Encuentro Internacional de Educación en Ingeniería ACOFI
2º Congreso Latinoamericano de Ingeniería
2019 10 al 13 de septiembre - Cartagena de Indias, Colombia
RETOS EN LA FORMACIÓN DE INGENIEROS EN LA ERA DIGITAL

# CIBERSEGURIDAD Y ETHICAL HACKING: LA IMPORTANCIA DE PROTEGER LOS DATOS DEL USUARIO

**Luis Armando Gaona Páez, Jesús Emiro Trillos Arenas, Andrea Natalia Bayona Moreno**

**Universidad Francisco de Paula Santander**
**Ocaña, Colombia**

## Resumen

El riesgo cibernético es un riesgo de carácter operacional que ocurre en el ciberespacio, puede comprenderse como aquel peligro o amenaza que surge al usar sistemas tecnológicos interconectados y se materializa cuando se produce una afectación a uno o varios de los tres atributos de la información, como son la confidencialidad, la integridad y la disponibilidad.

Los riesgos cibernéticos se están convirtiendo en una de las grandes preocupaciones para las organizaciones. Según el Barómetro de Riesgos de Allianz 2019, el informe anual sobre riesgos globales para las empresas elaborado por Allianz Global Corporate & Specialty (AGCS) en el que se incorpora la opinión de 2.415 expertos de 86 países, los incidentes cibernéticos, con un 37% de respuestas, aparecen entre las primeras posiciones de los *principales riesgos globales para las empresas*. Durante el 2018, la privacidad digital de más de 2,000 mil millones de personas estuvo en riego por algún problema relacionado con la seguridad de los datos. Antes de alcanzar la mitad del 2018, cinco organizaciones como lo son Aadhaar, Exactis, Under Armour, MyHeritage, y Facebook, habían expuesto cerca de 1,800 millones de registros de usuarios activos en sus plataformas.

En Colombia, 446 empresas vinculadas al sector productivo del país, reportaron haber sido víctimas de ciberataques en 2017, lo que equivale a un incremento cercano a 30% frente a los reportados un año atrás. En ocasiones, los datos que las organizaciones han expuesto surgen de productos que se comportan de acuerdo a su diseño inicial, y que con el tiempo dejan de recibir actualizaciones en la tecnología que han sido desarrolladas. De esta manera, la información personal de un usuario puede verse comprometida por fallos en el diseño del producto, es decir, del código de la misma, permitiendo el acceso no autorizado a través de la explotación de vulnerabilidades en estas aplicaciones web. Un claro ejemplo fue el bug en la red social de Google

*(Google +)*, que expuso las cuentas de más de medio millón de usuarios afectando la integridad, confiabilidad y disponibilidad de la información que se almacenaba en dicho servicio, contribuyendo al cierre de la plataforma.

Por otra parte, se reconoce que los altos costos en la implementación de mecanismos de ciberseguridad y la escasez de recursos por parte de las empresas, con llevan a que muchas organizaciones no implementen políticas y procedimientos de ciberseguridad para prevenir amenazas cibernéticas. Por lo tanto, el nivel del riesgo cibernético aumenta, esto significa que una empresa puede experimentar perdidas financiaras al verse afectada la información sensible de los usuarios de su negocio.

El propósito de nuestra investigación, fue realizar un análisis sobre la importancia de la ciberseguridad y la aplicación de técnicas de ethical hacking para proteger los datos de los usuarios, donde se abarca la definición de estándares y técnicas establecidas a nivel mundial, a fin de que las organizaciones puedan implementarlas para prevenir posibles amenazas cibernéticas y garantizar la protección de los datos de los usuarios.

**Palabras clave**: cybersecurity; ethical hacking; riesgo cibernético

***Abstract***

*The cyber risk is a risk of an operational nature that occurs in cyberspace, can be understood as that danger or threat that arises when using technological systems interconnected and materializes when there is a violation of one or more of the three attributes of information, such as the confidentiality, integrity and availability.*

*Cyber risks are becoming one of the major concerns for organizations. According to the barometer of risks of Allianz 2019, the annual report on global risks for companies prepared by Allianz Global Corporate & Specialty (AGCS), incorporating the views of 2,415 experts from 86 countries, cyber incidents, with a 37% of answers, appear among the top positions of major global risks for companies. During 2018, the digital privacy more than 2.000 billion people was in irrigation by any problem related to data security. Before reaching the half of 2018, five organizations such as Aadhaar, Exactis, Under Armour, MyHeritage, and Facebook, had exposed close to 1.800 million records of active users in their platforms.*

