ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR

Jorge Enrique ALVARADO CHANG*
Departamento de TICs, Instituto Superior Tecnológico Juan Bautista Aguirre,
Licenciado en Sistemas de Información, Daule, Ecuador

* Autor para correspondencia: jeach2000@hotmail.com

RESUMEN

El ciber ataque es uno de los delitos informáticos que más ha crecido desde el 2005, el robo de información y la afectación a instituciones públicas y privadas son las principales consecuencias de los ataques cibernéticos. Mundialmente, las organizaciones y compañías de seguridad establecen medidas para prevenir los ataques. El presente análisis aplica una investigación descriptiva y tiene el interés de evaluar si en la República del Ecuador existen actualmente las medidas que permitan contrarrestar los crecientes ataque cibernéticos que se han detectado.

Palabras clave: amenaza, análisis, ciberdefensa, ciberseguridad, ataque, prevención.

ABSTRACT

Cyber-attack is one of the computer crimes that has grown the most since 2005, theft of information and the involvement of public and private institutions are the main consequences of cyber-attacks. Worldwide, security organizations and companies establish measures to prevent attacks. This analysis applies descriptive research and has the interest of evaluating whether in the Republic of Ecuador there are currently measures to counteract the growing cyber-attacks that have been detected.

Keywords: threat, analysis, cyber defense, cyber security, attack, prevention.

INTRODUCCIÓN

En la sociedad actual, donde la información se transmite utilizando las computadoras y las redes, el internet se ha convertido en el principal medio del avance económico, político y social. La vida cotidiana de las personas se ha adaptado a las nuevas tecnologías de la información; así también se ha abierto un nuevo campo de ataques del tipo informático, que ponen en alto riesgo a las sociedades actuales (Vargas, Recalde y Reyes, 2017). El mundo moderno se ha visto afectado por grupos de delincuentes informáticos llamados "Hackers", que debido a la globalización, no están limitados por las fronteras. Las grandes potencias como los países en desarrollo, y en especial estos últimos, son susceptibles de recibir ciberataques; existe por lo tanto la necesidad de realizar un estudio obligado para establecer las político-estratégicas de la defensa de los estados; la ciberdefensa y ciberseguridad son las áreas claves de los estudios estratégicos para proteger el ciberespacio (Vargas, Recalde y Reyes, 2017; Llangarí, 2016; Freire, 2017; Izaguirre y León, 2018; Tates y Recalde, 2018).

Las compañías de seguridad cibernética y organizaciones privadas a nivel mundial establecen medidas y prevenciones de ataques y robo de información. Latinoamérica no

está exenta de código malicioso denominado malware; países como Brasil, Argentina, Uruguay, Chile, Colombia, Costa Rica, El Salvador, Guatemala, Honduras, México, Nicaragua, Paraguay, Perú y Venezuela han tenido ataques de malware comprometiendo sistemas informáticos e información restringida. En el 2016 la compañía de seguridad informática ESET informo que 49 % de las empresas pequeñas y 30 % de empresas medianas o grandes reportaron problemas de código malware, y de manera más vulnerable se encuentra el sector público, debido que no se aplica una política homogénea de identificación de riesgos y por lo tanto no se pueden tomar las medidas de ciberseguridad, necesarias. Algunas compañías han sufrido otro tipo de ataques enfocados a nivel de red o por conexiones remotas, que son ataques que anteriormente no eran considerados importantes, pero que hoy en día son un alto riesgo para el sector público y privado (Yépez, Alvarado, Ortíz y Acosta, 2017; Freire, 2017; Carrera, 2019; Alcívar, Blanc y Calderón, 2018; Rocha, 2019).

