https://repository.uaeh.edu.mx/revistas/index.php/investigium/issue/archive

Boletín Científico INVESTIGIUM de la Escuela Superior de Tizayuca

Publicación semestral, Vol. 10, No. 20 (2025) 8-17

InvESTigium

ISSN: 2448-4830

Riesgo cibernético en el entorno educativo de la Escuela Superior de Tizayuca

Cyber risk in the educational environment of Superior School of Tizayuca

Myriam Coronado-Meneses [a], *Maribel González-Cadena* [b], *Víctor H. Guadarrama-Atrizco* [c], *Elba M. Pedraza-Amador* [d], *Mayra A. Valerio Nolasco* [e], Maribel Navarro-Gálvez [f]

Abstract:

To strengthen their academic training, students need access to online digital tools; in addition, the COVID-19 health emergency affected all systems. Faced with this scenario, educational institutions reoriented their teaching-learning activities to serve their students during the emergency. The International Telecommunication Union reports that the use of the Internet, applications and virtual environments increased by up to 50%, and policies and strategies for access to online resources were developed. In Mexico, the General Education Law (LGE, 2019) indicates that educational training must take into account "the use of information, communication, knowledge and digital learning technologies to strengthen the development of skills" and establishes that the Digital Education Agenda includes guidelines for their responsible use.Similarly, the Ministry of Communications and Transportation is establishing a cybersecurity guide, as the use of telecommunications networks and devices increases students' exposure to online risks.

This research, which diagnoses the cybernetic risk in the educational environment of the students of the Bachelor's Degree in Information Technologies at ESTi, is constituted with the methodology of Context, Input, Process and Product of Stufflebeam (1987) in four stages that take into account the policies, the capacity of the institution and the perception of the students regarding cybernetic risks.

The results show that students are mainly exposed to fraud, malicious code in technological devices, cyberbullying in online games, unwanted sexting, information that generates fear and annoying links or links with inappropriate content. It also shows that students share personal information, accept friends without knowing them, and have met in the real world with friends they made online.

Keywords:

Cybersecurity, *Competencies, Cyber threats, CIPP Methodology*

Resumen:

Para fortalecer su formación académica, los alumnos necesitan acceso a herramientas digitales en línea; aunado a ello, la emergencia sanitaria por COVID-19 impactó a todos los sistemas. Ante este panorama, las instituciones educativas reorientaron sus acciones de enseñanza-aprendizaje para atender a sus alumnos durante la contingencia. La Unión Internacional de Telecomunicaciones señala que el uso de internet, de aplicaciones y de entornos virtuales, se incrementó hasta un 50% y elaboró políticas y estrategias para el acceso a recursos disponibles en línea. En México, la Ley General de Educación (LGE, 2019) indica que la formación educativa debe considerar “el empleo de tecnologías de la información, comunicación, conocimiento y aprendizaje digital con la finalidad de fortalecer el desarrollo de habilidades” y establece que la Agenda Digital Educativa incluya directrices para su uso responsable; de igual manera, la Secretaría de Comunicaciones y Transportes establece una guía de Ciberseguridad debido a que, con el uso de redes y dispositivos de telecomunicaciones, se incrementa la exposición de los estudiantes a riesgos en línea.

Esta investigación, que diagnostica el riesgo cibernético en el entorno educativo de los alumnos de la Licenciatura en Tecnologías de Información de la ESTi, se constituye con la metodología basada en el Modelo de Evaluación de Contexto, Entrada, Proceso y

[a] Universidad Autónoma del Estado de Hidalgo | Escuela Superior de Tizayuca | Tizayuca, Hidalgo | México, https://orcid.org/0000-0003-0818-0897, Email: myriam_coronado3187@uaeh.edu.mx; [b] https://orcid.org/0000-0001-5371-0442, Email: maribel_gonzalez4257@uaeh.edu.mx; [c] https://orcid.org/0000-0001-9125-7677, Email: victor_guadarrama@uaeh.edu.mx; [d] https://orcid.org/0000-0002-7182-2437, Email: elbam@uaeh.edu.mx; [e] https://orcid.org/0000-0003-2155-1250, Email: mayra_valerio@uaeh.edu.mx; [f] https://orcid.org/0000-0001-5723-0817, Email: maribel_navarro4807@uaeh.edu.mx

Fecha de recepción: 08/04/2024, Fecha de aceptación: 04/06/2024, Fecha de publicación: 05/01/2025

DOI: https://doi.org/10.29057/est.v10i20.12683

Producto (CIPP) de Stufflebeam (1987) en cuatro etapas que consideran políticas, capacidad de la institución y la percepción de los estudiantes respecto a riesgos cibernéticos.

Los resultados exhiben que los alumnos están expuestos, principalmente, a fraudes, códigos maliciosos en dispositivos tecnológicos, ciberacoso en juegos en línea, sexting no deseado, información que genera miedo y enlaces molestos o con contenido inadecuado. De igual manera, se identifica que los estudiantes comparten información personal, aceptan amigos sin conocerlos y que se han reunido en el mundo real con amigos hechos en línea.

