COMERCIO ELECTRÓNICO Y RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DURANTE LA PANDEMIA DE COVID-19

ELECTRONIC COMMERCE AND INFORMATION SECURITY RISKS DURING THE COVID-19 PANDEMIC

Clara Guadalupe Pozo Hernández [1*]

[1] Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen, carrera de Ingeniería en Tecnologías de la Información. Ecuador. ORCID: https://orcid.org/0000-0001-6186-1099. Correo: clara.pozo@uleam.edu.ec

Raúl Saed Reascos Pinchao [2]

[2] Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen, carrera de Ingeniería en Tecnologías de la Información. Ecuador. ORCID: https://orcid.org/0000-0002-7903-4312. Correo: raul.reascos@uleam.edu.ec

Renelmo Wladimir Minaya Macías [3]

[3] Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen, carrera de Ingeniería en Tecnologías de la Información. Ecuador. ORCID: https://orcid.org/0000-0002-0418-6864. Correo: renelmo.minaya@uleam.edu.ec

*** Autor para correspondencia: clara.pozo@uleam.edu.ec**

Resumen

El Covid 19 fue una pandemia que obligó a personas, instituciones y empresas, cambiar su forma de trabajar y debido a las restricciones que se impusieron, internet se convirtió en la herramienta fundamental, para que todos continuaran realizando sus actividades de forma virtual. Las aplicaciones y servicios que se ofrecen en internet fueron de gran beneficio, especialmente para las pequeñas empresas quienes vieron en el comercio una oportunidad de llegar con sus productos a sus clientes y estos por su parte una forma segura de abastecerse; pero es importante considerar al utilizar estas tecnologías, que existen amenazas y riesgos de seguridad informática que podrían afectar en caso de no estar protegidos. La presente investigación tuvo por objetivo analizar los principales riesgos de seguridad informática a los que se exponen los habitantes del cantón El Carmen al realizar actividades de comercio electrónico en tiempos de pandemia; se aplicó una investigación cuantitativa para estudiar los posibles riesgos y su nivel de gravedad, se utilizó una metodología de análisis de Riesgos MAGERIT, considerando como activo a proteger la información personal, se realizó una

investigación bibliográfica para seleccionar los riesgos de seguridad online más comunes y se diseñaron instrumentos con base a la norma ISO 27001 enfocados en evaluar los controles para evitar los riesgos seleccionados; para el estudio se aplicó una encuesta utilizando un formulario en línea a una muestra de 384 personas, quienes han realizado compras a través de internet. De los resultados obtenidos se destaca que las plataformas más utilizadas para realizar comercio electrónico son WhatsApp, Facebook y tiendas en línea encontrando mayor nivel de riesgo en las transacciones con tiendas en línea, los riesgos de seguridad con mayor probabilidad de riesgos encontrados fueron: *adware*, *phishing* y *baiting*.

Palabras clave: riesgo; amenaza; vulnerabilidad; seguridad informática

Abstract

Covid 19 was a pandemic that forced people, institutions and companies to change the way they work and due to the restrictions that were imposed, the internet became the fundamental tool for everyone to continue carrying out their activities virtually. The applications and services offered on the internet were of great benefit, especially for small businesses who saw in commerce an opportunity to reach their customers with their products and these, in turn, a safe way of supplying themselves; but it is important to keep in mind when using these technologies that there are threats and computer security risks that could affect if you are not protected. The objective of this investigation was to analyze the main computer security risks to which the inhabitants of the El Carmen canton are exposed when carrying out electronic commerce activities in times of pandemic; A quantitative investigation was applied to analyze the possible risks and their level of severity, a MAGERIT Risk analysis methodology was used, considering the protection of personal information as an asset, a bibliographical investigation was carried out to select the most common online security risks and Instruments were designed based on the ISO 27001 standard focused on evaluating the controls to avoid the selected risks; For the study, a survey was applied using an online form to a sample of 384 people, who have made purchases over the Internet. From the results obtained, it stands out that the most used platforms for electronic commerce are WhatsApp, Facebook and online stores, finding a higher level of risk in transactions with online stores, the security risks with the highest probability of risks found were: adware, phishing and baiting.