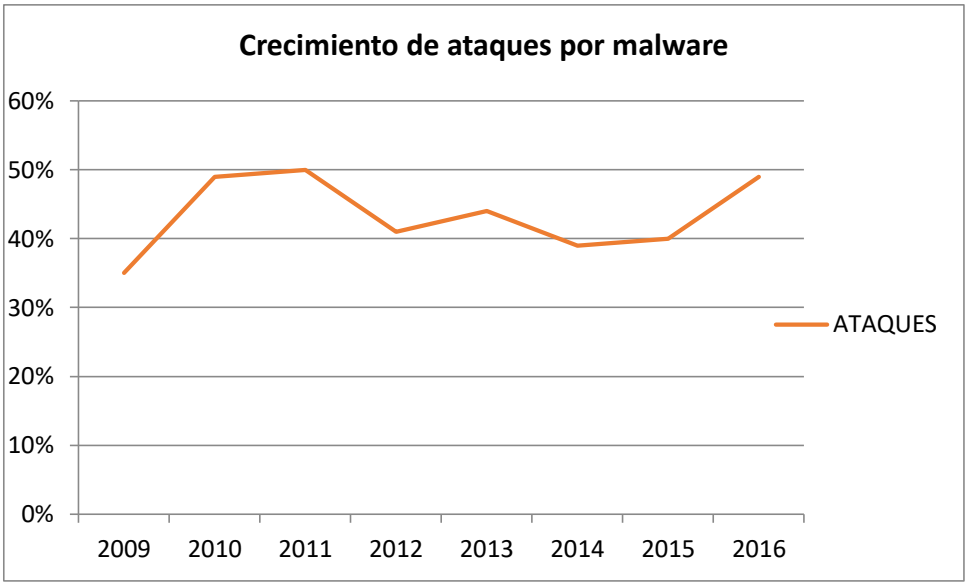

Figura 1. *Evolución de ataques por malware desde 2009 a 2016. Fuente: ESET. (2017)*

En la República del Ecuador, estos temas se han discutido ampliamente y se enfocan en lograr un modelo nacional de gobernanza y ciberdefensa, modelo que según las estadísticas de los resultados, aún requiere trabajo y maduración para prevenir y sancionar los ataque cibernéticos (Vargas, Recalde y Reyes, 2017; Llangarí, 2016). Según datos de Kaspersky Lab en su informe de amenazas en tiempo real, en junio del año 2017, Ecuador ocupó en América del Sur el primer lugar con el 2,8 % y el quinto lugar a nivel mundial en cuanto a ciberataques a sus redes. El 49,05 % de estos fueron ocasionados por ataques de fuerza bruta (denominado Bruteforce Generic RDP) a servidores de RDP; este ataque explora los rangos de IPs y de puertos TCP predeterminado de los servidores y se hacen pasar como clientes autorizados del servicio; una vez que se ha encontrado el servidor RDP vulnerable, se accede con rol de administrador auto asignado y puede tener el control total de todos los recurso almacenados (Freire, 2017; Betz, 2019).

En Ecuador el 43 % de los ciudadanos tiene acceso a internet, sin embargo la gran mayoría de estos, desconocen medidas de protección y prevención sobre las amenazas y peligros de su uso, debido a que carecen de una educación formal sobre el tema informático, siendo fácilmente víctimas de los ciberataques; por otro lado las políticas de ciber seguridad en las empresas del Ecuador, tampoco se aplican de manera rigurosa.

El caso del asilo político al representante de wikileaks, Julián Assange, ha provocado que

los hackers simpatizantes de este grupo, pongan atención sobre los movimientos políticos que realiza el gobierno del Ecuador, pero a pesar de esto, los planes de contingencia y el fortalecimiento jurídico e institucional del país, aún se consideran en desarrollo; entonces, ante estas amenazas globales a las que Ecuador está expuesto, surge la pregunta de: ¿Cuál es la situación actual del Ecuador con respectos a todo este contexto socio político internacional que se vive actualmente?.

En este trabajo de análisis, se aplica el método descriptivo-analítico que consiste en describir los hechos que ocurren y descomponer cada uno de los elementos que conforman el problema, para examinarlos individualmente en su naturaleza, se identifican sus causas y sus efectos; al observarlos se puede conocer su esencia, hacer analogías y probar teorías para comprender mejor su comportamiento y entender cómo se relaciona con los otros elementos ayudando a entender el contexto.

METODOLOGÍAS

El presente análisis aplica una investigación descriptiva-analítica de los principales ataques y hechos que se han suscitado en el entorno del país en los últimos años, ataques que han ocurrido a nivel global, donde el Ecuador también ha sufrido incidentes importantes; y ataques focalizados de grupos de hackers, como una represalia a decisiones políticas del Gobierno Central, que han colocado al Ecuador en los primeros lugares de las listas de los países con mayor números de ataques cibernéticos.

DESARROLLO

Cuando se habla de soberanía, se entiende que si un grupo de personas, locales o extranjeras conocidos como hackers, están ingresando sistemáticamente y sin autorización a redes informáticas de naturaleza privada o pública, entonces los organismos de seguridad y defensa, deben actuar en respuesta a esa situación de amenaza a la seguridad interna y externa, y establecer las respectivas políticas, regulaciones y estrategias para cuidar la privacidad de las personas y la información, servicios e infraestructura sensible del Estado (Ramos, 2014; Castro, 2015).

