DOI: http://dx.doi.org/10.23857/dc.v8i1.2622

Ciencias Técnicas y Aplicadas
Artículo de Revisión

Análisis de ciberataques sobre el uso de redes sociales en relación a la protección de datos personales en Ecuador

Analysis of cyberattacks in social media related to the protection of personal data in Ecuador

Análise de ataques cibernéticos no uso de redes sociais em relação à proteção de dados pessoais no Equador

Ariana Dennise Escobar-Macías [I]
ariana.escobar.60@est.ucacue.edu.ec
https://orcid.org/0000-0003-2630-3328

María Daniela Álvarez-Galarza [II]
maria.alvarez@ucacue.edu.ec
https://orcid.org/0000-0001-6702-7783

Correspondencia: ariana.escobar.60@est.ucacue.edu.ec

*Recibido: 19 de diciembre del 2021 *Aceptado: 15 de enero de 2022 * Publicado: 18 de febrero de 2022

I. Estudiante de la Maestría en Ciberseguridad, Universidad Católica de Cuenca, Cuenca, Ecuador.
II. Magíster en Seguridad Informática Aplicada, Máster Universitario en Derecho de la Ciberseguridad y Entorno Digital, Ingeniero de Sistemas, Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

El internet es actualmente una de las áreas de mayor crecimiento debido a sus diversas áreas de aplicación, por esta razón el número de usuarios de redes sociales se ha incrementado en gran parte en la última década, así como también los ciberataques ocurridos en dichos sitios en línea. La investigación consiste en analizar los ciberataques en sitios de redes sociales y su relación con la protección de datos personales. Para ello, se utilizó la tipología de investigación mixta basada en la revisión documental y en las encuestas realizadas a una muestra establecida a personas entre 18-29 años, que utilizan redes sociales y viven en el territorio nacional. Los resultados obtenidos muestran que, aunque gran parte de la población ecuatoriana ha sido víctima de ciberataques, los usuarios no son conscientes de los riesgos y las medidas de seguridad que se pueden emplear para mitigar amenazas en redes sociales. Adicionalmente, se destacan los esfuerzos del gobierno ecuatoriano por proponer iniciativas que ayuden a frenar este problema y se presentan recomendaciones que pueden ser adoptadas por los usuarios para prevenir que sean víctimas de ciberataques y lograr así un entorno cibernético más seguro.

Palabras clave: Ciberataque; redes sociales; protección de datos personales; ciberseguridad; ciberriesgos; delitos informáticos.

Abstract

The internet is currently one of the fastest growing areas due to its various application areas, for this reason the number of users of social networks has increased greatly part in the last decade, as well as cyberattacks that occurred on such online sites. The investigation consists of analyzing cyberattacks on social networking sites and their relationship with the protection of personal data. For this, the mixed research typology was used based on the documentary review and on the surveys carried out on a sample of people between 18 and 29 years old, who use social networks and live in the national territory. The results showed that, although a large part of the Ecuadorian population has been the victim of cyberattacks, users are not aware of the risks and the security measures that can be used to mitigate threats on social networks. In addition, the efforts of the Ecuadorian government to propose initiatives that help curb this current problem are highlighted and recommendations are presented that can be chosen by users to prevent them from being victims of cyber attacks and thus achieve a safer cyber environment.

Keywords: Cyber attack; social networks; personal data protection; cybersecurity; cyber risks; cybercrime.

