**Fecha de presentación**: octubre, 2023, **Fecha de Aceptación:** noviembre, 2023, **Fecha de publicación**: enero, 2024

68

# PROGRAMA DE PREVENCIÓN DE CIBERDELITOS EN INSTITUCIONES EDUCATIVAS DE ECUADOR

## CYBERCRIME PREVENTION PROGRAM IN EDUCATIONAL INSTITUTIONS OF ECUADOR

Jorge Gabriel Del Pozo Carrasco[1]
E-mail: uq.jorgedc77@uniandes.edu.ec
ORCID: https://orcid.org/0000-0003-4793-847X
Steven Joel Lumbi Salazar[1]
E-mail: ab.stevenlumbisalazar@outlook.com
ORCID: https://orcid.org/0009-0009-4544-6712
César Elías Paucar Paucar[1]
E-mail: uq.cesarpaucar@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-3133-8827
[1] Universidad Regional Autónoma de Los Andes, Quevedo. Ecuador

Cita sugerida (APA, séptima edición)

Del Pozo Carrasco, J. G., Lumbi Salazar, S. J., y Paucar Paucar, C. E. (2024). Programa de prevención de ciberdelitos en instituciones educativas de Ecuador. *Revista Conrado, 20*(96), 675-686.

RESUMEN

El artículo destaca la transformación de la vida cotidiana debido a la evolución tecnológica, subrayando la necesidad de prevenir ciberdelitos en instituciones educativas. La metodología, de enfoque cualitativo, utiliza entrevistas estructuradas y mapas cognitivos difusos para el procesamiento de la información. Se identifican obstáculos clave, como falta de conciencia en seguridad informática, así como, déficit en formación y actualización en ciberseguridad. Se propone un programa integral de prevención de ciberdelitos para instituciones educativas de Ecuador. El programa aborda estos desafíos, reconociendo la interconexión de factores determinantes. La implementación exitosa del programa fortalece la seguridad informática y fomenta la conciencia digital y responsabilidad en el entorno educativo. Además, se enfatiza la importancia de medidas específicas y soluciones educativas y legales para contrarrestar los desafíos identificados, contribuyendo a la formación de una generación consciente y responsable en el entorno digital.

Palabras clave:

Ciberdelitos, seguridad informática, prevención.

ABSTRACT

The article highlights the transformation of daily life due to technological evolution, emphasizing the need to prevent cybercrimes in educational institutions. The methodology, with a qualitative approach, employs structured interviews and fuzzy cognitive maps for information processing. Key obstacles are identified, such as a lack of awareness in information security and a deficit in training and updating in cybersecurity. A comprehensive program for preventing cybercrimes in educational institutions in Ecuador is proposed. The program addresses these challenges, recognizing the interconnection of determining factors. The successful implementation of the program strengthens information security and promotes digital awareness and responsibility in the educational environment. Furthermore, the importance of specific measures and educational and legal solutions is emphasized to counteract identified challenges, contributing to the development of a conscious and responsible generation in the digital environment.

Keywords:

Cybercrimes, information security, prevention.

## INTRODUCCIÓN

La vertiginosa evolución de la tecnología experimenta una transformación fundamental en el modo de vida de las personas, proporcionando una multitud de beneficios y oportunidades para la conectividad, la información y la eficiencia. En la actual era digital, la tecnología deja de ser simplemente una herramienta para convertirse en un componente integral que permea numerosos aspectos de la vida cotidiana. Desde facilitar la comunicación instantánea hasta revolucionar la forma en que las personas acceden a la educación y desempeñan sus labores profesionales. La omnipresencia de la tecnología marca una era de cambios rápidos y significativos (Jin et al., 2023)11 variables were selected from the perspective of sociology and demography. These variables include one dependent variable, three independent variables, and seven control variables. A binary logistic model was used to study the effects of the three dimensions of Internet use in the digital age (independent variables.

Las conductas ilícitas perviven en diversas facetas y circunstancias de la cotidianidad, y el ámbito informático no es una excepción. Se observa un incremento progresivo de actividades delictivas en el entorno digital, comúnmente denominadas como ciberdelitos, las cuales se materializan específicamente en el espacio virtual de Internet (Wright & Kumar, 2023).

El ciberdelito, también conocido como delito informático, se refiere a cualquier actividad ilícita llevada a cabo por un ciberdelincuente en el entorno digital mediante el uso de redes informáticas y dispositivos electrónicos diversos (Pascagaza & Carrascal, 2022). Conforme a diversos informes emitidos por Proveedores de Servicios de Internet (ISP), se evidencian deficiencias en las medidas de seguridad informática, dado que los ciberdelincuentes han llevado a cabo exploraciones e intrusiones en una variedad de dispositivos, incluyendo teléfonos inteligentes y sistemas informáticos pertenecientes tanto a usuarios privados como gubernamentales. Este accionar ha ocasionado perjuicios significativos (Macías Lara et al., 2022).

A pesar de las considerables inversiones realizadas en seguridad informática (SI), se observa que los ciberdelincuentes identifican estrategias para eludir estas medidas, ocasionando pérdidas económicas sustanciales. En respuesta, los profesionales en SI se ven obligados a emprender esfuerzos adicionales para actualizarse en nuevas técnicas y teorías criminológicas, con el objetivo de comprender de manera más efectiva las modalidades emergentes de delitos cibernéticos. Un error de magnitud significativa radica en la divulgación de las últimas técnicas empleadas en el control de ciberdelitos a través de revistas científicas, criminológicas y de actualidad (Macías Lara et al., 2022). Estas publicaciones, accesibles al público en general, brindan información a una audiencia diversa, incluidos los ciberdelincuentes. La preocupación se centra en la posibilidad de que estos últimos, al tener acceso a estas nuevas técnicas de seguridad, puedan identificar deficiencias existentes y buscar vías para eludirlas.