Las nuevas guerras modernas están formadas por unidades de ciberguerreros que se preparan al nivel informático, colocando puertas traseras y bombas lógicas listas para ser activadas en un momento de conflicto, sin que nadie lo note, algunos de estos ataque pueden ser patrocinados por el interés de un tercero que financia la operación, ya sea por interés privado, político o ideológico, o por motivos más peligrosos como crimen organizado, terrorismo o hacktivismo, la anatomía de un ataque generalmente está compuesta por 5 fases:

- Reconocimiento del objetivo
- Exploración de vulnerabilidades
- Obtención del acceso
- Mantener acceso
- Eliminación de evidencias

Por ejemplo, los sistemas de control y comunicación podrían ser desactivados en un momento de ataque, trasgredir el sistema financiero de un gobierno, auto designarse administrador de la red y eliminar información digital, solo por citar alguna posibilidad (Ramos, 2014; Freire, 2017).

Lo más común del robo de información digital es aprovechar las fallas encontradas de

software (múltiples programadores) y hardware (múltiples proveedores), donde las víctimas no conocen que su información ha sido comprometida por un ataque de los hackers que aprovechan las debilidades mencionadas para engañar a los usuarios. Para tener una referencia, en 2009 se estimó que un nuevo tipo malware ingresaba al ciberespacio cada 2,2 segundos, los expertos han indicado que software de "gran tamaño" contienen puertas traseras o vulnerabilidades de seguridad. En el año 2017, Ecuador quedo en tercer lugar de afectación en América Latina por el virus Wannacry, y en el 2019 toda la información de los 17 millones de ecuatorianos quedó expuesta a los hackers y fue la empresa de seguridad VPNMENTOR de Israel quien encontró la falla de seguridad en un servidor en Miami, siendo la más grande filtración de seguridad en América Latina (Ramos, 2014; Llangarí, 2016; Carrera, 2019; Rocha, 2019; Arciniegas, 2019).

Industrias militares del primer mundo, fabrican ellos mismos sus propios componentes y soluciones casa adentro, y rechazan hardware y software de producción extranjera para mitigar los riesgos, la tecnología desarrollada por terceros puede facilitar la instalación o actualización de huecos de seguridad implantados de forma deliberada, simplemente esperando la señal de un conflicto. Mientras más dependan las organizaciones de tecnologías informáticas que utilizan internet, más vulnerables son a recibir algún tipo de ataque cibernético; por ello, se hace necesario implementar técnicas criptográficas de alta seguridad, pero estas deben evolucionar constantemente en un corto margen de tiempo, lo que genera grandes costos operativos que son necesarios adoptarlos para estar protegidos contra los ataques cibernéticos, en el largo plazo los beneficios superan la inversión (Ramos, 2014; Freire, 2017; Jaramillo y Medina, 2014; Alcívar, Blanc y Calderón, 2018).

Ser responsable de la seguridad, implica tomar en serio las amenazas y los riesgos, y adoptar políticas de regulación y estrategias de seguridad y defensa lo suficientemente robustas que permitan el control sobre los aspectos más importantes del funcionamiento del Estado, por ejemplo, crear redes propias diferenciando la infraestructura crítica de la internet pública o abierta. Lograr la seguridad absoluta es imposible, pero si es posible incrementar los niveles de previsión, ya que no se puede confiar en las grandes proveedoras de redes monopolizadas o servicios de internet donde un país ejerce el pleno control de toda su infraestructura, ni en el uso de software comercial cuyo código está protegido por la ley de propiedad intelectual, ambas constituyen un riesgo por lo que se debe planificar de manera independiente. Lograr soberanía y seguridad nacional en el ciberespacio, es un proceso a largo plazo, resulta fundamental tomar conciencia de los pasos que se deben seguir para conseguirla (Ramos, 2014; Uquillas, 2018; Rocha, 2019).

La República del Ecuador ofrece servicios automatizados a los ciudadanos que tiene como objetivo mejorar y agilitar los trámites públicos, como la entrega del pasaporte y el documento de identidad, entre otros. Por tanto, el Gobierno debe implementar las políticas, regulaciones y estrategias para lograr niveles de seguridad y defensa adecuados para proteger el ciberespacio; existe la propuesta de la creación de un Comando Operacional de Ciberdefensa compuestas por profesionales en la materia similar a como se procede con otros especialistas, el uso de dispositivos de hardware o software de países extranjeros debe descartarse pues compromete la seguridad nacional, se debe trabajar en una estructura tecnológica que nos garantice seguridad integral y lograr soberanía en materia de TICs (Ramos, 2014; Freire, 2017; Tates, 2018; Moran, 2017).

