Ciberdefensa, Ciberseguridad Y Sus Efectos En La Sociedad

Cyberdefense, Cybersecurity And Its Effects In The Society

***Ing.Yan Cornejo Montoya**.[1]
[1]Universidad Tecnológica Empresarial de Guayaquil
*yan.cornejom@ug.edu.ec

****Ing.Victor Hugo Verdezoto.[2]**
[2] Universidad de Guayaquil.
**victor.verdezotov@ug.edu.ec

Ing.Andrea Villacis Ramírez[3].
[3]andrea.villacis.ramirez@gmail.com

***Resúmen*—Los procesos de digitalización, el uso de nuevas herramientas tecnológicas y las debidas protecciones, hacen que las organizaciones sean más competitivas, en donde intervienen la sociedad de la información, las redes informáticas y los métodos de ciberdefensa, cuya expansión ha hecho surgir a lo que se conoce como la quinta dimensión de la guerra moderna. A partir de esto se realiza un análisis sobre ciberdefensa, ciberseguridad y su efecto en el ámbito de la seguridad de la información en Latinoamérica, así como políticas y programas de prevención para minimizar ataques en el ciberespacio y sus consecuencias económicas al no estar protegidos, evaluando ventajas y desventajas donde se dan recomendaciones y aconsejan buenas prácticas.**

Palabras clave: ***ciberataque, ciberespacio, ciberterrorismo, cibernética, digitalización.***

***Abstract*—The processes of digitalization, the use of new technological tools and due protections, make organizations more competitive, where the information society, computer networks and cyber defense methods intervene, whose expansion has given rise to what it is known as the fifth dimension of modern warfare. Based on this, an analysis is carried out on cyberdefense, cybersecurity and its effect in the field of information security in Latin America, as well as policies and prevention programs to minimize attacks in cyberspace and its economic consequences by not being protected, evaluating advantages and disadvantages where recommendations are given and good practices are advised.**

Keywords—cyberattack,cyberspace, cyberterrorism, cybernetics, digitalization.

I. INTRODUCCIÓN

En la actualidad hablar sobre ciberseguridad no solo trata de la protección de la información, el cual es el activo más valioso en una organización, sino todo lo relacionado a una infraestructura tecnológica de los sectores principalmente financiero, comercial, servicios de emergencia, servicios públicos, defensa de gobiernos, que constituyen el motor donde funciona la sociedad actual y que con el objetivo de minimizar y controlar la probabilidad de sufrir un ciberataque, se deben gestionar los riesgos debido a una sociedad interconectada tecnológicamente, donde los atacantes buscando vulnerabilidades, participan en acciones maliciosas por diversas razones, sean retos, lucro o por curiosidad, y surge esta atracción por la facilidad e impunidad de estas actividades.[26]

¿Pero qué piensan algunos expertos sobre la ciberseguridad, ciberamenazas y el ciberespacio?

En general, se podría decir que la **ciberseguridad** se refiere a métodos de uso, procesos y tecnologías para prevenir, detectar y recuperar daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. [16]

La **ciberseguridad** es el conjunto de políticas y acciones dirigidas a proteger los activos de información de una organización en general, y a la comunidad en el ciberespacio [44].

Las **ciberamenazas**, se refieren a las debilidades y ausencia de protección de los sistemas informáticos, lo cual conduce a un riesgo potencial. La ciberseguridad se puede ver afectada por fenómenos naturales, fallas técnicas y ataques cibernéticos.[6]

El **ciberespacio** es el conjunto de dispositivos conectados por redes en las que se almacena y se utiliza información electrónica, donde interactúan personas con información digital, siendo susceptibles a sufrir ciberamenazas (Machin and Gazapo 2016).[29]

Teniendo en cuenta la información anterior y lo bastante vulnerables que pueden ser los sistemas informáticos en su globalidad que ocasionarían pérdida económica y de imagen corporativa, se considera importante invertir para mejorar la seguridad de la información, a fin de minimizar riesgos que pueden poner en peligro la integridad física de las personas o la paralización del funcionamiento digital de las organizaciones [37]

Según la firma Gartner (2016), las ventas de drones se incrementaron en todo el mundo en un 84% con un aumento de los ingresos llegando a los $4500 millones de dólares. Esto debido al gran crecimiento en el sector agrícola que se estima que representaría el 48% de todas las ventas de dicho artefacto, así como en el sector de producción de

películas, tanto que ha llegado al punto de ser una realidad esperanzadora en el continente africano, debido a los logros obtenidos en sectores como: el industrial, económico, humanitario , agrícola, etc.; inclusive en el sentido de proveer seguridad y defensa [34]. Se ha logrado en algunos países (España, Brasil, Argentina, México), la aceptación de drones en el sector agrícola, cuya presencia ha sido crucial al momento de tomar decisiones, debido a que les ha permitido mediante la informática, el uso de sensores que puedan realizar análisis de datos y capturar imágenes satelitales, para determinar el rendimiento de cultivos, analizar la presencia de plagas y como consecuencia determinar la aplicación de fertilizantes. [3]

La aplicación de tecnología con drones, aumenta la productividad, así como la reducción de tiempos y costos, ya que estos instrumentos usan cámaras multiespectrales de alta resolución para obtener datos relacionados con la agricultura de precisión en zonas reducidas o grandes extensiones, para determinar focos de plagas o posibles enfermedades en las plantaciones [35]. (Niño y Rodriguez 2017).Adicional a esto, se puede indicar que las ofertas de tecnología se complementan con otras, como es el caso de: drones, sensores inteligentes, controladores, plataformas electrónicas, sistemas de localización, sistemas de autoidentificación y *blockchain*, que se los considera como los pilares tecnológicos y que a su vez desempeñan un rol importante en la matriz tecnológica de actualidad, por ende se los conoce como “nuevas tecnologías industriales digitales” o “ tecnologías 4.0” [3]

Y es aquí, donde se vislumbra como algunos países de Latinoamérica vienen organizándose para tomar medidas de protección y control por posibles ciberataques, al promover estrategias en sus políticas de seguridad nacional, donde se implementen estándares tecnológicos globales que permitan contrarrestar riesgos al fomentar buenas prácticas de seguridad para mitigar ataques cibernéticos.[37]

El objetivo de esta investigación se enfoca en el análisis de información sobre ciberdefensa y ciberseguridad y su efecto en el ámbito de la sociedad de la información en Latinoamérica.