Keywords: *risk; threat; vulnerability; computer security*

Fecha de recibido: 24/07/2023
Fecha de aceptado: 27/09/2023
Fecha de publicado: 19/10/2023

Introducción

El comercio electrónico, *e-comerce*, consiste en la compra y venta de información, servicios y productos, utilizando medios electrónicos sin la necesidad de contacto físico entre vendedor y comprador, este tipo de transacción tuvo un considerable crecimiento a razón del confinamiento debido al Covid 19; muchos usuarios

utilizaron este servicio de tecnología para adquirir productos variados y los comerciantes por su parte aprovecharon plataformas virtuales para ofrecer sus productos y llegar a más clientes en medio de las restricciones de movilidad por la situación sanitaria.

En la actualidad acceder a aplicaciones por medio de internet conlleva riesgos de seguridad informática que muchos usuarios de estas plataformas desconocen y se exponen a dichos peligros porque no aplican políticas y controles de seguridad para proteger su información; por lo tanto es importante evaluar las vulnerabilidades de seguridad que tienen las personas al momento de utilizar aplicaciones informáticas. La seguridad informática consiste en proteger los elementos de un sistema de información, implementar métodos para asegurar la información, descubrir incidentes, intrusos, entre otros; cuando la información se encuentre en riesgo (Figueroa Suárez, Rodríguez Andrade, Bone Obando, & Saltos Gómez, 2017).

Existen metodologías de análisis de riesgos que especifican el proceso a seguir para determinar las vulnerabilidades existentes en los sistemas y analizar la gravedad de riesgos en función de su probabilidad e impacto.

Marco teórico

Seguridad Informática

La seguridad informática es el proceso de proteger a los sistemas informáticos y a la información digital, por medio de normas, políticas o protocolos que impiden el acceso a intrusos o personal no autorizado minimizando el factor riesgo de ataques digitales (Baca Urbina, 2018). Tiene como objetivo respaldar la confidencialidad e integridad de la información impidiendo operaciones que no estén permitidas, sobre todo la publicación, modificación o eliminación (Alvarez Basaldúa, 2005).

Seguridad de la Información

Según la Norma ISO 27001 es la "preservación de la confidencialidad, la integridad y disponibilidad de la información, pudiendo además abarcar otras propiedades como autenticidad, responsabilidad, fiabilidad y no repudio". Garantiza un proceso libre de peligro, riesgo o daño. Por su parte Gascó(2013) la define como conjunto de políticas, medidas y procedimientos, que se realizan con la finalidad de proteger la confidencialidad, disponibilidad e integridad de la información.

Principios de Seguridad de la Información

Los principios de seguridad de la información según ISO 27001 son:

- **Confidencialidad**: es la propiedad que garantiza que la información sea utilizada por personas o máquinas debidamente autorizadas, utilizando para ello mecanismos como: autenticación, cifrado y autorización. (Buendía, 2013, pag.15)
- **Integridad:** se refiere a la exactitud y consistencia generales de los datos o expresado de otra forma, la información que se recibe sea precisa y completa, de acuerdo con los valores y expectativas del negocio. (Urbina, 2016,pag.13)
- **Disponibilidad:** En el contexto de los sistemas de información se refiere a la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto (ISO 27001, s.f.)

Análisis de Riesgos

Es una tarea esencial que permite determinar indicios de amenazas, además de realizar la preparación, comprobación y búsqueda de las estrategias de seguridad con el propósito de brindar seguridad de la información a empresas o instituciones (Villalba Fernández & Corchado Rodríguez, 2017).

El análisis de riesgo consiste principalmente en estudiar las vulnerabilidades en sistemas informáticos, plataformas educativas, entre otros. El riesgo permite tomar decisiones para proteger de mejor manera los sistemas de información y se enfoca en velar que se cumplan las políticas de seguridad de la información, privacidad o contraseñas, siendo un proceso riguroso que va desde la identificación de los activos informáticos, y la información que se encuentre vulnerable (Avenía, 2017)

Vulnerabilidad

Según Romero (2018, pág. 41) una vulnerabilidad es "un fallo en un sistema que puede ser explotada por un atacante generando un riesgo para la organización o para el mismo sistema, esta puede ser lógica o física", esta condición puede significar que un atacante comprometa la integridad, confidencialidad e integridad de la información.