Con el internet de las cosas, mantener soberanía se vuelve un tema progresivamente más complejo, los sistemas de información están conectados a las redes al igual que los

dispositivos inteligentes de aplicaciones variables, y por ello las redes se vuelven más vulnerables, se torna imposible controlar todas sus funciones. Actualmente la necesidad de una nueva arquitectura de internet que considere ampliamente los temas de seguridad es inevitable, la arquitectura actual no fue concebida para todas las capacidades y servicios actuales. El común de los usuarios, desconocen que los dispositivos actuales tienen la capacidad de espiar con imagen, incluso se pueden utilizar las imágenes como medio de transporte de información oculta; el incremento de dispositivos inteligentes conectados a la red, provoca cada vez más incidentes de seguridad, si un usuario es de interés de alguien, a través de sus dispositivo inteligente, será ubicado y espiado, se podrán conocer sus movimientos, escuchar sus conversaciones y conocer sus datos privados; será entonces necesario analizar y revisar las políticas de conectividad a la red, para encontrar la solución a los problemas de seguridad que se originan a largo plazo (Ramos, 2014; Jaramillo y Medina, 2014; Granda,s.f.; Cano y Toulkeridis, 2019; Alcívar, Blanc y Calderón, 2018; Betz, 2019).

Caso Julian Assange

En el año 2013, Julián Assange denunció a la comunidad mundial que la red internet no es privada y que los militares estadounidenses observan el tráfico y contenido como una estrategia para poder incidir en las sociedades, indicó por ejemplo que la soberanía digital de América Latina y el Caribe no puede estar garantizada si utilizan un canal de comunicaciones cuya fibra óptica pasaba por USA (Izaguirre y León, 2018; Castro, 2015).

El retiro del asilo político al reconocido hacker Julian Assange, fundador de WikiLeaks, es un tema controversial para el Ecuador; al retirar el asilo las autoridades de gobierno presumieron un inminente incremento de ataques cibernéticos a entidades públicas y privadas, mantener el asilo de Assange representó cerca de 20 millones de dólares en temas de seguridad, alimentación y medicina según declaraciones a la Asamblea Nacional del canciller José Valencia. Incluso el presidente de la República Lenin Moreno denunció el hackeo de su dispositivo móvil personal y el de su familia, señalando a Assange como responsable de este y otros actos que irrespetaban el acuerdo de asilo político (Moncayo, 2019; Carrera, 2019).

El 11 de abril del 2019, se retira el asilo a Julian Assange y a partir de ese evento se recibieron 40 millones de ciberataques a sitios web de entidades como el Banco Central, la Presidencia, la Cancillería, el Consejo de la Judicatura, el Ministerio del Interior, el SRI, la Corte Constitucional del Ecuador, gobiernos autónomos, etc. Ecuador ocupó el primer lugar de países atacados en el ciberespacio, perpetuado por grupos de hackers que reprobaron la decisión tomada por el Gobierno del Ecuador con respecto al caso de Julian Assange. En consecuencia, el Ministerio de Defensa activó un protocolo de seguridad con el propósito de fortalecer la ciberseguridad del país, no se ha dado a conocer los resultados de la aplicación de protocolo ni como era su funcionamiento. El caso Assange ha demostrado a las autoridades que el país no estaba preparado para contener los ciberataques, aunque si existe una tenue legislación, las entidades no están debidamente coordinadas siendo esta una debilidad al momento de aplicar políticas de seguridad. Ecuador también recibió ofertas de ayuda de países como Israel para fortalecer su seguridad informática y el de sus sitios web (Moncayo, 2019; Granda y Saquisela, 2017; Carrera, 2019; Rivadeneira, 2019).

