UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÀTICA, CIENCIAS DE LA COMPUTACIÒN E INNOVACIÒN TECNOLOGÌCA.

CARRERA DE INGENIERÍA DE SISTEMAS.

VULNERABILIDADES GENERADAS POR EL USO DE LAS REDES SOCIALES, EN LOS ESTUDIANTES DE BACHILLERATO DEL CENTRO URBANO DEL CANTÒN CAÑAR.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS.

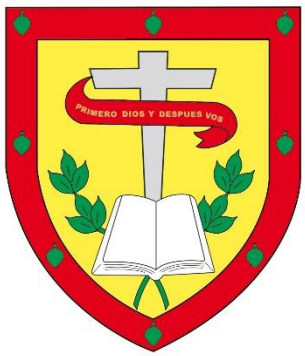
AUTOR: JENNY ALEXANDRA VAZQUEZ LAZO

DIRECTOR: ING. CRISTINA MARIUXI FLORES ÙRGILES

CAÑAR – ECUADOR

2021

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÀTICA, CIENCIAS DE LA COMPUTACIÒN E INNOVACIÒN TECNOLOGÌCA.

CARRERA DE INGENIERÌA DE SISTEMAS

VULNERABILIDADES GENERADAS POR EL USO DE LAS REDES SOCIALES, EN LOS ESTUDIANTES DE BACHILLERATO DEL CENTRO URBANO DEL CANTÒN CAÑAR.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

AUTOR: JENNY ALEXANDRA VAZQUEZ LAZO.

DIRECTOR: ING. CRISTINA MARIUXI FLORES ÙRGILES.

CAÑAR - ECUADOR

2021

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARACIÓN

Yo, Jenny Alexandra Vázquez Lazo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad Católica de Cuenca extensión Cañar puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y la Normativa actual de la institución.

Jenny Alexandra Vázquez Lazo

C.I.:0302111463

CERTIFICACIÒN

Certifico que el presente trabajo fue desarrollado por Jenny Alexandra Vazquez Lazo, bajo mi supervisión.

_____

Ing. Cristina Mariuxi Flores Urgilés

DIRECTOR DELTRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA

RESUMEN

El presente artículo presenta un estudio realizado en el cantón Cañar, provincia de Cañar-Ecuador donde participaron adolescentes entre los 14 a 19 años, estudiantes de 5 instituciones educativas del centro urbano del cantón. Los objetivos planteados en el presente estudio fueron: a) Establecer el estado del arte sobre los riesgos relacionados al uso de las redes sociales, b) Identificar el marco metodológico necesario para el análisis de la problemática sobre riesgos asociados con el uso de las redes sociales, c) Aplicar el análisis de riesgos sobre los datos levantados, para determinar el nivel de vulnerabilidad de los estudiantes de bachillerato frente a las amenazas generadas por el uso de las redes sociales y d) Establecer controles que permitan disminuir el nivel de vulnerabilidad de los estudiantes de bachillerato frente a las amenazas generadas por el uso de las redes sociales. Se realizó un análisis mediante la aplicación de encuestas enfocadas en seguridad informática y mediante la matriz de riesgos conocida como MAGERIT, se estableció un análisis de riesgos. Los resultados demostraron que los adolescentes se encuentran vulnerables a los peligros de la red y se requiere mayores controles que permitan reducir el riesgo al cuál se enfrentan en el día a día.

ABSTRACT

This research work shows a study carried out in the Cañar Canton, Cañar province, Ecuador, in which some adolescents from 5 educational units from the urban part of the canton, ranging in ages from 14 to 19 years took part. The objectives of the study include: a) to stablish the state of art on the risks related to the use of social networks. b) to identify the methodological framework needed for the analyses of the risk associated with the use of social networks. c) to apply the risk analyses about the gathered information in order to determine the level of vulnerability of high school students before the threats generated by the use of social networks. d) to establish the controls that will allow to decrease the level of vulnerability of high school students before the threats generated by the use of social networks. An analysis through the application of a survey focused on technological safety was conducted through the open methodology MAGERIT, a risk analyses was stablished. Results showed that adolescents are vulnerable to the risks in the web, therefore, more control that allows to decrease the threats that they face daily is necessary.

Vulnerabilidades generadas por el uso de las redes sociales, en los estudiantes de bachillerato del centro urbano del cantón Cañar.

Vulnerabilities generated by the use of social networks in high school students of the urban center of Cañar canton.

Jenny Alexandra Vázquez Lazo[1] , Cristina Mariuxi Flores Urgilés[2], Cristhian Humberto Flores Urgilés[3], Julio Jhovany Santacruz Espinoza[4].

Categoría profesional, Universidad Católica de Cuenca, Ecuador

Javazquezl63@est.ucacue.edu.ec

ORCID

RESUMEN

El presente artículo presenta un estudio realizado en el cantón Cañar, provincia de Cañar-Ecuador donde participaron adolescentes entre los 14 a 19 años, estudiantes de 5 instituciones educativas del centro urbano del cantón. Los objetivos planteados en el presente estudio fueron: a) Establecer el estado del arte sobre los riesgos relacionados al uso de las redes sociales, b) Identificar el marco metodológico necesario para el análisis de la problemática sobre riesgos asociados con el uso de las redes sociales, c) Aplicar el análisis de riesgos sobre los datos levantados, para determinar el nivel de vulnerabilidad de los estudiantes de bachillerato frente a las amenazas generadas por el uso de las redes sociales y d) Establecer controles que permitan disminuir el nivel de vulnerabilidad de los estudiantes de bachillerato frente a las amenazas generadas por el uso de las redes sociales. Se realizó un análisis mediante la aplicación de encuestas enfocadas en

[1] Título de pregrado, título de posgrados (si lo tiene)
[2] Título de pregrado, título de posgrados (si lo tiene)
[3] Título de pregrado, título de posgrados (si lo tiene)
[4] Título de pregrado, título de posgrados (si lo tiene)

seguridad informática y mediante la matriz de riesgos conocida como MAGERIT, se estableció un análisis de riesgos. Los resultados demostraron que los adolescentes se encuentran vulnerables a los peligros de la red y se requiere mayores controles que permitan reducir el riesgo al cuál se enfrentan en el día a día.

