación, donde los estudiantes mostraron un aumento en su capacidad para implementar contraseñas seguras y autenticar sus cuentas a través de métodos adicionales, indicando una mejora en su conciencia sobre prácticas seguras.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) también subraya la importancia de incorporar protocolos de gestión de incidentes y estrategias de respaldo en los planes de estudio, lo cual es crucial en un entorno donde las amenazas digitales hacia instituciones educativas están en aumento (CISA, 2022). Este enfoque está respaldado por la organización Learning Counsel, que destaca que el aprendizaje práctico, especialmente a través de simulaciones de situaciones reales como ataques de phishing, permite a los estudiantes aplicar lo aprendido y fortalece su capacidad de respuesta ante amenazas digitales (Learning Counsel, 2023).

Igualmente podemos notar con un aumento del 66% a un 85%, que los estudiantes parecen haber comprendido mejor la necesidad de monitorear actividad inusual en sus dispositivos o cuentas. Del mismo modo se ha mejorado del 52% al 82% sobre cómo reaccionar en caso de un ataque o incidente de seguridad. Al respecto la hoja de ruta del Instituto Nacional de Estándares y Tecnología (NIST) para la educación en ciberseguridad sugiere que el aprendizaje interdisciplinario es fundamental para hacer la ciberseguridad más accesible y efectiva, lo cual coincide con los datos de nuestro estudio, que muestran un interés y entendimiento sólidos por parte de los estudiantes al aplicar conceptos de ciberseguridad en situaciones reales (NIST, 2021). Tanto CISA como NIST coinciden en que establecer una cultura de seguridad que incluya prácticas familiares y comunitarias es clave para consolidar un enfoque a largo plazo en la seguridad digital de los estudiantes.

La capacitación ha tenido un impacto positivo general, ya que en casi todos los temas se observa una mejora del 20-30% en el porcentaje de respuestas correctas. Esto demuestra que el programa educativo fue efectivo en lograr que los estudiantes adquirieran conocimientos más profundos sobre ciberseguridad. Los resultados también reflejan que los estudiantes ahora no solo comprenden los conceptos, sino que probablemente estén aplicando prácticas de seguridad de manera consciente y sistemática. Es decir, las investigaciones sugieren que una educación en ciberseguridad dinámica y basada en la práctica logra una comprensión más profunda y una

aplicación efectiva de prácticas seguras. A medida que se integran actividades prácticas, actualizaciones continuas y metodologías interdisciplinarias, se potencian los conocimientos y habilidades de los estudiantes para enfrentar los riesgos cibernéticos en el entorno digital educativo y cotidiano.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

Los resultados de la evaluación post-implementación muestran un progreso significativo en los conocimientos y prácticas de ciberseguridad de los estudiantes, reflejando así la efectividad del programa de capacitación en temas clave como el uso de contraseñas seguras, la autenticación multifactorial y la protección de redes Wi-Fi. Estos cambios evidencian que los estudiantes, tras la capacitación, comprendieron mejor los conceptos de ciberseguridad y lograron aplicar medidas de protección personal de forma más consciente y constante. La importancia de la formación estructurada y la aplicación práctica es evidente en estos resultados, ya que los estudiantes lograron incrementar su capacidad para identificar y manejar riesgos asociados a amenazas comunes en el entorno digital educativo.

Pese a los avances alcanzados, aún persisten áreas que requieren mayor refuerzo, especialmente en prácticas más complejas, como la gestión y eliminación de datos personales y la implementación de políticas de privacidad. Aunque la capacitación contribuyó a mejorar en estos temas, los resultados sugieren que los estudiantes podrían beneficiarse de actividades adicionales que les permitan comprender y practicar estos aspectos de seguridad en contextos prácticos. La incorporación de actividades y simulaciones que reproduzcan situaciones de riesgo real resulta fundamental para consolidar estos conocimientos y lograr que los estudiantes adquieran una competencia más integral en ciberseguridad.

Finalmente, la capacitación también fomentó una cultura de seguridad que se extiende al entorno familiar y comunitario, lo cual es esencial para crear una base sólida de prácticas seguras que trascienda el aula. Los estudiantes mostraron una mayor inclinación a compartir y aplicar estos conocimientos en sus hogares, generando un impacto positivo que puede fortalecer la seguridad digital en su círculo cercano. Los resultados, en conjunto, reflejan la necesidad de mantener y expandir este tipo de programas educativos, promoviendo así una cultura de seguridad digital que sea sostenible y accesible en el tiempo.