Amenaza

Es toda acción que, aprovechando una vulnerabilidad atenta a la seguridad de un sistema, provocando un efecto negativo sobre algún elemento, sus orígenes pueden ser diversos: sucesos físicos, fraudes, robos, malware, incluso efectos de decisiones internas o negligencias.

Riesgo

Para Postiguio (Postigo Palacios, 2020) un riesgo es la posibilidad que se produzca un impacto en la organización, esencialmente la posibilidad de ocurrencia de un evento no deseadode consecuencias negativas, en el contexto, sobre la seguridad de los recursos de información

Principales riesgos asociados al comercio electrónico

Las amenazas y ataques en la red son cada vez más sofisticados y sus consecuencias más costosas para las personas y empresas.

- **Malware:** Programas creados para causar daño a un dispositivo tecnológico y lograr algún tipo de beneficio (Ujaen, 2018).
- **Phishing:** Es la forma de engañar, suplantar la identidad con el fin de conseguir contraseñas o cualquier información personal (Cruz Gavilanes & Martínez Santander, 2017). Tipo de ataque de ingeniería social utilizado con frecuencia para robar datos personales a usuarios, el atacante finge ser una entidad de confianza para engañar a su víctima para que abra mensajes de texto, correo (Mittnick, 2022).
- **Baiting:** Es un cebo que utilizan los atacantes para transmitir algún tipo de virus a sus equipos y conseguir información sensible (Cortés Hernández, 2019).
- **Spam:** Son mensajes no solicitados, molestosos que pueden provocar daños en los equipos o hurtar información personal (Sevilla, 2011).

Comercio Electrónico

El comercio electrónico o e-commerce, consiste en la compra y venta de productos y servicios a través de medios electrónicos empleando las tecnologías de la información y la comunicación que permiten evitar el contacto físico entre comprador y vendedor para realizar compras o ventas por internet. Hoy en día, con la sociedad de la información y el libre acceso a internet, el comercio electrónico ha experimentado un auge espectacular con cientos de páginas activas ya que en la actualidad se realizan actividades electrónicas a gran escala (Martín, 2018).

El comercio electrónico o comercio en línea facilita a las personas que tienen negocios interactuar con otros comerciantes, proveedores y clientes de diferentes lugares en tiempo real (Gutiérrez Torres, 2017). E-comerce ayuda a muchas empresas y negocios para alcanzar sus objetivos, con inversiones económicas menores a diferencia del comercio físico y además a obtener ventajas competitivas en el mercado.

El comercio electrónico permite enviar mensajes de textos y ficheros de diferentes tipos a usuarios a través del internet desde diferentes lugares; estos mensajes son transmitidos de un usuario a otro en cuestión de segundos y además se puede enviar todo tipo de información o programas, ayudando a que el proceso sea más versátil y rápido a diferencia del correo tradicional o el fax (Palomar Delgado, 2019)

Ventajas del comercio electrónico

El comercio electrónico puede utilizarse en cualquier entorno en el que intercambie productos o servicios entre el vendedor y el consumidor. Los beneficios que se obtienen son varios, entre ellos: reducción del trabajo administrativo, transacciones comerciales inmediatas, precisas y eficientes, facilidad de acceso a la información y a los productos que ofrece la empresa; y reducción de la necesidad de reescribir la información en los sistemas de información (Basantes et al, 2016).

Materiales y métodos

Se aplicó una investigación bibliográfica para analizar los riesgos de seguridad más comunes que afectan a las transacciones a través de internet.

Investigación Cuantitativa

Para el presente estudio se aplicó investigación cuantitativa para ello se elaboró una encuesta estandarizada diseñada con base a la Norma ISO 27001, enfocada a evaluar qué controles de seguridad aplican las personas al momento de utilizar plataformas virtuales para actividades de comercio electrónico. Una vez aplicadas fueron tabuladas en una hoja de cálculo y aplicando una matriz de riesgos se valoró la gravedad de cada uno.

Población y Muestra

La población que se tomó para esta investigación fueron los habitantes del cantón El Carmen mayores de 18 años los según el censo del 2010 corresponde a 791.100 habitantes.

Se obtuvo un tamaño de muestra de 384 habitantes del cantón El Carmen, se calculó mediante muestreo probabilístico aleatorio estratificado, se consideraron grupos: personas que realizaron compras y personas que ofrecieron y vendieron sus productos a través de canales electrónicos, con un nivel de confianza del 95% y con un margen de error del 5 %.