*In Colombia, 446 companies linked to the productive sector of the country, reported having been victims of cyber attacks in 2017, which is equivalent to an increase close to 30% compared to those reported a year ago. Sometimes, the data that organizations have exposed arise from products that behave according to their initial design, and that over time cease to receive updates in technology that have been developed. In this way, a user's personal information can be compromised by failures in the design of the product, that is to say, of the code of the same, allowing unauthorized access through the exploitation of these vulnerabilities in web applications. A clear example was the bug in the social network of Google (Google +), which exposed the accounts for more than half*

*a million users affecting the integrity, reliability and availability of the information that's stored in that service, contributing to the closure of the platform.*

*On the other hand, it is recognized that the high costs in implementing mechanisms of cybersecurity, and the lack of resources from enterprises, with lead to many organizations do not implement policies and procedures of cyber-security to prevent cyber threats. Therefore, the level of the risk increases, cyber this means that a company can experience financial losses to be affected sensitive information from users of your business.*

*The purpose of our research, was to conduct an analysis of the importance of cybersecurity and the application of ethical hacking techniques to protect users' data, where you get the definition of standards and techniques established at the global level, so that organizations can implement to prevent potential cyber threats and to ensure the protection of data of user.*

***Keywords****: cybersecurity; ethical hacking; cyber risk*

## 1. Introducción

Actualmente, las empresas ofrecen sus servicios a través de Internet, en el ciberespacio se conecta la organización con cualquier persona en distintos puntos geográficos del mundo (Allhoff & Henschke, 2018). La ventaja de la conectividad a Internet es que proporciona un acelerado crecimiento económico y crea oportunidades para los negocios y el comercio (De & Ciberseguridad, 2016). Sin embargo, la implementación de tecnologías de la información en los modelos de negocios de la empresa trae sus riesgos, uno de ellos es el riego cibernético, mediante el cual una organización puede sufrir daños en sus operaciones al producirse afectaciones a uno o varios de los tres atributos de la información, que acaban por dañar sus sistemas tecnológicos (Giant, 2016). Muchas organizaciones suelen emplear medidas como nombres de usuarios y contraseña débiles, cortafuegos con parámetros de configuración por defecto, cifrado de datos y protección antivirus, pero no implementan medidas más avanzadas para contrarrestar las amenazas cibernéticas y disminuir el riesgo cibernético (Kryszczuk, Krzysztof & Richiardi, 2011). Es importante señalar que siempre se podrá ser vulnerable a un ciberataque si no se toman las medidas básicas de seguridad para salvaguardar los datos de la empresa (Academy, 2019). "Las amenazas están evolucionando. Los ciberdelincuentes menos capacitados se ven obligados a abandonar el negocio, mientras que los más aptos intensifican su juego para sobrevivir. Eventualmente, nos quedaremos con menos adversarios, pero más inteligentes y fuertes" mencionó Joe Levy, CTO de Sophos (SOPHOS, 2019).

Según (International Telecommunication Union, 2008), "La ciberseguridad es la colección de los instrumentos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, enfoques de gestión de riesgos, acciones de formación, las mejores prácticas, de aseguramiento y las tecnologías que se pueden utilizar para proteger el medio ambiente cibernético y la organización y los activos de los usuarios. La organización y los activos de los usuarios conectados incluyen dispositivos de informática, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones, y la totalidad de la información transmitida y/o almacenada en el entorno

cibernético. La ciberseguridad se esfuerza por garantizar la consecución y el mantenimiento de las propiedades de seguridad de la organización y los activos de los usuarios contra los riesgos de seguridad pertinentes en el entorno cibernético". No obstante, una organización puede aplicar este concepto de ciberseguridad y técnicas de ethical hacking para reducir riesgos cibernéticos y posibles impactos sobre la reputación y los datos de la misma, por lo que se podrá conservar la privacidad digital de los usuarios, adelantarse a posibles ciberataques y evitar que estos ocurran. Los riesgos cibernéticos se están convirtiendo en una de las grandes preocupaciones para las organizaciones. Según el Barómetro de Riesgos de Allianz 2019, el informe anual sobre riesgos globales para las empresas elaborado por Allianz Global Corporate & Specialty (AGCS) en el que se incorpora la opinión de 2.415 expertos de 86 países, los incidentes cibernéticos, con un 37% de respuestas, aparecen entre las primeras posiciones de los principales riesgos globales para las empresas (Allianz Global Corporate & Specialty SE, 2019), de ahí la importancia de implementar ciberseguridad y técnicas de ethical hacking en una organización para preservar los activos digitales.