6.2. Recomendaciones

Es recomendable que se mantenga un programa continuo y actualizado de capacitación en ciberseguridad en las instituciones educativas. Esto permitiría a los estudiantes mantenerse informados sobre las amenazas emergentes y estar preparados para enfrentarlas. Integrar simulaciones prácticas y escenarios reales, como intentos de phishing, contribuiría a fortalecer el conocimiento y la capacidad de respuesta de los estudiantes. Además, realizar actividades periódicas ayudaría a que las habilidades de seguridad se afiancen en su vida cotidiana, aumentando así su eficacia en la prevención de riesgos cibernéticos.

También es importante que las instituciones educativas adopten políticas de seguridad digital bien definidas que aborden temas esenciales como la protección de datos personales, el uso de contraseñas seguras y la actualización de sistemas y software. Las políticas de privacidad y medidas de protección de datos deben implementarse en las plataformas educativas y reforzarse regularmente para garantizar que todos los estudiantes comprendan y respeten las prácticas adecuadas de seguridad. De este modo, las instituciones no solo protegerán los datos de sus usuarios, sino que también establecerán un estándar de seguridad que los estudiantes podrán seguir en otros contextos.

Finalmente, se recomienda extender los esfuerzos de sensibilización a los entornos familiares y comunitarios de los estudiantes. Incluir a las familias en el proceso de educación en ciberseguridad crea un entorno de apoyo que refuerza las prácticas seguras tanto dentro como fuera de la escuela. Los programas que promueven la concienciación en el hogar pueden ayudar a reducir los riesgos y a fomentar una cultura de seguridad compartida que beneficie a toda la comunidad. De esta manera, se fomenta una cultura de seguridad digital sostenible y colaborativa que puede adaptarse y crecer frente a las amenazas cambiantes del entorno digital.

REFERENCIAS

Andrade, J. F. (2023). PLAN DE CIBERSEGURIDAD PARA EDUCACIÓN BÁSICA ECUATORIANA CONTRA EL CIBERDELITO POR COVID-19. *InnDev, 2*(1), 24-43. https://doi.org/https://doi.org/10.69583/inndev.v2n1.2023.52

Beltrán Muñoz, A. (2024). *Análisis de la educación en ciberseguridad: situación actual, estrategias y retos.* https://digibug.ugr.es/bitstream/handle/10481/92804/101464.pdf?sequence=4&isAllowed=y

Calzada, A., E., F.-M., & Piattini, M. (2010). MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 91-103.

CISA. (2024). *Cybersecurity and Infrastructure Security Agency (Agencia de Seguridad de Infraestructura y Ciberseguridad)*. Cybersecurity Awareness Month Creating partnerships to raise cybersecurity awareness at home and abroaD: https://www.cisa.gov/cybersecurity-awareness-month

Corozo, K. E. (2023). Modelo de evaluación de seguridad de la información en centros de datos. *Revista Cumbres*, 39-50.

CYBER.ORG. . (2023). *National Center for Cybersecurity Education.* K-12 Cybersecurity Standards: A Comprehensive Review of Cybersecurity Education in Schools.: https://cyber.org/standards

Díaz, E. (2021). Cartografía conceptual: hacia la ciberseguridad proactiva para la educación, obligación de todos. . *HETS Online Journal, 12*(1), 90-117. https://doi.org/hets.org/ojournal/index.php/hoj/article/view/46

El método MAGERIT. (s.f). Retrieved 1 de 9 de 2023, from https://www.um.es: https://www.um.es/docencia/barzana/GESESI/GESESI-Metodo-MAGERIT.pdf

Fernández, L. M., & Sussi de Oliveira, J. (2021). Cultura, economía y educación : nuevos desafíos en la sociedad digital. *Dykinson*. https://www.torrossa.com/en/resources/an/5087596#page=985

Galvá, R. L. (2018). La Seguridad de la Información: Desde la Antigüedad hasta el Internet de las Cosas. *Seguridad, Ciencia & Defensa*, , 60-69.

