Articles

Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador

Cybersecurity and Cyberdefense: Perspective of the current situation in Ecuador

Roxana Patricia Cedeño Villacís*

REVISTA TECNOLÓGICA
ciencia y educación
Edwards Deming

ISSN: 2600-5867

Editado por: Tecnológico Superior Corporativo Edwards Deming
Enero - Marzo Vol. 6 - 1 - 2022
https://revista-edwardsdeming.com/index.php/es
e-ISSN: 2576-0971
Recibido: 22 julio 2021
Aprobado: 16 septiembre, 2021
Pag 50 - 62

RESUMEN

El avance de la ciencia ha generado un acelerado y desmesurado crecimiento de la tecnología de la información y comunicación - TIC, llevando a las personas a modificar sus paradigmas de comunicarse y de efectuar actividades de una manera diferente a lo tradicional. Este siglo ha traído consigo un sinnúmero de herramientas informáticas que están siendo utilizadas en el ciberespacio por los ciudadanos ecuatorianos, para actividades financieras, educativas, sociales, de recreación, entre otras; esto ha traído la atención de los ciberdelincuentes, quienes han detectados vulnerabilidades en las TIC; convirtiéndose esto, en un camino viable para penetrar los sistemas informáticos y cometer actividades ilícitas e ilegales. El presente trabajo de investigación, a través de una perspectiva literaria pretende dar a conocer cómo se encuentra la ciberseguridad y ciberdefensa en el Ecuador actual. En la primera parte del artículo que corresponde al marco teórico se abordará las definiciones, tipologías de ciberataques y sus afectaciones en el país; en la segunda parte, se expondrá la metodología utilizada, mismo que fue desarrollado bajo un enfoque cualitativo y de tipo documental; en la tercera parte, la autora presenta los resultados; y al final, las conclusiones y recomendaciones.

Palabras clave: Ciberseguridad, Ciberdefensa, Ecuador, Tecnología.

ABSTRACT

* Magíster en Sistemas de Información Gerencial, Universidad Tecnológica Empresarial de Ecuador, Guayaquil, Ecuador, rcedenov@hotmail.com, https://orcid.org 0000-0002-7210-2642

The advance of science has generated an accelerated and disproportionate growth of information technology, leading people to modify their paradigms to communicate and carry out activities in a different way to the traditional. This century has brought with it countless computer tools that are being used in cyberspace by Ecuadorian citizens, for financial, educational, social, recreational activities, among others; this has brought the attention of cybercriminals, who have detected vulnerabilities in information and communication technologies (ICT); becoming this, in a viable way to penetrate the computer systems and commit illicit and illegal activities. This research work, through a literary perspective, aims to publicize how cybersecurity and cyber defense is in Ecuador today. In the first part of the article that corresponds to the theoretical framework, the definitions, types of cyberattacks and their effects on the country will be addressed; in the second part, the same methodology that was developed under a qualitative and documentary approach will be presented; in the third part, the author presents the results; and in the end, the conclusions and recommendations.

Keywords: Cybersecurity, Cyberdefense, Ecuador, Technology.

INTRODUCCIÓN

Tras recientes ataques informáticos del cual ha sido objeto el Ecuador, todo esto, debido al caso de Julián Assange y su salida del consulado en Londres, capital de Reino Unido; el país ecuatoriano, ha tenido la necesidad de buscar asistencia internacional para apoyarse del expertise en temas de ciberseguridad.

El 11 de abril del 2019, Ecuador recibió de los hackers más de 40 millones de ataques, la mayoría, a los portales web de entidades públicas, algunas de ellas viéndose afectadas para la atención al público, debido a las intermitencias.

Hasta antes de esa fecha, en el país se conocía poco del cibercrimen, se leía en la prensa local de ataques sufridos a países como Estados Unidos, Rusia, e incluso a empresas de gran prestigio internacional. Se veía algo muy lejano que ese tipo de evento podría suceder en el ciberespacio ecuatoriano.