La mayoría de los dispositivos y servicios en la nube recopilarán datos personales básicos que pueden incluir el nombre, la dirección, la fecha de nacimiento, el correo electrónico y el número de teléfono. Los datos que cada dispositivo y aplicación puede recopilar figuran en la política de privacidad de la empresa o aplicación (Anscombe, 2018). Durante el 2018, la privacidad digital de más de 2,000 mil millones de personas estuvo en riesgo por algún problema relacionado con la seguridad de los datos. Antes de alcanzar la mitad del 2018, cinco organizaciones como lo son Aadhaar, Exactis, Under Armour, MyHeritage, y Facebook, habían expuesto cerca de 1,800 millones de registros de usuarios activos en sus plataformas (ESET, 2019). En Colombia la mayoría de los usuarios de internet y empresas no se encuentran preparados para salvaguardar la información de los ciberdelincuentes (Manuel, Rodríguez, & Informática, 2015). Por otra parte, se reconoce que los altos costos en la implementación de mecanismos de seguridad informática y la escasez de recursos por parte de las empresas (DNP, MinTIC, MDN, & DNI, 2016), con llevan a que muchas organizaciones no implementen políticas y procedimientos de ciberseguridad para prevenir amenazas cibernéticas. Por lo tanto, el nivel del riesgo cibernético aumenta, esto significa que una empresa puede experimentar perdidas financiaras al verse afectada la información sensible de su negocio. Este estudio de investigación tiene como objetivo analizar la importancia de la ciberseguridad y la aplicación de técnicas de ethical hacking para proteger los datos de los usuarios, los diferentes estándares y técnicas establecidas a nivel mundial, a fin de que las organizaciones puedan implementarlas para prevenir posibles amenazas cibernéticas y garantizar la protección de los datos de los usuarios.

## 2. Desarrollo

Muchas veces, en medios de comunicación se escuchan términos como "Mi compañía fue hackeada", "Ataques de hackers dañan sistemas", "Una nueva vulnerabilidad afecta las plataformas Windows", pero detrás de estos términos existen diferencias y muchos son utilizados de manera incorrecta, es importante conocer los conceptos de ciberseguridad y ethical hacking para no cometer errores al momento de utilizarlos.

- **Conceptos básicos**

**Vulnerabilidad:** Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información que permite que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible (INCIBE, 2017).

**Amenaza:** Se considera una amenaza toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información o la infraestructura tecnológica. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas (INCIBE, 2017).

**Riesgo cibernético:** Es un riesgo de carácter operacional que ocurre en el ciberespacio, puede comprenderse como aquel peligro o amenaza que surge al usar sistemas tecnológicos interconectados y se materializa cuando se produce una afectación a uno o varios de los tres atributos de la información (Biener, Eling, & Wirfs, 2015).

**Ataque cibernético:** Es lo que se conoce como una acción organizada por un grupo de expertos informáticos, con el objetivo de infringir daños a la red o un sistema determinado, por lo general tienen como objetivo extraer información privada, robar, espiar o extorsionar (Gobierno Nacional de Colombia, 2017).

**Hacker:** Según la (Real Academia Española, 2018), un hacker es una "Persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora", aunque en el mundo de la ciberseguridad este concepto es más amplio y se dividen en tres categorías: *Hacker Black Hat, Hacker Grey Hat, Hacker White Hat*, una diferencia importante es la intención de cada individuo al vulnerar una organización (Mansfield-Devine, 2017). Los *Hackers Black Hat* buscan fallos en la infraestructura tecnológica de la empresa, con intenciones maliciosas como el robo de datos para obtener beneficios económicos (Alvarez Basaldúa, 2005). Los *Hackers Grey Hat* utilizan ataques similares para penetrar en un sistema sin permiso, pero no para obtener ganancias financieras propias o causar daños, su intención es informar a la compañía sobre problemas de seguridad (Morales Bonilla, 2015). Los *Hacker White Hat*, son hackers éticos que emplean técnicas para explorar, probar y corregir fallos en los sistemas de una organización, el dueño de la empresa conoce los procedimientos y los diferentes análisis de seguridad que realiza el Hacker White Hat (Salinas, 2013).