II. METODOLOGIA

Esta investigación es de carácter descriptiva - interpretativa, porque se está considerando como ejemplo de estudio, varios programas cibernéticos de seguridad de algunos países de Latinoamérica y Europa, como el caso del Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo; los cuales cuentan con una política y/o estrategia nacional de ciberseguridad, cuyo avance ha sido reconocido por la National Cyber Security Index[1], elaborado por la prestigiosa e-Governance Academy Foundation de Estonia que avala el nivel de preparación en ciberdefensa de dichos países.

A su vez, la investigación es documental porque la información ha sido recopilada de artículos científicos y repositorios bibliográficos basados en proyectos concretos como ciberdefensa, ciberterrorismo e innovación disruptiva; cuyas propuestas han sido analizadas, resaltándose la importancia estratégica de defensa y protección de una posible ciberguerra en un futuro no muy lejano, como el caso de un estudio preparado y publicado por el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo[2], titulado “Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe”, cuyo contenido es avalado por la OEA[3].[36]

En las últimas décadas, en América Latina, pocos países van adhiriéndose a esta nueva iniciativa de vital importancia, porque la innovación disruptiva, las estrategias de protección digital, la protección contra posibles riesgos, los ataques cibernéticos, las tecnologías inteligentes, el IoT[4] y la adopción de la industria 4.0; obligan a desarrollar programas específicos de respuestas a estos posibles incidentes de ICS (Ciberseguridad en Infraestructuras Críticas), en donde las empresas, la sociedad, el gobierno y la defensa nacional dependen del buen manejo de las tecnologías de la información y la comunicación (TIC´s)[5] y de la operación de las Infraestructuras Críticas de Información (ICIs), en donde todos los sectores públicos y privados se apoyan en la disponibilidad, integridad y confidencialidad de la información.

El auge de las TIC´s, la protección y la disponibilidad de los activos de información críticos, constituyen escenarios vulnerables a las amenazas que podrían afectar de manera crítica el buen funcionamiento de los sistemas informáticos, la banca, la industria, gobiernos y la economía.

III. DESARROLLO

Antecedentes Históricos de Ataques Cibernéticos.

Villanueva [47], relata un historial de ataques más significativos de la era digital:

A. *Estonia, 2007*

En abril de 2007, las instituciones de Estonia se paralizaron por los ciberataques que sufrieron numerosas instituciones públicas, entre ellas, el Parlamento y varios ministerios, además de bancos, partidos políticos y medios de comunicación. Numerosos botnets enviaron mensajes spam para colapsar los servidores, como consecuencia no servían los cajeros automáticos ni la banca online. Estonia tuvo que cortar toda la línea de Internet y formatear sus sistemas. Todo esto sucedió luego de que el gobierno estonio reubicara la estatua del soldado de Bronce de Tallin.

B. *El Gran Colisionador de Hadrones*

[1] https://ncsi.ega.ee/

[2] cybersecurity@oas.org
[3] Organización de los Estados Americanos
[4] Internet of Things. Internet de las cosas
[5] Tecnologías de la Información y la Comunicación

Cuando se estrenó oficialmente el 12 de septiembre de 2008, el “acelerador de partículas”, conocido como el Gran Colisionador de Hadrones (LHC), el grupo griego ‘Green Security Team’ consiguió hackear los sistemas informáticos del CERN (Organización Europea para la Investigación Nuclear) en Ginebra, cuyo objetivo fue demostrar las debilidades que tenía el sistema.

C. *Stuxnet*

En enero de 2010, hubo una inspección en la planta nuclear Natanz en Irán, donde las máquinas centrifugadoras de uranio comenzaron a fallar. El evento se repitió 5 meses después y se detectó que era un malicioso virus informático, un gusano conocido como Stuxnet, el cual tomo el control de 1000 máquinas encargadas de operar el material nuclear dándoles la orden de autodestruirse. Era la primera vez que un ataque cibernético lograba destruir físicamente una infraestructura. El código fue diseñado con finalidad bélica, donde los hackers podían manipular equipos físicos, como plantas de energía eléctrica, presas, y otros complejos industriales.[4]

D. *Duqu.*

Fue descubierto el 19 de octubre de 2011. Este malware es una variante del arma cibernética destinada a retrasar la capacidad de Irán para fabricar bombas nucleares, Stuxnet. Su función era reunir datos de Inteligencia y activos de entidades.

E. *Flame*

Fue descubierto el 28 de mayo de 2012, diseñado para recopilar información sensible y presente en ordenadores de Irán, Oriente Próximo e incluso Estados Unidos, llevaba activo al menos 5 años cuando lo detectaron y afectó a más de 5000 equipos.

F. *Gauss*

El 1 de agosto de 2012, se descubrió Gauss, otro virus derivado de Stuxnet. Llegó a afectar a más de 2.500 ordenadores y concentró sus ataques en el Líbano, Israel y territorios palestinos. Su principal objetivo era recabar información de las instituciones bancarias, transacciones comerciales y otros datos.

G. *China*

Hasta el 5 de noviembre de 2012, China solo había podido fabricar aviones de hasta 3ª generación. Pero en esta fecha, anunció la creación del J-31, de 5ªgeneración. Esto despertó las alarmas de Estados Unidos y de Japón, ya que la estructura y la apariencia física eran casi idénticas a aviones creados por ellos ¿Ingenio o ciberespionaje?

H. *Octubre Rojo*

Investigadores rusos detectaron el 14 de enero de 2013 un ciberataque que podría haber estado robando documentos confidenciales encriptados desde 2007 de instituciones gubernamentales como embajadas y de centros de investigación nuclear y compañías estatales de gas y petróleo.