El país ha entrado en esta vanguardia de sistematizarse y ofrecer a sus ciudadanos trámites más ágiles a través de sitios web, mismo que se ha fortalecido en estos últimos años; requiriendo del uso de internet y de acceso a las redes, lo cual implica el establecimiento de regulaciones en temas de defensa del ciberespacio (Ramos M. , 2014).

Este acontecimiento que sufrió el Ecuador recientemente ha hecho repensar si el ciberespacio se encuentra realmente protegido y si existe la legislación idónea que regule estos eventos y las sanciones aplicables para cada situación. Según Choucri, para que exista realmente la seguridad en el ciberespacio, se requiere del involucramiento del gobierno nacional y de las compañías (Vargas, Recalde, & Reyes, 2017).

El presente artículo tiene como propósito conocer la perspectiva de la ciberseguridad y ciberdefensa en el Ecuador, señalando sus definiciones, tipos de ciberataques y sus afectaciones, resultados, conclusiones y recomendaciones.

Ciberespacio, Ciberseguridad y Ciberdefensa

El ciberespacio, según los definen varios autores no es más que un grupo de equipos electrónicos conectados en redes haciendo uso de software, de datos y de humanos que interactúan de manera global con ellas (Llorens, 2017).

La ciberseguridad es el resultado del proceso acelerado de la globalización, que ha permitido la continua innovación en la tecnología de la información y comunicación, logrando con ello el uso constante del ciberespacio (Sancho Hirare, 2017); es un conjunto de acciones que persigue la protección de la información de las organizaciones y en general de toda la comunidad que está en el ciberespacio (Cornejo, Verdezoto, & Villacís, 2019).

El término "defensa" se lo relaciona con el resguardo y la protección ante las amenazas y peligros dando respuesta inmediata a estos eventos; es así que, Virilio define a la ciberdefensa como aquellas acciones que un Estado ejecuta en pos de controlar los peligros y amenazas de naturaleza cibernética que se dan en el ciberespacio (Vargas, Recalde, & Reyes, 2017).

En la actualidad, se vive una dependencia del internet, donde a través de esta autopista fluye un sinfín de tecnologías de información, las personas cada vez más acceden al ciberespacio, siendo este último un lugar propicio para que se presenten los ciberdelitos, generando pérdidas incluso económicas y provocando que los gobiernos empiecen a generar políticas de seguridad nacional (Tates & Recalde, 2019). Esta cultura de estar conectado en redes imposibilita el poder controlar todas las funcionalidades de las aplicaciones, provocando que estas sean cada más vulnerables (Ramos M. , 2014).

Ciberdelincuencia

Este fenómeno de la ciberdelincuencia apareció por primera vez en el siglo XX con la llegada de los virus informáticos; incluso, muchos de ellos con gran trascendencia en los medios de comunicación por su afectación en los ordenadores; despertó en la ciudadanía la conciencia de un antes y después de la ciberseguridad; siendo este último, un asunto que involucra a todos (Hernández, 2017).

Según Cortés, no es un fenómeno exclusivo que ocurre en los países en vías de desarrollo, pues se ha conocido por los medios que la economía y la seguridad nacional de otros gobiernos de diferentes lugares del planeta se han visto afectados, viéndose forzados a implementar políticas públicas con relación a la ciberseguridad y ciberdefensa (2015).

Algunas empresas que se han visto afectadas por la ciberdelincuencia son por ejemplo Facebook, Youtube, Skype, Apple, AOL, Yahoo, Microsoft, Google (Aranda, Riquelme, & Salinas, 2015).

Se vive una época en que toda la ciudadanía y per sé toda la sociedad en general mantiene una gran dependencia a la tecnología de la información y comunicación, pues requiere de esto, para generar actividades propias de la economía y de aspectos sociales. Este crecimiento acelerado de la TIC ha permitido abrir la puerta a los ciberdelitos que son ejecutados por delincuentes y terroristas (Pons, 2017).
Un informe presentado en Europa reveló que el 80% de las empresas de ese continente han sufrido al menos un incidente de este tipo en el año 2016, siendo el sector industrial uno de los que más se afectó, creciendo un 38% en comparación al 2015, concluye que los ciberdelitos se han multiplicado por 5 en los últimos años (Ribagorda, 2018).
Para Joyanes-Aguilar, los ciberdelincuentes están aprovechando la tecnología de la información y comunicación y las innovaciones que estas traen consigo para desarrollar sus actividades delictivas, siendo un ejemplo el uso de las redes sociales donde los terroristas aprovechan este medio para ejecutar sus ataques especialmente con la propagación de malware en juegos donde aparentemente son inofensivos (2010, pág. 36).