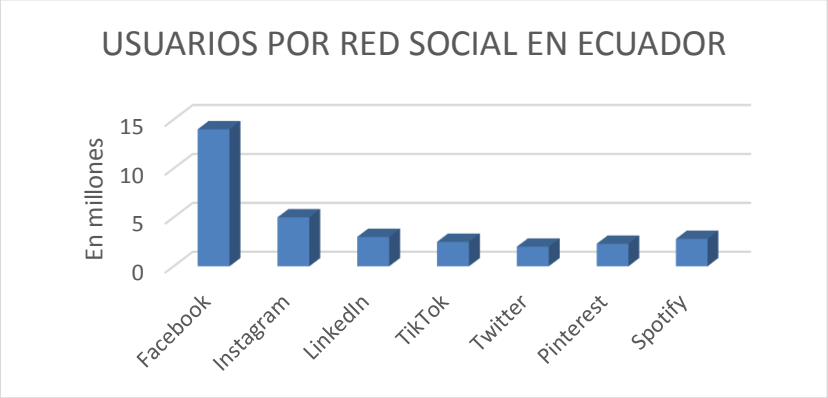
Resumo

A internet é atualmente uma das áreas que mais cresce devido às suas diversas áreas de aplicação, por este motivo o número de utilizadores das redes sociais aumentou muito na última década, assim como os ciberataques que têm ocorrido nestes sites em linha. A pesquisa consiste em analisar ciberataques em sites de redes sociais e sua relação com a proteção de dados pessoais. Para isso, utilizou-se a tipologia de pesquisa mista com base em revisão documental e levantamentos realizados em uma amostra estabelecida de pessoas entre 18-29 anos, que usam redes sociais e vivem em território nacional. Os resultados obtidos mostram que, embora grande parte da população equatoriana tenha sido vítima de ataques cibernéticos, os usuários não estão cientes dos riscos e das medidas de segurança que podem ser usadas para mitigar as ameaças nas redes sociais. Além disso, destacam-se os esforços do governo equatoriano para propor iniciativas que ajudem a conter esse problema e são apresentadas recomendações que podem ser adotadas pelos usuários para evitar que sejam vítimas de ataques cibernéticos e, assim, alcançar um ambiente cibernético mais seguro.

Palavras-chave: Ataque cibernético; redes sociais; proteção de dados pessoais; cíber segurança; riscos cibernéticos; Cibercrime.

Introducción

Sin duda alguna, vivimos en un mundo hiperconectado lo cual ha favorecido en gran medida al desarrollo de las actividades diarias de la sociedad actual, pues permite una comunicación directa y permanente entre los millones de dispositivos conectados al internet. En el Ecuador, hasta enero de 2021 aproximadamente más de 14.25 millones de personas cuentan con perfiles en redes sociales, siendo la más popular Facebook seguida de Instagram (Alcázar, 2021).



Fuente: (Alcázar, 2021)

Actualmente, las redes sociales y los servicios en línea se han convertido en parte de la vida del ser humano, a diario compartimos gran cantidad de información en estas plataformas, lo cual representa un riesgo para los usuarios ya que muchas veces desconocemos el tratamiento que los fabricantes de estas herramientas puedan darles a los datos personales que compartimos en dichas redes.

Los datos personales se definen como "registros u otra información que por sí sola o vinculada con otros datos, puede revelar la identidad de una persona viva. Así, por ejemplo, puede utilizar números en lugar de nombres como identificadores (CEPAL, 2020). Estos datos pueden ser: nombre completo, edad, teléfono y también puede incluir creencias, procedimientos jurídicos, cuentas personales, etc.

Durante el avance de la sociedad se establece también el desarrollo tecnológico, donde hay nuevos riesgos para la protección de datos personales; por ello, se debe reconocer la transferencia de datos como un comportamiento o "causa ineludible de la titularidad del derecho a la intimidad y el innato poder de control de datos" (Villalba, 2017, pág. 11).

En el caso de Ecuador para la protección de datos se ha establecido un modelo de integración que va alineado con el proyecto de Ley Orgánica sobre la Protección de Datos Personales donde, además se consolida la Ley Interamericana con los principios y estudios elaborados por la Organización de Estados Americanos (OEA). Es así, como se ingresa a una era globalizada donde resalta la importancia del formato jurídico, asegurando así el ejercicio pleno de los derechos en la evolución del paradigma tecnológico y constitucional (Ordóñez, 2017).