ABSTRACT

This research work shows a study carried out in the Cañar Canton, Cañar province, Ecuador, in which some adolescents from 5 educational units from the urban part of the canton, ranging in ages from 14 to 19 years took part. The objectives of the study include: a) to stablish the state of art on the risks related to the use of social networks. b) to identify the methodological framework needed for the analyses of the risk associated with the use of social networks. c) to apply the risk analyses about the gathered information in order to determine the level of vulnerability of high school students before the threats generated by the use of social networks. d) to establish the controls that will allow to decrease the level of vulnerability of high school students before the threats generated by the use of social networks. An analysis through the application of a survey focused on technological safety was conducted through the open methodology MAGERIT, a risk analyses was stablished. Results showed that adolescents are vulnerable to the risks in the web, therefore, more control that allows to decrease the threats that they face daily is necessary.

PALABRAS CLAVE

Vulnerabilidad informática, Redes Sociales, ciber amenazas, Riesgos informáticos, Ciber seguridad.

KEYWORDS

Computer vulnerability, Social Networks, Cyber threats, Computer risks, Cyber security.

INTRODUCCIÓN

La comunicación siempre ha formado parte del ser humano debido a su necesidad intrínseca de buscar, conocer y obtener información de otros. La tecnología ha avanzado en la forma de interacción y comunicación entre individuos. Uno de estos cambios involucra el desarrollo de las tecnologías de información y comunicación TICs, causando impacto principalmente en niños, adolescentes y jóvenes (Prats et al., 2018). Las TICs en los últimos tiempos ha permitido el flujo de datos, recursos tecnológicos que capturan, almacenan, procesan y distribuyen información (Quispe-Otacoma Ana Lucía et al., 2017; Rodríguez-Moreno, 2017). Estas están siendo usadas en diferentes ámbitos de la vida cotidiana del ser humano.

Las redes sociales son una de estas tecnologías ampliamente usadas, mediante la interacción y colaboración de sus usuarios, permitiendo el intercambio de ideas, la creación y edición de contenidos, así como la construcción de relaciones, siendo una herramienta importante para la comunicación en diferentes ámbitos (Buxarrais María Rosa, 2016; Méndez-Bravo, 2018). Estas estructuras sociales se componen de grupos de personas, conectadas entre sí por diversos fines, ya sea amistad, parentesco, intereses en común o para compartir conocimientos (Veloz, 2017).

Los sistemas han permitido un cambio importante en la manera de interactuar entre los individuos, brindando diversos beneficios, también ha traído consigo riesgos acerca de la seguridad e integridad de las personas como pueden ser Cyberbullying, gromming, sexting, entre otros. Debido al crecimiento de las redes sociales la mayoría de personas no utiliza con responsabilidad, siendo la población más joven la más vulnerable (Arab & Díaz, 2015)(Veloz, 2017).

Beneficios del internet.

El internet es usado en diferentes ámbitos de la vida cotidiana presentando diversas ventajas, así: en el ámbito político, partidos, personajes políticos y autoridades poseen

páginas web y redes sociales relacionándose con la ciudadanía por estos medios. En lo económico, las empresas mediante la red buscan llegar a sus clientes y clientes potenciales promocionando sus productos y servicios. En el ámbito social, internet se ha vuelto un amplio espacio para la interacción de personas conocidas y desconocidas alrededor del mundo. En el ámbito educativo, los estudiantes, padres de familia y docentes interactúan mediante estos medios digitales así también existe gran cantidad de información y recursos educativos a los que se puede acceder (Molina-Gómez Ana María et al., 2015; Veloz, 2017).

Riesgos en el internet y redes sociales

Un riesgo informático es la probabilidad de que una amenaza se lleve a efecto debido a vulnerabilidades existentes y que un daño a bienes y servicios informáticos ocurra. Estas amenazas pueden ser filtraciones de información, amenazas de falla del sistema, virus y uso indebido de software (Flores Urgilés et al., 2019).

Es necesario definir lo que es amenaza y vulnerabilidad. Una amenaza es una condición del entorno de los medios que contienen información importante y que es fuente potencial de incidentes no deseados que puede dar lugar a daño de los recursos informáticos. Por otro lado, la vulnerabilidad es la condición de fragilidad o debilidad de un recurso informático, una actividad o hecho que hace susceptible a dicho recurso a ser afectado por una amenaza (Baca-Urbina Gabriel, 2016; Quiroz-Zambrano & Macías-Valencia, 2017).

Debido al anonimato y falseamiento de identidad al que se prestan las redes sociales, las mismas son susceptibles a ser escenarios de conductas inadecuadas, siendo los niños y adolescentes los más vulnerables a estas (Arab & Díaz, 2015). Dentro de los peligros a los que niños y adolescentes se ven expuestos están:

- *Gromming*

Consiste en una persona adulta se contacta por la red con un menor de edad haciéndose pasar por otro menor. Aprovechándose de su inocencia e ingenuidad, se gana su confianza, posteriormente finge enamoramiento a fin de conseguir contenido sexual del menor (fotos y/o videos) y comienza el chantaje para obtener más contenido sexual. Esto trae como consecuencia la afectación psicológica del niño/a o adolescente pudiendo llegar hasta el suicidio (Arab & Díaz, 2015; Astorga-Aguilar & Schmidt-Fonseca, 2019).

- *Cyberbulling*

Se refiere a violencia ejercida por los medios de comunicación virtuales. publicarse, fotos, videos, memes o información personal que perjudica o avergüenza a alguien. La víctima suelo sufrir de bullying físico siendo el cyberbullying una extensión del mismo (Arab & Díaz, 2015).

- *Sexting*

Los menores de edad en su afán de sentirse aceptados en su círculo social o por intereses sentimentales, comparten imágenes con connotación sexual y personal, corriendo el riesgo que dichas imágenes sean publicadas sin permiso y su intimidad se vea expuesta (Arab & Díaz, 2015).