La ejecución de un acto delictivo mediante un dispositivo electrónico interconectado a la red de Internet plantea peligros significativos. La identificación del individuo que perpetra tal acción se torna compleja y fácilmente evitable para las fuerzas del orden (policía). Esto se debe a la posibilidad de realizar la actividad delictiva desde un servidor distinto al propio, mediante la conexión a una red wifi, dificultando la atribución precisa de responsabilidad y facilitando la evasión de las autoridades (Ayyoub et al., 2022).

Ignacio José Subijana, destaca la presencia de cuatro características particulares que definen la naturaleza de estos actos. Estas características delinean la singularidad y la complejidad de los ciberdelitos en comparación con otros delitos convencionales: se cometen fácilmente, requieren escasos recursos en relación al perjuicio que causan, pueden cometerse sin presencia física en el territorio sometido a la misma y se benefician de lagunas de punibilidad que existen en determinados Estados (Subijana Zunzunegui, 2008).

Los delitos cibernéticos más frecuentes abarcan una amplia variedad de actividades, que incluyen, pero no se limitan a estafas, robos, extorsiones, falsificación, suplantación de identidad, delitos sexuales y la interferencia ilícita en la integridad de la información o datos. Esta diversidad de conductas ilícitas en el ámbito digital refleja la complejidad y la adaptabilidad de los ciberdelincuentes para aprovechar las vulnerabilidades presentes en la esfera virtual. Estas acciones transgreden los límites tradicionales, generando una serie de retos para la seguridad y exigiendo respuestas innovadoras y sofisticadas para contrarrestarlas de manera efectiva (Pascagaza & Carrascal, 2022).

Ecuador se encuentra entre los países que demuestran un limitado interés en abordar y contrarrestar los delitos cibernéticos (Ortiz Campos, 2019). Actualmente, el presupuesto asignado al cuerpo policial ha experimentado una reducción drástica, lo que resulta insuficiente para cubrir sus necesidades básicas, y aún menos para proporcionar capacitación adecuada al personal en el ámbito de la delincuencia digital. Es importante destacar que, a pesar de estos desafíos, la Policía Nacional de Ecuador

ha desplegado esfuerzos significativos, superando las limitaciones impuestas por recursos financieros, con el objetivo de abordar los problemas asociados con los delitos en línea. Las investigaciones llevadas a cabo por los agentes de la policía nacional ecuatoriana son extensas, extendiéndose por meses e incluso años, con el fin de lograr resultados eficaces en la resolución de los problemas sociales relacionados con los delitos en el entorno virtual.

En la actualidad, los ataques perpetrados por cibermafias se han vuelto más frecuentes en el territorio nacional. Conforme a un informe estadístico emitido por la Unidad de Ciberdelitos de la Policía, se revela a la sociedad ecuatoriana que, desde el año 2020 hasta julio de 2022, se han documentado aproximadamente 3933 delitos informáticos (Tamayo Benavides, 2023).

Es imperativo señalar que, en el contexto contemporáneo, las Tecnologías de la Información y las Comunicaciones (TIC) ofrecen utilidades y ventajas que superan las dificultades derivadas de un uso indebido. Al ser evaluadas en el ámbito educativo, estas tecnologías han reconfigurado los paradigmas que guían los procesos de enseñanza y aprendizaje. Sus beneficios han propiciado modificaciones en las percepciones sobre tiempo, espacio, roles de estudiantes y profesores, así como en las formas de adquirir conocimiento. Estas transformaciones han propiciado el acceso libre a repositorios digitales, la optimización de la formación continua y la mejora de los procesos de autoformación (Molina Gutiérrez et al., 2019).

Entre las diversas aplicaciones que las TIC despliegan en el ámbito educativo, los sistemas virtuales de enseñanza han surgido como valiosos aliados para la implementación de nuevas metodologías pedagógicas. En estas modalidades, el papel del docente se redefine como un facilitador, mientras que los estudiantes adoptan roles activos y responsables en la construcción del conocimiento. Los ambientes interactivos de aprendizaje, logrados a través de las aulas virtuales, integran elementos innovadores, interactivos, realidad virtual y recursos visuales (Nakano et al., 2013).

En el contexto ecuatoriano, a pesar de la existencia de una marcada disparidad en el ámbito tecnológico, se evidencia una tendencia significativa hacia la generalización del uso de las TIC. Este fenómeno se manifiesta mediante un aumento en la adopción de computadoras y, por ende, de las herramientas que permiten la difusión de información a través de Internet. En consecuencia, se incrementan las oportunidades diarias para que menores y adolescentes se vean expuestos a ciberdelitos, una situación de particular inquietud dada la limitada capacidad de los adolescentes para identificar los riesgos potenciales asociados con las TIC, siendo este grupo demográfico uno de los usuarios más frecuentes de estas tecnologías (Quezada Sarmiento et al., 2022).

Las entidades encargadas reconocen que el ciberacoso, siendo un delito novedoso, se manifiesta como una conducta criminal en aumento. Sin embargo, la falta de denuncias dificulta la obtención de cifras concretas. Esta falta de información contribuye a la ausencia de medidas legales y educativas que podrían ser implementadas para controlar y sancionar este ilícito.

La proliferación del uso de las redes sociales con objetivos de naturaleza sexual en Ecuador, está en ascenso. Esta tendencia incluye a los menores de edad como blancos de interés por parte de ciberdelincuentes. Se deduce, por consiguiente, que los medios informáticos se han transformado en herramientas aliadas para la búsqueda de satisfacción sexual, a menudo a través de prácticas de chantaje y acoso dirigidas específicamente a menores de edad (Recalde Monar, 2021). La mayoría de los adolescentes emplea de manera poco selectiva los recursos tecnológicos, enfrentándose a riesgos tales como acceder a sitios web con contenido inapropiado, participar en juegos violentos, recibir mensajes alienantes y de adoctrinamiento, caer presa de pandillas o sectas, y convertirse en blancos de ataques sexuales. Una de las causas fundamentales de esta falta de supervisión radica en la escasa familiaridad con la cultura informática por parte de los padres y responsables.