Sin embargo, pese a los esfuerzos a nivel legal han ocurrido varios incidentes de ciberataques, que ha ubicado a Ecuador en el séptimo lugar dentro de los países de la región como inseguro. Los

delincuentes utilizan diferentes técnicas como el phishing, spear-phishing, el watering-hole e incluso la infección de infraestructura utilizando todo tipo de malware (UNIR, 2021).

El objetivo general señalado es analizar los ciberataques sobre el uso de las redes sociales en relación a la protección de datos personales en Ecuador, de donde se desprende tres objetivos específicos: Reconocer la magnitud de los ciberataques a través de las redes sociales; Verificar la ciberdefensa de Ecuador y sugerir estrategias a los usuarios de redes sociales para protegerse de los ciberataques.

Metodología

La investigación fue desarrollada bajo la tipología mixta reconocida por una "mixtura (mezcla) de los métodos cualitativos y cuantitativos" (Pacheco, 2015, pág. 731). En este punto se establecieron estrategias y procedimientos relacionados con la recolección de datos desde las teorías, los instrumentos, la muestra, el análisis de datos, la interpretación y la discusión de resultados.

La población de estudio correspondió a los ecuatorianos entre 18 a 29 años de edad, de acuerdo con las proyecciones censales realizadas por el Instituto Nacional de Estadísticas y Censos INEC, esta cifra corresponde a 3.550.102 personas (Cervantes, 2020); para calcular la muestra, se utilizó la siguiente fórmula:

$$n = \frac{k^2 * p * q * N}{(e^2 * (N-1) + k^2 * p * q} = 384$$

Donde las variables corresponden a:

n = Población

k = 1,96 (nivel de confianza).

p = 0,5 (probabilidad de éxitos).

q = 0,5 (probabilidad de fracaso).

E=5% (error de estimación)

El instrumento de recolección de datos necesario para complementar la investigación se basó en la definición que comprende "herramientas conceptuales o materiales, mediante los cuales se recogieron los datos e informaciones, mediante preguntas, ítems que exigen respuestas del investigado" (Ñaupas, Valdivia, Palacios, & Romero, 2018, pág. 273).

Uno de los instrumentos más utilizados es la encuesta como un modelo, consistente en "formular un conjunto sistemático de preguntas escritas, en una cédula, que están relacionadas a hipótesis de trabajo y por ende a las variables e indicadores de investigación" (Ñaupas, Valdivia, Palacios, & Romero, 2018, pág. 291). El formato de la encuesta estubo conformado por preguntas cerradas, dicotómicas y politómicas enviadas por medios digitales para garantizar la confidencialidad y resultados óptimos.

Resultados y discusión

De la muestra de 384 personas, se puede observar que un 25% corresponden al grupo de 22 - 24 años, un 20% tienen entre 20 – 22 años, un 19% tienen entre 26-28 años, un 15% tienen entre 24- 26 años, un 11% tienen entre 28 – 29 años y un 10% tienen entre 18 – 20 años. Con el objetivo de analizar qué tipo de información puede ser vulnerable desde los dispositivos electrónicos, se consultó acerca de qué otras actividades realizan en su celular además de gestionar sus redes sociales, y se pudo observar que, un 45% realizan descarga de archivos, un 23% realizan pagos por aplicaciones, un 22% realizan actividades relacionadas con el comercio electrónico y un 10% gestionan su correo electrónico. Todas estas actividades comprometen datos personales del usuario y generan una mayor probabilidad de ser víctimas de un ciberataque.

Para verificar la vulnerabilidad de las personas en redes sociales, se consultó también si alguna vez han sido víctimas de un ciberataque, donde un 75% indicaron que en efecto han sido víctimas de un ciberataque, entre los cuales mencionan ciberbullying o ciberacoso, chantaje sexual, suplantación de identidad y robo de información o publicación de información privada, mientras que un 25% no han sido víctimas de un ciberataque a través de sus redes sociales. Finalmente, se consultó si conocen las medidas de ciberseguridad generadas por el gobierno ecuatoriano para la protección de los datos personales de los ecuatorianos, con lo cual un 33% indicaron que si lo conocen mientras que un 67% indicaron que no. Por lo que, se denota la falta de concienciación en relación a la ciberseguridad y la protección de datos personales, siendo esta última un derecho de los ciudadanos.