***Palabras Clave**:*

Ciberseguridad, Competencias, Amenazas cibernéticas, Metodología CIPP.

Introducción

Planteamiento del problema

La aplicación de las Tecnologías de la Información y las Comunicaciones (TIC) en el sector educativo se ha popularizado; de acuerdo con la Unión Internacional de Telecomunicaciones (2009), los usuarios de Internet en el mundo incrementaron considerablemente, de un 16% en 2005 a un 66% en 2022 (UNESCO, 2023). En la Agenda 2030, en el Objetivo de Desarrollo Sostenible (ODS) 4, que persigue garantizar una educación inclusiva, equitativa y de calidad y promover oportunidades de aprendizaje durante toda la vida para todos, establece compromisos globales para incrementar el porcentaje de jóvenes y adultos con conocimientos de TIC (UNESCO, 2022).

Derivado de los retos educativos para el uso de la tecnología, aunados a las metas del ODS 4, las instituciones educativas han adoptado el manejo de herramientas digitales para fortalecer sus procesos de formación; además, la pandemia de COVID-19 condujo al cierre de escuelas y a la adecuación de los entornos de enseñanza presenciales a entornos híbridos y virtuales; lo anterior, incrementó de manera drástica el acceso de la población escolar a recursos digitales de enseñanza-aprendizaje-evaluación. En el Informe Mundial de Seguimiento de la Educación 2023, se reconoce que existen desafíos del uso apropiado de la tecnología, dado que muchas de ellas no fueron diseñadas para la enseñanza y el constante cambio tecnológico dificulta la adaptación de los sistemas educativos, sumado a que el personal docente suele sentirse con baja capacitación sobre la incorporación de las TIC en el desarrollo de competencias y en conocimientos de ciberseguridad (GEM, 2023).

En este contexto, el Índice de Civilidad Digital de Microsoft señala que de 2016 a 2020 se incrementó, a nivel global, la incivilidad en línea que perciben los usuarios cotidianos de redes sociales (ICD, 2020). De acuerdo con la Secretaría de Comunicaciones y Transportes (SCT, 2020), la mayor dependencia y uso cotidiano de las comunicaciones y tecnologías de la información en el ámbito educativo incrementa la exposición de los estudiantes y docentes a riesgos en línea y amenazas de ciberseguridad (GEM, 2023).

De acuerdo con el Semáforo Delictivo, la incidencia de extorsión en el Estado de Hidalgo se encuentra por arriba de la media nacional y en el año 2023 ha incrementado en un 50% en comparación con el año 2022 (Semáforo Delictivo, 2023).

Justificación

La mayor dependencia de los entornos educativos a las Tecnologías de la Información y la Comunicación incrementa la exposición de Niñas, Niños y Adolescentes (NNA), jóvenes estudiantes y docentes a amenazas y riesgos en línea. En este contexto, la Secretaría de Comunicaciones y Transportes (SCT) advierte que la comunidad educativa se encuentra en un entorno propicio y exposición de ciberseguridad; por lo anterior, emite la Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo a la educación, con el objetivo de prevenir incidentes de ciberseguridad.

De igual forma, el Foro Económico Mundial manifiesta que se debe incrementar la importancia de la ciberseguridad y recomienda que las organizaciones deben tener medidas prácticas respecto a intensificar las normas de higiene digital, ser cuidadoso en la verificación de fuentes fiables y asegurarse de actualizar regularmente el software y las aplicaciones oficiales (FEM, 2020).

Por su parte, el Código de Conducta de las Autoridades y el Personal de la Universidad Autónoma del Estado de Hidalgo (2019) indica, en el apartado de Conductas y prohibiciones, que las autoridades y el personal están obligados a prevenir y combatir el hostigamiento, el acoso sexual, la discriminación y la violencia, así como de:

> Abstenerse de difundir, compartir, entregar o reenviar a otra persona, sin que exista consentimiento, aceptación o bienvenida previa de quien lo reciba, por cualquier medio, incluidos los digitales, electrónicos y redes sociales, videos o imágenes personales de carácter sexual o erótico explícito (UAEH, 2019).

En este contexto la Dirección de Superación Académica de la UAEH, por medio del Programa Estratégico de Formación Integral Permanente del Personal Académico (PROEFI), es la encargada de brindar capacitación a los docentes de la institución. En su página se puede apreciar que oferta 11 cursos en el área de tecnologías de la información y la comunicación; no obstante, la diversificación de opciones, en el listado no se encuentra capacitación sobre seguridad digital.

Por lo anterior y al ser parte de la formación del alumnado, se considera relevante realizar un diagnóstico sobre los riesgos y amenazas más comunes en el ámbito escolar con la finalidad de coadyuvar a promover información sobre medidas de prevención de incidentes digitales.

Objetivo general

Diagnosticar el riesgo cibernético en el entorno educativo de los alumnos de la Licenciatura en Tecnologías de Información de la Escuela Superior de Tizayuca.