Reconociendo que el empleo de las TIC da lugar a comportamientos perjudiciales que afectan aspectos legales, como el derecho a la integridad psíquica y moral de los individuos (Fernández Montalvo et al., 2015), resulta esencial proponer soluciones tanto de índole legal como educativa para contrarrestar el crecimiento de los ciberdelitos. En tal sentido se plantea como objetivo del presente artículo: Desarrollar un programa integral de prevención de ciberdelitos adaptado a las necesidades específicas de las instituciones educativas en Ecuador, con el propósito de salvaguardar la SI y fomentar una cultura de conciencia y responsabilidad en el uso de tecnologías de la información en el entorno educativo.

## MATERIALES Y MÉTODOS

La metodología usada en la investigación es de tipo aplicada en educación, de enfoque cualitativo (Orozco Alvarado, 2018). Brinda una propuesta a partir de los procesos teóricos, metodológicos, categorías apriorísticas y emergentes, proceso de codificación y triangulación, entre otros aspectos vinculados a la propuesta que se

construye a partir de la modelación. También se realiza el acopio de información documental, utilizando libros, informes de investigación, revistas especializadas, internet: bibliotecas virtuales, bases de datos académicas digitalizadas, entre otros (Hernández & Mendoza, 2018).

Dentro de la presente investigación se aplica el método analítico sintético, por cuanto, de la bibliografía obtenida se desintegra la información total para sintetizar de manera ordenada el tema planteado, guardando la sincronía de la sintaxis (Finol de Franco & Vera Solórzano, 2020).

Se emplea una entrevista estructurada como método de recolección de datos, la cual es concebida mediante la inclusión de un cuestionario especialmente diseñado (Tabla 1). La aplicación de la entrevista es dirigida a diversos grupos de interés de la Unidad educativa ¨Siete de Octubre¨ de Quevedo. Este cuestionario tiene como objetivo identificar la necesidad del desarrollo de un programa integral de prevención de ciberdelitos en las instituciones educativas de Ecuador, salvaguardando la confidencialidad de las respuestas brindadas durante la entrevista.

Tabla 1: Cuestionario aplicado para diagnosticar la situación actual sobre ciberdelitos en la Unidad educativa ¨Siete de Octubre¨ de Quevedo

| Estudiantes. |
|---|
| Edad.<br>( ) Menos de 12 años ( ) 13-15 años ( ) 16-18 años |
| Frecuencia de uso de dispositivos electrónicos.<br>( ) Diariamente, ( ) Semanalmente, ( ) Mensualmente. |
| ¿Sabes qué son los ciberdelitos? ( ) Si ( ) No<br>En caso afirmativo, ¿puedes mencionar ejemplos? |
| ¿Has tenido alguna experiencia negativa en línea? (Acoso, suplantación, etc.)<br>( ) Si ( ) No |
| ¿Sigues prácticas seguras al compartir información en internet? ( ) Si ( ) No<br>En caso afirmativo, ¿puedes mencionar ejemplos? |
| ¿Has recibido educación sobre ciberseguridad en la escuela?<br>( ) Si ( ) No |
| ¿Te sientes preparado/a para identificar y evitar ciberdelitos?<br>( ) Si ( ) No |
| Docentes. |
| ¿Cómo percibe la seguridad informática en la institución?<br>( ) Muy segura, ( ) Segura, ( ) Poco segura, ( ) Insegura. |
| ¿Has integrado temas de seguridad informática en tus clases?<br>( ) Si ( ) No |
| ¿Consideras que los estudiantes están conscientes de los riesgos en línea?<br>( ) Si ( ) No |
| ¿Cree que los docentes necesitan más formación en ciberseguridad?<br>( ) Si ( ) No |
| Personal administrativo. |
| ¿Cómo evalúa la infraestructura tecnológica actual de la institución?<br>( ) Excelente, ( ) Buena, ( ) Regular, ( ) Deficiente. |
| ¿Existen medidas de seguridad implementadas en los sistemas informáticos? ( ) Si ( ) No<br>En caso afirmativo, ¿puedes mencionar algunas? |
| ¿Se han establecido políticas específicas de seguridad informática en la institución?<br>( ) Si ( ) No |
| ¿Se llevan a cabo prácticas regulares para garantizar la seguridad de la información?<br>( ) Si ( ) No |
| Personal técnico o de soporte informático. |
| ¿Existen áreas de vulnerabilidad en la infraestructura tecnológica actual de la institución?<br>( ) Si ( ) No |
| ¿Se realizan evaluaciones regulares de seguridad? ( ) Si ( ) No |

| |
|---|
| ¿Cuentan con personal capacitado para abordar cuestiones de ciberseguridad?<br>( ) Si ( ) No |
| ¿Qué medidas se toman para garantizar la protección de datos sensibles? |
| ¿Qué áreas específicas crees que necesitan mejoras en términos de seguridad informática? |

Fuente: Elaboración propia

En relación a la población y la muestra, se identifica que el grupo de estudio comprende un total de 200 individuos, entre estudiantes, docentes, administrativos y personal de soporte informático, de la Unidad Educativa ¨Siete de Octubre¨ de Quevedo.

Con el propósito de determinar el tamaño de la muestra en una población finita, se emplea la fórmula que se expone a continuación. La fórmula 1 que se aplica considera diversos factores, como el nivel de confianza y el margen de error, para garantizar la precisión y validez de los resultados obtenidos a través de la investigación.

$$n = \frac{Z^2 pqN}{E^2(N-1) + Z^2 pq} \quad (1)$$

Donde:

N = 200 (tamaño de la población)

Sustituyendo los valores en la ecuación 1, se obtuvo como número de muestra (n) a un total de 65 entrevistados de la institución ¨Siete de Octubre¨ de Quevedo.