De acuerdo a la revisión bibliográfica se verifica que, desde el gobierno ecuatoriano los esfuerzos para proteger a la ciudadanía frente a amenazas cibernéticas empezaron en 2019, con la creación de un plan para el manejo de crisis y junto con el Ministerio de Telecomunicaciones, inició la consultoría para la elaboración de su Estrategia Nacional de Ciberseguridad, que tiene como objetivo "…*que*

Ecuador fortalezca y asegure su entorno digital…" (Gobierno de la República del Ecuador, 2019), lo cual sin duda supone un avance en cuanto a políticas orientadas a detener el aumento de ciberataques que puedan suponer un riesgo tanto para la seguridad del estado como sus ciudadanos; así como también limitar el uso inapropiado de la información personal de los ecuatorianos, creando la guía de protección de datos personales y la Ley Orgánica de Protección de Datos Personales, aprobada por el ejecutivo en el mes de mayo de 2021. (Ministerio de Telecomunicaciones, 2020) Adicionalmente, se ha establecido un esquema de seguridad de la información, implementando así las Normas Técnicas Ecuatorianas para la Gestión de Seguridad de la Información, el Plan Nacional de Seguridad Integral (PNSI) 2014-2017 y más recientemente en conjunto con el Ministerio de Educación, se elaboró la política pública sobre internet seguro para niñas, niños y adolescentes, la cual está "…*destinada a promover conductas protectoras o preventivas de factores de riesgos que pueden poner en peligro la integridad y dignidad de niñas, niños y adolescentes ante el acceso y uso de internet; y cuando tales vulneraciones han sucedido, promover protocolos adecuados de atención para la protección, atención y reparación..*." (Ministerio de Telecomunicaciones, 2020)

De acuerdo, a los datos obtenidos en la encuesta realizada, se verifica que, pese a los esfuerzos públicos realizados, aún existe un alto nivel de desconocimiento acerca de las mejores prácticas que se deben seguir para prevenir un ciberataque y así mismo, se desconoce cómo actuar frente a un caso de ciberdelincuencia.

Por otro lado, a nivel internacional, un estudio realizado por (Centeno, 2015) compara los ciberataques con el terrorismo convencional como primera amenaza a los E.E.U.U. ya que, al sustraer información confidencial, produce graves pérdidas en las industrias. Se calcula que ataques causados por robo de información le costaron cerca de 300.000 millones de dólares a E.E.U.U en el año 2012. Así como también, (Ritter et al., 2015) en su estudio "Weakly Supervised Extraction of Computer Security Events from Twitter" menciona que todos los días se informa una gran cantidad de eventos de seguridad en las redes sociales, los cuales incluyen desde usuarios promedio que se quejan de que sus cuentas de correo electrónico han sido secuestradas hasta filtraciones masivas de datos que involucran a corporaciones internacionales.

Así mismo, con base a la revisión realizada acerca de las dimensiones vinculadas a la seguridad y protección de datos donde Ecuador ocupa el séptimo lugar en ciberseguridad en América latina (UNIR, 2021), esta incidencia se puede verificar en los datos obtenidos en la encuesta donde un alto

porcentaje de usuarios de redes sociales han indicado que han sido víctimas de ciberataques. A continuación se presenta un resumen de los ciberataques más comunes:

Ciberacoso o ciberbullying: Se conoce así a la intimidación o agresión por medios digitales, se basa en la propagación de contenido perjudicial sobre una persona.

Suplantación de identidad: Ocurre mediante el robo de datos generalmente a través de técnicas de phishing. Los atacantes hacen uso de dichos datos para su beneficio, usualmente de forma fraudulenta o actividades ilegales.

Sextorsión: Conocido también como chantaje sexual, tiene como objetivo obtener dinero a cambio de la no publicación de contenido de carácter sexual autogenerado.