Sistema jurídico

La difusión y acceso a las Tecnologías de la Información y la Comunicación (TIC) ha incrementado el uso a nivel mundial del denominado ciberespacio; la ciberseguridad en

es implementada globalmente por todos los países, ya que ninguno está exento de un ataque de este tipo. En el Ecuador aún no se aborda el tema de la ciberseguridad como tema en la política exterior, las amenazas no tradicionales no se consideran seriamente para prevenir ataques a las infraestructuras críticas, no se cuenta con herramientas suficientes para una adecuada protección en temas de ciberseguridad. Es deber del Estado impulsar y garantizar el cumplimiento de los derechos ciudadanos, con base en los principios de equidad e inclusión, buscando el acceso equilibrado a las Tecnologías de la Información y Comunicación el cual es el propósito del Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL) aunque se sabe de su importancia, en el campo jurídico es difícil conseguir dicho objetivo (Moncayo, 2019; Jaramillo y Medina, 2014; Tates, 2018; Moran, 2017).

Son instalaciones del estado de Infraestructura Crítica (IC) aquellas que utilizan sistemas que ofrecen servicios esenciales y cuyo funcionamiento no admite soluciones alternativas; son instalaciones de redes y servicios, equipos de tecnología de la información cuya inhabilitación o destrucción generarían un impacto sobre la salud, la seguridad, la economía de los ciudadanos o el funcionamiento de las instituciones gubernamentales que son vulnerables; por citar un ejemplo, que pasaría si se pierde o elimina la información de los datos del Servicio de Rentas Internas (SRI), tanto los contribuyentes como la propia institución dejarían de cumplir sus obligaciones y el país tendría graves pérdidas económicas. Otro escenario es el Instituto Ecuatoriano de Seguridad Social (IESS), el cual ofrece sus servicios de salud de manera electrónica, donde los antecedentes de los pacientes se encuentran registrados en sus redes de datos y la pérdida de esta información implica que toda su historia clínica se perdería, provocando un estado de crisis social en el país. Se debe conocer cuál es la infraestructura crítica para poder aplicar una estrategia de ciberseguridad, de lo contrario no se tendrá claro lo que se quiere proteger. El gobierno central aún no ha definido cuáles son las infraestructuras críticas que se deben proteger y sin embargo el estado maneja una gran cantidad de información de los ciudadanos en varias bases de datos digitales de las diferentes plataformas utilizadas instituciones del Estado; los sectores estratégicos que se deberían proteger por su gran importancia son: sistemas hidrocarburíferos, sistemas eléctricos, sistemas financieros, sistemas de armas, mando y control militar (Moncayo, 2019; Uquillas, 2018; Izaguirre y León, 2018; Granda y Saquisela, 2017; Tates, 2018; Carrera, 2019; Castro, 2015; Rocha, 2019).

En la Unión Europea (UE) en materia de ciberseguridad se utilizan dos herramientas jurídicas institucionales que son: la creación de la primera estrategia de seguridad cibernética y el reglamento que crea la Agencia Europea de Seguridad de la Información de la Red (European Union Agency for Network and Information, ENISA). Un importante sitio web para la revisar información de herramientas jurídico-institucionales es el "Índice Nacional de Seguridad Cibernética" (National Cyber Security Index, NCSI). La base de datos global del NCSI, incluye información de 126 países y ofrece enlaces y documentos sobre ciberseguridad nacional de cada país. La Unión Internacional de Telecomunicaciones (International Telecomunication Union, ITU) es fundadora de la Agenda de Ciberseguridad Global (Global Cybersecurity Agenda, GCA). Se utiliza la agenda para un trabajo de cooperación internacional en el área de ciberseguridad. La GCA crea el Índice de Ciberseguridad Global (Global Cybersecurity Index, GCI) cuyo objetivo es evaluar mediante un cuestionario de veinticuatro indicadores el compromiso de cada país en la materia ciberseguridad. Estas organizaciones tienen como objetivo garantizar la privacidad y seguridad de la información privada y la regulación en lo que respecta al robo de identidad, especialmente

en países donde los niveles de prevención y control son muy bajos (Moncayo, 2019; Jaramillo y Medina, 2014).