Para el procesamiento de la información se emplean Mapas Cognitivos Difusos (MCD), los cuales se configuran como una modalidad de grafo en el que los nodos representan conceptos y los enlaces simbolizan las relaciones causales entre ellos. Dentro de estos mapas, los valores se sitúan en el intervalo [-1, 1], ofreciendo una graduación minuciosa entre los conceptos en función de sus relaciones. Este enfoque proporciona una representación detallada y matizada de la estructura cognitiva, permitiendo analizar las interconexiones entre los diversos elementos conceptuales de manera precisa (Hatwágner et al., 2018).

En los MCD se reconocen tres categorías potenciales de relaciones causales entre conceptos. Este sistema de clasificación permite distinguir y analizar de manera precisa las interconexiones y dependencias entre los diversos elementos conceptuales presentes en el contexto del mapa. (Mar Cornelio et al., 2020):

- Causalidad positiva ($W_{ij} > 0$): Indica una causalidad positiva entre los conceptos $C_i$ y $C_j$ , es decir, el incremento (disminución) en el valor de $C_i$ lleva al incremento (disminución) en el valor de .
- Causalidad negativa ($W_{ij} < 0$): Indica una causalidad negativa entre los conceptos $C_i$ y , $C_j$ es decir, el incremento (disminución) en el valor de $C_i$ lleva la disminución (incremento) en el valor de $C_j$.
- No existencia de relaciones ( $W_{ij} = 0$): Indica la no existencia de relación causal entre $C_i$ y $C_j$ .

Para cumplir con lo expuesto en el objetivo se sigue el siguiente algoritmo:

1. Modelar el MCD mediante un grafo y su matriz de adyacencia.
2. Análisis estático. Las siguientes medidas se calculan para los valores absolutos de la matriz de adyacencia:

1. ***Outdegree***, denotado por od (vi), que es la suma por cada fila de los valores absolutos de una variable de la matriz de adyacencia difusa. Es una medida de la fuerza acumulada de las conexiones existentes en la variable.
2. ***Indegree***, denotado por id (vi), que es la suma por cada columna de los valores absolutos de una variable de la matriz de adyacencia difusa. Mide la fuerza acumulada de entrada de la variable.

3. La centralidad o grado total, de la variable es la suma de od (vi), con id (vi), como se indica a continuación en la ecuación 2:

$$td(vi) = od(vi) + id(vi) \quad (2)$$

4. Clasificar las variables según el criterio siguiente, véase:

Las variables transmisoras son $od(v_i)>0$ aquellas con e $od(v_i)>0$ .

Las variables receptoras son $od(v_i)=0$ aquellas con y $id(v_i) >0$..

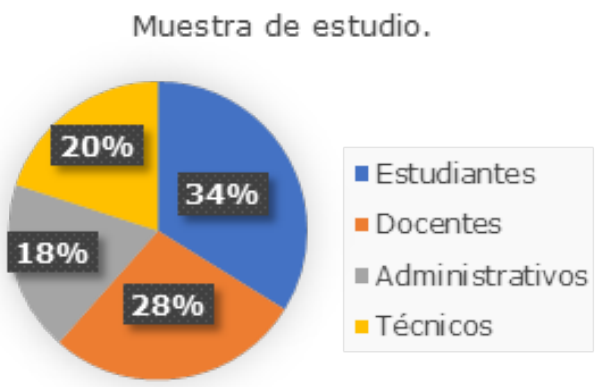
Las variables ordinarias satisfacen a la vez od $(v_i)\neq 0$ y y $id(v_i) \neq 0$.

5. Se ordenan de manera ascendente acorde al grado de centralidad.

## RESULTADOS Y DISCUSIÓN

En un primer momento, se decide realizar una caracterización de la muestra de estudio, cuya estructura se exhibe en la Figura 1.

Fig. 1: Estructura de la muestra de estudio.




Fuente: Elaboración propia

La muestra del estudio incluye un grupo diverso de participantes, abarcando estudiantes, docentes, personal administrativo y técnicos de soporte informático. Se llevan a cabo entrevistas con 22 estudiantes, 18 docentes, 12 miembros del personal administrativo y 13 técnicos. Esta variedad de perfiles permitió obtener una representación integral de la comunidad educativa y de los profesionales involucrados en el entorno estudiado.

Los estudiantes, como parte esencial de la población estudiantil, ofrecen perspectivas valiosas sobre sus experiencias y conocimientos en relación con la SI y las prácticas en línea. Por otro lado, los docentes, con su rol pedagógico, aportaron visiones fundamentales sobre la integración de temas de SI en el proceso educativo. El personal administrativo, siendo parte fundamental de la gestión escolar, proporcionan información crucial sobre las políticas y prácticas institucionales relacionadas con la SI. Los técnicos, con su conocimiento especializado, contribuyen con perspectivas importantes sobre la infraestructura tecnológica y las medidas de seguridad implementadas en el entorno educativo.

En conjunto, esta diversidad de participantes enriqueció la comprensión del panorama de SI en la institución educativa "Siete de Octubre", permitiendo una evaluación más completa de las necesidades y desafíos que necesitan abordarse en el desarrollo de un programa integral de prevención de ciberdelitos. Es fundamental asegurar que los participantes comprendan la importancia del programa integral de prevención de ciberdelitos y que sus respuestas contribuyen a su desarrollo y efectividad.

Las respuestas proporcionadas por los estudiantes de la institución educativa, reflejan una variedad de percepciones y experiencias en relación con la SI. En cuanto al nivel de conocimiento sobre ciberdelitos y riesgos en línea, se observa que pocos estudiantes muestran un entendimiento sólido, mientras que la mayoría expresa falta de conciencia. Las prácticas en línea revelan una diversidad de comportamientos, desde el cuidado meticuloso al compartir información hasta prácticas más arriesgadas. En lo referente a la recepción de educación sobre SI, la mayoría de los estudiantes expresan la necesidad de más orientación en este ámbito. Además, las experiencias personales compartidas en el cuestionario, destacan situaciones de riesgo en línea que van desde el acceso a contenido inapropiado hasta la interacción con desconocidos. Estas respuestas subrayan la importancia de abordar las brechas de conocimiento y fomentar prácticas seguras en línea, respaldando la necesidad de un programa integral de prevención de ciberdelitos en la institución educativa.