Como podemos observar, los ciberataques màs comunes están intrinsecamente ligados con la protección de los datos personales, de aquí la importancia de tomar medidas que ayuden a proteger los datos que compartimos en línea a través de las diferentes redes sociales.

Conclusiones

La creciente popularidad de las redes sociales ha ocasionado que estos sitios se conviertan en el principal campo de ataque de cibercriminales, lo cual conlleva nuevos desafíos en cuanto a la seguridad y privacidad de la información que compartimos en línea.

Actualmente los ciberdelitos van en aumento y representan un riesgo para la seguridad nacional, en especial de la población joven, quienes son los mayores consumidores de redes sociales. Por esta razón, se deben tomar las medidas adecuadas de seguridad que permitan mitigar las vulnerabilidades frente a ataques cibernéticos que compromentan los datos personales y evitar así el robo o uso indebido de los mismos.

Adicionalmente, se debe trabajar en conjunto con profesionales de la seguridad de la información y funcionarios gubernamentales para desarrollar herramientas que prevengan potenciales amenazas en internet.

Basado en las conclusiones obtenidas por la investigación se obtienen las siguientes recomendaciones:

Educar a las personas sobre el uso correcto de las redes sociales y las medidas de protección de datos personales.

A través de diferentes organizaciones fomentar y sumar esfuerzos para crear campañas de concienciación en relación al buen uso de las redes sociales y navegar seguros a través de la red.

El gobierno a través del MINTEL o la entidad correspondiente debe desarrollar un plan de comunicación para fomentar el cambio cultural en la ciudadanía en relación a las buenas prácticas de seguridad.

A través de los medios de comunicación el Gobierno debe fomentar la difusión de las buenas prácticas de seguridad de la información relacionados a la protección de datos personales y al buen uso de las redes sociales.

Dentro de la Estrategia de Ciberseguridad Nacional se debe considerar como uno de los puntos más importantes la Concienciación

Desde las escuelas tanto públicas como privadas el Ministerio de Educación debe coordinar la socialización y fomentar campañas relacionadas a concienciar sobre los riesgos relacionados a: ciberacoso, sexting, suplantación de identidad.

Referencias

1. Alcázar, J. P. (2021). *Ecuador Estado Digital Enero 2021*.
2. Cervantes, R. (2020). JÓVENES: UNA BREVE MIRADA A SU INCLUSIÓN SOCIAL. *Ministerio de Igualdad*.
3. Ministerio de Telecomunicaciones. (2020). *Política pública sobre internet seguro para niñas, niños y adolescentes*.
4. CEPAL. (2020). *Gestión de datos de investigación.* Obtenido de https://biblioguias.cepal.org/c.php?g=495473&p=4398118
5. Global Cybersecurity Index (GCI). (2018). *Global Cybersecurity Index (GCI).* Obtenido de https://drive.google.com/file/d/1roXfVn3K-DiMSlWuTvyEklfNCK7gyb15/view
6. Ñaupas, H., Valdivia, M., Palacios, J., & Romero, H. (2018). *Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis.* Bogotá: Ediciones de la U.
7. Ordóñez, L. (2017). La protección de datos personales en los estados que conforman la Comunidad Andina. *Revista de Derecho*.
8. Pacheco, M. (2015). Metodología mixta: su aplicación en México en el campo de la demografía. *Estudios Demográficos y Urbanos*.

9. UNIR. (2021). *La I Jornada Internacional de Ciberdefensa, Inteligencia y Seguridad de las Fuerzas Armadas del Ecuador y UNIR analizó las amenazas latentes de ciberataques a una nación.* Obtenido de https://ecuador.unir.net/actualidad-unir/la-i-jornada-internacional-de-ciberdefensa-inteligencia-y-seguridad-de-las-fuerzas-armadas-del-ecuador-y-unir-analizo-las-amenazas-latentes-de-ciberataques-a-una-nacion/
10. Vargas, R., Recalde, L., & Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. *Revista Latinoamericana de Estudios de Seguridad*, 31-45.
11. Villalba, A. (2017). Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa. *Revista de Derecho*.