Los ciberdelincuentes, responden a estructuras muy bien organizadas que reclutan a individuos de prestigiosas universidades del mundo ofreciendo sueldos muy atractivos y difíciles de obtener en las empresas (Chelala, 2016).

Tipos de Ciberataques, afectaciones y obstáculos

Los ciberataques se pueden dar por amenazas que pueden ser de origen o externo; y también por las vulnerabilidades del sistema informático, afectando la integridad, disponibilidad y confidencialidad de la información que gestiona la organización (Huerta, 2015).

Según Caro, estos ataques se pueden clasificar por su autoría, por ejemplo aquellos que son patrocinados por un estado con la intención de dañar alguna infraestructura de otro país; los de servicios de inteligencia y contrainteligencia para robar información o avances tecnológicos; los extremistas políticos e ideológicos para reclutar adeptos a su organización; y, la delincuencia organizada que roba información para su beneficio económico (2010).

Por lo general, los ciberataques que se presentan con mayor regularidad son los que se originan por causa de la ingeniería social*, que es por desconocimiento del usuario cuando cae en un engaño del ciberdelencuente y termina proporcionándole información condifencial (Marin, Nieto, Huertas, & Montenegro, 2019); pero, además existen ataques a los ordenadores dejándolos zombis, a esto se llama botnet "red de robots", porque

* Técnica para obtener información confidencial a través de engaños

van infectando a todos sin que su propietario tenga conocimiento alguno de lo ocurrido y solo realizan las instrucciones del ciberdelincuente (Joyanes Aguilar, 2010).

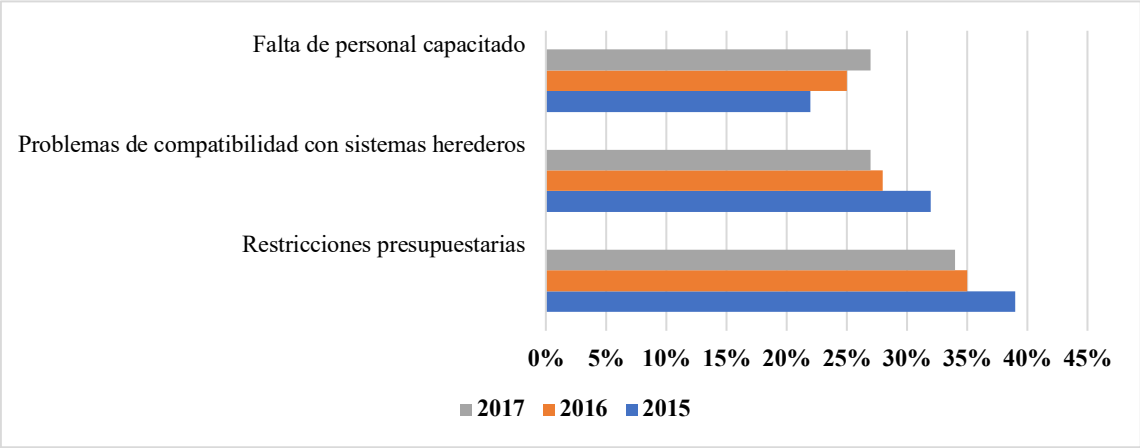
Indistintamente del tipo de ciberataque que ha infectado el sistema informático, esto puede provocar afectaciones en el rendimiento de los computadores, alteración o eliminación de los ficheros, que las aplicaciones se cierren o se ejecuten sin consentimiento del usuario, reciban correos que no fueron enviados por el usuario (suplantación de identidad), decodifiquen las contraseñas de las redes inalámbricas, denegación de servicio (DoS) y denegación de servicio distribuido (DDoS), incluso hasta ataques combinados.