I. *Mandiant APT-1*

La empresa Mandiant publicó (2013), un informe en el que dice que un grupo de piratas informáticos, identificados como APT-1, cuentan con el "apoyo directo del Gobierno chino", para perpetrar una "amplia campaña de espionaje cibernético a largo plazo". Manuel Benet en SecurityArtWork explica "esto ya no es informática, es política", China desea fervientemente ser la próxima potencia mundial, y una de las cosas que necesita para cumplir su objetivo es capacidad científico tecnológica.[40] (Sanz 2013)

J. *Ramsomware6 - Wannacry*

Ransomware o cibersecuestro, llamado Wannacry por sus creadores, apareció el 12 de mayo de 2017, donde más de 200.000 computadoras colapsaron en 150 países como Rusia, Alemania, China, Corea del Norte, Japón, Indonesia, India, Francia, Reino Unido, etc. por utilizar obsoletas versiones de Windows. Es un programa dañino que se transmite utilizando un troyano o un gusano para infectar el sistema operativo, a través de un gusano que se autoreplica y autotransmite. De esta manera, se cifran todos los archivos y el usuario sólo podrá volver a acceder a los mismos mediante una clave que sólo conoce el creador del ransomware, quien reclama un rescate. [1]

K. *Wipeware*

Se refiere a ataques que, disfrazados de ransomware, no permiten recuperar los datos ni siquiera pagando. Estos troyanos y gusanos pueden venir escondidos en archivos adjuntos de correos electrónicos, videos webs de dudoso origen, actualizaciones de sistemas o programas que resultan confiables y familiares, como Windows, Adobe Flash, etc. Por eso, el wipeware es más usado por fuerzas estatales, mientras que el ransomware tiene objetivos de lucro. [1]

L. *Win32/ Diskcoder. C (Petya / NotPetya/ ExPtr)*

Fue reportado el 27 de junio de 2017, y es un ransomware que cifra el MBR (master boot record) dejando inutilizado el sistema operativo, además de encriptar los archivos con cierto tipo de extensión. Se propaga como gusano a través de diferentes técnicas de red para afectar nuevos equipos y explota debilidades de aquellos equipos que no tienen parches de actualización. Es un *exploit* modificado de EternalBlue, (Kaspersky 2017) [15]que está siendo utilizado para su propagación, por lo menos dentro de

[6] Ransomware es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados. El virus lanza una ventana emergente en la que nos pide el pago de un rescate, dicho pago se hace generalmente en moneda virtual (bitcoins, por ejemplo).

redes corporativas, y piden los atacantes un rescate en bitcoins ($300). No sirve de nada pagar el rescate porque su ataque hace imposible la recuperación de dichos [38]

M. *Equifax Data Breach*

La empresa Equifax, en julio del 2017, sufrió el robo de nombres, números de seguro social, fechas de nacimiento, direcciones y, en algunos casos, números de licencia de conducir de residentes en EEUU, así como de personas en Reino Unido y Canadá.

También administra datos sobre préstamos, pagos, tarjetas de crédito, límites de crédito, rentas y pagos de servicios públicos, entre otras informaciones.

Según informa Equifax, manejan los datos de más de 820 millones de personas y más de 91 millones de empresas en todo el mundo.

N. *Malware Ploutus*

Su primera aparición fue en septiembre de 2013 en México, es un software de venta a ciberdelincuentes en América Latina y EEUU, lo vendían bajo licencia y daban capacitación laboral, cuyo objetivo era atacar a cajeros automáticos (ATM). Después en el 2017 apareció Ploutus-D, que permite a un atacante dar instrucciones al ATM para dispensar dinero sin la necesidad de una tarjeta de crédito o débito, luego activa un mecanismo de limpieza por el cual se elimina cualquier rastro del ataque.[36]

IV. El problema de la Ciberdefensa y la Ciberseguridad en Latinoamérica

Un informe presentado por el Instituto Nacional de Estadísticas y Censos [21] (INEC 2016), en los últimos 5 años, el servicio de internet ha registrado un incremento del 22,5% en el 2012 y que llegó al 32,8% en el 2015. Esto hizo que el sector bancario incremente las ofertas de servicios en línea ej.: banca electrónica, transacciones electrónicas, etc.), así como otras entidades públicas, como el pago de los predios urbanos, pago de impuestos, matriculación y revisión vehicular, compras en línea en establecimientos de Ecuador, etc.

Estos avances tecnológicos hicieron surgir nuevos tipos de ataques hacia dispositivos móviles, como el primer caso del malware conocido como “Octubre Rojo”, que apareció en el 2007, y que robaba datos de teléfonos móviles, como smartphones (iPhone, Nokia y Windows Mobile). [30]

Los ciberataques también tuvieron como objetivo el área de procesos electorales [16], donde se recomendó que los funcionarios tengan una formación en ciberseguridad para la toma de decisiones con precisión, porque los atacantes buscan y detectan debilidades en diferentes actividades ya sea en los sectores académicos, de comunicación, servicios, etc.

En el sector agrícola, la agricultura de precisión (AP), los drones (UAV)[7] sobrevuelan zonas logrando cubrir 200 hectáreas en un vuelo de 30 minutos, permitiéndole procesar información más ágil, para realizar análisis de riesgos que mediante otras tecnologías convencionales podría durar días o semanas; sin embargo, hoy en día se dispone de sensores que pueden identificar plagas y enfermedades, en donde la capacidad robótica del dron recolecta insectos e incluso tender trampas, pero también son silenciosos por lo que pueden ser utilizados en ataques selectivos [5]. Pablo Bergel (2014), en calidad de legislador de Argentina, declaró “que los drones no solo tienen usos positivos, sino que podría usarse su tecnología para violar la intimidad y la represión, así como transportar armas o sustancias químicas letales”.

“La agricultura 4.0 con sus avances tecnológicos, permiten precisión, análisis y gran alcance, versus las ventajas comerciales de las posibles ventas online a través de redes sociales” indicó Javier Fernandez (2018), CEO de Tropicall Millenium, en donde los agricultores pueden acceder a sus datos de cosecha, envases, cuentas financieras a través de la web, así como manejar el control de fincas, riego controlado y todo esto con la inteligencia artificial. (Diaz 2018).[11] Se mencionan beneficios así como efectos adversos en este nuevo tema de la Agricultura 4.0, debido a que los drones son equipos aéreos, deberán cumplir con regulaciones legales acordes a cada país, lo que ha traído una nueva denominación: Actividades de Aprendizaje de E-agricultura. (FAO 2018)[13], que indica que se deberán tomar las debidas protecciones, como una tecnología emergente en el sector de la agricultura.

Como la tecnología avanza vertiginosamente y surgen nuevos riesgos de ataques que obligan a tener preparación, adoptar e implementar medidas para proteger la disponibilidad y confidencialidad de la información; el ciberdelito se caracteriza por: a) ser de rápida ejecución y amplio alcance, b) de fácil encubrimiento, c) novedoso, d) no siempre fácil de tipificar, e) intangible, f) difíciles de vigilar, g) transitorios por su naturaleza, h) pueden ser disociados en el tiempo, i) difícil identificación del autor; por lo tanto, son difíciles de investigar, perseguir y juzgar.[19]

El concepto de ciberseguridad debe contener lineamientos de tecnología y soluciones que puedan ser implementadas, brindando el nivel de protección adecuado a cada entorno productivo, basado en la gestión, protección e implementación de las políticas necesarias a nivel global.[36] (OEA) [8].