Herrero, J., Rodríguez, C., Valdivielso, R., & Amo, D. (2022). Formación en ciberseguridad y educación. Variables de sensibilidad y cambio en la formación del profesorado. *En In-Red 2022 - VIII Congreso Nacional de Innovación Educativa y Docencia en Red. Editorial Universitat Politècnica de València*, 856-864. https://doi.org/https://doi.org/10.4995/INRED2022.2022.15855

Kingsley, A. (Octubre de 2024). *Learning Counsel, Inc.* What Students Should Know About Digital Citizenship: https://thelearningcounsel.com/articles/what-students-should-know-about-digital-citizenship/

Loja-Tepán, E. A., & Cuenca-Tapia, J. P. (2020). Propuesta de guía rápida de un sistema de gestión de la seguridad de la información, para el Registro de la Propiedad del Cantón Cuenca. *Dominio de las ciencias*, 27. https://www.dominiodelasciencias.com: https://www.dominiodelasciencias.com/ojs/index.php/es/article/view/1566/2953

Medina Ampuero, P. J., Zavaleta Lores, M. A., & Ravichagua Inga, C. J. (2023). *Método para la optimización de inversión en ciberseguridad aplicado a una institución educativa de educación básica basado en un modelo determinístico.* Universidad Peruana de Ciencias Aplicadas (UPC).

Moreno Valencia, E. F., & Mejía Cardona, G. A. (2023). *Guía de ciberseguridad orientada a la comunidad educativa.* https://repositorio.ucm.edu.co/handle/10839/4467

Muñoz Castillo, S. E. (2024). *Ciberseguridad y educación: Uso de videojuegos como estrategia pedagógica para adolescentes de Colombia sobre los riesgos en redes sociales.* https://scholar.google.com/scholar?hl=es&as_sdt=0%2C5&as_ylo=2020&q=+CIBERSEGURIDAD+Y+EDUCACI%C3%93N+ONLINE&btnG=

National Institute of Standards and Technology. (2021). *National Institute of Standards and Technology*. National K12 Cybersecurity Education Roadmap: https://www.nist.gov/cybersecurity

Pacheco, F., Staino, D., & Sliafertas, M. (2021). *Educación en ciberseguridad mediante estrategias de Gamificación.* Universidad Tecnológica Nacional, IUPFA, Universidad Nacional de Quilmes. https://researchgate.net/profile/Federico-Pacheco-2/publication/385096975_Educacion_en_ciberseguridad_mediante_estrategias_de_Gamificacion/links/671646c1035917754c121a5d/Educacion-en-ciberseguridad-mediante-estrategias-de-Gamificacion.pdf

Paredes, P., & Chicaiza, R. P. (2021). Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador. *Dialnet, 10*(2), 49-75. https://doi.org/https://dialnet.unirioja.es/servlet/articulo?codigo=8091394

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020). *Marco del personal para la ciberseguridad.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1es.pdf

Pillajo Garcia, P. A., & Avila Pesantez, D. (2023). Análisis de ciberseguridad en plataformas e-learning: revisión sistemática de la literatura. *Perspectivas, 5*(1), 19-29. https://doi.org/https://doi.org/10.47187/perspectivas.5.1.179

Salazar Mata, J., Cruz Navarro, C., Balderas Sánchez, A., & Díaz Uribe, H. (2021). La seguridad informática en las instituciones de educación superior. *Dialnet, 7*(2), 2444-4944. https://dialnet.unirioja.es/servlet/articulo?codigo=8524233