- *Ciberadicción o adicción al internet*

Existe una pérdida de control en el uso de internet, el individuo permanece en uso constante del mismo. Se da un aislamiento, descuido de las relaciones sociales, de las actividades académicas, actividades recreativas, salud e higiene personal. Incluye también el Gambling que refiere a la adicción de los videojuegos (Arab & Díaz, 2015).

1.1. Ciber seguridad.

La ciber seguridad engloba a los instrumentos, políticas, conceptos de seguridad, medidas de seguridad, directrices, enfoques de gestión de riesgos, prácticas, garantías y las tecnologías que se utilizan con el fin de controlar, proteger y defender la información

y las interacciones en el ciberespacio (Astorga-Aguilar & Schmidt-Fonseca, 2019; Raudales, 2018). Los actores implicados en la ciber seguridad con el uso de redes sociales por niños/as y adolescentes son los docentes, estudiantes, padres de familia y la comunidad educativa. (Astorga-Aguilar & Schmidt-Fonseca, 2019).

Dentro de las estrategias que pueden será aplicadas para minimizar los riesgos, tenemos los siguientes:

- Realizar una lista de reglas con los sitios permitidos, horarios, tiempo límite de uso (una o dos horas) y establecer sanciones ante el incumplimiento.
- Definir en la familia espacios libres de aparatos electrónicos.
- Buscar y educar en un equilibrio de las actividades online y offline. Fomentar actividades que no impliquen el uso de equipos tecnológicos.
- Educar en tema de seguridad cibernética y trabajar en las consecuencias de lo que se hace y dice en la web.
- Como padres, educarse en las innovaciones tecnológicas, lenguaje de internet, jergas, redes sociales, etc.
- Colocar computadores en zonas comunes.
- Instalar filtros de contenido en los navegadores.
- Averiguar las medidas de ciber seguridad que tienen las instituciones educativas a la que asisten los menores.
- Establecer una buena comunicación con los menores y estar alerta a cualquier cambio en el comportamiento (Arab & Díaz, 2015; Astorga-Aguilar & Schmidt-Fonseca, 2019).

MAGERIT.

MAGERIT o Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", es una metodología enfocada al análisis y la gestión de riesgos,

desarrollada por el Consejo Superior de Administración Electrónica CSAE y pertenece al Ministerio de administraciones públicas de España. Esta metodología permite investigar los riesgos a los que se enfrentan los sistemas de información a fin de establecer medidas que permitan controlar dichos riesgos. El método se resume en los siguientes pasos:

A. Análisis de riesgos

1. Se determina los activos, su valor y nivel de criticidad en caso de ser afectados.
2. Determinar las amenazas que pudieran afectar a los activos considerando factores tanto internos como externos a la organización.
3. Determinar las salvaguardas o controles y su nivel de eficacia frente a las amenazas.
4. Se estima el impacto residual, es decir el impacto sobre el activo una vez materializada la amenaza aun existiendo las salvaguardas.
5. Se calcula el riesgo residual con base en el impacto residual y la probabilidad de ocurrencia de la amenaza.

B. Gestión de riesgos

Una vez finalizado el análisis, se procede con la gestión, se da una calificación a cada riesgo a fin de determinar la acción a tomar para enfrentarlo. (Ministerio de Hacienda y Administraciones Públicas, 2012a, 2012c, 2012b).

Estudios previos

En un estudio realizado en la ciudad de San Diego Cuentla en México (Arellano-Martínez, 2017), con estudiantes de preparatoria sobre el riesgo de uso de redes sociales se encontró que el 91% de los alumnos pertenece a alguna red social. Estos están conscientes de los riesgos que implica su uso sin embargo no toman las medidas para proteger su información. Concluyó que es necesario difundir información a los jóvenes sobre la seguridad al usar redes sociales.

Mediante la aplicación de una encuesta a estudiantes entre 13 a 17 años de centros educativos tanto públicos como privados en España, se buscó evaluar cómo los adolescentes usan las redes sociales, su conciencia sobre los riesgos y cómo los enfrentan. Se evidenció que los estudiantes usan las redes sociales principalmente por la necesidad de comunicarse con sus compañeros. Lamentablemente, un gran porcentaje de los estudiantes expresaron fiarse de los contenidos en la red y no comprobar su privacidad. Así también, los adolescentes aceptaron que no permiten el acceso a sus padres a sus perfiles y si lo hacen restringen el acceso; esto los vuelve más vulnerables a los peligros informáticos (Plaza, 2016).

Con el fin de evidenciar el efecto de la concientización sobre la importancia de la seguridad en el uso de redes sociales investigadores de la Universidad Ramon Llull (Prats et al., 2018) realizaron un estudio en la ciudad de Cataluña. Talleres sobre funcionamiento, uso y riesgo de las redes sociales fueron impartidos tanto a estudiantes como a padres de familia y profesores. Los estudiantes expresaron que muchos de los temas abordados en los talleres no fueron explicados antes ni por parte de sus maestros ni sus padres y se mostraron interesados en recibir más talleres acerca del tema. Los padres y maestros demostraron preocupación respecto a los riesgos que corren los adolescentes en las redes sociales. Los padres buscaron orientación respecto a las pautas para controlar el uso de redes por parte de sus hijos.

Con el mismo fin, otro estudio fue realizado en la ciudad de Cañar por investigadores de la Universidad católica de Cuenca (Flores-Urgilés et al., 2019) donde aplicaron una encuesta a estudiantes previa capacitación sobre uso seguro de redes sociales y otra encuesta posterior a dicha capacitación. Los resultados demostraron que al conocer los riesgos y peligros ante el uso de redes sociales los estudiantes cambiaron su comportamiento al usar internet y las redes. Además, el estudio concluyó que es

trascendental capacitar a los padres para que puedan guiar y ayudar a sus hijos en caso de enfrentarse a peligros en redes.