Materiales y métodos

Esta investigación, que diagnostica el riesgo cibernético en el entorno educativo de los alumnos de la Licenciatura en Tecnologías de Información de la ESTi, se constituye con la metodología de Contexto, Entrada, Proceso y Producto de Daniel Stufflebeam (1987). En la etapa de Contexto, se considera investigación documental de políticas y contextos globales respecto a ciberseguridad; en la etapa de Entrada, se valora la capacidad de la institución respecto al tema de estudio y, por último, en las etapas de Proceso y de Producto, se diseñó y aplicó un instrumento de investigación que brinda información primaria sobre la percepción de los estudiantes respecto a riesgo cibernético en el ámbito educativo.

MARCO TEÓRICO – CONTEXTUAL

1.1 Ciberseguridad

La ciberseguridad protege los dispositivos que todos usamos y los servicios a los que accedemos en línea, tanto en la casa y en la escuela como en el trabajo. A través de ella se busca evitar el acceso no autorizado a la información personal que almacenamos en estos dispositivos y en línea.
De acuerdo con la Guía de ciberseguridad para los países en desarrollo, el objetivo principal de la ciberseguridad es garantizar que ningún agravio ponga en riesgo las actividades de la organización y de los individuos al reducir los inconvenientes inducidos por amenazas, ataques o siniestros que deriven en problemas de funcionamiento y costos (SCT, 2020).

1.2 Competencias

Se considera a Chomsky (1965), quien trabajó la competencia lingüística desde una perspectiva de la Psicología Cognitiva, como el autor que inició el estudio y el uso del término, quien refirió a las competencias como “un conocimiento organizado que se actualiza en situaciones concretas, teniéndolas como una representación, un conocimiento implícito en la actuación que se utiliza en ella” (citado por Guzmán & Campos, 2009).

De formación en la educación superior.

Manjón & López (citados por Pelayo, 2012) refieren que mediante la educación superior se adquieren competencias profesionales, mismas que incrementan la posibilidad de los individuos a conseguir un empleo por medio de criterios académicos y calificación profesional que responda a lo que el mercado laboral requiere.

Competencias digitales.

Las tecnologías emergentes generan nuevas exigencias de alfabetización digital, por lo que es importante tener en cuenta los conocimientos, habilidades y actitudes que requiere la población para mejorar sus capacidades ante la transformación digital. En este contexto, el Centro de Investigaciones Comunes de la Comisión Europea proporciona una base que coadyuva al desarrollo y medición del concepto desde el punto de vista tecnológico (ECJRC, 2022):

La competencia digital implica el uso seguro, crítico y responsable de las tecnologías digitales para el aprendizaje en el trabajo y para la participación en la sociedad, así como la interacción con éstas. Incluye la búsqueda y gestión de información y datos, la comunicación y la colaboración, la creación de contenidos digitales (incluida la programación), la seguridad (incluido el bienestar digital y las competencias relacionadas con la ciberseguridad) y la resolución de problemas.

1.3 Amenazas cibernéticas

Se consideran riesgos y amenazas de ciberseguridad aquellas que están asociadas al uso de las redes y los dispositivos de telecomunicaciones. De acuerdo con la Secretaría de Comunicaciones y Transportes (2020), las amenazas más comunes a la ciberseguridad de la comunidad educativa son:

•Malware, también conocido como código malicioso o de programa maligno, entre los que se encuentran virus, gusanos, troyanos, principalmente.

•Phishing, el cual aglutina ataques a través del correo electrónico por un delincuente pretendiendo ser otra persona.

•Smishing, que se genera al recibir mensaje de texto corto (SMS) para llamar a un número de teléfono o ir a un sitio web.

•Vishing, que es una estafa mediante una llamada que, suplantando la identidad de una persona, solicita información privada o realizar alguna acción en contra de la víctima.

•Online grooming, que aglutina actividades de acoso sexual en línea e implica la interacción de un adulto con jóvenes para ganarse su confianza e involucrarlos en alguna actividad sexual.

•Cyberbullying o ciberacoso, el cual implica publicar o compartir información personal o privada que cause vergüenza o humillación en Redes sociales, Mensajería, Teleconferencias, Foros en línea y Salas de chat, Correo electrónico, Comunidades de juegos en línea, por tener alguna discapacidad y por ser percibido como diferente.

•Sexting, el cual se genera al solicitar envío de contenidos de tipo sexual, principalmente fotografías y/o videos.

1.4 Metodología basada en el Modelo de Evaluación de Contexto, Entrada, Proceso y Producto (CIPP) de Stufflebeam (1987)

El Modelo de Evaluación de Contexto, Entrada, Proceso y Producto es una alternativa para realizar evaluaciones que contempla, como propósito más importante, no sólo el demostrar sino el perfeccionar para que los programas a enjuiciar sean mejores a la gente a quien deben servir o, en su caso, eliminarlos si se consideran innecesarios. Básicamente el modelo se utiliza para ayudar a los directivos y personal de una institución a obtener y utilizar datos sistemáticos con el afán de promover el desarrollo de la organización (Stufflebeam & Shinkfield, 1987).