Metodología

Para el desarrollo de la presente investigación se aplicó una metodología de análisis de riesgos MAGERIT, con sus respectivas fases:

1. Determinación de activos
2. Determinación de amenazas
3. Valoración de Riesgos

1. Determinación de activos

Datos personales: Los datos personales son considerados como cualquier información vinculada o que pueda asociarse a una o varias personas naturales identificadas o identificables: nombre y apellido, fecha de nacimiento, dirección domiciliaria, correo electrónico, número de teléfono, número de cédula, matrícula vehicular, información patrimonial e información académica o cualquier otra información vinculada con la identidad del titular (Enríquez Álvares, 2017).

2. Determinación de Amenazas

Se establecieron como posibles amenazas las siguientes: *baiting*, ataques vía web y ataques a las aplicaciones web.

Tabla 1: Definición de Activos.

No.	Amenazas	Vulnerabilidad
A1	Malware	Pérdida de información
		Descargas no controladas de internet
		Almacenamiento sin protección
		Falta de actualización del sistema
		Carencia de antivirus
		Falta de actualización de antivirus
		Falta de actualización de navegadores
A2	Phishing	Carencia de mecanismos de autenticación
		Inadecuada gestión de contraseñas
		Inadecuada protección de contraseñas
		Sesiones de usuarios habilitadas
		Pérdida, modificación o eliminación de información
		Carencia de antivirus
		Falta de actualización de antivirus
		Poca aplicación de políticas
A3	Spam	Pérdida de información
		Carencia de filtros anti-spam
		Carencia de antivirus
		Falta de actualización de antivirus
A5	*Baiting*	Carencia de antivirus
		Falta de actualización de antivirus

		Pérdida de información
		Descargas no controladas
		Acceso no autorizado
		Entrega de información sensible

3. Valoración de Riesgos

Para determinar el nivel de riesgo se diseñó un instrumento que evaluó los controles de seguridad aplicado por las personas al momento de realizar sus transacciones electrónicas, el mismo que constó de 20 preguntas por cada riesgo identificado, el mismo que fue llenado en un formulario en línea. Se procedió a la tabulación de los datos con la siguiente consideración:

1= Existe el control (es seguro).
0= No existe el control (no es seguro).
2= No aplica.

Con la información obtenida se procedió a valorar el riesgo, para lo cual se consideró la probabilidad y el impacto, utilizando una matriz de riesgos.

Gravedad de riesgo= probabilidad* impacto

El diseño de instrumentos se muestra a continuación:

Cuestionario **para identificar riesgos asociados al realizar transacciones electrónicas**			
Riesgo: Adware		**SI**	**NO**
Cuestionario para identificar riesgos asociados al realizar transacciones electrónicas			
Riesgo: Phishing		**SI**	**NO**
1	¿Conoce sobre el robo de datos mediante medios electrónicos?		
2	¿Utiliza contraseñas fuertes mayores de 10 dígitos en su cuenta?		
3	¿Su contraseña contiene letras mayúsculas, números y caracteres especiales?		
4	¿Usted suele compartir copias de su cédula de identidad con personas extrañas?		
5	¿Actualiza con frecuencia la contraseña de sus redes sociales?		
6	¿La información en sus redes sociales está visibles para todas las personas?		
7	¿Conoce sobre las políticas de privacidad de WhatsApp?		
8	¿La información de su perfil de WhatsApp se encuentra disponible para todos?		
9	¿Proporciona sus datos sensibles a terceras personas?		
10	¿Comparte su ubicación en tiempo real?		
11	¿Conoce las políticas de seguridad que ofrece WhatsApp?		
12	¿Usted comparte su contraseña de redes sociales con otras personas?		
13	¿Usted tiene activado la verificación en dos pasos (PIN de verificación) en WhatsApp?		
14	¿Usted conoce si el sitio donde realiza compras en línea es seguro?		
15	¿Usted suele dejar olvidado sus dispositivos en lugares públicos?		
16	¿Utiliza una red privada para realizar sus compras en línea?		
17	¿Ha utilizado redes wifi-públicas para realizar transacciones electrónicas?		
18	¿Usted publica fotos de información confidencial en sus redes sociales?		
19	¿Ha facilitado información confidencial algún desconocido en redes sociales?		
20	¿Tiene limitaciones de quien pueden ver sus publicidades?		
Riesgo: Malware			
1	¿Usted accede a ofertas especiales que aparecen como anuncios?		
2	¿Usted verifica la dirección de los correos que recibe antes de abrirlos?		
3	¿Usted descarga archivos que le envían a su correo de sitios desconocidos?		
4	¿Cuenta con programas de antivirus en sus equipos electrónicos?		
5	¿Mantiene actualizado el programa de antivirus en sus equipos?		
6	¿Usted descarga sus aplicaciones de sitios oficiales?		
7	¿Usted utiliza los links que le envían a su correo para acceder algún sitio?		
8	¿Usted abre correos de remitentes desconocidos?		
9	¿Usted suele conectar dispositivos de almacenamiento externo de otras personas en su ordenador?		
10	¿Usted descarga aplicaciones de Play Store en su teléfono?		
11	¿Usted realiza respaldo de su información?		
12	¿Usted mantiene actualizado su sistema operativo?		
13	¿Su red Wifi cuenta con una contraseña segura?		
14	¿Usted navega a través de redes Wifi-públicas?		
15	¿Usted visita sitios web desconocidos?		
16	¿Usted mantiene seguro sus documentos personales?		
17	¿Usted utiliza la misma contraseña para todas sus cuentas?		
18	¿Utiliza la misma dirección de correo en todas sus cuentas?		
19	¿Su contraseña contiene letras mayúsculas, números y caracteres especiales?		
20	¿Utiliza fechas en sus contraseñas?		