Tabla I. Herramientas jurídico-institucionales que garantizan la ciberseguridad en Ecuador

Leyes/acuerdos y organizaciones
a) Constitución de la República del Ecuador b) Ley de Seguridad Publica y del Estado c) Ley de Comercio electrónico, firmas electrónicas y mensajes de datos d) Acuerdo No. 166, emitido por la secretaria Nacional de la Administración Publica (SNAP) 1. Ministerio de Defensa Nacional: ▪ Política de la Defensa Nacional "Libro Blanco" ▪ Acuerdo Ministerial No. 281 2. Dirección Nacional de Registro de Datos Públicos: ▪ Dato Seguro 3. Ministerio de las Telecomunicaciones y Sociedad de la Información (MINTEL): ▪ Plan Nacional de Gobierno Electrónico ▪ Ecuador Digital ▪ Plan de la Sociedad de la Información y del Conocimiento 2018 - 2021 4. Agencia de Regulación y Control de las Telecomunicaciones: ▪ Centro de Respuesta a incidentes informáticos del Ecuador (EcuCERT)

En 2009 se crea la Secretaría Nacional de Inteligencia (SENAIN) en su calidad de ente coordinador del Sistema Nacional de Inteligencia, tenía como principal función la de coordinar los subsistemas de inteligencia que pertenezcan a las Fuerzas Armadas y de la Policía Nacional para realizar labores de contrainteligencia, además eran parte de sus funciones la planificación, coordinación, supervisión, control y ejecución de todas las acciones de inteligencia que se encuentren en un nivel estratégico y operacional en la coordinación política y técnico operativo de los sistemas de inteligencia militar y policial, la seguridad interna de la Presidencia de la República y de los sistemas de inteligencia que podrían crearse a futuro; a pesar de que esta institución apuntaba a la adecuada protección de la defensa nacional del Ecuador, en 2018 se suprime la Secretaría de Inteligencia y crea el Centro de Inteligencia Estratégica (CIES), que adquiere todas las funciones que pertenecían a la Secretaría Nacional de Inteligencia y no se tiene información suficiente para poder determinar sus funciones específicas actuales (Moncayo, 2019; Moran, 2017).

Ecuador está en el puesto 82 del NCSI, clasificado como un país con ciberseguridad deficiente en general, que coincide con la percepción de los usuarios, sin embargo su gestión de incidentes y crisis, dirigido por el Comando Cibernético del Comando Conjunto de las Fuerzas Armadas, le da una ventaja en la protección de los intereses del país, a través de estrategias de ciberdefensa; otro aspecto positivo del Ecuador es la identificación electrónica y servicios de confianza, el ranking le da un porcentaje del 67 %, es decir cada ciudadano posee un número único (número de cédula), con el cual podrán acceder a todos los servicios ofrecidos por el Estado y sus diferentes entidades (Moncayo, 2019; Llangarí, 2016; Tates, 2018; Granda y Saquisela, 2017).

Tabla II. Síntesis de Ciberseguridad de Ecuador según el NCSI

De un total de 77 puntos contenidos en el Ranking Nacional de Ciberseguridad (NCSI) Ecuador cuenta con 25 puntos	**TOTAL**

INDICADORES GENERALES DE SEGURIDAD CIBERNÉTICA		6/27 (22,22 %)
Desarrollo de políticas de seguridad cibernética	0/7 (0 %)	
Análisis e información de amenazas cibernéticas	0/5 (0 %)	
Educación y desarrollo profesional	4/9 (44 %)	
Contribución a la seguridad cibernética global	2/6 (33 %)	
INDICADORES DE CIBERSEGURIDAD DE LÍNEA BASE		7/24 (29,16 %)
Protección de servicios digitales	1/5 (20 %)	
Protección de servicios esenciales	0/6 (0 %)	
Identificación electrónica y servicios de confianza	6/9 (67 %)	
Protección de datos personales	0/4 (0 %)	
INDICADORES DE GESTIÓN DE INCIDENTES Y CRISIS		12/26 (46,15 %)
Respuesta a incidentes cibernéticos	3/6 (50 %)	
Gestión de crisis cibernéticas	1/5 (20 %)	
Lucha contra el ciberdelito	4/9 (44 %)	
Ciberoperaciones militares	4/6 (67 %)	

Fuentes: National Ciber Security Index (2018)

Las medidas de ciberseguridad en Ecuador se aún no están claramente definidas, hasta la presente fecha aún no se conocen los objetivos de las entidades de control a nivel nacional, aun no se han identificado cuáles son todas las entidades críticas del país y cuáles serían los daños en caso de un ataque cibernético; los indicadores de la ciberseguridad del país, son muy bajos en comparación con países de la región. Ecuador no ha sido ajeno a los cambios por la globalización, pero debido a la lentitud en poder realizar las reformas jurídicas, y a la falta de comprensión de los gobernantes en cuanto a los peligros existentes en el ciberespacio, las políticas no están organizadas y estandarizadas en todas sus entidades gubernamentales, en el área de seguridad informática, entendiéndose que la seguridad es tan fuerte como su eslabón más débil.