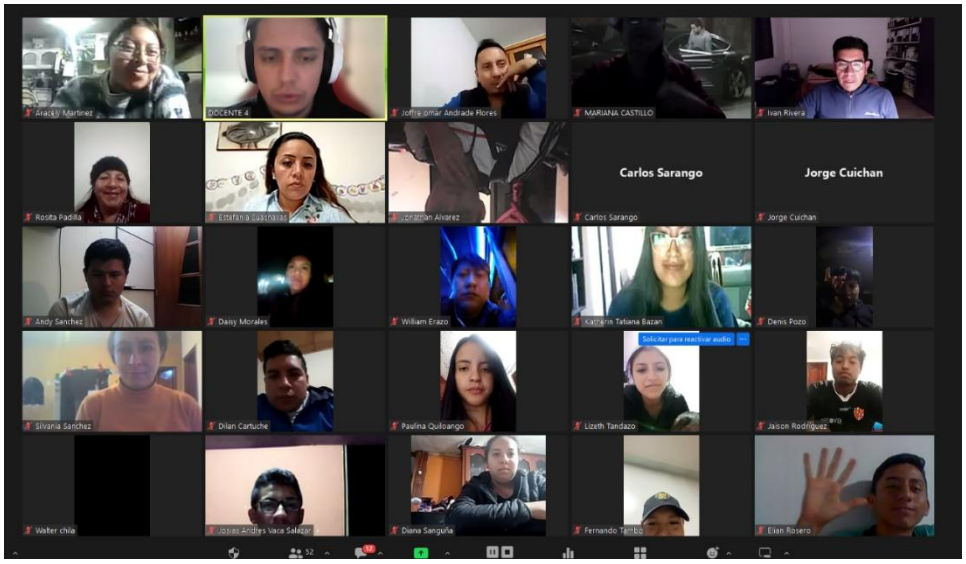
Suárez, G. Y., Bolino, P. E., Venosa, P., & Queiruga, C. A. (2023). *Acercando la ciberseguridad a la escuela secundaria desde una perspectiva lúdica.* https://sedici.unlp.edu.ar/handle/10915/165631

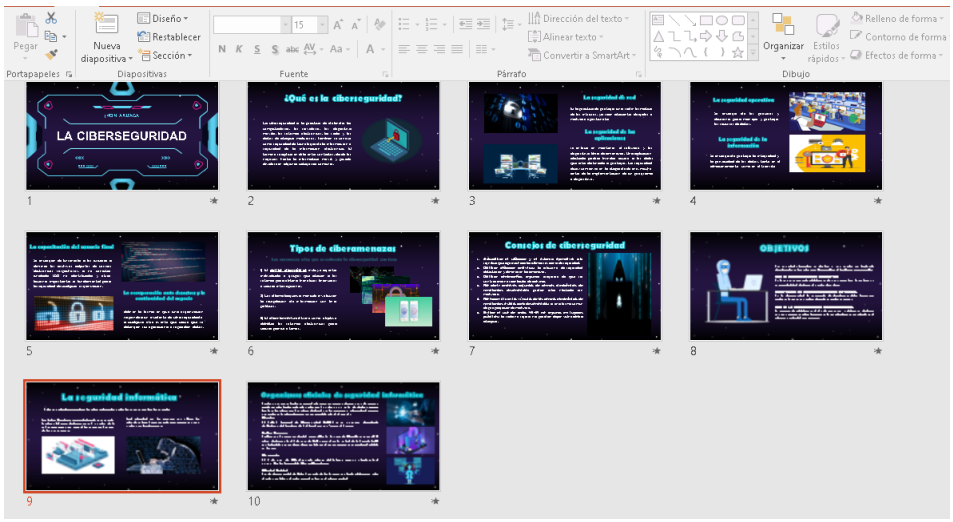
Tamayo Pérez, V., & Cuervo Quiroga, C. C. (2022). *Conocimientos sobre ciberseguridad en jóvenes y su impacto durante la virtualidad.* Universidad Cooperativa de Colombia, Facultad de Ingenierías, Ingeniería de Sistemas, Bogotá. https://repository.ucc.edu.co/entities/publication/a8c2cfae-bc83-4b50-abf5-9ae2fd39d673

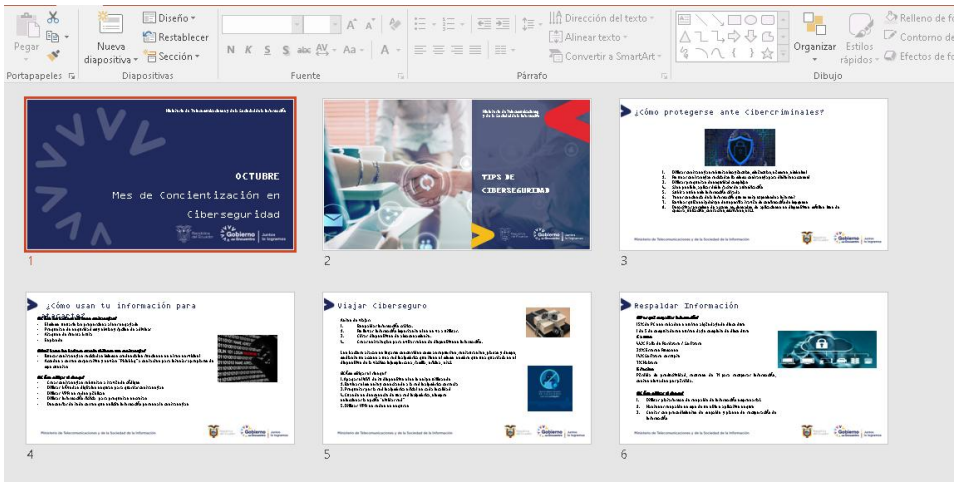
weforum. (2021). *The Global Risks Report 2021* . https://www.weforum.org: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