Existen diferentes conceptualizaciones sobre el término de evaluación, Scriven (como se citó en Stufflebeam & Shinkfield, 1987) se refiere al concepto como “la valoración sistemática del valor o del mérito de las cosas” en donde es importante no sólo que la evaluación determine si las metas han sido alcanzadas o no sino también, y más importante aún, el evaluar si contribuyen al bienestar de los consumidores ya que los objetivos propuestos pueden atender a fines inmorales, ser limitados o tener consecuencias críticas.

La etapa de Contexto identifica la población objeto de estudio; el propósito general de la etapa de Entrada es identificar y valorar la capacidad del sistema en el que se desenvuelve el objeto con la finalidad de que las estrategias a considerar sean acordes al contexto; por su parte, la etapa de Proceso proporciona información sobre el eficiente uso de los recursos disponibles e identifica defectos de la planificación y realización del procedimiento; por último, la etapa de Producto valora, interpreta y enjuicia el rendimiento del programa educativo con la finalidad de obtener un indicador de satisfacción a las necesidades de los grupos a los que pretende servir.

LA ESCUELA SUPERIOR DE TIZAYUCA DE LA UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

La Escuela Superior de Tizayuca (ESTi) está ubicada en el municipio de Tizayuca, Hgo. Empezó a operar en julio de 2001 con dos programas educativos. Actualmente, oferta la Maestría en Gestión y Desarrollo de Nuevas Tecnologías, la Licenciatura en Turismo, la Ingeniería en Automatización Industrial, la Licenciatura en Tecnologías de la Información y Bachillerato.

El Modelo Curricular Integral de la UAEH (2010), que supedita a los programas educativos de la institución, considera dos tipos de competencias: las genéricas y las específicas. Las competencias genéricas que promueve la institución educativa y que deben tener sus profesionistas son siete: Formación, Liderazgo colaborativo, Comunicación, Creatividad, Pensamiento crítico, Uso de la tecnología y Ciudadanía; son independientes del área de estudio y se pueden formar en cualquier profesión. Las competencias específicas son trascendentales para cualquier titulación, ya que confieren identidad y consistencia a las diferentes disciplinas.

Para propósito de este documento se hará énfasis en la competencia genérica de Uso de la Tecnología.

2.1 Plan de estudios de la Licenciatura en Tecnologías de la Información.

En el año 2017 la División de Docencia, de la Universidad Autónoma del Estado de Hidalgo, realizó estudios de pertinencia y factibilidad que fundamentaron al programa educativo de la Licenciatura en Tecnologías de la Información para formar egresados que contribuyan a potenciar esta actividad en el Estado de Hidalgo (UAEH, 2017). En dicho documento se incorporan preceptos conforme a lo que dicta tanto el Modelo Educativo como el Modelo Curricular Integral de la UAEH para la educación superior; los cuales, exponen las características genéricas que definen a un profesionista y que son determinantes para la integración del sujeto, mismas que se especifican en conocimientos, habilidades, actitudes, aptitudes y valores (UAEH, 2010) como se aprecia en la Tabla 1.

Tabla 1. Indicadores de formación en la competencia genérica de Uso de la Tecnología

Nivel	Indicadores
1	1. Identifican las diversas tecnologías de la información y comunicación (TIC's) con aplicación en el campo profesional y social. 2. Utilizan las TIC's como herramientas de apoyo en el desarrollo de los contenidos básicos (Sistemas operativos básicos y software de aplicación, entre otros).
2	1. Desarrollan apropiadamente las aplicaciones específicas del aprendizaje, la comunicación, el área disciplinar y la investigación, como herramientas de apoyo.
3	1. Aplican la tecnología de la información y la comunicación como herramientas de apoyo para la solución de problemas del campo profesional y social.

Fuente: Modelo Curricular de la UAEH (2010).

El Perfil de egreso que caracteriza al Licenciado en Tecnologías de la Información es el siguiente (UAEH, 2023):

•Competitivo en el análisis, diseño y desarrollo de sistemas informáticos complejos, empleando tecnologías de la información vanguardistas, que le permiten dar solución a problemas del área de manera efectiva cumpliendo estándares de calidad.

•Desarrolla y evalúa proyectos sustentables que contribuyan en el crecimiento económico y social del país.

•Posee conocimientos y habilidades sobre la creación de aplicaciones, el manejo y la administración de información a través de bases de datos garantizando seguridad e integridad de la información.

•Analiza, administra y evalúa proyectos tecnológicos.

•Administra e implementa tecnología de redes.

INVESTIGACIÓN DE CAMPO

Este trabajo tiene el objetivo de diagnosticar el riesgo cibernético en el entorno educativo de los alumnos de la Licenciatura en Tecnologías de Información de la ESTi. La investigación que aglutina este apartado contempla, en primer lugar, el procedimiento con el que se integró el instrumento de investigación y la muestra de alumnos a quienes se les aplicó dicho cuestionario; en segundo lugar, se presentan los resultados de la aplicación de cuestionario a los alumnos del programa educativo en los meses de agosto y septiembre del año 2023.