Según datos proporcionados por Cisco, el 53% de estos ataques han generado afectación financiera en más de $500.000,00 (2018). Los especialistas de la Universidad Autónoma de México prevén que las ganancias por el cibercrimen lleguen a seis trillones de dólares para el 2021; es decir, el doble de lo alcanzado en el 2015 (UNAM, 2016).

La no existencia de personal capacitado en las organizaciones para atender con inmediatez y hacer frente a estas situaciones, la dificultad para emprender los proyectos de cambios tecnológicos y que estos se integren a las plataformas existentes, incluso hasta la falta de presupuesto para administrar apropiadamente la seguridad, son algunas de las razones que impiden combatir eficazmente los ciberataques.

El siguiente gráfico muestra el comportamiento en los años 2015, 2016 y 2017 de las razones mencionadas en el párrafo anterior, donde se puede apreciar que las restricciones presupuestarias bajaron al 34% en el 2017 en comparación del 2015 que fueron del 39%, los problemas de compatibilidad también disminuyeron del 32% al 27%; pero, la falta de personal capacitado aumentó pasando del 22% al 27%.

F*igura 1.* Obstáculos para enfrentar los Ciberataques



Fuente: (CISCO, 2018, pág. 50)

En cuanto a los problemas que se están presentando en el ciberespacio, que difícilmente se resolverán a corto plazo, existe ya una marco jurídico internacional que proporciona una referencia y marco normativo que guía el camino a seguir, pero si es necesario que cada país promueva de manera independiente su propia legislación en este ámbito (Llorens, 2017).

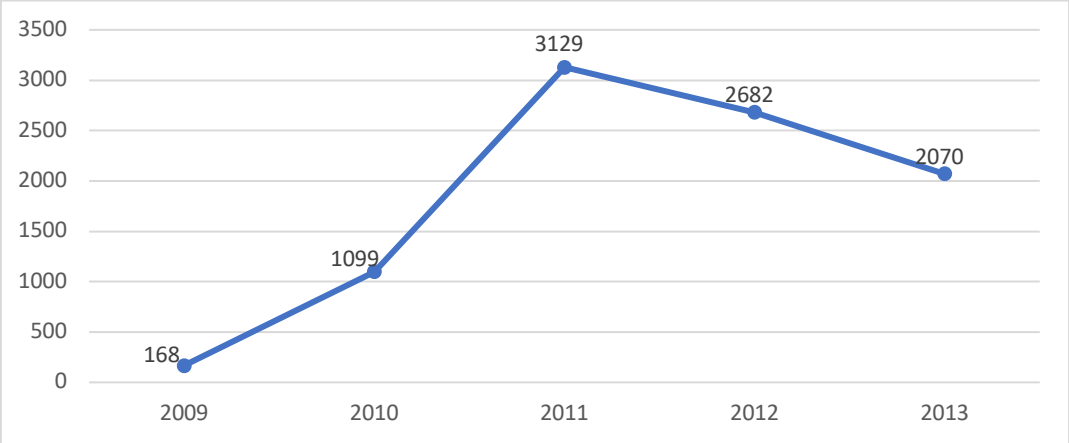
Se requiere de la sinergia entre las empresas públicas, privadas y las académicas en relación al tema de la seguridad del ciberespacio; es por ello, que ésta última ha tenido la necesidad de crear estudios a nivel de postgrado en materia de ciberseguridad para suplir la demanda profesional; el perfil del especialista debe poseer competenecias en el manejo de redes, seguridad informática, comunicaciones, criptografía, análisis forense, técnicas de prevención, capacidad de respuesta ante incidentes, aplicación de normas (Paya, Cremades, & Delgado, 2017).