CONCLUSIONES

El Ecuador presenta falencias considerables para identificar los riesgos, además no terminan de organizarse las instituciones de control y mucho menos tener un plan de respuesta ante ataques a la información; además faltan las suficientes herramientas jurídicas-institucionales para tener un nivel ciberseguridad adecuada, y no se ha ratificado ningún convenio internacional en materia de ciberseguridad.

Para implementar una adecuada ciberseguridad en Ecuador se debe crear una entidad cuyo principal objetivo se enfoque en la protección cibernética a nivel nacional, identificando y clasificando cuáles son las infraestructuras críticas del país y que sectores pueden ser los más afectados en caso de un ataque cibernético.

El país presenta indicadores muy bajos en comparación con países de la región. El MINTEL ya inicio la creación de una importante herramienta jurídica que consiste en implementar la estrategia de ciberseguridad; la cual debería estar enfocada en la protección de los recursos que están en peligro dentro del contexto del uso del ciberespacio en Ecuador, con una postura realista y actualizada y con la participación de los sectores público y privado, acompañados de profesionales expertos del área.

Los ciudadanos deben estar informados de los riesgos que se presentan al utilizar el ciberespacio; las entidades de control correspondiente deben publicar un informe anual de todos los ataques cibernéticos que han recibido y de las medidas de contingencia que se utilizaron para combatirlos, con el propósito de crear conductas individuales de protección ciudadana.

REFERENCIAS

Alcívar C., Blanc G., Calderón J. (2018). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. *Espacios, Vol. 39 (Nº 42) Año 2018 • Pág. 15*. Disponible en: http://www.revistaespacios.com/a18v39n42/a18v39n42p15.pdf

Arciniegas Y. (2019). Falla informática en Ecuador: los datos de casi toda la población quedaron expuestos. France24 con Reuters y EFE. Disponible en: https://www.france24.com/es/20190917-ecuador-datos-expuestos-informacion-filtracion

Betz, C. (2019). Informe sobre amenazas 2019. CenturyLink. Disponible en: https://info.centurylinkforbusiness.com/rs/131-SYO-861/images/CenturyLink-Report-Sep2019%20_sp.pdf?aliId=eyJpIjoiMFpxaGp5dFliZlZvVStXZyIsInQiOiJ0bklTZlNYUmo3OFBlcHdFWmdYdVFnPT0ifQ%25253D%25253D

Cano C., Toulkeridis T. (2019). Propuesta de un nuevo modelo de planificación para El diseño de operaciones de apoyo a la seguridad Integral del estado del Ecuador - ámbito interno. *Revista de Ciencias de Seguridad y Defensa (Vol. IV, No. 4, 2019)*. Disponible en: https://www.researchgate.net/profile/Theofilos_Toulkeridis/publication/330935031_propuesta_de_un_nuevo_modelo_de_planificacion_para_el_diseno_de_operaciones_de_apoyo_a_la_seguridad_integral_del_estado_del_ecuador-ambito_interno/links/5c5c5aafa6fdccb608af306e/propuesta-de-un-nuevo-modelo-de-planificacion-para-el-diseno-de-operaciones-de-apoyo-a-la-seguridad-integral-del-estado-del-ecuador-ambito-interno.pdf

Carrera M. (2019). El cambio de las políticas de seguridad informática ocurridas por la creación de nuevas políticas a partir del 2013 en el Ecuador. Escuela de Ciencias Políticas y Relaciones Internacionales, Ecuador. Disponible en: http://dspace.udla.edu.ec/bitstream/33000/11169/1/udla-ec-tlcp-2019-37.pdf

Castro E. (2015) Estudio prospectivo de la ciberdefensa en las fuerzas armadas del Ecuador. Universidad de las Fuerzas Armadas, Departamento de Seguridad y defensa, Sangolquí: Ecuador. Disponible en: http://repositorio.espe.edu.ec/jspui/bitstream/21000/11583/1/T-ESPE-049543.pdf

Freire K. (2017). Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad. Universidad Católica de Santiago de Guayaquil, Facultad de educación técnica para el desarrollo Carrera de Ingeniería en Telecomunicaciones, Guayaquil: Ecuador. Disponible en: http://192.188.52.94:8080/bitstream/3317/9203/1/T-UCSG-PRE-TEC-ITEL-245.pdf