3.1 Instrumento de investigación

El instrumento de investigación que se presenta en este apartado se diseña con las sugerencias de Brown (1980) quien señala que, al aplicar una prueba a una muestra representativa de sujetos, debe haber consistencia en los resultados de ésta. El cuestionario se constituyó por bloques de ítems que aglutinan extracto de aspectos importantes en:

•La Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo a la educación, de la Secretaría de Comunicaciones y Transportes (SCT, 2020).

•Las Directrices de Protección de la Infancia en Línea, de la Unión Internacional de Telecomunicaciones (UIT, 2009).

3.2 Población y muestra.

Hernández, Fernández y Baptista (2010) definen como unidades de análisis a los individuos u organizaciones que son sujetos de estudio. En atención al objetivo de investigación, la población se constituyó por parte de los alumnos de la Escuela Superior de Tizayuca y las unidades de análisis que se examinaron en este estudio son los alumnos adscritos a la Licenciatura en Tecnologías de la Información.

Para determinar el tamaño de la muestra en poblaciones finitas se adoptaron las recomendaciones de Castañeda, De la Torre, Morán y Lara (2002) y se optó por tolerar un porcentaje de error del 4% con un nivel de confianza del 95% para aplicar en la ecuación propuesta por los autores:

$$n = \frac{Z^2 pqN}{Ne^2 + Z^2 pq}$$

En donde:
n= tamaño de la muestra
Z^2= nivel de confianza
p= variabilidad positiva
q= variabilidad negativa
N= tamaño de la población
e^2= precisión o error

Al aplicar la ecuación se determinó el tamaño de la muestra como se aprecia en la Tabla 2.

1. 116 alumnos de la Licenciatura en Tecnologías de la Información

$$n = \frac{(1.96)^2\,(.95)(.05)(116)}{(116)(.04)^2 + (1.96)^2\,(.95).05)}$$

Tabla 2. Muestra de unidad de análisis para aplicación del instrumento

Unidad de análisis	Tamaño de la población	Tamaño de la muestra
Alumnos de la LTI	116	58

Fuente: Elaboración propia.

Dentro de las formas de medir la confiabilidad en las pruebas se encuentra la del coeficiente de confiabilidad Alfa de Cronbach, la cual puede oscilar entre 0.00 y 1.00 y no existe un acuerdo unánime sobre los valores aceptables como mínimo entre los científicos. De Vellis (como se citó en Landero & González, 2006) sugiere niveles de confiabilidad aceptables en los instrumentos de medición y considera un nivel de 0.80 a 0.90 como “muy bueno”.

El instrumento que se aplica a las unidades de análisis posee una consistencia interna de 0.90 con el coeficiente Alfa de Cronbach.

3.3 Principales resultados

3.3.1 Contexto

En esta etapa, para identificar el objeto de estudio, se realiza exploración documental que se presenta en el apartado de marco teórico-referencial sobre:

Las directrices para prevenir riesgos y enfrentar amenazas de ciberseguridad que emanan de la Unión Internacional de Telecomunicaciones, en el marco de la Protección de la Infancia el Línea (COP) del cual se decide tomar un apartado de recomendaciones, derivado de que en el primer semestre del programa educativo, algunos alumnos manifestaron ser menores de edad; así como de la Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo a la educación.

El Marco de Competencias Digitales para la Ciudadanía que propone el Centro de Investigaciones Comunes de la Comisión Europea en el apartado de Seguridad y que aglutinan conocimientos, habilidades y actitudes para prevenir riesgos y amenazas en los entornos digitales.

3.3.2 Entrada

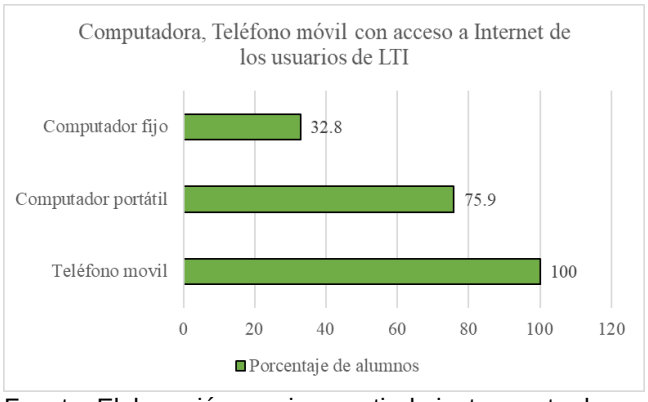
En esta segunda etapa se identifican los recursos de la Licenciatura en Tecnologías de la Información para llevar a cabo la encomienda del objetivo de estudio; por consiguiente, se desarrollaron tres categorías:

La categoría formación profesional identificó, con investigación documental expuesta en el apartado dos, denominado Plan de estudios de la Licenciatura en Tecnologías de la Información, las facultades de la institución educativa en materia de formación de competencias genéricas y de perfil de egreso.