Ciberataques sufridos en el Ecuador

El Ecuador, aún no cuenta con estudios que revelen datos precisos sobre las afectaciones económicas y reputacionales en el tema de los ciberataques, se conoce por reportes de denuncias en Fiscalía y que son presentados en medios de comunicación que estas cifras han ido aumentando, de 168 reportados en el año 2009 a 2.070 en el año 2013, entre los casos más concurridos está el hackeo del correo electrónico, violación a la intimidad, apropiación fraudulenta por medios electrónicos. La siguiente figura muestra el comportamiento de los ciberataques en el Ecuador en el rango de 2009 hasta 2013.

Figura 2. *Ciberataques reportados en Ecuador*

Desde el año 2009 hasta el 2013



Fuente: (El Comercio, 2015)

En el 2018, un ciberataque afectó al sistema de la Agencia Nacional de Tránsito del Ecuador beneficiando ilegalmente a 15.970 usuarios con lincencias de conducir de diferentes tipos, concediendo este documento a personas que no habían aprobado los exámenes de rigor previamente para su obtención; se determinó que, usuarios externos detectaron las vulnerabilidades del sistema informático, penetraron al mismo y cometieron el ílicito, generando un perjuicio de más de un millón de dólares para el estado (El Telégrafo, 2018).

En Abril del 2019, el gobierno del Ecuador tomó la decisión de dar por terminado el asilo el a Julián Assange en la embajada ubicada en Londres; esto provocó que el país sufriera atentados cibernéticos, los cuales llegaron a 40 millones de ataques causados por delincuentes informáticos; el objetivo fue saturar los sitios web con el propósito de impedir que los usuarios puedan acceder a estos, este tipo de ataque es llamado denegación de servicio – DoS (El Comercio, 2019).

Decenas de hackers participaron de este ciberataque, con la intención de provocar afectación a la infraestructura tecnológica de las entidades del estado; de acuerdo con los datos estadísiticos de Kapersky de las ciberamenazas en tiempo real, el Ecuador, que ocupaba el puesto 56 subió hasta el 25 en el ranking de los países más vulnerables en el mundo, en apenas pocas horas (Expreso, 2019).

Entre las entidades ecuatorianas que fueron atacadas podemos mencionar a la Cancillería, los Ministerios, la Presidencia de la República, Servicio de Rentas Internas, algunos Gobiernos Autónomos Descentralizados (Expreso, 2019); los ciberataques se originaron en países como Gran Bretaña, Estados Unidos, Holanda, Francia, Austria, Rumania, Alemania, Brasil e incluso de Ecuador (El Telégrafo, 2019).

El Código Orgánico Integral Penal del Ecuador (COIP , 2013), establece una serie de artículos que sancionan estas actividad ilícitas; Meléndez refiere algunos de ellos que se ilustran en la siguiente figura:

Figura 3. Artículos COIP que sanciona los delitos informáticos

Artículo COIP	Descripción del artículo	Sanción
174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.	7 a 10 años
178	Violación a la intimidad	1 a 3 años
190	Apropiación fraudulenta por medios electrónicos	1 a 3 años
191	Reprogramación o modificación de información de equipos terminales móviles	1 a 3 años
192	Intercambio, comercialización o compra de información de equipos terminales móviles	1 a 3 años
193	Reemplazo de identificación de terminales móviles	1 a 3 años
194	Comercialización ilícita de terminales móviles	1 a 3 años
229	Revelación ilegal de base de datos	1 a 3 años
230	Interceptación ilegal de datos	3 a 5 años
231	Transferencia electrónica de activo patrimonial	3 a 5 años
232	Ataque a la integridad de sistemas informáticos	3 a 5 años
233	Delitos contra la información pública reservada legalmente	5 a 7 años
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	3 a 5 años

Fuente: (Meléndez, 2018)

Para mejorar la seguridad en el ciberespacio, se requiere la colaboración entre la empresa privada y el sector público, involucrando además a las ONG´s, a las corporaciones vinculadas con las tecnologías de la información y comunicación y a toda la sociedad en general (Castro & Monteverde, 2018).

Se requiere de infraestructura adecuada y protección de los datos como aspectos cruciales para la ciberseguridad, pero aún no se ha desarrollado un marco jurídico idóneo que tome los lineamientos internacionales e incluso la legislación de otros países (Almeida, 2017).