Es por esto que los conflictos se están trasladando al ciberespacio, porque los atacantes pueden hacerlo de forma anónima y de difícil rastreo, siendo ineficaz

[7] Vehículos aéreos no tripulados

[8] https://www.siemens.com/content/dam/internet/siemens-com/ar/comunicado-de-prensa/la-ciberseguridad-como-clave-del-xito-de-la-digitalizacion-gg-ods.pdf

la identificación del ciberdelincuente, lo que implica que cualquier sector de la sociedad se enfrente a vacíos legales de normativas internacionales, al exigir castigo por la violación de sus derechos de la integridad de su información, lo cual promueve la violación de la legislación de cualquier estado. [39]

La "digitalización de la sociedad" exhorta que existan garantías en el uso de herramientas tecnológicas para que brinden un nivel de confianza contra cualquier acción ilícita que pueda comprometer la disponibilidad, autenticidad, integridad y la confidencialidad de aquellos datos almacenados o transmitidos en la red. (Galán y Galán C. 2016)[14]

En el sector industrial, la digitalización está cambiando el mercado, debido a la innovación de productos, por la interconectividad y gran cantidad de información generada digitalmente lo que conlleva a la revolución de procesos de la industria 4.0, que impacta sobre la cadena de valor industrial como son las comunicaciones y la ciberseguridad, donde se conectan máquinas y plantas, lo que exige una implementación de medidas de protección de propiedad intelectual, multicapa como (ICS-Industrial Control Systems) recomendados por ISA 99(International Society of Automation, "Normativas de seguridad en sistemas de control) / IEC 62443 (Nueva numeración de la ISA 99 por nomenclatura de actualidad) / ISO 27001 (ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan) y sus normativas particulares dependiendo de la industria y locación donde se implementen (por ejemplo, NERC/CIP/son estándares de ciberseguridad , que el Gobierno Federal ha establecido como de obligado cumplimiento, para compañías relacionadas con el subsector eléctrico de la alta tensión en los Estados Unidos. NIST (Instituto Nacional de Estándares y Tecnología, cuyo laboratorio se encarga de la medición, los estándares y la tecnología en formas que mejoren la seguridad económica y mejorar la calidad de vida).[17]

Según el informe del Observatorio de la Ciberseguridad en América Latina y el Caribe, el uso de Internet, las tecnologías de información y las TIC's han afectado el crecimiento de la economía, gobiernos y sociedades a nivel mundial. Mckinsey[9] reitera que el acceso a internet está creciendo cuatro veces más rápido en países en vías de desarrollo, que aquellos países desarrollados y cuya intervención ha permitido que los estados miembros se beneficien con nuevas oportunidades económicas y sociales para sectores rurales y urbanos en donde se han renovado con nuevos servicios como: los bancarios, educación, salud. (Melissa and Francesca 2016)[32]. Además, el Foro Económico Mundial informó que las finanzas digitales pueden fomentar el PIB de varias maneras, Dos tercios serian por el incremento de la productividad y un tercio por el incremento de la inversión en toda la economía; y una menor proporción de los trabajadores que hacen depósitos en sus cuentas bancarias. Las finanzas digitales dan beneficios no solo a las personas sino a empresas pequeñas. Esto dentro de un ambiente donde se establezcan formas de identidad universalmente aceptadas para controlar el fraude. La inclusión financiera es de vital importancia tanto a nivel económico como de igualdad de género, tanto así que el banco Mundial tiene como objetivo llegar a una inclusión financiera universal en el 2020, debido a que millones de personas en las economías emergentes ya usan teléfonos móviles y porque las finanzas digitales permiten que este objetivo sea alcanzables (Lund, D'Andrea and Mckinsey 2016).[28]

Para iniciar un estudio de ciberseguridad, se recomienda una evaluación del estado actual de la organización, el cual contempla un análisis de amenazas y vulnerabilidades a las normativas de ciberseguridad vigentes, permitiendo identificar y clasificar los riesgos, evaluar el impacto empresarial, para implementar las protecciones necesarias y alcanzar el nivel de seguridad requerido. [27]

Expertos opinan que en el futuro, actividades relacionadas al cibercrimen serán del tipo como: el "Crime-as-a-Service", "Ransomware", "Uso criminal de datos", "Fraude de pago", "Abuso sexual infantil en línea", "Abuso de la Darkenet", "Ingeniería Social", "Monedas Virtuales"[10], así como el ataque a infraestructuras críticas, lo cual implicaría un peligro de vidas humanas y el colapso de la economía de los países. [19]

V. Algunos Tipos De Ataques De Vulnerabilidades

Garantivá [15] indica las tendencias más recientes sobre ataques a las debilidades de cualquier organización y que se generan por los siguientes ataques:

A. *Ransomware of things:*

Posibilidad de los ciberdelincuentes a secuestrar dispositivos a cambio de un rescate para devolverlo.

B. *Denegar el acceso a datos y sistemas (DDoS):*

Se incrementan los ataques debido a las motivaciones de los hackivistas.

C. *Privacidad de información en móviles:*

Descarga de aplicaciones gratuitas que extraen información.

D. *Movilidad:*

[9] Mckinsey Global Institute es una compañia que publica sobre productividad, competitividad y crecimiento en mercados financieros y el impacto de las tecnologías en la economia

[10] http://www.ituser.es/seguridad/2016/10/europol-presenta-su-informe-sobre-el-cibercrimen-en-europa

El Malware y su Realidad ¿Aumentada? (La realidad virtual incorpora nuevos riesgos a la seguridad de la información digital y al bienestar físico del usuario).

E. *Amenazas a infraestructuras críticas por Internet:*

Un código malicioso puede ocasionar grandes daños como a sectores eléctricos e industriales secuestrando datos o denegando servicios a cambio de un rescate.

F. *Plataformas de juego por consolas integradas:*

Posible fuga de información desde y hacia muchos dispositivos y plataformas [43]

VI. MEDIDAS DE PROTECCIÓN

Debido al incremento de ciberataques a nivel mundial en sectores como el financiero, gubernamental, público y privado; los diversos gobiernos, han conformado organizaciones de protección, como lo hicieron en España [45]:

- El Catálogo de Infraestructuras Críticas (CIC),
- Red de Emergencias CERT (Computer Emergency Response Team),
- CSIRT (Computer Security Incident Response Team); y,
- CCN-CERT (Centro Criptológico Nacional).