Los docentes de la institución brindan respuestas significativas durante el cuestionario enfocado en la identificación de la necesidad de un programa integral de prevención de ciberdelitos. En cuanto a la percepción de la SI en la institución, algunas respuestas destacan la conciencia de la importancia de esta temática, aunque se señalaron áreas de mejora en términos de implementación de medidas específicas. Al abordar la integración de temas de SI en las clases, se observó una variedad de enfoques, desde la inclusión activa hasta la necesidad de más recursos y capacitación para una implementación efectiva. En relación con la conciencia de los riesgos en línea por parte de los estudiantes, algunas respuestas indican un reconocimiento limitado por parte de los estudiantes, sugiriendo una oportunidad para fortalecer la educación en SI. Finalmente, en cuanto a la necesidad de formación en ciberseguridad para los docentes, hubo consenso en que

se beneficiarían de programas de capacitación adicionales para mejorar sus conocimientos y habilidades en este ámbito emergente. Estas respuestas proporcionan una visión inicial valiosa que orienta el diseño y la implementación del programa integral de prevención de ciberdelitos en la institución.

Las respuestas proporcionadas por los administrativos, brindan una visión integral de la situación actual en cuanto a la infraestructura tecnológica y SI en la institución. En relación con la evaluación de la infraestructura tecnológica, se destacan observaciones negativas sobre la eficiencia y capacidad de los sistemas actuales, así como la identificación de posibles áreas de mejora. En cuanto a las medidas de seguridad implementadas en los sistemas informáticos, las respuestas indican falta de conciencia de la importancia de la SI, y no se logran detallar medidas específicas, como firewalls y sistemas de detección de intrusiones. En relación con las políticas de SI, se observa un reconocimiento de la necesidad de establecer pautas específicas, y algunas respuestas indican la existencia de políticas formales en proceso de implementación, pero aun deficientes. Además, las prácticas regulares para garantizar la seguridad de la información son reconocidas como una necesidad, y algunas respuestas indican la ausencia de procedimientos de auditoría y actualizaciones periódicas de software. Estas respuestas proporcionan una base valiosa para evaluar las áreas de fortaleza y oportunidad en la SI de la institución y orientar la implementación de un programa integral de prevención de ciberdelitos.

Los técnicos de soporte informático entrevistados reflejan una evaluación integral de la infraestructura tecnológica de la institución. En relación con la primera pregunta, se identificaron ciertas áreas de vulnerabilidad, destacando la importancia de implementar medidas adicionales para fortalecer la seguridad. Asimismo, se confirma que no se llevan a cabo evaluaciones regulares de seguridad, lo que evidencia falta de compromiso continuo con la monitorización y mejora del sistema. En cuanto a la capacidad del personal, se obtuvo la confirmación de que no cuentan con profesionales capacitados para abordar cuestiones de ciberseguridad. Se destacó la ausencia de medidas específicas destinadas a garantizar la protección de datos sensibles, indicando una inconsciente atención hacia la confidencialidad y privacidad de la información. Al abordar áreas específicas que necesitan mejoras en términos de seguridad informática, se señalan algunas sugerencias concretas. Estas recomendaciones incluyeron actualizaciones en software, implementación de firewalls y medidas de prevención de intrusiones, así como el uso de protocolos más rigurosos para el manejo y resguardo de datos críticos. Estas respuestas proporcionan una base sólida para la identificación de necesidades y la necesidad imperiosa de un programa integral de prevención de ciberdelitos adaptado a los requisitos específicos de instituciones educativas.

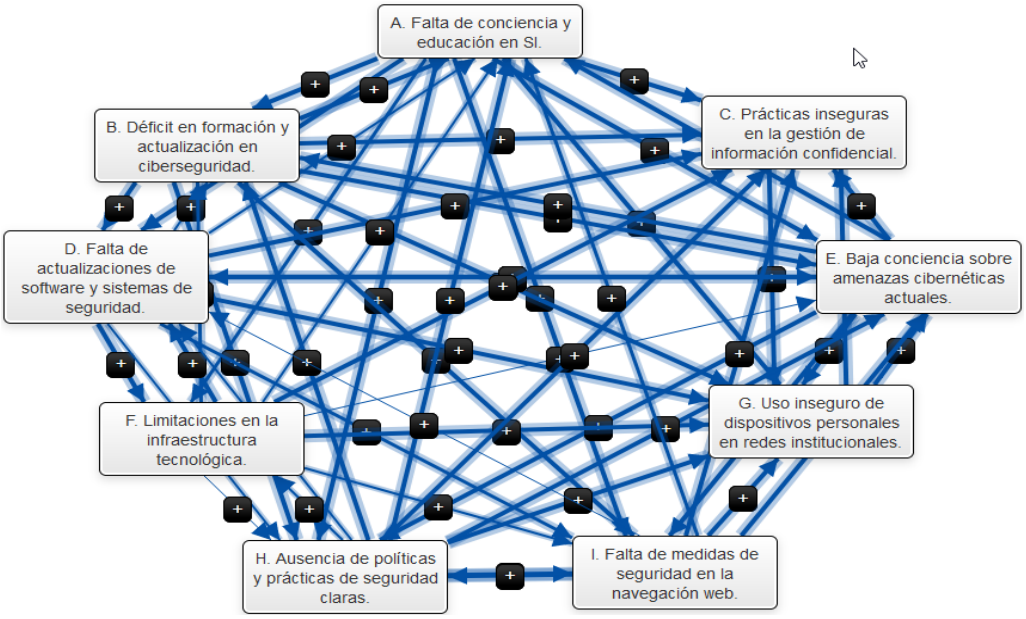
Tras llevar a cabo un análisis exhaustivo de las respuestas recopiladas, se identifican diversos factores determinantes que representan obstáculos para la prevención de ciberdelitos en la Unidad Educativa “Siete de Octubre” de Quevedo. Estos elementos determinantes se describen detalladamente a continuación:

a. Falta de conciencia y educación en SI: la carencia de conocimientos sólidos sobre SI expone al personal a prácticas riesgosas en línea y los hace más susceptibles a ser víctimas de estafas o ataques cibernéticos.
b. Déficit en formación y actualización en ciberseguridad: la falta de formación continua en ciberseguridad provoca personas menos preparadas para enfrentar las amenazas actuales en el entorno digital, aumentando la probabilidad de caer en trampas cibernéticas.
c. Prácticas inseguras en la gestión de información confidencial: malas prácticas en la gestión de información confidencial, como el manejo descuidado de contraseñas o la compartición irresponsable de datos sensibles, pone en riesgo la seguridad de la información.
d. Falta de actualizaciones de software y sistemas de seguridad: la omisión de actualizar regularmente los software y sistemas de seguridad en los dispositivos utilizados por el personal deja vulnerabilidades abiertas, facilitando posibles ataques.
e. Baja conciencia sobre amenazas cibernéticas actuales: la falta de conciencia sobre las tácticas y amenazas cibernéticas actuales hace que el personal no reconozca indicios de posibles ataques, aumentando así el riesgo de caer en trampas digitales.
f. Limitaciones en la infraestructura tecnológica: limitaciones en la infraestructura tecnológica de la institución resulta en sistemas menos seguros, creando oportunidades para la explotación por parte de ciberdelincuentes.
g. Uso inseguro de dispositivos personales en redes institucionales: el uso de dispositivos personales de manera insegura en las redes institucionales introduce amenazas externas no controladas, comprometiendo la seguridad global del entorno digital.
h. Ausencia de políticas y prácticas de seguridad claras: la falta de políticas y prácticas de SI claras y bien comunicadas deja al personal sin guías efectivas para protegerse contra amenazas cibernéticas.

i. Falta de medidas de seguridad en la navegación web: la carencia de medidas de seguridad adecuadas al navegar por internet expone al personal de la institución a sitios web maliciosos o fraudulentos, incrementando el riesgo de ser víctima de ciberdelitos.

Con el propósito de identificar el factor determinante de mayor influencia, teniendo en cuenta la interconexión entre estos componentes, se plantea el MCD. Figura 2.

Fig. 2: Interrelación entre nodos (factores influyentes).




Fuente: Elaboración propia.

A continuación, se presenta la matriz de adyacencia que muestra las conexiones entre los nodos causales del grafo representadas en una estructura de tabla bidimensional. Tabla 2

Tabla 2: Matriz de adyacencia.

| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| A | | 1 | 1 | 1 | 1 | 0.6 | 1 | 1 | 1 |
| B | 1 | | 1 | 1 | 1 | | 1 | 1 | 1 |
| C | | | | | | | 1 | | |
| D | 0.3 | 0.4 | 1 | | 0.5 | 1 | 1 | 0.4 | 0.6 |
| E | 1 | 1 | 1 | 1 | | | 1 | 1 | 1 |
| F | 0.3 | 0.5 | 1 | 1 | 0.2 | | 1 | 0.2 | 0.2 |
| G | | | 1 | | 1 | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| H | 1 | 1 | 1 | 0.4 | 0.9 | 0.3 | 1 | | 1 |
| I | 0.6 | | 1 | 0.1 | 1 | | 1 | 1 | |

Fuente: Elaboración propia.

La observación de la matriz de adyacencia anterior proporciona una base sólida para la realización de un análisis estático detallado de las asociaciones establecidas entre los nodos o factores influyentes. Esta herramienta permite examinar exhaustivamente las relaciones interconectadas entre los elementos y, a su vez, facilita la clasificación y la identificación de los nodos o factores influyentes dentro del contexto del estudio. Dicho análisis se muestra en la Tabla 3.

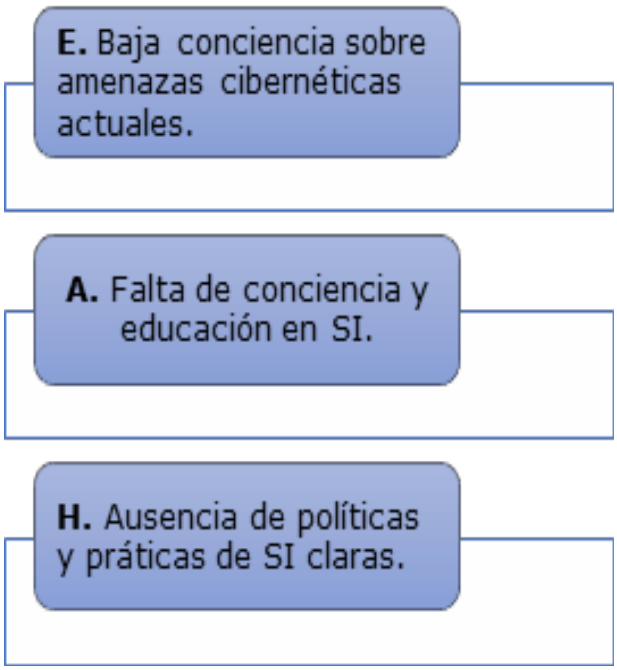
Tabla 3: Análisis estático de las asociaciones definidas y clasificación de los nodos (factores influyentes).

| Nodos | ID | OD | TD | Clasificación |
|---|---|---|---|---|
| A | 4.2 | 7.6 | 11.8 | Ordinaria |
| B | 3.9 | 7 | 10.9 | Ordinaria |
| C | 8 | 1 | 9 | Ordinaria |
| D | 4.6 | 5.2 | 9.7 | Ordinaria |
| E | 5.5 | 7 | 12.5 | Ordinaria |
| F | 1.9 | 4.4 | 6.2 | Ordinaria |
| G | 8 | 2 | 10 | Ordinaria |
| H | 4.6 | 6.6 | 11.1 | Ordinaria |
| I | 4.9 | 4.7 | 9.5 | Ordinaria |

Fuente: Elaboración propia.