El desconocimiento del marco legal respecto a delitos informáticos y la falta de especialistas en seguridad informática dentro de la policía, así como de protocolos claros para actuar en caso de estos delitos en Ecuador ha llevado a que no se actúe de la mejor manera en estos casos. Así lo evidencia el estudio denominado "Delitos a través redes sociales en el Ecuador: una aproximación a su estudio" (Jara-Obregón Luis et al., 2017), mediante encuestas a varios grupos de la población analizaron el uso de las redes sociales. Se encontró que si bien la mayoría de la población estudiada usa y tiene conocimiento de los riesgos en redes sociales al verse víctimas de algún delito no ponen la denuncia respectiva, así también el estudio concluye que la policía cuenta con pocos agentes especializados en esta área y lamentablemente no tienen definida una metodología de investigación exclusiva para delitos de este tipo.

METODOLOGÍA.

La presente investigación fue realizada mediante la aplicación del método deductivo. Así, partimos de la premisa que los adolescentes son vulnerables a diversos riesgos en redes sociales, esto se definió mediante revisión de literatura dónde diversos estudios demuestran que adolescentes se ven expuestos a diversos peligros en internet y específicamente redes sociales siendo altamente vulnerables (Arellano-Martínez, 2017; Flores-Urgilés et al., 2019b; Jara-Obregón Luis et al., 2017; Plaza, 2016; Prats et al., 2018). Dado esto se ha planteado realizar una investigación con un grupo de estudiantes de 5 instituciones educativas pertenecientes al cantón Cañar. Para demostrar la premisa se decidió aplicar una encuesta a los adolescentes y se realizó un análisis de riesgos mediante la matriz de Magerit(Ministerio de Hacienda y Administraciones Públicas, 2012a, 2012c, 2012b).

Diseño

El presente estudió es descriptivo, se aplicó el método inductivo y un análisis de riesgos mediante la matriz de Magerit, para ello nos basamos en los estudiantes de bachillerato de 5 instituciones educativas del centro urbano del cantón Cañar. Las instituciones educativas que participaron en la investigación fueron:

- Unidad Educativa Andrés F. Córdova
- Unidad Educativa José Peralta
- Unidad Educativa Fiscomisional San José De Calasanz
- Unidad Educativa Fiscomisional Santa Rosa De Lima
- Colegio De Bachillerato Particular Justiniano Crespo Verdugo

En total 1759 estudiantes cursan el bachillerato en estas instituciones. La información analizada en el presente estudio se obtuvo mediante la aplicación de una encuesta desarrollada a través de la herramienta Google Forms. Mediante esta encuesta se analizaron diversas variables:

- Modalidad de acceso a Internet.
- Tiempo diario de conexión a Internet.
- Redes sociales más usadas.
- Comportamiento en Internet y redes sociales.
- Control parental respecto a uso de internet y redes sociales.
- Conocimiento sobre ciber seguridad.

Las variables analizadas fueron definidas en base a diferentes estudios previos realizados tanto a nivel local como internacional en donde también se aplicaron encuestas a fin de analizar el comportamiento de los jóvenes en internet y redes sociales (De-Frutos-Torres & Marcos-Santos, 2017; Flores et al., 2018; García-Jiménez et al., 2020; Jasso Medrano et al., 2017).

Población y muestra

La población estudiada fue de 1759 estudiantes, se definió una muestra mediante la aplicación de la fórmula estadística para una muestra finita:

$$\boldsymbol{n} = \frac{N * Z^2 * p * q}{e^2 * (N-1) + Z^2 * p * q}$$

Donde:

n= tamaño de la muestra.

N= tamaño de la población.

e= error de estimación máximo aceptado.

Z=Estadístico en función del nivel de confianza.

p= probabilidad de que ocurra el evento estudiado.

q=(1-p) probabilidad de que no ocurra el evento estudiado (Suárez Mario & Tapia Fausto, 2012).

Con un nivel de confianza del 95% y un error del 5% se obtuvo una muestra de 316 estudiantes.

Aplicación de la metodología MAGERIT

Análisis de riesgos

Como primer paso, se 0determinaron los tipos de activos y activos a evaluar siendo estos:

- Aplicaciones (software)-Redes Sociales: Facebook, WhatsApp, Instagram, Telegram, Tiktok, Twitter y Snapchat
- Dispositivos electrónicos: Computadora de mesa, computadora portátil, Tablet y celular o móvil
- Redes de comunicación: Internet
- Datos e información: Información personal

- Personas: Se establecen 2 grupos, adolescentes de 14 a 16 años de edad y adolescentes de 17 a 19 años de edad.

Las dimensiones de seguridad (disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad) para cada activo fueron evaluadas con la siguiente escala de valoración:

Tabla 1 Escala de valoración de las dimensiones de seguridad.

Nivel	Valoración
Bajo	1
Medio	2
Alto	3
Muy alto	4
Crítico	5

La valoración final fue obtenida mediante sumatoria de cada dimensión. Se establecieron las amenazas con base al catálogo disponible en las guías para el posterior cálculo de riesgo (Ministerio de Hacienda y Administraciones Públicas, 2012c, 2012a, 2012b). El cálculo de riesgo fue realizado mediante el método de panel de expertos (Andrés, 2000), participando 3 expertos. Los profesionales que participaron en el proceso son expertos en ingeniería en sistemas en psicología y derecho informático. El impacto y la probabilidad de cada amenaza planteada, fueron evaluadas por cada experto de forma individual aplicando las escalas mostradas en la tabla y posteriormente se realizó un promedio de las evaluaciones obtenidas.

Tabla 2 Escala de valoración de impacto y probabilidad de ocurrencia de amenazas.

Impacto		Probabilidad	
Insignificante	1	Improbable	1
Menor	2		
Moderado	3	Probable	2
Mayor	4		

Catastrófico	5	Casi Seguro	3

Se calculó la exposición con la fórmula:

$$Factor\ de\ exposición = Impacto\ x\ Probabilidad$$

Y el riesgo:

$$Riesgo = Valoración\ x\ Factor\ de\ exposición$$

Gestión de riesgos

Con base en las guías se definieron los controles aplicables a las amenazas establecidas y se evaluó la eficiencia de dicho control:

Tabla 3 Escala de valoración de la eficiencia de control.