Vargas [46], indica que también están las Instituciones de Vigilancia de Organizaciones Nacionales e Internacionales como:

- La Agencia Europea de Seguridad de las Redes y de la Información (ENISA), que asesora y coordina las medidas adoptadas por la Comisión y los países de la Unión Europea que darán seguridad a sus redes y a los Sistemas de Información.
- El Centro de Ciberdefensa de la OTAN creado en el 2008, se encarga de analizar y responder a los ataques informáticos y amenazas provenientes de Internet, cuyo sitio tiene como sede Estonia.
- El Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), quien es responsable de impulsar, supervisar y coordinar aquellas actividades encomendadas a la Secretaria de Estado de Seguridad del Ministerio del Interior, que se relaciona con la Protección de las Infraestructuras críticas españolas que fueron aprobadas en el año 2002.
- Para enfrentar las ciberamenazas y/o disminuir su impacto, Alemania, en el 2011, lanzó su Estrategia de Seguridad Cibernética, y creó el Centro Nacional de Ciberdefensa y la publicación de su Plan Nacional para la Protección de Infraestructuras de Información (NPIIP).
- Francia, en el 2011, ha creado una Agencia de Seguridad para las Redes e Información (ANSSI) y una Estrategia de Defensa y Seguridad de los Sistemas de información.
- En Ecuador, por decreto ejecutivo, se creó el Plan Nacional de Seguridad Integral (PNSI) 2014-2017, así como el Plan Estratégico Institucional 2015-2017, y dentro de las Fuerzas Armadas se creó el Comando de Ciberdefensa. Así también fue creado el plan de gobierno electrónico 2014-2017 [10], el cual incrementó los controles de calidad a las empresas que prestan servicios de internet, así como la creación de redes comunitarias en zonas rurales [33] (Ministerio Coordinador de Seguridad, 2014), y las políticas de Gobierno para la transformación productiva y el desarrollo del Ecuador, entre otros.[46]

Algunas Organizaciones Internacionales han promovido estrategias para afrontar las amenazas de ciberdefensa y ciberseguridad a diferentes países, como la publicación de varios documentos o estándares, entre ellos el National Cybersecurity Strategy Guide [22] (ITU 2011)[11]

La conformación ***del Grupo e-Justicia de Cumbre Judicial Iberoamericana*** y a la colaboración de cada uno de sus miembros, ponen a disposición el "*Compendio Normativo sobre Ciberdelincuencia*" como un aporte al Derecho, donde se podrá encontrar legislación sustantiva y procesal referente a los delitos informáticos, así como aspectos relacionados con la estructura organizativa, jurisprudencial y convenios suscritos por sus respectivos países con información remitida por los Poderes Judiciales de: Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, México, Nicaragua, Paraguay, Portugal, República Dominicana y Uruguay.[18]

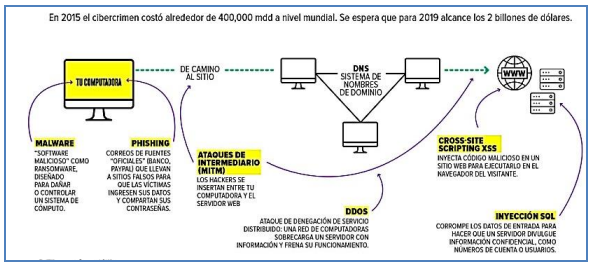
El análisis de este documento, se basa en las posibles formas de ciberataques y las medidas de protección, a tomarse en cuenta para minimizar o controlar cualquier riesgo.

En el 2014, se registró un aumento de 37% de robos a la banca virtual, 14% en tarjetas de crédito y 46% en cajeros electrónicos [33] (Ministerio Coordinador de Seguridad 2014). Pero estos inconvenientes no han sido solo en los sistemas de la banca, también los supuestos ataques cibernéticos procedentes de Colombia, Estados Unidos, Rusia, China y Francia sobre cuentas o datos personales de ciudadanos ecuatorianos [9], portales web de opinión libre (El Universo 2016), entre otros.[46].

Como se puede apreciar en la siguiente imagen, la revista Forbes (2018), muestra seis posibles formas de ciberataques.

[11] Organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

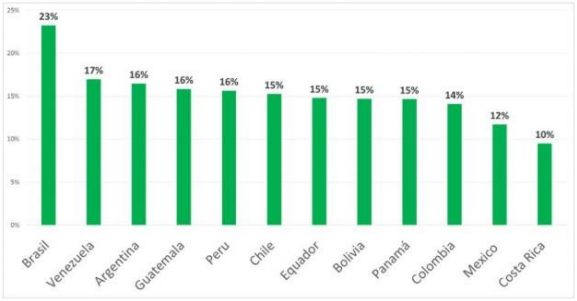
Figura 1. Diferentes tipos de Ciberataques



Fuente: Forbes 2018 [12]

En la siguiente figura, se muestra un diagrama de barras de países latinoamericanos afectados por phishing.

Figura 2. Países afectados por ataques de



phishing en Latinoamérica los primeros 7 meses de 2018.[13]

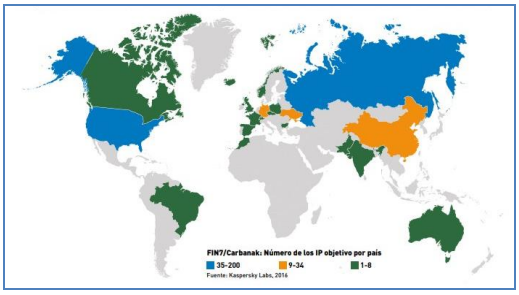
Fuente: Kaspersky 2018

De igual manera, Kaspersky (2018)[25], indica que mientras se está navegando, descargando archivos o cuando se reciben adjuntos de correos electrónicos engañosos, los más afectados son los usuarios domésticos que las empresas".

El sector financiero es quien recibe más ciberataques, es el que ha tenido un mayor porcentaje de riesgo, como lo indica un estudio realizado por la OEA[14] [36] ,"La ciberseguridad sigue siendo una preocupación de alto riesgo, para el 84% de los ejecutivos y directivos, seguido por el riesgo de cumplimiento (49%) y el riesgo estratégico (38%)." [2] [15].