Riesgo: Baiting			
	PREGUNTA	SI	NO
1	¿Conoce sobre los peligros del Baiting?		
2	¿Usted revisa de donde proviene un correo antes de abrirlo?		
3	¿Usted accede a publicidades sobre descuentos especiales?		
4	¿Usted ha accedido alguna oferta de un producto a través de un enlace?		
5	¿Usted se ha encontrado algún pendrive en la calle?		
6	¿Ha insertado en su ordenador algún pendrive que se haya encontrado botado?		
7	¿Usted accede a anuncios de publicidades?		
8	¿Cuenta con programas de antivirus en sus equipos electrónicos?		
9	¿Actualiza con frecuencia los programas que utiliza a las últimas versiones?		
10	¿Utiliza su correo personal para registrarse en ofertas o promociones?		
11	¿Ha accedido algún link sin verificar su procedencia?		
12	¿Usted analiza sus archivos con un programa de antivirus antes de descargarlos?		
13	¿Usted suele conectar dispositivos de almacenamiento externo de otras personas en su ordenador?		
14	¿Utiliza contraseñas seguras mayores de 10 dígitos?		
15	¿Ha dado clic sobre algún enlace para solucionar problemas de su equipo?		
16	¿Realiza respaldo de su información?		
17	¿Usted mantiene activado el programa de antivirus en sus equipos?		
18	¿Usted proporciona información personal en enlaces desconocidos?		
19	¿Accede a sitios web a través de enlaces que recibe por correo?		
20	¿Usted actualiza constantemente sus programas de antivirus?		

Riesgo: Spam			
1	¿Usted cuenta con más de una cuenta de Email?		
2	¿Usted suele registrarse en páginas que no son fiables?		
3	¿Usted ha utilizado la opción CCO de Gmail?		
4	¿Ha recibido correos donde le solicitan que lo comparta con amigos?		
5	¿Usted facilita información confidencial a través de enunciados enviados al correo?		
6	¿Usted acostumbra a escribir su correo en lugares donde hay acceso al público?		
7	¿Utiliza su correo personal para registrarse en juegos o tiendas en línea?		
8	¿Usted recibe correos de spam frecuentemente?		
9	¿Usted revisa las políticas de privacidad de los sitios donde debe registrar su correo?		
10	¿Usted revisa detenidamente las condiciones de suscripción cuando se registra en un sitio web?		
11	¿Usted revisa los correos de spam que recibe en su correo?		
12	¿Usted suele reenviar cadenas que le comparten en su correo?		
13	¿Usted ha respondido algún correo de spam?		
14	¿Actualiza con frecuencia los programas que utiliza a las últimas versiones?		
15	¿Cuenta con programas de antivirus en sus equipos electrónicos?		
16	¿Usted reconoce los correos de spam?		
17	¿Usted suele abrir los enlaces que le envían a su correo?		
18	¿Usted realiza respaldo de su información?		
19	¿Usted suele compartir su dirección de correo con personas desconocidas?		
20	¿Usted mantiene actualizado su sistema operativo?		