La categoría socio demográfica proporciona la distribución de las unidades de análisis por edad y sexo. Respecto a la proporción de los alumnos por sexo, se encuentra que el 24.1% son mujeres y el 75.9% son hombres. Respecto a la edad, el 48.3% los alumnos tienen entre 18 y 21 años, 43.1% tienen de 22 a 25 años y el 8.6% son menores de 18 años.

Por último, de los alumnos encuestados, el teléfono móvil es el aparato con mayor nivel de adopción (100%); además, el 75.9% de los alumnos, también poseen computadora portátil y el 32.8% de ellos indicó poseer también computador fijo.

Figura 1. Adopción de Computadora, Teléfono móvil e Internet de los usuarios de TIC



Fuente: Elaboración propia a partir de instrumento de investigación

3.3.3 Proceso

Para diagnosticar los riesgos en línea y amenazas de ciberseguridad a los que se han enfrentado los alumnos de la Licenciatura en Tecnologías de la Información con el uso de las tecnologías digitales, la aplicación de instrumento de investigación proporcionó los siguientes resultados:

A. Variables de la protección en línea.

Como se aprecia en la Tabla 3. Dentro de los factores positivos de esta variable, se encuentra que el 63.8% de los alumnos utiliza y actualiza el antivirus con regularidad y el 77.6% utiliza contraseñas a fin de restringir acceso a personas no autorizadas; sin embargo, 41.4% de ellos han encontrado contenido pornográfico o inadecuado y al 46.6% le han ofrecido regalos o dinero al realizar búsquedas sobre actividades académicas.

Tabla 3. Variables de la protección en línea		Alumnos	
		Total No.	Total Porcentaje
Utiliza y actualiza el Antivirus	Si	37	63.8%
	No	21	36.2%
Cambia las contraseñas establecidas de manera predeterminada	Si	21	36.2%
	No	37	63.8%
Utiliza contraseñas en dispositivos y cuentas a fin de restringir acceso a personas no autorizadas	Si	45	77.6%
	No	13	22.4%
Ha encontrado contenido pornográfico o inadecuado al realizar búsquedas sobre actividades académicas	Si	24	41.4%
	No	34	58.6%
Le han ofrecido regalos o dinero al realizar búsquedas sobre actividades académicas	Si	27	46.6%
	No	31	53.4%

Fuente: elaboración propia a partir de instrumento de investigación

B. Amenazas más comunes a la ciberseguridad de los alumnos

En este apartado, como se muestra en la Tabla 4, prevalece que la mitad de los alumnos ha padecido amenazas de Smishing, el 43.1% ha tenido afectaciones en sus dispositivos tecnológicos con códigos maliciosos y el 41.4% revela que tuvo amenaza de Vishing. Cabe resaltar que 2 de cada 10 alumnos refieren acoso sexual en línea.

Tabla 4. Amenazas más comunes a la ciberseguridad los alumnos.		Alumnos	
		Total No.	Total Porcentaje
Códigos maliciosos o de programa maligno (virus, gusanos, troyanos, etc.)	Si	25	43.1%
	No	33	56.9%
*Phishing (*ataque a través del correo electrónico por un delincuente pretendiendo ser otra persona)	Si	17	29.3%
	No	41	70.7%
*Smishing (*recibir mensaje de texto corto (SMS) para llamar a un número de teléfono o ir a un sitio web	Si	30	51.7%
	No	28	48.3%
*Vishing (*estafa mediante llamada que suplantando la identidad de una persona solicita información privada o realizar alguna acción en contra de la víctima)	Si	24	41.4%
	No	34	58.6%
*Online grooming (*acoso sexual en línea que implica la interacción de un adulto con jóvenes para ganarse su confianza e involucrarlos en alguna actividad sexual)	Si	11	19.0%
	No	47	81.0%

Fuente: elaboración propia a partir de instrumento de investigación

C. Cyberbullying o ciberacoso

Como se aprecia en la Tabla 5, los estudiantes han estado expuestos al contacto con depredadores en línea; de acuerdo con los resultados, prevaleció que 43.1% de los alumnos ha recibido contenido dañino hacia su persona, principalmente, en comunidades de juegos en línea y que en igual porcentaje ha padecido Sexting.

Tabla 5. *Cyberbullying* o ciberacoso (publicar o compartir información personal que cause vergüenza o humillación) en:		Alumnos	
		Total No.	Total Porcentaje
Redes sociales	Si	8	13.8%
	No	50	86.2%
Mensajería	Si	3	5.2%
	No	55	94.8%
Teleconferencias, foros en línea y salas de chat	Si	2	3.4%
	No	56	96.5%
Comunidades de juegos en línea	Si	25	43.1%
	No	33	56.9%
Por tener alguna discapacidad	Si	1	1.7%
	No	57	98.3%
Por ser percibido como diferente	Si	8	13.8%
	No	50	86.2%

Sexting (solicitar o enviar contenidos de tipo sexual, principalmente fotografías y/o videos)	Si	25	43.1%
	No	33	56.9%

Fuente: elaboración propia a partir de instrumento de investigación

D. Acceso a contenido potencialmente dañino o ilegal. Los resultados de investigación exhiben que 4 de cada 10 alumnos ha:

- Estado expuesto a información errónea que podría generarles miedo y ansiedad
- Recibido contenido potencialmente dañino que incita a que atenten contra su propia integridad como el suicidio, la autolesión o a desórdenes como la bulimia, anorexia u otras conductas violentas.
- Recibido mercadotecnia en línea que promueve alimentos poco saludables, estereotipos de género o resulta inapropiada para la edad
- 32.8% manifiesta que estuvo expuesto a información que incita al racismo o a la violencia.