En la figura 3 se muestra los diferentes países que sufrieron ataques por el grupo Carbanak:

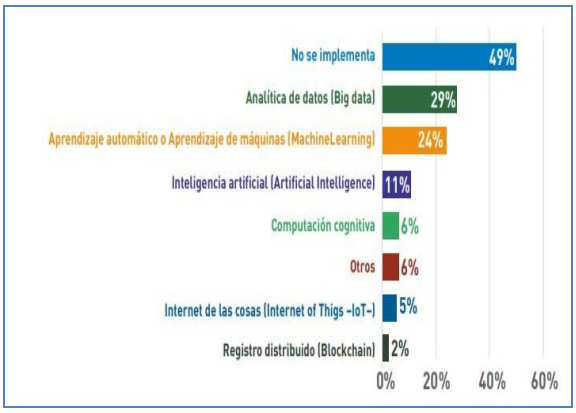
Figura 3. Jurisdicciones en el que el grupo Fin7/Carbanak[16] atacó al sector financiero.



Fuente: OEA 2018:22

Como medidas de protección, utilizadas en América Latina y el Caribe, se pueden visualizar las siguientes acciones en la figura 4:

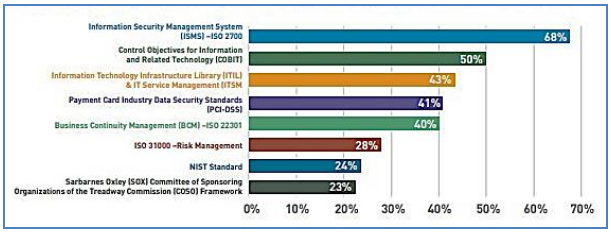
Figura 4. Medidas técnicas de seguridad digital para proteger los sistemas de información críticos en el sector bancario.



Fuente: (OEA 2018) [36]

Así mismo en la figura 5, se mencionan los marcos de seguridad y/o estandares internacionales adoptados como medidas de proteccion en el sector bancario en America Latina y el Caribe.

Figura 5. Controles de seguridad digital aplicados en entidades bancarias.



Fuente: OEA O., 2018

El sector público debería enfrentar a tres posibles ciberriesgos que son: 1) el posible robo o alteración a la información de los ciudadanos, 2) afectaciones a la operación de servicios públicos y 3) la operaciones de entidades gubernamentales, lo que conllevaría a causar daño a la confianza de dichas instituciones.[7]

[12] https://www.forbes.com.mx/seis-ciberataques-de-los-que-debes-protegerte-en-2018/

[13] https://elcomercio.pe/tecnologia/actualidad/ataques-ciberneticos-crecieron-60-america-latina-noticia-546790

[14] Organización de los Estados Americanos

[15] http://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

[16] Delincuentes cibernéticos que han atacado desde el 2013 y fueron capturados con ayuda de EEUU, Ucrania, Alemania entro otros.

Para enfrentar posibles ciberataques y responder a emergencias informáticas, todo dependerá de que tan capacitados esté el personal a cargo, cuyo conocimiento le permita aplicar estrategias de protección con tecnología de ciberseguridad. [26]

En la figura 6, e muestran los ciberataques sufridos en diferentes países en el 2017.

Figura 6. Ataques producidos en Latinoamérica 2017.

Fuente: kaspersky, 2017

La mayoría de estos ataques se dieron fuera de línea, es decir, fueron detectados y bloqueados en el disco duro de los usuarios. La infección se pudo efectuar a través de memorias USB, redes de trabajo u otros medios. Sin embargo, los ciberataques se realizaron vía Web (85%), mientras que 15% se realizó vía Email. El correo electrónico se destaca en los círculos cibercriminales para divulgar troyanos bancarios [24].

Es importante también la protección y saber cómo responder a emergencias informáticas sobre eventos de cibercrímenes, donde existan sistemas de protección contra el robo de identidad, que pueda ocasionar posibles fraudes, necesitándose la colaboración internacional para formar un marco multilateral de defensa, que brinde la cooperación entre países para enfrentar ciberriesgos. [31]

La ciberdelincuencia actúa sin dar aviso y causa grandes estragos afectando pérdidas económicas a nivel mundial; según estudios realizados, el total de costos financieros causados por dichos ataques superan los UD.$ 125.900 millones de dólares[41].

También el ser capaces de reaccionar y detectar la presencia de un ciberataque, proveniente de las inspecciones y los monitoreos de su red [12].

CONCLUSIONES

En los eventos de seguridad digital en contra de las entidades bancarias, así como en otro ámbito de manejo de información digital, es importante destacar algunas conclusiones en torno a la materia:

- El correo electrónico malicioso y el correo no deseado siguen siendo herramientas vitales para que los atacantes distribuyan malware, porque es donde las amenazas llegan directamente al objetivo con facilidad. Aplicando la combinación de técnicas de ingeniería social, phishing y enlaces maliciosos, así como archivos adjuntos, los adversarios solo tienen que sentarse y esperar a que los usuarios desprevenidos activen sus exploits. [8]

- La ingeniería social sigue siendo el preferido por muchos ataques. La autenticación de transacciones a través de aplicaciones móviles o mensajes de texto crece en popularidad, también aumenta el malware en los móviles, que intentan robar estas credenciales. [42]

- “Los ciberataques no solo están dirigidos a los clientes de los Bancos, también los han realizado contra las propias instituciones financieras, para realizar transferencias de grandes sumas en transacciones interbancarias fraudulentas”[42]

- Intercambiar información entre entidades bancarias, para aumentar la ciberresiliencia17 en el sistema financiero y conseguir la reducción del costo financiero, así como el control de la reputación en el mercado.

- La ciberdefensa no solo debe ser implementada en el sector militar o financiero sino también en el industrial y en otros sectores, por lo que se sugiere protección de redes Scada18, por su gran capacidad de reacción en tiempo real sin la intervención humana, aplicando el concepto de interfaz hombre máquina.[23]

- Para el manejo de drones (cinematografía, ganadería, deportes, seguridad privada, agricultura, ámbito policial, etc.), el crimen organizado podría interceptar las comunicaciones y redirigirlos para su beneficio, puesto que son más económicos y silenciosos que un helicóptero, pudiendo robar bienes transportados, misiones de vigilancia, así como ataques selectivos , lo que implicaría invertir en ciberseguridad para minimizar y controlar este tipo de situaciones.[34]

- Implementar herramientas, controles o procesos usando Tecnologías Digitales Emergentes, tales como Big Data, Machine Learning o Inteligencia Artificial para prevenir ciberataques o determinar patrones sospechosos asociados a fraude, entre otras capacidades de detección.[36]

- Los ciberdelincuentes encontraron una forma de obtener dinero sin estar expuestos físicamente y que, al utilizar tácticas tecnológicas, evaden o se infiltran por los puntos débiles de las organizaciones, lo que deja en evidencia los sistemas obsoletos y que fomenta que estos ciberataques sigan aumentando y evolucionando.