ANEXOS

Anexo 1. Registro Fotográfico







Anexo 2. Encuesta Pre Implementación

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACION MENCION EN SEGURIDAD INFORMÁTICA

Encuesta Pre-Implementación de Ciberseguridad

Instrucciones: Responde cada pregunta seleccionando "Sí" o "No" según corresponda a tu experiencia y prácticas actuales. Esta encuesta tiene como objetivo evaluar tus conocimientos y prácticas en ciberseguridad antes de la capacitación.

---

1. **¿Asegura que su sistema operativo y software están siempre actualizados?**
   - Sí / No
2. **¿Utiliza contraseñas robustas y únicas para sus cuentas en línea?**
   - Sí / No
3. **¿Implementa la autenticación de dos factores?**
   - Sí / No
4. **¿Está al tanto de las amenazas de seguridad cibernética como phishing, malware y estafas?**
   - Sí / No
5. **¿Realiza copias de seguridad periódicas de datos importantes?**
   - Sí / No
6. **¿Utiliza conexiones seguras (HTTPS) y cifra archivos sensibles?**
   - Sí / No
7. **¿Protege su red Wi-Fi con contraseña sólida y evita redes públicas no seguras?**
   - Sí / No
8. **¿Utiliza software de seguridad confiable como antivirus?**
   - Sí / No
9. **¿Limita el acceso a su dispositivo a personas autorizadas?**
   - Sí / No
10. **¿Define un período para retener datos personales y elimina la información no necesaria?**
    - Sí / No
11. **¿Dispone de una política de privacidad clara?**
    - Sí / No
12. **¿Realiza evaluaciones de seguridad para detectar vulnerabilidades?**
    - Sí / No
13. **¿Cuenta con sistemas de registro y monitorización de actividad inusual?**
    - Sí / No
14. **¿Tiene un plan de respuesta a incidentes de seguridad informática?**
    - Sí / No
15. **¿Mantiene su sistema y aplicaciones actualizados con parches de seguridad?**

- Sí / No

16. **¿Sigue una política de contraseñas que promueve cambios regulares?**
    - Sí / No
17. **¿Se mantiene informado sobre prácticas seguras de seguridad cibernética?**
    - Sí / No
18. **¿Implementa políticas de seguridad para dispositivos móviles?**
    - Sí / No
19. **¿Utiliza firewalls y sistemas de detección de intrusos para proteger su red?**
    - Sí / No
20. **¿Participa activamente en la concienciación de seguridad cibernética con familiares?**
    - Sí / No

Anexo 3. Encuesta Post-Capacitación

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACION MENCION EN SEGURIDAD INFORMÁTICA

Encuesta Post-Capacitación en Ciberseguridad para Educación Online

Objetivo: Evaluar el nivel de conocimiento y aplicación de buenas prácticas de ciberseguridad en los estudiantes luego de haber completado el programa de formación.

Sección 1: Conocimientos Generales de Ciberseguridad

1. **¿Qué tan seguro/a te sientes aplicando los conocimientos adquiridos para proteger tus datos personales en línea?**
    - Muy seguro/a
    - Algo seguro/a
    - Poco seguro/a
    - Nada seguro/a
2. **¿Comprendes los riesgos de ciberataques como phishing y malware?**
    - Sí, comprendo completamente
    - Algo, pero tengo algunas dudas
    - Muy poco
    - No comprendo los riesgos

Sección 2: Prácticas de Seguridad y Protección de Datos

3. **¿Mantienes tu sistema operativo y tus aplicaciones actualizadas regularmente?**
    - Sí, siempre
    - A veces