MATERIALES Y MÉTODOS

Este trabajo de investigación fue desarrollado bajo un enfoque cualitativo, utilizando una tipología descriptiva, siguiendo la metodología de revisión documental que permitiera la búsqueda, selección y análisis de la información, obtenida de fuentes secundarias de artículos científicos, sitios web y periódicos que tuvieran relevancia en el tema de investigación. En el mismo, se expone la perspectiva de la ciberseguridad desde sus definiciones, los tipos de ciberataques y sus afectaciones en el Ecuador.

RESULTADOS

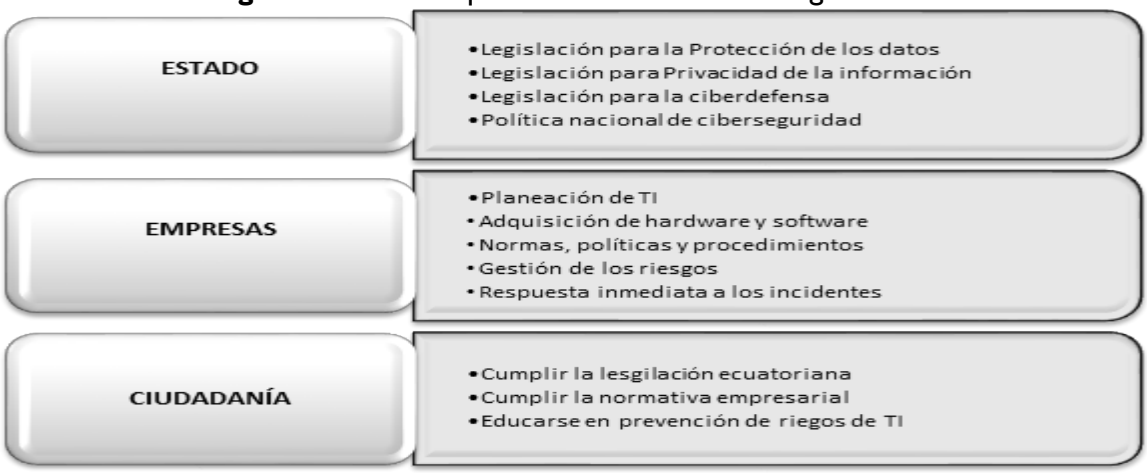
Es evidente que todo lo que ocurre en el ciberespacio ecuatoriano, no solo pone en riesgo la información y la reputación de la persona que se vio afectada por la sustracción de fotos personales o por el hackeo de su correo electrónico, sino que además las infraestructuras de las entidades públicas corren peligro.

Pareciera una tarea sencilla el adquirir el hardware y software para la ciberserguridad, pero no es así, esto requiere de inversión, conocimiento en la configuración de las herramientas informáticas, y la capacidad de integrarlas a las plataformas empresariales. Sin dejar a un lado al usuario que labora en la organización, al cual se le debe capacitar en políticas institucionales para la prevención.

Una organización, que ya está trabajando con un modelo de madurez adquiere compromisos insitucionales enfocados en proteger sus activos, es así, que en los planes estratégicos de TI contempla objetivos claros en temas de ciberseguidad.

Los actores involucrados en precautelar la seguridad en el ciberespacio, deben impulsar mecanismos que atiendan de manera prolija el cribercrimen; es así, que el primer actor debe ser el "Estado", con la promulgación de legislación que aterrice los lineamientos, buenas prácticas y sanciones para esta práctica ilícita o ilegal.

Figura 4. Actores que intervienen en Ciberseguridad



Fuente: Elaboración propia

Como segundo actor están las "Empresas", quienes deben de impulsar al interior de sus organizaciones un sistema de gestión específico para precautelar la seguridad, esto es posible a través de una planeación de tecnología de la información, adquiriendo hardware y software idóneo para prevenir las amenazas y vulnerabilidades, incorporando políticas y normativas que regulen los procesos, actividades y accionar del personal, teniendo una administración de gestión de riesgos que ayude a prevenir y mitigarlos y por último que sea capaz de atender con inmediatez los incidentes que se presenten en temas de ciberseguridad.