E. Recomendaciones de ciberseguridad para el uso seguro de las redes y dispositivos de telecomunicaciones en apoyo a la educación

Siete de cada 10 alumnos cierran la sesión de la nube al concluir sus actividades, usan carpetas con contraseña y acceso restringido y utilizan contraseñas robustas para su acceso, respectivamente. El 65.5% respalda periódicamente su información almacenada y el 58.6% deshabilita enlaces y accesos no necesarios de carpetas.

Respecto a las actividades de educación en línea y los alumnos que utilizan las redes sociales, la Tabla 6 exhibe que el 91.4% percibe un ambiente de respeto, el 69% manifiesta que se mantiene un perfil u orientación académica y el 63.8% refiere que se publica información sólo relativa a las actividades educativas.

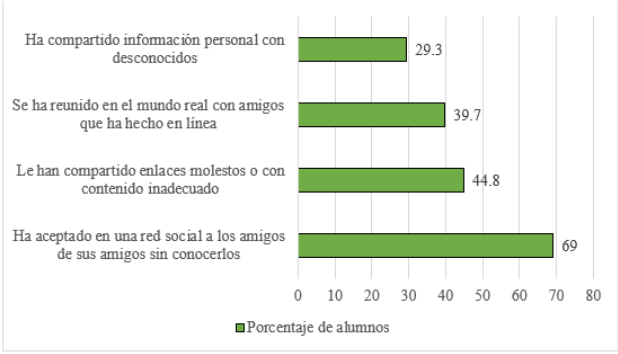
Tabla 6. Respecto a las actividades de educación en línea, al hacer uso de redes sociales para impartir o complementar clases		Alumnos	
		Total No.	Total Porcentaje
Se mantiene un perfil u orientación académica	Si	40	69.0%
	No	18	31.0%
Se publica información sólo relativa a las actividades educativas	Si	37	63.8%
	No	21	36.2%
Se respeta la opinión de los demás y se aceptan los diferentes puntos de vista	Si	53	91.4%
	No	5	8.6%

Fuente: elaboración propia a partir de instrumento de investigación

Por último, la conexión en línea permite a los alumnos comunicarse con personas que no conocen en el mundo real y, por lo anterior, son susceptibles de aceptar invitaciones o amistades; en este contexto, como se exhibe en la Figura 2, los resultados refieren que:

- El 69.0% ha aceptado en una red social a los amigos de sus amigos sin conocerlos
- Al 44.8% le han compartido enlaces molestos o con contenido inadecuado
- 39.7% se ha reunido en el mundo real con amigos que ha hecho en línea
- El 29.3% ha compartido información personal con desconocidos

Figura 2. Comunicación con personas que no conoce en el mundo real



Fuente: elaboración propia a partir de instrumento de investigación

CONCLUSIONES

La educación en línea ofrece posibilidades infinitas de acceso a contenido digital y representa una oportunidad innovadora para el desarrollo de competencias; no obstante, es importante sensibilizar a la comunidad educativa de los riesgos y amenazas que existen en línea.

Esta investigación que tiene por objetivo diagnosticar el riesgo cibernético en el entorno educativo de los alumnos de la Licenciatura en Tecnologías de Información, de la Escuela Superior de Tizayuca, se constituyó con la metodología CIPP de Daniel Stufflebeam (1987). Los resultados conducen a las siguientes conclusiones:

Respecto al uso de las redes y dispositivos de telecomunicaciones en apoyo a la educación:

Factores que coadyuvan a mantener la ciberseguridad de los alumnos:

- Los alumnos manifiestan que nueve de cada diez docentes brindan respeto y mantienen un perfil orientado a la educación al hacer uso de redes sociales en las actividades de educación.
- Mas del 70% de los alumnos mantienen los dispositivos electrónicos, las carpetas digitales y las sesiones de la nube con uso de contraseñas seguras, a fin de restringir el acceso a personas no autorizadas.
- Seis de cada diez alumnos realizan periódicamente un respaldo de la información almacenada.

Amenazas de ciberseguridad que han padecido los alumnos de la LTI:

- La mitad de los alumnos ha recibido amenazas relacionadas con la ingeniería social como el Smishing (recibir mensaje de texto solicitando llamar a un número de teléfono o ir a un sitio web) y fraudes.
- Cuatro de cada diez alumnos han visto afectados sus dispositivos electrónicos con amenazas de malware (código malicioso).
- Cuatro de cada diez alumnos han recibido ciberacoso de comportamientos ilegales en comunidades de juegos en línea, sexting no deseado e información errónea que podría generar miedo y ansiedad.
- Cuatro de cada diez alumnos han encontrado contenido pornográfico o inadecuado al realizar búsquedas sobre actividades académicas.