- Expertos sugieren utilizar métodos de protección como doble factor de autenticación o multifactor, así como claves adicionales de tipo biométrico para robustecer la seguridad y proteger su información financiera.[20]

[17] Capacidad de prevenir, detectar y responder ante los ciberataques
[18] Supervisory Control and Data Acquisition. Sistema de automatización industrial y máquinas

- Apoyo a la gestión del riesgo de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) por parte de la alta dirección de la entidad bancaria, se informa que más del 60% del total de las entidades bancarias en la región lo demuestran: a) exigiendo la adopción de buenas prácticas de seguridad (65%), b) capacitando y sensibilizando en seguridad digital (63%) y c) promoviendo planes de seguridad digital (60%).[36]

- Un reto para el tema de ciberseguridad es la protección en los sectores en general hacia el IoT, ya que se interconectan las cosas y se comparte datos.

- Por último, para neutralizar los ataques, la organización, debe capacitar en fundamentos técnicos a su fuerza laboral y en la gobernanza de la seguridad cibernética.

REFERENCIAS

[1]Balbi, Muriel. Las cinco principales ciberamenazas para 2018 y cómo combatirlas. 9 de diciembre de 2017. https://www.infobae.com/tendencias/innovacion/2017/12/09/las-cinco-principales-ciberamenazas-para-2018-y-como-combatirlas/.

[2]BANKDIRECTOR. «Bankdirector. (2018). 2018 Risk Survey.» 2018. https://www.accenture.com/t20170419T051104Z__w__/us-en/_acnmedia/PDF-49/Accenture-Building-Confidence-Solving-Bankings-Cybersecurity-Conundrum-Info.pdf#zoom=50.

[3] Basco, Ana, Gustavo Beliz, Diego Coatz, y Paula Garnero. «Industria 4.0 Fabricando el Futuro.» julio de 2018. https://publications.iadb.org/bitstream/handle/11319/9015/Industria-4-0-Fabricando-el-futuro.pdf?sequence=1&isAllowed=y (último acceso: 14 de noviembre de 2018).

[4] BBC News, Mundo. «El virus que tomó control de mil máquinas y les ordenó autodestruirse.» octubre de 2015. https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet.

[5] Bonanno, Gonzalez, y Laccarino. *"Uso de tecnología drone para controlar campos agricolas".* 2014. https://repositorio.uade.edu.ar/xmlui/bitstream/handle/123456789/2482/Bonanno.pdf?sequence=1.

[6] Briones Riverosa, D. «Reflexiones sobre la Estrategia de Seguridad Nacional Española: lecciones para Sudamérica. Revista Científica "General José María Córdova", 12 (13),.» Revista Científica "General José María Córdova" , 2014: 107-124. .

[7] Castañares, Itzel. *el posible robo o alteración a la información de los ciudadanos.* 27 de 07 de 2018. http://www.elfinanciero.com.mx/tech/cibercrimen-afecto-a-1-de-cada-4-mexicanos-en-2017-pero-creen-navegar-seguros.

[8] Cisco. «Cisco. (2018). Reporte Anual de Ciberseguridad CISCO 2018.» 2018. https://www.cisco.com/c/es_co/products/security/security-reports.html#~stickynav=3.

[9] Comercio., El. *"Hackers de Rusia, China, EE.UU. y Francia dirigen ataques a Ecuador".* 29 de octubre de 2016. http://www.elcomercio.com/actualidad/hackers-rusia-ecuador-ciberataques-seguridad.html.

[10] COSEDE. «(Corporación del Seguro de Depósitos, Fondo de Liquidez y Fondo de Seguros Privados). 2014. "Plan de Gobierno Electrónico".» 2014. , http://www.cosede.gob.ec/?p=3677.

[11] Diaz, Andrea. «Agricultura 4.0.» *Vida Economica*, 2018: p.18.

[12] Eset. «TENDENCIAS EN ciberseguridad 2018: El costo de nuestro mundo conectado.» 2018. https://www.welivesecurity.com/wp-content/uploads/2017/12/Tendencias_2018_ESET.pdf (último acceso: noviembre9 de 2018).

[13] FAO, FAO. *e-agricultura.* 05 de 02 de 2018. http://www.fao.org/e-agriculture/news/african-union-embraces-drones-technology-agriculture.

[14]Galán, C., y C. Galán C. «La ciberseguridad pública como garantía del ejercicio de derechos.» En *Derecho & Sociedad*, 47, 293-306. 2016.

[15]Garantivá, Edgar. «Retos de Seguridad Informatica y Seguridad de la Informacion.» 2015. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2890/00002246.pdf?sequence=1.

[16]Gil, Javier. *LA INTEGRACIÓN DEL CIBERESPACIO EN EL ÁMBITO MILITAR.* 11 de octubre de 2017. http://www.seguridadinternacional.es/?q=es/content/la-integraci%C3%B3n-del-ciberespacio-en-el-%C3%A1mbito-militar.

[17]Guitera, Gustavo. *Canal Ar, Digitalizacion y Ciberseguridad.* 14 de septiembre de 2018. http://canal-ar.com.ar/26332-Digitalizacion-&-Ciberseguridad.html.

[18]Iberoamericana, Cumbre Judicial. «XIX Edición – Cumbre Judicial Iberoamericana.» abril de 2018. http://www.cumbrejudicial.org/asamblea-plenaria/documentacion-posterior-asamblea-plenaria-edicion-xix/download/1003/673/15.

[19]Iberoamericana, Cumbre Judicial. «Ciberdelincuencia - Cumbre Judicial Iberoamericana.» 16 de febrero de 2018. http://www.cumbrejudicial.org/ii-reunion-preparatoria/documentacion-posterior-segunda-preparatoria-edicion-xix/item/593-compendio-normativo-sobre-ciberdelincuencia.

[20]Incibe. «Dos mejor que uno: doble factor para acceder a servicios críticos.» 22 de febrero de 2017. https://www.incibe.es/protege-tu-empresa/blog/dos-

mejor-uno-doble-factor-acceder-servicios-criticos (último acceso: 3 de Noviembre de 2018).