- Rara vez
- Nunca

4. **¿Utilizas contraseñas robustas y únicas para cada cuenta?**
   - Sí, en todas mis cuentas
   - Solo en algunas cuentas
   - Pocas veces
   - No, uso la misma para varias cuentas
5. **¿Has configurado la autenticación de dos factores en tus cuentas más importantes (correo, redes sociales, plataformas educativas)?**
   - Sí, en todas mis cuentas importantes
   - En algunas cuentas importantes
   - Lo he intentado, pero no siempre funciona
   - No he configurado la autenticación de dos factores

Sección 3: Protección de Dispositivos y Redes

6. **¿Cuentas con antivirus actualizado en tu dispositivo?**
   - Sí, y lo mantengo actualizado
   - Sí, pero no lo actualizo regularmente
   - Tengo antivirus, pero no sé si está actualizado
   - No tengo antivirus
7. **¿Realizas copias de seguridad de tus datos importantes?**
   - Sí, periódicamente
   - Algunas veces
   - Rara vez
   - Nunca

Sección 4: Buenas Prácticas en Redes Sociales y Manejo de Información

8. **¿Limitas la cantidad de información personal que compartes en redes sociales?**
   - Sí, siempre
   - A veces
   - Rara vez
   - Nunca

Sección 5: Evaluación del Programa

9. **¿Consideras que el programa de capacitación te proporcionó las herramientas necesarias para identificar y gestionar riesgos de ciberseguridad?**
   - Totalmente de acuerdo
   - De acuerdo
   - En desacuerdo
   - Totalmente en desacuerdo
10. **¿Recomendarías este programa de ciberseguridad a otros estudiantes?**
    - Sí
    - No

Anexo 4. Evaluación de Conocimientos en Ciberseguridad

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACION MENCION EN SEGURIDAD INFORMÁTICA

Evaluación de Conocimientos en Ciberseguridad

Instrucciones: Selecciona la opción que mejor responda cada pregunta. Esta evaluación tiene como objetivo medir tu comprensión de los temas abordados en la capacitación de ciberseguridad.

---

1. **¿Por qué es importante mantener el sistema operativo y software siempre actualizados?**
   - A) Para mejorar la velocidad del dispositivo.
   - B) Para proteger contra vulnerabilidades y amenazas de seguridad.
   - C) Para reducir el consumo de batería.
   - D) Para evitar el uso de aplicaciones antiguas.
2. **¿Qué características debe tener una contraseña robusta y única?**
   - A) Ser corta y fácil de recordar.
   - B) Ser larga y contener una combinación de letras, números y símbolos.
   - C) Usar solo números para mayor seguridad.
   - D) Ser la misma en todas las cuentas para facilitar el acceso.
3. **¿Cuál es la ventaja de implementar autenticación de dos factores (2FA)?**
   - A) Permitir acceso a la cuenta sin necesidad de contraseña.
   - B) Agregar una capa de seguridad adicional que requiere dos métodos de verificación.
   - C) Aumentar la velocidad de inicio de sesión.
   - D) Evitar que otros dispositivos puedan acceder a la cuenta.
4. **¿Qué es phishing y por qué es una amenaza de seguridad?**
   - A) Un software de seguridad contra virus.
   - B) Un ataque que utiliza correos falsos para robar información confidencial.
   - C) Un tipo de autenticación que permite acceso a la cuenta.
   - D) Un programa que detecta vulnerabilidades en dispositivos.
5. **¿Por qué es importante realizar copias de seguridad periódicas de datos importantes?**
   - A) Para mejorar la velocidad del dispositivo.
   - B) Para asegurar la recuperación de datos en caso de pérdida o ataque.
   - C) Para liberar espacio en el dispositivo.
   - D) Para reducir el uso de datos.
6. **¿Por qué es fundamental usar conexiones seguras (HTTPS) y cifrar archivos sensibles?**
   - A) Para mejorar la velocidad de carga de páginas web.
   - B) Para proteger la privacidad y seguridad de los datos transmitidos en línea.
   - C) Para acceder a plataformas educativas sin restricciones.