Amenazas que se consideran prioritarias de abordar:

Además de la incidencia de exposición de los alumnos a delitos de ciberseguridad, existen variables de riesgo que comprometen su seguridad física, ya que los resultados de investigación exhiben que:

- Siete de cada diez alumnos han aceptado amigos en alguna red social sin conocerlos.
- Al 45% de los alumnos les han compartido enlaces molestos o con contenido inadecuado.
- Cuatro de cada diez alumnos se han reunido en el mundo real con amigos que ha hecho en línea
- Tres de cada diez estudiantes comparten información personal.

RECOMENDACIONES

Para coadyuvar a la operación de las directrices nacionales e internacionales, respecto a minimizar los riesgos y amenazas de ciberseguridad derivados del uso de redes y dispositivos de telecomunicaciones, así como las institucionales sobre código de conducta, se propone lo siguiente:

A nivel institucional adoptar la formación de competencias digitales y aspectos de ciberseguridad en el Modelo Educativo y Curricular de la UAEH.

Diseñar cursos de actualización a los docentes sobre riesgos cibernéticos y de seguridad digital del uso de redes y dispositivos de telecomunicaciones en el ámbito educativo.

Fortalecer compromisos de trabajo colegiado en el desarrollo de competencias digitales y crear conciencia en el alumnado con relación a la privacidad y protección de la información en línea durante los procesos de enseñanza aprendizaje.

Referencias

Castañeda, J., de la Torre, M., Morán, J., & Lara, L. (2002). Metodología de la investigación. México: McGraw Hill.

European Commission's Joint Research Centre [ECJRC]. (2022). DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes" ©European Union. Recuperado de: https://publications.jrc.ec.europa.eu/repository/handle/JRC128415

Guzmán, Y., & Campos, V. (2009). Las competencias profesionales: Una visión desde diferentes enfoques teóricos. Guantánamo: Universitaria

Hernández, R., Fernández, C., & Baptista, P. (2010). Metodología de la investigación. México: Mc Graw Hill.

Landero, R., & González, M. (2006). Estadística con SPSS y metodología de la investigación. México: Trillas.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO]. (2022). Desglosar el Objetivo de Desarrollo Sostenible 4. Educación 2030.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO]. (2023). Tecnología en la educación: ¿Una Herramienta en los Términos de Quién? Recuperado de https://mexico.un.org/sites/default/files/2023-07/PUBLICACION4.pdf

Pelayo, M. (2012). Capital social y competencias profesionales: Factores condicionantes para la inserción laboral. Disponible en http://www.eumed.net/

Secretaría de Comunicaciones y Transportes. (2020). Guía de Ciberseguridad para el Uso Seguro de Redes y Dispositivos de Telecomunicaciones en apoyo a la Educación. Recuperado de:

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/gui_a_de_ciberseguridad_sct_vf.pdf

Semáforo Delictivo. (2023). Obtenido de http://hidalgo.semaforo.com.mx/

Stufflebeam, D., & Shinkfield, A. (1987). Evaluación sistemática. Guía teórica y práctica. Barcelona: Paidos

Universidad Autónoma del Estado de Hidalgo [UAEH]. (2010). Modelo Curricular Integral UAEH. Reforma del Nivel Licenciatura. Pachuca, Hidalgo

Universidad Autónoma del Estado de Hidalgo [UAEH]. (2017). Documento de Diseño de la Licenciatura en Tecnologías de la Información. Pachuca, Hidalgo.

Universidad Autónoma del Estado de Hidalgo [UAEH]. (2019). Código de Conducta de las Autoridades y el Personal de la Universidad Autónoma del Estado de Hidalgo. Pachuca, Hidalgo

Universidad Autónoma del Estado de Hidalgo [UAEH]. (2023). Licenciatura en Tecnologías de la Información. https://www.uaeh.edu.mx/campus/tizayuca/licenciatura/tecnologias-informacion/

Unión Internacional de Telecomunicaciones. (2013). Protección de la Infancia en Línea: Directrices para los niños. Recuperado de: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-COP.CHILD-2013-PDF-S.pdf

Unión Internacional de Telecomunicaciones. (17 de septiembre de 2023). Sobre la Unión Internacional de Telecomunicaciones. Recuperado de: https://www.itu.int/es/about/Pages/default.aspx

Unión Internacional de Telecomunicaciones. (17 de septiembre de 2023). Sobre la Unión Internacional de Telecomunicaciones. Recuperado de: https://www.itu.int/es/about/Pages/default.aspx

Vega, R., & De Armas, R. (2009). Tuning-Amèrica Latina y su compatibilidad con el modelo curricular cubano. Reencuentro, (54), 73-81.

World Economic Forum [WEF]. ¿Por qué la ciberseguridad es más importante que nunca durante la pandemia de coronavirus? Recuperado de: ¿Por qué la ciberseguridad es más importante que nunca durante la pandemia de coronavirus? | Foro Económico Mundial (weforum.org)