Eficiencia de control	
Bajo	1
Medio	2
Optimo	3

Finalmente se calculó el riesgo residual para cada amenaza:

$$Riesgo\ residual = \frac{Eficiencia\ de\ control}{Riesgo}$$

RESULTADOS

Encuestas.

Los estudiantes encuestados se encuentran entre los 14 a 19 años de edad, siendo los estudiantes de 15 y 16 años los que representan los porcentajes más altos de los encuestados siendo un 36,4% y 22,5% respectivamente. El 70,6% pertenecen al género femenino y el 29,4 al género masculino.

Un 88% de los estudiantes se conectan a internet mediante un celular siendo poco los que usan un computador ya sea de mesa o portátil o una Tablet. La mayoría interactúa mediante la red Facebook con un 43,7%, seguida de TikTok con 30,1% y WhatsApp con 25,3%. El 76,9% de los estudiantes admite usar internet por un tiempo entre 4 a 8 horas,

sin embargo, existe un porcentaje de 16,5% que admite estar conectado a internet por más de 12 horas lo cual no es sano para el adolescente ya que conlleva consecuencias físicas y psicosociales (Ferreiro et al., 2017).

Respecto a control parental, un 82,9% de los adolescentes admite que no solicita permiso a los padres o tutores al momento de conectarse a internet, un 55,7% de los estudiantes admiten no tener reglas impuestas por los padres o tutores para utilizar internet y un 44,3% reconoce que, si se le han impuesto reglas, lamentablemente un 44,6% admite que si bien existen reglas impuestas no existen sanciones en caso del incumplimiento de las mismas.

Un hallazgo bastante positivo fue que la gran mayoría de estudiantes (95,9%) reconoció que ha recibido información sobre ciber seguridad y los peligros de las redes. No obstante, existieron estudiantes que mencionaron no haber recibido dicha información y si bien es un pequeño porcentaje es primordial que se trabaje en llegar a todos los adolescentes con esta información a fin de reducir su vulnerabilidad a los peligros de internet. La información sobre ciber seguridad es recibida mayormente por parte de los maestros lo que demuestra el interés de las instituciones educativas en la seguridad de los estudiantes durante su interacción en internet. Otros adolescentes admiten que ha obtenido información sobre seguridad informática en internet, de sus padres, así como de sus amigos.

Si bien los estudiantes están conscientes que es más sencillo que una persona mienta sobre su información personal en el mundo virtual (99,7%), los hallazgos respecto al comportamiento de estos en redes sociales resultan preocupantes pues un alto porcentaje de los adolescentes, el 44% admite que acepta solicitudes de amistad de personas que no conocen y el 98,4% de los adolescentes comparte su información personal en redes sociales. Esto los hace vulnerables a los peligros cibernéticos y los predispone a ser

víctimas de delitos. La gran mayoría de estudiantes un 96,5% menciona que han conocido en la vida real a personas con quienes en un momento solo habían interactuado por redes sociales.

Ante un caso de usurpación de identidad en redes, un 52,2% de los estudiantes mencionan que bloquearían la cuenta falsa, un 36,1% daría aviso a sus padres o tutores, un 8,9% denunciaría la cuenta falsa y un 2,8 preferiría ignorar la situación, demostrando que la mayoría de estudiantes buscarían tomar acción ante el delito que se está cometiendo. Los adolescentes al recibir contenido inapropiado mediante internet son con un 54,4% bloquear al usuario y con un 42,1% denunciar al usuario del que recibió el contenido; otra acción es la de denunciar con las autoridades. Lamentablemente hay un porcentaje de los adolescentes que admiten aceptar el contenido inapropiado que reciben, la gran mayoría de adolescentes encuestados se han sentido acosados o incómodos en internet lo cual es preocupante y se evidencia que es necesario un mayor control de la interacción de estos en redes, así como una mejor guía por parte de padres y maestros.

La gran mayoría de adolescentes han sido testigos de acoso a otras personas en internet, un 95,9% admitió que han observado dicho acoso. Solo un 41,5% de los adolescentes mencionan defender a la persona agredida, lamentablemente un 50% decide ignorar la situación y un 8,5% de los estudiantes admiten incluso haberse unido a la situación de acoso. Por otro lado, al enfrentarse a una situación de acoso, el 49,1% de los estudiantes denuncian la situación de acoso en la red social, un 26,3% bloquea al usuario y 13,6% enfrenta al acosador. En un porcentaje menor de los casos los adolescentes dan aviso a sus padres, denuncian a las autoridades y otros simplemente ignoran.

Los estudiantes fueron cuestionados respecto a las actividades que se han visto afectados con la aparición de internet redes sociales, en su mayoría consideran que la interacción con otras personas de manera física es la que se ha visto mayormente afectada

y un porcentaje menor considera que actividades como el deporte, lectura de periódico o consumo de programas televisivos han disminuido también.

Matriz de MAGERIT.

Los resultados obtenidos de la aplicación de la matriz de MAGERIT resultan preocupantes pues la mayoría de activos presentan un riesgo alto ante las amenazas a las que se enfrentan, muy pocos se catalogaron con riesgo bajo y medio y en ciertos casos el riesgo llega incluso a ser crítico tenemos así:

Tabla 4 Activos que resultaron con riesgo crítico en el análisis de matriz MAGERIT.