   - D) Para evitar el acceso a redes públicas.
7. **¿Qué debes hacer para proteger tu red Wi-Fi?**
   - A) Usar una contraseña compleja y evitar redes abiertas.
   - B) Cambiar la contraseña cada año.
   - C) Permitir solo el acceso de familiares.
   - D) Dejar la red sin contraseña para facilitar el acceso.
8. **¿Qué función cumple un software antivirus?**
   - A) Acelerar la conexión a Internet.
   - B) Detectar y eliminar amenazas como virus y malware.
   - C) Recordar todas las contraseñas.
   - D) Reducir el consumo de energía del dispositivo.
9. **¿Por qué es importante limitar el acceso a tu dispositivo a personas autorizadas?**
   - A) Para evitar el uso excesivo de batería.
   - B) Para prevenir accesos no autorizados que puedan comprometer la seguridad.
   - C) Para mejorar la velocidad del dispositivo.
   - D) Para reducir el almacenamiento utilizado.
10. **¿Cuál es la ventaja de definir un período para retener datos personales y eliminar información innecesaria?**
    - A) Para liberar espacio de almacenamiento.
    - B) Para reducir el riesgo de acceso no autorizado a datos sensibles.
    - C) Para evitar el uso de contraseñas.
    - D) Para mejorar la velocidad de navegación.
11. **¿Por qué es importante que las plataformas dispongan de una política de privacidad clara?**
    - A) Para asegurar que la información esté disponible para todos.
    - B) Para garantizar la protección de los datos personales de los usuarios.
    - C) Para facilitar el acceso a redes sociales.
    - D) Para reducir el uso de datos.
12. **¿Por qué se deben realizar evaluaciones de seguridad regularmente?**
    - A) Para identificar y corregir vulnerabilidades en el sistema.
    - B) Para reducir el tiempo de carga de las aplicaciones.
    - C) Para facilitar el acceso a plataformas.
    - D) Para mejorar la velocidad de conexión.
13. **¿Qué es un sistema de registro y monitorización de actividad inusual?**
    - A) Un sistema que permite a cualquiera acceder a la red.
    - B) Un sistema que registra y detecta actividades sospechosas en el dispositivo.
    - C) Un software que almacena todas las contraseñas.
    - D) Un programa que mejora el rendimiento del sistema.
14. **¿Para qué sirve un plan de respuesta a incidentes de seguridad informática?**
    - A) Para evitar el uso de contraseñas.
    - B) Para definir pasos a seguir en caso de un incidente de seguridad.
    - C) Para facilitar el acceso a redes Wi-Fi públicas.
    - D) Para mejorar el rendimiento de los dispositivos.
15. **¿Qué significa mantener las aplicaciones actualizadas con parches de seguridad?**
    - A) Descargar solo las aplicaciones necesarias.
    - B) Aplicar actualizaciones que corrigen vulnerabilidades.
    - C) Reducir el tiempo de carga de aplicaciones.
    - D) Aumentar la velocidad del dispositivo.
16. **¿Qué es una política de contraseñas que promueve cambios regulares?**
    - A) Una política que permite usar la misma contraseña en todas las cuentas.
    - B) Una política que sugiere cambiar las contraseñas periódicamente para mayor seguridad.

- C) Una política para reducir el tiempo de inicio de sesión.
- D) Una política para evitar el uso de redes públicas.

17. **¿Por qué es importante mantenerse informado sobre prácticas seguras de ciberseguridad?**
    - A) Para reducir el uso de contraseñas.
    - B) Para estar al tanto de nuevas amenazas y formas de protección.
    - C) Para mejorar la velocidad de conexión.
    - D) Para reducir el almacenamiento utilizado.
18. **¿Por qué implementar políticas de seguridad para dispositivos móviles?**
    - A) Para mejorar la duración de la batería.
    - B) Para proteger los datos almacenados y reducir el riesgo de ataques.
    - C) Para aumentar la velocidad de conexión.
    - D) Para evitar el uso de contraseñas en el dispositivo.
19. **¿Cuál es la función de firewalls y sistemas de detección de intrusos?**
    - A) Mejorar la velocidad de carga de las aplicaciones.
    - B) Proteger la red y detectar accesos no autorizados.
    - C) Facilitar el acceso a plataformas educativas.
    - D) Reducir el tiempo de conexión.
20. **¿Por qué es importante la concienciación en ciberseguridad entre familiares?**
    - A) Para mejorar el acceso a redes sociales.
    - B) Para proteger a toda la familia contra riesgos cibernéticos.
    - C) Para reducir el uso de datos.
    - D) Para facilitar el uso de aplicaciones.