Y por último, está la "ciudadanía" en general quien debe cumplir las leyes del estado y las normativas institucionales que promulgan las empresas donde laboran; a más de ello,

se requiere de la conciencia y compromiso por educarse en prevención de riesgos de TI, pues se ha conocido que muchas de las afectaciones en las redes corporativas se ha dado porque los usuarios acceden a páginas no oficiales o redes sociales con malware, en horas de oficina.

DISCUSIÓN

El Ecuador ya está trabajando en una estrategia de nacional ciberseguridad que es impulsado desde el Ministerio de Telecomunicaciones y que persigue fortalecer el ciberespacio, crear planes, guías y metodologías para este ámbito; pero es innegable, que también es fundamental a priori la promulgación de leyes que centren y regulen todos los aspectos relacionados a la ciberserguridad en este país.

Las empresas por su parte, deberán trabajar planificadamente en estrategias que permitan mitigar sus riesgos tecnológicos, contar con una asociación ecuatoriana de ciberseguridad será benificioso, pues permitirá cada vez más adquirir mayor conocimiento de este ámbito.

Las universidades ecuatorianas, tienen el gran reto de promover carreras en el ámbito de ciberseguridad, de impulsar cursos cortos de capacitación continua relacionadas a este tema, de fomentar en sus alumnos la cultura de prevención de riesgos tecnológicos especialmente en las redes sociales.

La ciudadanía en general que usa equipos electrónicos como ordenadores, tablets o dispositivos móviles, deben adquirir antivirus con licencia para que puedan protegerse del software malicioso, evitar usar la misma contraseña para el ingreso a diferentes aplicaciones, usar contraseñas robustas con caracteres especiales y longitudes más amplias, eliminar periodicamente los archivos temporales, evitar descargar software no licenciado, y lo posible no acceder a sitios web que no cuenten con protocolos de seguridad https.

Las empresas deben trabajar con modelos de madurez que permitan a sus organizaciones poder identificar en que etapa se encuentran, y con base a ello, desarrollar estrategias que le permitan encausar lineamientos para la ciberseguridad; requieren de personal especializado en seguridad informática que sea capaz de enfrentar las amenazas, detectar las vulnerabilidades y aplicar políticas para la seguridad de la información.

Utilizar dispositivos de seguridad como Firewalls son herramientas que habitualmente se usan para contrarrestar los ciberataques, existen de diferentes tipos que pueden hacer filtrados en las capas sean estas de red, transporte, aplicación; los mismos que integrados a los IPS, Routers, VPN y junto a software para prevenir el malware conforman elementos ideales para prevenir ciberataques, pues lo que se persigue es evitar el ataque, y de no ser posible, al menos poder detectarlo los más pronto posible, en tiempo real.

El estado debe trabajar continuamente en desarrollar estrategias, planes y acciones para evitar o mitigar el impacto de los ciberataques, se requiere de leyes claras y concretas que aborden estos temas y sancionen a los ciberdelincuentes.

REFERENCIAS

Almeida, A. (2017). La Ciberseguridad, y su incidencia en las políticas de la seguridad de la información de la Armada del Ecuador. *YURA: Relaciones Internacionales*(11), 306-323.

Aranda, G., Riquelme, J., & Salinas, S. (2015). La ciberdefensa como parte de la agenda de integración sudamericana. 100-116. Línea Sur.

Caro, M. (2010). Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Recuperado de http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Castro, H., & Monteverde, A. (2018). Seguridad hemisférica latinoamericana adaptada a las nuevas tecnologías: Ciberseguridad y avances de cooperación regional e internacional para la sanción del ciberdelito. *39(39)*. Revista Espacios.

Chelala, R. (2016). El nuevo entorno digital de la actividad criminal. *Boletín de Estudios Económicos, LXXI*(219), 591-612.