Resultados y discusión

Con relación al objetivo de la investigación de evaluar los riesgos asociados al comercio electrónico se obtuvieron los siguientes resultados:

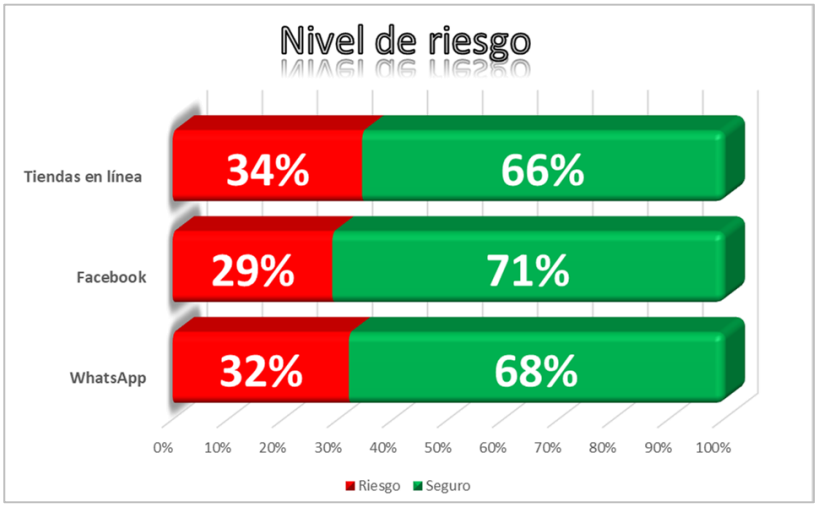

Figura 1. Nivel de Riesgo General.

Las tres plataformas más utilizadas para actividades de comercio electrónico fueron: Whatsapp, Facebook y Tiendas en línea, el nivel de seguridad en general está dentro del rango medio, presentando más vulnerabilidades al utilizar tiendas en línea.

Nivel de Riesgo por plataforma utilizada

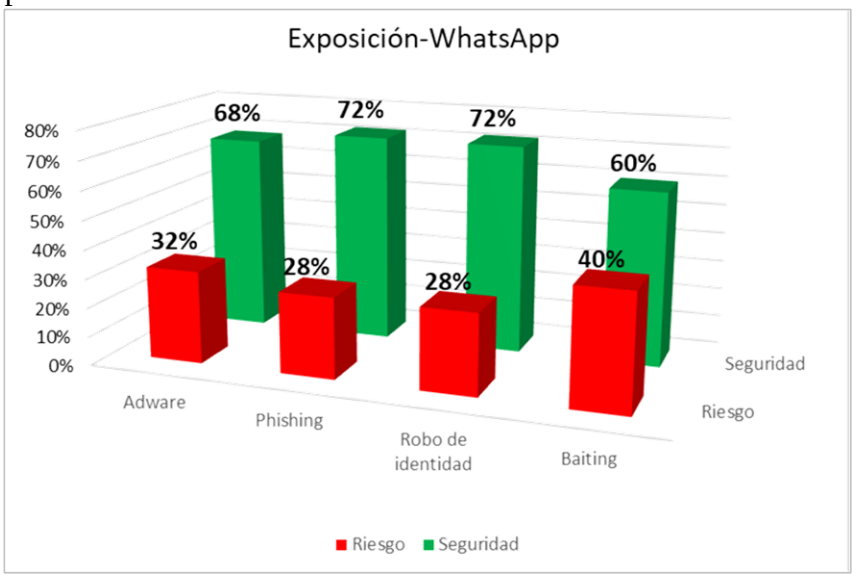

Figura 2: Nivel de Riesgo plataforma WhatsApp.

Al utilizar WhatsApp el riesgo más representativo es *Baiting* cerca de la mitad de las personas no cumplen con normas mínimas de seguridad, entre las principales vulnerabilidades están**:**

- No conocen los peligros de Baiting.
- No verifican el origen de remitente de mensajes.
- No analizan con un programa de antivirus los archivos al descargarlos.
- Conectan dispositivos de almacenamiento externo de otras personas en sus equipos.
- No cierran sesión cuando acceden a la aplicación desde un ordenador.
- No borran las descargas de archivos cuando utilizan la aplicación desde un ordenador.