Tipo de activo	Codigo	Activo	Dimenciones de Valoracion						Bajo	1	Catalogo de Amenazas	Calculo del Riesgo					R= VA*FE	
									Medio	2		Insignificante	1	Improbable	1		Bajo	1–37
									Alto	3		Menor	2					
									Muy Alto	4		Moderado	3	Probable	2	FE = I*P	Medio	38–74
									Critico	5		Mayor	4				Alto	75–111
												Catastrofico	5	Casi Seguro	3		Critico	112–375
			Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	TOTAL /25			Amenazas	Impacto		Probabilidad		Factor de Exposición		RIESGO
[SW] aplicaciones (software)-Redes Sociales	RS-Ac1	Facebook	4	5	2	2	2	15			[E.1] Errores al aceptar solicitudes de amistad a personas extrañas o desconocidas.	4		3		12		180
											[A.5] Suplantación de la identidad del usuario	5		3		15		225
											[A.8] Difusión de software dañino	5		3		15		225
	RS-Ac2	Whatsapp	4	5	3	2	2	16			[A.5] Suplantación de la identidad del usuario	5		3		15		240
	RS-Ac3	Instagram	4	5	3	2	2	16			[A.5] Suplantación de la identidad del usuario	5		3		15		240
	RS-Ac4	Telegram	4	5	2	2	2	15			[A.5] Suplantación de la identidad del usuario	5		3		15		225
	RS-Ac6	Twitter	4	5	2	2	2	15			[A.5] Suplantación de la identidad del usuario	5		3		15		225
											[A.8] Difusión de software dañino	5		3		15		225
	RS-Ac7	Snapchat	4	5	2	2	2	15			[A.8] Difusión de software dañino	5		3		15		225
Redes de comunicación	RC.Ac1	Internet	5	3	2	1	2	13			[A.5] Suplantación de la identidad del usuario	5		3		15		195
Personas	P-Ac1	Edades 16-19	4	3	3	2	2	14			[E.7] Deficiencias en la organización	4		3		12		168
											[E.19] Fugas de información	4		3		12		168
	P-Ac2	Edades 14-16	5	3	3	2	2	15			[E.31] Ingeniería social (picaresca)	4		3		12		180
											[E.19] Fugas de información	4		3		12		180
											[A.29] Extorsión	5		3		15		225

La suplantación de identidad es una de las amenazas con riesgo crítico que resulta un factor común entre algunos activos como lo son las redes sociales y redes de comunicación. En cuanto a los activos de personas el análisis arrojó que las fugas de información es una de las amenazas con riesgo crítico y que se presenta tanto en el rango de edad de 14 a 16 años como de 16 a 19 años. Otras de las amenazas a la que se enfrentan son deficiencias en la organización, ingeniería social y extorsión.

De las amenazas evaluadas para cada activo el 8,43% representa un riesgo bajo (con valoración entre 1-37), el 19,10% un riesgo medio (valoración 38-74), el 64,04% un riesgo alto (valoración 75-111) y el 8,43% un riesgo crítico (valoración 112-375). En cuanto al riesgo residual una vez evaluada la eficiencia de los controles si bien en un 46,63% de las amenazas se logra reducir o mantener a un nivel de riesgo bajo, el 52,81 de estas siguen con un riesgo medio e inclusive la extorsión presenta un riesgo residual alto siendo uno de los factores a tomar en cuenta para la mejora de los controles aplicados.

DISCUSIÓN

El estudio ha evidenciado que si bien los estudiantes en su mayoría admiten haber recibido información sobre ciber seguridad la misma debe ser reforzada. A pesar de tener ciertos conocimientos muchos admiten comportamientos que los vuelven vulnerables y propensos a ser víctimas de delitos informáticos. Se ha demostrado también que es necesario un trabajo conjunto de padres/tutores y las instituciones educativas a fin de brindar a los adolescentes las herramientas necesarias para enfrentarse a los peligros de las redes, como lo mencionan en un estudio realizado en Costa Rica (Astorga-Aguilar & Schmidt-Fonseca, 2019) es importante educar a todos los actores en el entorno de los adolescentes.

Otra situación que es preocupante es el tiempo que los adolescentes estudiados permanecen navegando en internet y usando redes sociales un 76,9% de estudiantes

admitió pasar de 4 a 8 horas conectado y un 16,6% se conecta por más de 12 horas. Este comportamiento también se ve evidenciado en otros estudios como el realizado en España con adolescentes entre 12 y 17 años donde ciertos adolescentes admiten conectarse por más de 5 horas además de reconocer que es sería muy difícil dejar de conectarse y que esto ha afectado a su vida cotidiana disminuyendo otras actividades como compartir con amigos y su vida estudiantil (Catalina-García et al., 2014). Así también, en otro estudio realizado en Chile se evidenció que los adolescentes pueden llegar a estar conectados hasta por 15 horas (Arnao Marciani & Surpachin Miranda, 2016).

Facebook y WhatsApp se han identificado como redes sociales ampliamente usadas por los adolescentes, el mismo resultado se obtuvo en un estudio realizado en España dónde evaluaron el uso de las redes sociales por parte de adolescentes (Álvarez et al., 2019). Es evidente entonces en que plataformas se debe poner especial énfasis en mejorar la ciber seguridad para una interacción más segura. En cuanto a su comportamiento ante situaciones de acoso, lo primordial es establecer una denuncia formal que se realiza en muy pocas ocasiones, lo mismo se ha evidenciado en otros estudios (Jara-Obregón Luis et al., 2017), donde debido a la falta de conocimiento del marco legal con respecto a estos delitos, entre otros factores, no se entablan las denuncias respectivas.

Las situaciones de acoso han sido observadas por los adolescentes evaluados, un alto porcentaje (95,9%) admite haber sido testigo de acoso en redes sociales y un menor porcentaje (8,5%) se han unido al acoso. Otros estudios también muestran que el ciberacoso es un gran problema presente entre los adolescentes, en Murcia, España en un estudio realizado con estudiantes de educación segundaria, se evaluó el comportamiento de los adolescentes en torno al ciberacoso, un 62,3% de los participantes fue testigo de una situación de acoso (Calatayud et al., 2020). Por otro lado, en otro estudio realizado en Lugo, España de los adolescentes que participaron del mismo solo el 28,57% admite

haber observado conductas de acoso, así también parte de los adolescentes admiten haber participado del acoso (Pardo, 2018).