Granda G. Metodología para el análisis forense de datos e imágenes de acuerdo a las leyes del Ecuador. Universidad Politécnica Salesiana, Carrera de Ingeniería de Sistemas, Cuenca. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/8943/1/UPS-CT005203.pdf

Granda K., Saquisela L. (2017). Análisis de vulnerabilidades del protocolo ssl/tls en las Páginas web gubernamentales del Ecuador más usadas en la carrera de ingeniería en Networking y Telecomunicaciones. Universidad de Guayaquil, Facultad de ciencias matemáticas y físicas, Carrera de ingeniería en Networking y telecomunicaciones, Guayaquil: Ecuador. Disponible en: http://repositorio.ug.edu.ec/bitstream/redug/24303/1/b-cint-ptg-n.234.%20granda%20katheryn%20del%20pilar.saquicela%20parra%20luis%20gustavo.pdf

Izaguirre J., León F. (2018). Análisis de los ciberataques realizados en América Latina. Universidad Internacional del Ecuador, Ecuador. Disponible en: http://revistas.uide.edu.ec/index.php/innova/article/view/837/779

Jaramillo F., Medina J. (2014). Análisis de la gobernanza de internet en el Entorno mundial y su impacto en Ecuador. Escuela Superior Politécnica del Litoral, Facultad de Ingeniería en Electricidad y Computación, Guayaquil: Ecuador. Disponible en: https://www.dspace.espol.edu.ec/retrieve/102140/D-84386.pdf

Llangarí A. (2016). Análisis de los delitos informáticos y de Telecomunicaciones en el Ecuador bajo las Nuevas normas jurídicas. Carrera de Ingeniería Electrónica, Redes y Comunicación de datos, Sangolquí: Ecuador. Disponible en: http://repositorio.espe.edu.ec/jspui/bitstream/21000/11654/1/T-ESPE-053079.pdf

Moncayo P. (2019). Herramientas jurídicas para garantizar a ciberseguridad del Estado. Análisis comparado de Colombia, Chile y Ecuador. Universidad Central del Ecuador, Facultad de Jurisprudencia, Ciencias Políticas y Sociales, Quito: Ecuador. Disponible en: http://www.dspace.uce.edu.ec/bitstream/25000/19494/1/T-UCE-0013-JUR-216.pdf

Moran C. (2017). Seguridad informática y realidad jurídica del ciberespacio en el Ecuador. Facultad de Derecho y Ciencias Sociales. Disponible en: http://dspace.udla.edu.ec/bitstream/33000/7974/3/udla-ec-tab-2017-70.pdf

Ramos M. (2014). Acerca de la soberanía del Ecuador en el Ciberespacio. CENAE. Disponible en: http://www.rebelion.org/docs/189922.pdf

Rivadeneira G. (2019). Ecuador ha recibido 40 millones de ataques cibernéticos. El universo. Disponible en: https://www.eluniverso.com/noticias/2019/04/15/nota/7287215/ecuador-ha-recibido-40-millones-ataques-ciberneticos-revela

Rocha C. (2019). Modelo de gestión de seguridad de la información para el sector público. Universidad Tecnológica Israel, Escuela de posgrados, Quito: Ecuador. Disponible en: http://157.100.241.244/bitstream/47000/1863/1/uisrael-ec-master%20-%20telem-378.242-2019-001.pdf

Tates C., Recalde L. (2018). La ciberseguridad en el Ecuador, una propuesta de organización. *Revista de Ciencias de Seguridad y Defensa (Vol. IV, No. 7, 2019) pp. 156-169*. Disponible en: http://geo1.espe.edu.ec/wp-content/uploads/2019/03/7art12.pdf

Uquillas R. (2018). Ciber defensa aseguramiento de las infraestructuras críticas. Quito, Comando de Ciberdefensa. Disponible en: http://portal.uasb.edu.ec/UserFiles/385/File/CYBER-RUQUILLAS.pdf

Vargas R., Recalde L., y Reyes R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO. *Revista Latinoamericana de Estudios de Seguridad, núm. 20, pp. 31-45*. Doi: https://doi.org/10.17141/urvio.20.2017.2571

Yépez J., Alvarado J., Ortíz M., y Acosta N. (2017). Análisis y prevención del Ransomware en la Universidad de Guayaquil, Universidad de Guayaquil, Facultad de Ciencias Matemáticas y Física, Carrera de Ingeniería en Sistemas Computacionales, Guayaquil: Ecuador. Disponible: http://www.revistaespirales.com/index.php/es/article/view/134/76