**Análisis de seguridad:** Existen múltiples tipos de análisis de seguridad, generalmente varían en su alcance y profundidad. Se deben tener en cuenta conceptos como visibilidad y posicionamiento. La visibilidad tiene que ver con la información que se nos brindará previo al análisis de seguridad sobre los sistemas de información. El posicionamiento tiene que ver desde donde se llevará acabo el análisis de seguridad, es decir, si es de manera interna o externa a la organización. Aquí mencionaremos tres tipos de análisis de seguridad muy implementados a nivel mundial en muchas organizaciones como lo son (Sallis, Caracciolo, & Rodríguez, 2010):

***Vulnerability assessment:*** Es el que menor nivel de profundidad alcanza, pero, por ende, el que menor cantidad de tiempo y recursos involucra. Análisis y pruebas relacionadas con la identificación de puertos abiertos, servicios disponibles, y vulnerabilidades conocidas en los sistemas de información objetivos.

**Penetration test:** Se le conoce test de intrusión, da lugar a realizar tareas asociadas a la explotación y post-explotación de vulnerabilidades. Otra definición de este tipo de análisis de seguridad es "Conjunto de pruebas objetivas con el fin de detectar las vulnerabilidades de un sistema, teniendo muy claro que ningún sistema es 100% seguro o inviolable" (López, 2017).

**Ethical Hacking:** Para este tipo de análisis de seguridad "todo es un objetivo", es el tipo de análisis de seguridad más profundo de los tres, su propósito es analizar integralmente la seguridad de los sistemas de información, con el fin de descubrir cuáles son las debilidades que podrían llegar afectar una organización.

Estos no son los únicos tipos de análisis de seguridad que pueden llevarse a cabo sobre sistemas de información, existen otros bien definidos como análisis de riesgos, auditorias de código, la implementación de uno de ellos depende de los requerimientos y objetivos de la organización.

- **Estándares**

Para aplicar una solución de Ciberseguridad y Ethical Hacking dentro de cualquier contexto organizacional, es necesario conocer y decidir los estándares con los que se desea trabajar, o qué combinación es adecuada para proporcionar una solución completa. A continuación, se describen los principales estándares sobre ciberseguridad:

**ISO/IEC TR 27103:2018: Tecnología de la información - Técnicas de seguridad - Ciberseguridad y normas ISO e IEC.** Este documento demuestra cómo un marco de ciberseguridad puede utilizar los estándares actuales de seguridad de la información para lograr un enfoque bien controlado para la gestión de la ciberseguridad (Organisation Internationale de Normalisation, 2018).

**NIST Cibersecurity Framework:** Este Marco voluntario consta de estándares, directrices y mejores prácticas para gestionar los riesgos relacionados con la seguridad cibernética. El enfoque prioritario, flexible y rentable del Marco de Ciberseguridad ayuda a promover la protección y la resistencia de la infraestructura crítica. (National Institute of Standards and Technology, 2018).

**Directiva UE 2016/1148 del Parlamento Europeo y del Consejo de la Unión Europea:** Su objetivo es formalizar "un planteamiento global en la Unión que integre requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales." (Unión Europea, 2016).

**Orden Ejecutiva (OE 13636) USA: "**Mejora de la seguridad cibernética en infraestructuras críticas", se expone la necesidad de conceder protección legal a las empresas que compartan con

el Gobierno información sobre amenazas cibernéticas, y la necesidad de proteger la infraestructura tecnológica de las organizaciones (Reed, 2017).

**ISO/IEC 27032:** "La norma ISO/IEC 27032 facilita la colaboración segura y fiable para proteger la privacidad de las personas en todo el mundo. De esta manera, puede ayudar a prepararse, detectar, monitorizar y responder a los ataques" (Organisation Internationale de Normalisation, 2012).

**UIT-T X.1205 de 2008:** La Recomendación UIT-T X.1205 ofrece una definición de ciberseguridad. En ella se expone la clasificación de las amenazas de seguridad desde el punto de vista de una organización (Unión Internacional de Telecomunicaciones, 2008).

**Convenio de Budapest:** El Convenio de Budapest es un instrumento internacional que busca hacer similar la manera en que los diversos países contratantes abordan y definen la cibercriminalidad (Serie de Tratados Europeos N-185, 2001).

Lo ideal es que la organización combine la implementación de estándares y análisis de seguridad al tiempo, para que pueda evaluar a qué está expuesta la empresa y tomar la decisión correcta sobre la gestión de los riesgos cibernéticos.