El análisis de riesgos resultó en que un 64,04% de las amenazas representan un riesgo alto para los activos y un 8,43% un riesgo crítico, siendo una situación preocupante pues además de representar un porcentaje alto de las amenazas, la eficiencia de control de las mismas aún deja un riesgo residual medio evidenciando que se requieren controles estrictos que permitan reducir el riesgo y crear espacios más seguros para los adolescentes. Dentro de las amenazas que se determinaron con riesgo crítico están aceptar solicitudes de amistad a personas extrañas o desconocidas, suplantación de la identidad del usuario, difusión de software dañino, fugas de información, extorsión estos resultados coinciden con un estudio realizado también en la provincia de Cañar dónde el análisis de riesgo resultó en que las mencionadas amenazas representan un riesgo alto (Flores et al., 2018)

Resulta fundamental un mejor control parental que permita vigilar la interacción de los adolescentes en las redes, identificar comportamientos que los estén poniendo en peligro o que vayan en contra de otras personas y tomar acción inmediata. De igual manera, analizar el conocimiento de padres y maestros respecto a ciber seguridad, delitos informáticos y conocimiento del marco legal referente a los mismos es un tema primordial que debería ser abordado en futuras investigaciones ya que para que puedan guiar correctamente a los adolescentes ellos deberían tener el conocimiento y las herramientas para hacerlo, así como para actuar en caso de enfrentarse a uno de estos delitos.

CONCLUSIONES

- Se identificó que el comportamiento de los adolescentes en redes sociales los expone y hace vulnerables a sufrir delitos informáticos y que no existe un adecuado control parental. Si bien existen reglas de uso de internet, no existen sanciones en caso de

incumplir las reglas. Los estudiantes pueden pasar hasta por más de 12 horas conectados, aceptan solicitudes de amistad de desconocidos poniéndose en riesgo, así como también admiten compartir información personal en redes, esto evidencia que hace falta una capacitación constante que les de las herramientas para enfrentarse a los peligros de la red, así como un control estricto por parte de los tutores.

- El análisis de riesgos mediante la matriz MAGERIT permitió identificar que las amenazas en su mayoría resultaron con un riesgo alto, incluso crítico y este riesgo se mantiene en un nivel medio aún aplicados los controles establecidos. Las amenazas identificadas con riesgo crítico fueron aceptar solicitudes de amistad a personas extrañas o desconocidas, suplantación de la identidad del usuario, difusión de software dañino, fugas de información y extorsión; el análisis MAGERIT resultó en catalogarlas como críticas debido a su impacto puede ser mayor o incluso catastrófico y debido a que su probabilidad de ocurrencia es casi segura.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, E., Heredia, H., & Romero, M. (2019). *La Generación Z y las Redes Sociales. Una visión desde los adolescentes en España. 40*. https://rodin.uca.es/bitstream/handle/10498/21358/Revista%20espacios.pdf?sequence=1&isAllowed=y

Andrés, C. P. (2000). ¿ Deben estar las técnicas de consenso incluidas entre las técnicas de investigación cualitativa? *Rev Esp Sal Ud Pública 2CGQ*, *74*, 319–321. https://www.scielosp.org/article/ssm/content/raw/?resource_ssm_path=/media/assets/resp/v74n4/editorial1.pdf

Arab, L. E., & Díaz, G. A. (2015). Impacto de las redes sociales e internet en la adolescencia: aspectos positivos y negativos. *Revista Médica Clínica Las Condes*, *26*(1). https://doi.org/10.1016/j.rmclc.2014.12.001

Arellano-Martínez, I. (2017). La cultura sobre seguridad informática en las redes sociales: el caso de los estudiantes de la Preparatoria de San Diego Cuentla, México. *RICSH Revista Iberoamericana de Las Ciencias Sociales y Humanísticas*, *6*(11). https://doi.org/10.23913/ricsh.v6i11.106

Arnao Marciani, J., & Surpachin Miranda, M. (2016). *Uso y abuso de las redes sociales digitales en adolescentes y jóvenes*. http://repositorio.cedro.org.pe/handle/CEDRO/310

Astorga-Aguilar, C., & Schmidt-Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciber seguridad. *Revista Electrónica Educare*, *23*(3). https://doi.org/10.15359/ree.23-3.17

Baca-Urbina Gabriel. (2016). *Introducción a la seguridad informática*. https://books.google.com.ec/books?hl=es&lr=&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=riesgo+inform%C3%A1tico&ots=0XMwaDyiGs&sig=nnFupHlb6jbX21M6Netkh8Ca5Ps&redir_esc=y#v=onepage&q=riesgo%20inform%C3%A1tico&f=false

Buxarrais María Rosa. (2016). Redes sociales y educación. *Education in the Knowledge Society*, *17*. https://www.redalyc.org/pdf/5355/535554762002.pdf

Calatayud, Ví. G., Espinosa, M. P. P., & Ruiz, C. B. (2020). Investigación sobre adolescentes que son observadores de situaciones de ciberacoso. *Revista de Investigación Educativa*, *38*(1), 259–273. https://doi.org/10.6018/RIE.370691

Catalina-García, B., López-de-Ayala, M.-C., & García-Jiménez, A. (2014). *Los riesgos de los adolescentes en Internet: los menores como actores y víctimas de los peligros de Internet*. https://doi.org/10.4185/RLCS-2014-1020

De-Frutos-Torres, B., & Marcos-Santos, M. (2017). Negative experiences and risk perception disconnection on the networking sites by teenagers. *Profesional de La Informacion*, *26*(1), 88–96. https://doi.org/10.3145/epi.2017.ene.09

Ferreiro, S. G., Folgar, M. I., Salgado, P. G., & Rial Boubeta, A. (2017). *Uso problemático de Internet y adolescentes: el deporte sí importa Problematic Internet use and adolescents: sport does matter*. *31*, 52. www.retos.org

Flores, C., Flores, C., Guasco, T., & León-Acurio, J. (2018). *A Diagnosis of Threat Vulnerability and Risk as It Relates to the Use of Social Media Sites When Utilized by Adolescent Students Enrolled at the Urban Center of Canton Cañar*. https://doi.org/10.1007/978-3-319-72727-1_15