[21]INEC. «(Instituto Nacional de Estadísticas y Censo). 2016. "Tecnologías de la Información y Comunicaciones 2015",.» 2016. http://www.ecuadorencifras.gob.ec/.inec/Estadisticas./2015/Presentacion_TIC_2015.pdf.

[22]ITU. «National Cybersecurity Strategy Guide.» 2011. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNational-CybersecurityStrategyGuide.pdf.

[23]Kamlofsky, Jorge, Masih Samira Abdel, Colombo Hugo, y Veiga Daniel. *Seguridad en Redes las Industriales: Clave para la Ciberdefensa de las Infaestructuras Criticas.* 2017. http://sedici.unlp.edu.ar/bitstream/handle/10915/62725/Documento_completo.pdf-PDFA.pdf?sequence=1 (último acceso: 1 de noviembre de 2018).

[24]Kaspersky Lab Daily. «33 ataques por segundo: Kaspersky Lab registra un aumento de 59% en ataques de malware en América Latina.» 12 de septiembre de 2017. https://latam.kaspersky.com/blog/33-ataques-por-segundo-kaspersky-lab-registra-un-aumento-de-59-en-ataques-de-malware-en-america-latina/11265/.

[25]Kaspersky. Nuevo brote de ransomware New Petya / NotPetya / ExPetr. 27 de junio de 2017. https://www.kaspersky.es/blog/new-ransomware-epidemics/13581/.

[26]Leiva, Eduardo Alfredo. «Estrategias Nacionales de Ciberseguridad: Estudio Comparativo basado en Enfoque Top Down desde una vision glibal a una vision local.» *Revisa lAtnoamericano de Ingenieria de Software*, 2015: 16.

—. «Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local.» Revista Latinoamericana de Ingeniería de Software, 2015. 161-176.

[27]Lozano O, Marisol. «DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE INFORMACIÓN (PESI) PARA UNA COMPAÑIA DE SEGUROS.» 2017. http://alejandria.poligran.edu.co/handle/10823/1004.

[28]Lund, Susan, Tyson D'Andrea, y Mckinsey. «La economía digital es vital para el crecimiento económico inclusivo.» 16 de diciembre de 2016. https://es.weforum.org/agenda/2016/12/la-economia-digital-es-vital-para-el-crecimiento-economico-inclusivo (último acceso: 10 de noviembre de 2018).

[29]Machin, Nieva, y Manuel Gazapo. «LA CIBERSEGURIDAD COMO FACTOR CRÍTICO EN LA SEGURIDAD DE LA UNION EUROPEA.» *Revista UNISCI, núm. 42, octubre, 2016,*, 2016: pp. 47-68.

[30]Macia, Lanfranco, Venosa, Piazza, y Pacheco. *Seguridad en dispositivos móviles: un enfoque práctico.* WICC 2014 XVI Workshop de Investigadores en Ciencias de la Computación, 2014.

[31]McKinsey & Company . «Perspectiva de ciberseguridad en México - Comexi.» junio de 2018. https://consejomexicano.org/multimedia/1528987628-817.pdf.

[32]Melissa, Hathaway, y Spidalieri Francesca. *Desarrollo sostenible y seguro: un marco para las sociedades conectadas resilientes.* 2016. http://www.iadb.org/ciberseguridad.

[33]Ministerio Coordinador de Seguridad. «"Ciberseguridad escenarios y recomendaciones". Revista Digital del Ministerio Coordinador de Seguridad.» 2014.

[34]Mora T, Juan. *Drones . ¿La clave para el Desarrollo y la seguridad en Africa?* 23 de 05 de 2018. http://www.ieee.es/Galerias/fichero/docs_analisis/2018/DIEEEA19-2018_Drones-Clave_Desarrollo_SeguridadAfrica_JAMT.pdf.

[35]Niño, Andrea, y Jimmy Rodriguez. «Determinación de la colorimetría de agroquímicos aplicados al cultivo de frijol, para el control fitosanitario a través de agricultura de precisión, en la finca Buena Vista del municipio de Cabrera, Cundinamarca.» *Revista de Tecnologia y Productividad*, 2017: 9-19.

[36]OEA. «Estado de la Ciberseguridad.» 2018. http://www.oas.org/es/sms/cicte/sectorbancariospa.pdf.

—. «Estado de la Ciberseguridad en el Sector Bancario en America Latina y el Caribe.» 25 de octubre de 2018. http://www.asbasupervision.com/es/bibl/x-lecturas-recomendadas/1782-el-estado-de-la-ciberseguridad-en-el-sector-bancario-en-america-latina-y-el-caribe/file.

[37]OEA, BID. «Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? .» 2016. www.observatorioseguridad.com.

[38]Perez, Diego. «WeliveSecurity.» 29 de junio de 2017. https://www.welivesecurity.com/la-es/2017/06/29/todo-sobre-nuevo-ataque-de-ransomware/.

[39]Romano O, Daniel. «Criminología Informática. Anonymous: ¿Justicia cibernética o terrorismo.» 5 de 12 de 2016. https://dialnet.unirioja.es/servlet/articulo?codigo=6028962.

[40]Sanz, Antonio. «China, EEUU y las APT: La importancia del informe Mandiant.» 28 de 02 de 2013. https://www.incibe-cert.es/blog/china-eeuu-apt-informe-mandiant.

[41]Symantec. «Informe Norton sobre Ciberseguridad 2016 - Symantec.» 2016. https://www.symantec.com/content/dam/symantec/mx

/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf (último acceso: 09 de nov de 2018).

[42]—. «Symantec .(2017). Internet Security Threat Report - Financial Threats Review 2017, An ISTR Special Report.» 2017. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pd.

[43]TechTarget. «Seguridad como rehén, tendencias de ciberseguridad para 2017.» 2017. https://searchdatacenter.techtarget.com/es/cronica/Seguridad-como-rehen-tendencias-de-ciberseguridad-para-2017.

[44]UIT. *http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx.* 2014. (último acceso: 2018).

[45]Urueña C, Francisco. *Ciberataques, la mayor amenaza actual.* 16 de enero de 2015. http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf (último acceso: 2018).

[46]Vargas, Recalde, Reyes. «Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa.» *Revista Latinoamericana de Estudios de Seguridad*, 2017: 31-45.

[47]Villanueva, Julio Cesar. «Universidad Piloto de Colombia.» 2014. http://polux.unipiloto.edu.co:8080/00002646.pdf.