## 3. Metodología

La metodología que se ha utilizado es cualitativa de alcance descriptivo que permite describir algunas características relacionadas a la ciberseguridad, tomando desde los conceptos básicos de ciberseguridad hasta los distintos análisis, estándares y metodologías utilizados en las organizaciones, con base en esta metodología se busca analizar la importancia de la ciberseguridad y la aplicación de técnicas de ethical hacking para proteger los datos de los usuarios. Este análisis se desarrolla teniendo en cuenta las siguientes fases: Recolección de información relacionada con los temas establecidos, conceptualización de la información obtenida y análisis de la importancia de la ciberseguridad.

## 4. Resultados

Para implementar políticas de ciberseguridad, la organización debe identificar sus necesidades y sobre la base de estas necesidades (Berger & Jones, 2016), se debe elegir cuál es el estándar y el análisis de seguridad que más aplica en un determinado periodo de tiempo. Sin embargo, con esta investigación hemos determinado que el análisis de seguridad recomendado y con una diferencia importante es el ***Ethical Hacking***, a diferencia de otros análisis las etapas del ethical hacking se ejecutan de manera profunda y compleja sobre la infraestructura tecnológica y los sistemas de información. Cualquier empresa es vulnerable, la seguridad total no existe, pero se pueden tomar decisiones que ayuden a reducir los riesgos cibernéticos. El cibercrimen seguirá incrementado, nuevas técnicas de ataque combinadas con Inteligencia artificial marcarán los

próximos años, las organizaciones deberán defenderse de cibercriminales y concientizar a los empleados sobre los riesgos cibernéticos a los que se exponen.

## 5. Conclusiones

Este documento se centra en una revisión bibliográfica de investigaciones relacionadas con ciberseguridad y ethical hacking. En general, las organizaciones deben crear e invertir en políticas de ciberseguridad y aplicación de técnicas de ethical hacking que les permitan proteger su infraestructura tecnológica, encaminados en salvaguardar el activo más valioso que tienen, la información de los usuarios. Una filtración de datos podría dañar la confianza que los usuarios depositan en las organizaciones y esto afectaría considerablemente las finanzas de la empresa. Se recomienda implementar mecanismos básicos de seguridad para el filtrado de paquetes, detección de intrusos, mantenimiento y actualización de los sistemas operativos y plataformas del negocio, sistemas de autenticación, encriptación de los datos que permita garantizar la confidencialidad, integridad y disponibilidad de la información.

## 6. Referencias

### Artículos de revista


- Academy, C. N. (2019). *Reporte Anual de Ciberseguridad*. (15), 5–10. https://doi.org/10.15446/dfj.n15.50535.
- Allhoff, F., & Henschke, A. (2018). The Internet of Things: Foundational ethical issues. *Internet of Things*, *1–2*, 55–66. https://doi.org/10.1016/j.iot.2018.08.005.
- Alvarez Basaldúa, L. D. (2005). Seguridad en informática (Auditoría de sistemas). *Universidad Iberoamericana*, *1*, 1–42.
- Anscombe, T. (2018). Protección completa para un hogar inteligente. *Eset*, 20.
- Berger, H., & Jones, A. (2016). *Cyber Security & Ethical Hacking For SMEs*. 1–6. https://doi.org/10.1145/2925995.2926016.
- Biener, C., Eling, M., & Wirfs, J. H. (2015). *Insurability of cyber risk : an empirical a alysis working papers on risk management and insurance o . 151 chair for risk management and insurance Insurability of Cyber Risk : An Empirical Analysis Every reported incident of data breach o*.
- Bolbot, V., Theotokatos, G., Bujorianu, L. M., Boulougouris, E., & Vassalos, D. (2019). Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review. *Reliability Engineering and System Safety*, *182*, 179–193. https://doi.org/10.1016/j.ress.2018.09.004.
- DNP, MinTIC, MDN, & DNI. (2016). *Consejo Colombiano de la Politica Ecnomica y Social-Politica Nacional de Seguridad Digital CONPES 3584*.
- Giant, N. (2016). *Ciberseguridad para la i-generación: usos y riesgos de las redes sociales y sus aplicaciones*. 158.
- International Telecommunication Union. (2008). Series X: Data Networks, Open System Communications and Security: Telecommunication security - Overview of cybersecurity. *ITU-*

*T X.1205 Recommendation*, *1205*(Rec. ITU-T X.1205 (04/2008)), 2–3. Retrieved from https://www.itu.int/rec/T-REC-X.1205-200804-I.