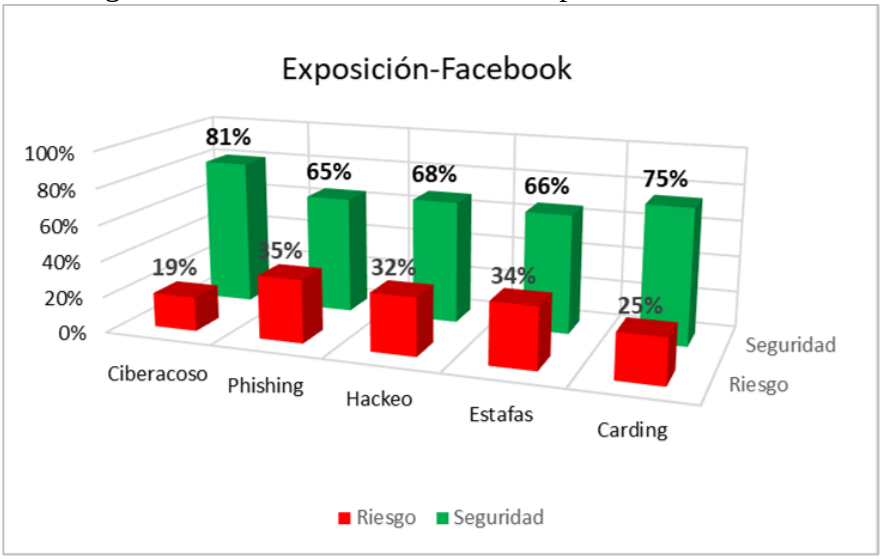

Figura 2: Nivel de Riesgos plataforma Facebook.

Al utilizar Facebook, el riesgo que tiene nivel más alto es *Phishing*, entre sus causas están:

- Las personas no actualizan con frecuencia la contraseña de sus redes sociales
- Las personas no mantienen activada la verificación en dos pasos de sus redes sociales
- Las contraseñas utilizadas no cumplen con característica de clave segura como: no están conformadas al menos por 8 caracteres, no combinan letras números y caracteres especiales, no son mezclas de mayúsculas y minúsculas.
- Mantienen abiertas las aplicaciones en los diferentes dispositivos que las utilizan
- Desconocen configuraciones de seguridad de la aplicación

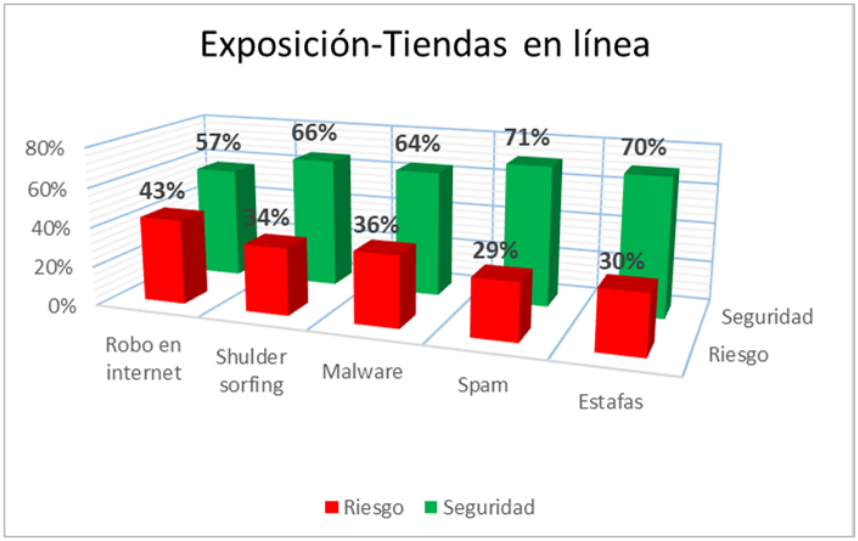

Figura 4: Nivel de Riesgos- Tiendas en Línea.