CISCO. (2018). Reporte anual de Ciberseguridad de Cisco 2018. Recuperado de https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

COIP . (2013). Código Integral Penal. Ecuador. Recuperado el 07 de 05 de 2018, de https://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

Cornejo, Y., Verdezoto, V., & Villacís, A. (2019). Ciberdefensa, Ciberseguridad y sus efectos en la sociedad. *4(2)*. International Multilingual Journal of Science and Technology.

Cortés, R. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa de Colombia. *(14)*. Revista de Derecho Comunicaciones y Nuevas Tecnologías.

El Comercio. (2015). *El Comercio*. Recuperado el 05 de 07 de 2019, de https://www.elcomercio.com/actualidad/interceptar-mensajes-presion-hackeo-ecuador.html

El Comercio. (2019). *El Comercio*. Recuperado el 16 de 04 de 2019, de https://www.elcomercio.com/actualidad/hackers-ofensiva-global-ataque-ecuador.html

El Telégrafo. (2018). *El Telégrafo*. Recuperado el 05 de 07 de 2018, de https://www.eltelegrafo.com.ec/noticias/judicial/12/hackers-ecuador-ant-licencias

El Telégrafo. (2019). *El Telégrafo*. Recuperado el 05 de 07 de 2019, de https://www.eltelegrafo.com.ec/noticias/politica/3/hackers-red-informatica-sector-publico

Expreso. (2019). *www.expreso.ec*. Recuperado el 05 de 07 de 2019, de https://www.expreso.ec/actualidad/hackers-ecuador-tecnologia-seguridad-ataques-BD2764517

Expreso. (2019). *www.expreso.ec*. Recuperado el 05 de 07 de 2019, de https://www.expreso.ec/ciencia-y-tecnologia/el-riesgo-informatico-de-tocar-a-un-hacker-DY2753014

Hernández, A. (2017). Ciberseguridad y confianza en el ámbito digital. *(897)*. Revista ICE.

Huerta, V. (2015). ALTAIR-SIGVI: Un nuevo sistema para combatir el cibercrimen mitigando las vulnerabilidades. *RUIDERAe: Revista de Uniandes de Información*(7).

Joyanes Aguilar, L. (2010). Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Recuperado de http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Llorens, M. (2017). Los desafíos del uso de la fuerza en el ciberespacio. *Anuario Mexicano de Derecho Internacional, XVII*, 785-816.

Marin, J., Nieto, Y., Huertas, F., & Montenegro, C. (2019). Modelo ontológico de los ciberdelitos: Caso de estudio Colombia. *RISTI, Revista Ibérica de Sistemas y Tecnologías de Información*(17).

Meléndez, J. (2018). *Derecho Ecuador*. Recuperado de https://www.derechoecuador.com/delitos-informaticos-o-ciberdelitos

Paya, C., Cremades, A., & Delgado, J. (2017). El fenómeno de la ciberdelincuencia en España: La propuesta de la universidad de Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito. *Revista Policía y Seguridad Pública, 1*, 237-270.

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *(20)*, 80-93. Quito, Ecuador: URVIO, Revista Latinoamericana de Estudios de Seguridad.

Ramos, M. (2014). Acerca de la sobernaría del Ecuador en el ciberespacio. Centro Andino de Estudios Estratégicos.

Ribagorda, A. (2018). Panorama actual de la ciberseguridad. *(410)*, 13-26. Economía Industrial.

Sancho Hirare, C. (2017). Ciberseguridad. Presentación del dossier. *(20)*, 8-15. Quito: URVIO, Revista Latinoamericana de Estudios de Seguridad.

Tates, C., & Recalde, L. (2019). La ciberseguridad en el Ecuador, una propuesta de organización. *4(7)*, 156-169. Revista de Ciencias de Seguridad y Defensa.

UNAM. (2016). Boletín UNAM-DGCS-770. Recuperado de http://www.dgcs.unam.mx/boletin/bdboletin/2016_770.html

Vargas, R., Recalde, L., & Reyes, R. (2017). Ciberdefensa y Ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *(20)*, 31-45. URVIO,