- Kryszczuk, Krzysztof & Richiardi, J. (2011). *Springer Encyclopedia of Cryptography and Security*. https://doi.org/10.1007/978-1-4419-5906-5_793.
- López, R. (2017). *Escuela Especializada En Ingenería Itca-Fepade / Revista Tecnológica N° 10. Enero -Diciembre 2017 C. Ataques a traves de Bases de Datos*. *10*, 13–19.
- Mansfield-Devine, S. (2017). Hiring ethical hackers: the search for the right kinds of skills. *Computer Fraud and Security*, *2017*(2), 15–20. https://doi.org/10.1016/S1361-3723(17)30016-7.
- Manuel, J., Rodríguez, A., & Informática, E. S. (2015). *Recomendaciones para prevenir ciberataques*.
- Morales Bonilla, J. E. (2015). *Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución*.
- National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. https://doi.org/10.6028/NIST.CSWP.04162018.
- Reed, B. J. (2017). Executive Orders. *Public Voices*, *3*(2), 124. https://doi.org/10.22140/pv.477.
- Satapathy, S., & Ranjan Patra, D. (2015). Ethical Hacking. In *International Journal of Scientific and Research Publications* (Vol. 5). https://doi.org/10.1016/B978-0-12-803843-7.00030-2
- Serie de Tratados Europeos N-185. (2001). *Convention on Cybercrime*.
- SOPHOS. (2019). *Informe de Amenazas 2019 de SOPHOSLABS*.
- Unión Europea. (2016). *Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo*.
- Unión Internacional de Telecomunicaciones. (2008). Uit-T X.1205 Aspectos generales de la ciberseguridad. *Sector De Normalización De Las Telecomunicaciones De La Uit*, *1205*.

## Libros

- Sallis, E. M., Caracciolo, C., & Rodríguez, M. (2010). *Ethical hacking : un enfoque metodológico para profesionales*. Buenos Aires: : Alfaomega.

## Fuentes electrónicas

- Allianz Global Corporate & Specialty SE. (2019). *Top Business Risks for 2019*. Retrieved from https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
- De, O., & Ciberseguridad, L. A. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Mejorando vidas*. Retrieved from www.observatoriociberseguridad.com
- ESET. (2019). *TENDENCIAS 2019: Privacidad e intrusión en la aldea global*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2018/12/Tendencias-Ciberseguridad-2019-ESET.pdf
- Gobierno Nacional de Colombia. (2017). Qué es, cómo prevenir y qué hacer en caso de un ataque cibernético. Retrieved from http://especiales.presidencia.gov.co/Documents/20170601-ataques-ciberneticos/sin-ciber-ataques.html
- INCIBE. (2017). Amenaza vs Vulnerabilidad. Retrieved from

https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian
- Organisation Internationale de Normalisation. (2012). ISO/IEC 27032:2012 Information technology Security techniques Guidelines for cybersecurity. Retrieved from https://www.iso.org/standard/44375.html
- Organisation Internationale de Normalisation. (2018). ISO / IEC TR 27103: 2018 (en), Tecnología de la información - Técnicas de seguridad - Ciberseguridad y estándares ISO e IEC. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:27103:ed-1:v1:en
- Salinas, J. (2013). *Diseño y Construcción de una Red IP Virtualizada para la Aplicación de Hacking Ético*. 108. Retrieved from https://dspace.ups.edu.ec/bitstream/123456789/4908/1/UPS-ST000994.pdf
- Real Academia Española. (2018). hacker | Definición de hacker - «Diccionario de la lengua española» - Edición del Tricentenario. Retrieved from https://dle.rae.es/?id=JxlUKkm

## Sobre los autores

- **Luis Armando Gaona Páez**: Estudiante de Ingeniería de Sistemas de la Universidad Francisco de Paula Santander Ocaña. lagaonap@ufpso.edu.co
- **Jesús Emiro Trillos Arenas**: Estudiante de Ingeniería de Sistemas de la Universidad Francisco de Paula Santander Ocaña. jetrillosa@ufpso.edu.co
- **Andrea Natalia Bayona Moreno**: Estudiante de Ingeniería de Sistemas de la Universidad Francisco de Paula Santander Ocaña. anbayonam@ufpso.edu.co

---