Como se evidencia en el análisis de estos factores, todos se encuentran categorizados como “ordinarios”, resaltando así una intrincada interconexión entre las diversas causas identificadas. Este nivel de interdependencia es de suma importancia para comprender la complejidad de la necesidad de un programa integral de prevención de ciberdelitos en instituciones educativas de Ecuador. La naturaleza entrelazada de estos factores indica que abordar cualquier elemento de manera aislada sería insuficiente para lograr un cambio significativo. Las causas más influyentes, en orden descendente de grado de influencia, son las siguientes (Figura 3):

Fig. 3: Factores más influyentes en orden del grado de influencia.




Fuente: Elaboración propia.

Sin embargo, esta interconexión no debe verse como un obstáculo insuperable, sino como una oportunidad para desarrollar programas y estrategias educativas, debido a la naturaleza común de las causas que las generaron. Como parte de la solución a tales problemas se desarrolla un programa de prevención de ciberdelitos para instituciones educativas en Ecuador (Tabla 4). En el cual se abordan de manera integral las amenazas cibernéticas y se promueve una cultura de SI entre estudiantes, personal docente, administrativos y técnicos.

Tabla 4. Programa de prevención propuesto.

| ¨Programa de prevención de ciberdelitos para instituciones educativas en Ecuador¨ | |
|---|---|
| Objetivo general. | Implementar un programa integral de prevención de ciberdelitos en instituciones educativas en Ecuador que salvaguarde la seguridad informática y fomente el uso responsable de la tecnología. |

| | |
|---|---|
| Objetivos específicos. | Sensibilizar a la comunidad educativa sobre las amenazas cibernéticas y la importancia de la SI.<br>Proporcionar formación y recursos para mejorar la competencia digital y la conciencia de seguridad entre estudiantes y personal.<br>Establecer protocolos de seguridad para la gestión de datos sensibles y la protección de la privacidad en entornos digitales.<br>Promover prácticas seguras en línea y concienciar sobre los riesgos asociados con el uso de redes sociales y otras plataformas en línea.<br>Desarrollar estrategias de respuesta ante incidentes cibernéticos para minimizar el impacto en la institución educativa.<br>Fomentar la colaboración con autoridades locales y expertos en ciberseguridad para mantenerse actualizado sobre las amenazas emergentes.<br>Evaluar periódicamente la eficacia del programa y realizar ajustes según sea necesario. |
| Estrategias y actividades. | |
| Campañas de concientización. | Organizar sesiones de concientización sobre ciberseguridad para estudiantes, padres y personal.<br>Distribuir materiales educativos sobre prácticas seguras en línea y reconocimiento de amenazas. |
| Formación continua. | Impartir talleres y cursos de formación en ciberseguridad para docentes y personal administrativo.<br>Integrar módulos de SI en el currículo educativo. |
| Desarrollo de políticas. | Establecer políticas claras y protocolos de seguridad para la gestión de datos y el uso de dispositivos electrónicos en la institución. |
| Simulacros de seguridad. | Realizar simulacros regulares para practicar respuestas ante posibles incidentes cibernéticos. |
| Colaboración con expertos. | Establecer alianzas con profesionales de ciberseguridad y agencias gubernamentales para recibir asesoramiento y capacitación. |
| Plataforma de denuncia anónima. | Implementar un sistema de denuncia anónima para que los miembros de la comunidad educativa puedan informar posibles amenazas cibernéticas. |
| Evaluación continua. | Realizar evaluaciones periódicas para medir la eficacia del programa y realizar ajustes según los resultados obtenidos. |

Fuente: Elaboración propia.

La implementación exitosa de este programa no solo fortalece la SI en las instituciones educativas, sino que también contribuye a la formación de una generación de estudiantes conscientes y responsables en el entorno digital.

Es recomendable utilizar las redes sociales con un propósito más allá de simplemente seguir la vida de otros o participar en confrontaciones de índole política, religiosa, deportiva o social. Es crucial adoptar un enfoque adecuado, centrándose en la obtención de información. Para evitar convertirse en víctimas de ciberdelincuentes, es esencial mantener una atención constante. Si bien es posible realizar negociaciones de manera virtual, se recomienda que las transacciones se lleven a cabo de manera presencial para garantizar la seguridad en la entrega del dinero y del producto, así como para verificar el estado del mismo. Se aconseja evitar proporcionar claves, contraseñas o datos personales a través de redes sociales o llamadas telefónicas. Cambiar regularmente las contraseñas de correos electrónicos, redes sociales y tarjetas de crédito es una medida preventiva esencial. Además, se insta a no aceptar invitaciones de personas desconocidas y a no abrir enlaces de origen no reconocido, ya que estos podrían brindar acceso a cuentas personales por parte de ciberdelincuentes. Mantener los programas antivirus actualizados y verificar la seguridad de los sitios web al ingresar. Por otra parte, supervisar el uso de internet por parte de los hijos, quienes son más susceptibles a la persuasión de ciberdelincuentes, son prácticas adicionales recomendadas para fortalecer la seguridad en línea.

## CONCLUSIONES

La rápida evolución tecnológica transforma diversos aspectos de la vida cotidiana, proporcionando beneficios y oportunidades, pero también da lugar a un aumento significativo de los ciberdelitos. A pesar de las inversiones

considerables en seguridad informática, los ciberdelincuentes eluden estas medidas, generando pérdidas económicas sustanciales y obligando a los profesionales en seguridad informática a actualizarse constantemente. Los ciberdelitos presentan características particulares, como su facilidad de comisión, bajo requerimiento de recursos, ejecución sin presencia física y la explotación de lagunas de punibilidad en algunos estados. Ecuador enfrenta un aumento de ciberdelitos, con limitados recursos asignados al cuerpo policial y una disminución drástica en el presupuesto, aunque la Policía Nacional realiza esfuerzos significativos para abordar estos problemas.