Flores Urgiles, M., Serpa Andrade, L., Flores Urgiles, C., Caiza Caizabuano, J., Ortiz Amoroso, M., Narvaez Calle, H., Santander Paz, M., & Guamán Guamán, S. (2019). Study of Social Networks as Research Entities Under the Threat of Identity and Information Vulnerability. *Advances in Intelligent Systems and Computing*, *782*, 222–228. https://doi.org/10.1007/978-3-319-94782-2_22

Flores-Urgiles, M., Serpa-Andrade, L., Flores-Urgiles, C., Caiza-Caizabuano, J., Ortiz-Amoroso, M., Narvaez-Calle, H., Santander-Paz, M., & Guamán-Guamán, S. (2019a). *Study of Social Networks as Research Entities Under the Threat of Identity and Information Vulnerability*. https://doi.org/10.1007/978-3-319-94782-2_22

Flores-Urgiles, M., Serpa-Andrade, L., Flores-Urgiles, C., Caiza-Caizabuano, J., Ortiz-Amoroso, M., Narvaez-Calle, H., Santander-Paz, M., & Guamán-Guamán, S. (2019b).

Study of Social Networks as Research Entities Under the Threat of Identity and Information Vulnerability. https://doi.org/10.1007/978-3-319-94782-2_22

García-Jiménez, A., López-de-Ayala López, M. C., & Montes-Vozmediano, M. (2020). Características y percepciones sobre el uso de las plataformas de redes sociales y dispositivos tecnológicos por parte de los adolescentes. *ZER - Revista de Estudios de Comunicación*, *25*(48), 269–286. https://doi.org/10.1387/zer.21556

Jara-Obregón Luis, Ferruzola-Gomez Enrique, & Rodríguez-López Guillermo. (2017). *Delitos a través redes sociales en el Ecuador: una aproximación a su estudio*. https://revistas.utp.ac.pa/index.php/id-tecnologico/article/view/1721

Jasso Medrano, J. L., López Rosales, F., & Díaz Loving, R. (2017). Conducta adictiva a las redes sociales y su relación con el uso problemático del móvil. *Acta de Investigación Psicológica*, *7*(3), 2832–2838. https://doi.org/10.1016/j.aipprr.2017.11.001

Méndez-Bravo, J. (2018). Redes sociales y la innovación social. *Caribeña de Ciencias Sociales*, *abril*. https://www.eumed.net/rev/caribe/2018/04/redes-sociales-innovacion.html

Ministerio de Hacienda y Administraciones Públicas. (2012a). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método*.

Ministerio de Hacienda y Administraciones Públicas. (2012b). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*.

Ministerio de Hacienda y Administraciones Públicas. (2012c). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas*.

Molina-Gómez Ana María, Roque-Roque Lian, Garcés-Garcés Blanca Rosa, Rojas-Mesa Yuniet, Dulzaides-Iglesias María Elinor, & Selín-Ganén Marina. (2015). El proceso de comunicación mediado por las tecnologías de la información. Ventajas y desventajas en diferentes esferas de la vida social. *SciELO*, *13*. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1727-897X2015000400004

Pardo, C. (2018). *Percepción del ciberacoso por adolescentes en el ámbito rural y urbano.* https://minerva.usc.es/xmlui/bitstream/handle/10347/18470/TFM_Ramos_Pardo_Claudia.pdf?sequence=1&isAllowed=y

Plaza, J. (2016). Impacto de las redes sociales virtuales en estudiantes adolescentes: Informe de investigación / Virtual Social nets Impact on Teenage Students: a Research Report. *Revista Internacional de Tecnologías En La Educación*, *3*(1). https://doi.org/10.37467/gka-revedutech.v3.281

Prats, M. Á., Rodríguez-Torres, A., Oberst, U., & Carbonell, X. (2018). Diseño y aplicación de talleres educativos para el uso saludable de internet y redes sociales en la adolescencia: descripción de un estudio piloto. *Pixel-Bit, Revista de Medios y Educación*, *52*. https://doi.org/10.12795/pixelbit.2018.i52.08

Quiroz-Zambrano, S. M., & Macías-Valencia, D. G. (2017). Seguridad en informática: consideraciones. *Dominio de Las Ciencias, ISSN-e 2477-8818, Vol. 3, Nº. Extra 3, 2017, Págs. 676-688*, *3*(3), 676–688. https://dialnet.unirioja.es/servlet/articulo?codigo=6137824&info=resumen&idioma=SPA

Quispe-Otacoma Ana Lucía, Padilla-Martínez Mario Patricio, Telot-González Julio Alfredo, & Nogueira-RiveraI Dianelys. (2017). Tecnologías de información y comunicación en la gestión empresarial de pymes comerciales. *Ingeniería Industrial*, *38*. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59362017000100008

Raudales, C. (2018). La brecha existente en la ciber seguridad en Honduras. *Innovare: Revista de Ciencia y Tecnología*, *6*(2). https://doi.org/10.5377/innovare.v6i2.5571

Rodríguez-Moreno, D. C. (2017). Tecnologías de información y comunicación para el turismo inclusivo. *Revista Facultad de Ciencias Económicas*, *26*(1). https://doi.org/10.18359/rfce.3142

Suárez Mario, & Tapia Fausto. (2012). *Interaprendizaje de estadistica basica*. http://repositorio.utn.edu.ec/handle/123456789/2341

Veloz, A. P. (2017). Las redes sociales y sus factores de riesgos. *Pro Sciences*, *1*(5). https://doi.org/10.29018/issn.2588-1000vol1iss5.2017pp10-13

Jenny Alexandra Vázquez Lazo portador(a) de la cédula de ciudadanía N.º **0302111463**. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"Vulnerabilidades generadas por el uso de las redes sociales, en los estudiantes de bachillerato del centro urbano del cantón Cañar"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, 15 de octubre de 2021

Jenny Alexandra Vázquez Lazo

CI:0302111463