Al acceder a tiendas en línea los riesgos de mayor riesgo están el robo y malware, las principales razones son:

- Descargan archivos que reciben a su correo de sitios desconocidos.
- Suelen conectar dispositivos de almacenamiento externo de otras personas en su ordenador.
- No mantienen actualizado el sistema operativo de su ordenador.
- Las personas no cuentan con contraseñas seguras para la red de Wifi.

Conclusiones

Existen estudios de amenazas y riesgos en el uso de redes sociales en niños y adolescentes, con respecto al comercio electrónico está la publicación de Chiriguano (2015) en su artículo Comercio Electrónico: Importancia de la Seguridad en las Transacciones Electrónicas, Amenazas y Soluciones a Implementar, quien cita como amenazas externas más comunes Virus, spyware, ataques de piratas informáticos, coincidiendo en parte con los obtenidos en este Phishing, baiting y robos a través de internet.

En la actualidad la tecnología ofrece muchos beneficios y en esta época de pandemia se incrementó el acceso a diversidad de servicios desde la comodidad del hogar, en el Cantón El Carmen las personas que realizaron actividades de comercio electrónico durante la pandemia del Covid, están expuestas a riesgos de seguridad informática, principalmente a Phishing, baiting y robos a través de internet.

La seguridad de la información digital encuentra su punto más vulnerable en el elemento humano, quien por desconocimiento o comodidad no pone en práctica mecanismos de seguridad para proteger su información personal, muchos de los cuales no requieren de inversión económica.

En el cantón El Carmen existe un alto porcentaje de la población que ha realizado algún tipo de transacción electrónica, pero desconoce de la existencia de las amenazas asociadas al uso de tecnología.

Referencias

Aguilera López, P. (2010). Seguridad informática. México: Editex.

Alvarez Basaldúa, L. D. (2005). Seguridad en Informática. México: Iberoamericana.

Baca Urbina, G. (2016). Introducción a la seguridad informática. México: Patria.

Briceño, E. V. (2021). Seguridad de la información. Alzamora: Editorial Área de Innovación y Desarrollo,S.L.

Chiriguayo Lozano, J. (2015). Comercio Electrónico: IMportancia de la Seguridad en las transacciones electrónicas, amenazas y soluciones a implementar. Revista Empresarial, ICE-FEE-UCSG, 8-14.

Cortés Hernández, A. (2019). Ingeniería social: Baiting. Science, 1-10.

Cruz Gavilanes, Y., & Martínez Santander, C. (2017). Ataques de ingeniería social. Dominio de las ciencias, 1-12.

Gascó, E. (2013). Seguridad Informática. Madrid: Macmillan Iberia.

Gutiérrez Torres, D. (2017). Comercio electrónico:creación y protección de un sitio web. Medellin Colombia: Ediciones Unaula . Obtenido de https://elibro.net/es/ereader/uleam/164536?page=25.

Mittnick, S. (2022). Seguridad Cibernética. SEguridad en internet y protección para niños, adolescentes padres y profesionales. Belbecub.

Murillo, Á., Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., . . . Castillo, M. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Alicante: Editorial Área de Innovación y Desarrollo, S.L.

Ovalle Vélez, K. (2019). Repository.ucatolica.edu.co. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/24062/1/Ciberseguridad%20WiFi%20en%20Hogares.pdf

Palomar Delgado , D. (2019). Introducción al comercio y negocio electrónico . Edicones Universidad de Salamanca(España). Obtenido de http://hdl.handle.net/10366/139689

Pérez Sánchez, V. (2017). Seguridad y salud. Málaga: IC.

Postigo Palacios, A. (2020). Seguridad Infromática. Madrid: Ediciones Paraninfo.

Robles Torrente, D. (2015). Análisis de la seguridad privada. Barcelona: UOC.

Romero, M., Figueroa, G., Vera, D., & Alava, J. (2018). Introducción a la seguridad informática y sus vulnerabilidades. Guayaquil: 3 Ciencias.

Sevilla, B. (2011). Spam. España: Facua.

Ujaen. (2018). Guías de seguridad. España: Universidad de Jaén. Obtenido de https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guiaspracticas/Guias%20de%20seguridad%20UJA%20-%203.%20Malware.pdf

Villalón Huerta, A. (2019). Seguridad en Unix y redes. Versión 2.1. España: Nau Llibres- Edicions Culturals Valencines, S.A.