Las TIC han transformado la educación, introduciendo sistemas virtuales de enseñanza que requieren una atención especial a la seguridad cibernética. A pesar de la creciente adopción de TIC en la educación ecuatoriana, se observa una falta de supervisión y conciencia sobre los riesgos cibernéticos, especialmente entre los adolescentes, que son usuarios frecuentes de estas tecnologías. El ciberacoso se manifiesta como un delito en aumento, especialmente dirigido a menores. La falta de denuncias contribuye a la falta de medidas legales y educativas para combatir este problema. Se identifican múltiples obstáculos en la Unidad educativa "Siete de Octubre", desde la falta de conciencia hasta la ausencia de políticas claras y medidas de seguridad. Se enfatiza la importancia de la conciencia digital, la formación continua en ciberseguridad y la implementación de medidas específicas para abordar los desafíos en la prevención de ciberdelitos en el ámbito educativo. La implementación exitosa del programa no solo fortalece la seguridad informática en instituciones educativas, sino que también contribuye a la formación de una generación consciente y responsable en el entorno digital.

## *REFERENCIAS BIBLIOGRÁFICAS*


Ayyoub, H. (2022). Awareness of electronic crimes related to E-learning among students at the University of Jordan. ***Heliyon***, ***8***(10), e10897. https://doi.org/10.1016/j.heliyon.2022.e10897

Fernández, J. (2015). Hábitos de uso y conductas de riesgo en Internet en la preadolescencia. ***Comunicar: Revista Científica de Comunicación y Educación***, ***22***(44), 113–121. https://www.revistacomunicar.com/index.php?contenido=detalles&numero=44&articulo=44-2015-12

Finol, M. (2020). Paradigmas, enfoques y métodos de investigación: análisis teórico. ***Mundo Recursivo***, ***3***(1), 1–24. https://atlantic.edu.ec/ojs/index.php/mundor/article/view/38

Hatwágner, M. (2018). Two-stage learning based fuzzy cognitive maps reduction approach. ***IEEE Transactions on Fuzzy Systems***, ***26***(5), 2938–2952. https://ieeexplore.ieee.org/abstract/document/8259309

Hernández, R. (2018). ***Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.*** México: Mc Graw Hill Education. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/SampieriLasRutas.pdf

Jin, L. (2023). The impact of internet use in the digital age on the subjective well-being of older adults -- an empirical study based on CGSS2021 data. ***Heliyon***, ***9***(11), e21528. https://www.sciencedirect.com/science/article/pii/S2405844023087364

Macía, R. (2022). Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática. ***Sapienza: International Journal of Interdisciplinary Studies***, ***3***(2), 231–243. https://www.journals.sapienzaeditorial.com/index.php/SIJIS/article/view/324

Mar Cornelio, O. (2020). Operador por selección para la agregación de información en Mapa Cognitivo Difuso. ***Revista Cubana de Ciencias Informáticas***, ***14***(1), 20–39. http://scielo.sld.cu/scielo.php?pid=S2227-18992020000100020&script=sci_arttext

Molina, T. (2019). Base de conocimiento en línea como recurso jurídico-educativo para la prevención del ciberacoso sexual en adolescentes ecuatorianos. ***Dilemas Contemporáneos: Educación, Política y Valores***, ***74***(Edición Especial), 1–24. https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/1385

Nakano, T. (2013). La integración de las TIC en la educación superior: reflexiones y aprendizajes a partir de la experiencia PUCP. ***En Blanco y Negro***, ***4***(2), 1–12. https://revistas.pucp.edu.pe/index.php/enblancoynegro/article/view/8936

Orozco, J. (2018). El Marco Metodológico en la investigación cualitativa. Experiencia de un trabajo de tesis doctoral. ***Revista Científica de FAREM-Estelí***, ***7***(27), 25–37. https://rcientificaesteli.unan.edu.ni/index.php/rcientifica/article/view/1440

Ortiz, N. (2019). Normativa legal sobre delitos informáticos en Ecuador. ***Revista Científica Hallazgos21***, ***4***(1), 100–111. https://dialnet.unirioja.es/servlet/articulo?codigo=7148227

Pascagaza, E. (2022). Redes sociales y construcción de la ciudadanía digital. ***Revista Boletín Redipe***, ***11***(9), 163–177. https://revista.redipe.org/index.php/1/article/view/1888

Quezada, P. (2022). Sobreexposición de adolescentes a Ciberdelitos en el Ecuador. ***Revista Ibérica de Sistemas e Tecnologias de Informação***, ***E54***, 419–435. https://www.proquest.com/openview/842ba867d3c582d682ae340ea7d29748/1?pq-origsite=gscholar&cbl=1006393

Recalde, J. (2021). ***El ciberacoso por redes sociales en el Ecuador***. [Trabajo de grado previo a la obtención del título de: Ingeniero de sistemas. Universidad Politécnica Salesiana Sede Guayaquil]. https://dspace.ups.edu.ec/bitstream/123456789/20945/1/UPS-GT003383.pdf

Subijana, I. (2008). El ciberterrorismo: Una perspectiva legal y judicial. ***Dialnet***, ***22***, 169–187. https://addi.ehu.es/handle/10810/24999

Tamayo, S. (2023). Preparación policial para responder al delito informático en Ecuador. ***PODIUM***, ***44***, 17–36. https://revistas.uees.edu.ec/index.php/Podium/article/view/1072

Wright, D. (2023). Assessing the socio-economic impacts of cybercrime. ***Societal Impacts***, ***1***(1), 100013. https://www.sciencedirect.com/science/article/pii/S2949697723000139