4.- ANÁLISIS DEFENSA NACIONAL

CIBERATAQUES: DESAFÍOS EN EL CIBERESPACIO

Mayo. de Com. Walberto Antonio Abad Páez[1]

RESUMEN

El presente trabajo de investigación, tiene el propósito de determinar los desafíos y blancos críticos actuales y futuros en el ciberespacio del Ecuador, se inicia con el desarrollo de un análisis exploratorio del ciberespacio, ciberataques y ciberdefensa mediante el uso de fuentes primarias y datos estadísticos, se desarrolla un entorno introductorio, el progreso del ciberespacio con su aporte y empleo inadecuado a la sociedad, se define una aproximación a la conceptualización de la ciberdefensa, la traslación de los conflictos al ciberespacio, se identifican estadísticos de incidentes para tratarlos con una metodología cuantitativa, empleando la analítica predictiva mediante herramientas informáticas de aprendizaje automático o machine learning, cuyos resultados darán la identificación actual y futura de recursos críticos en el ciberespacio; los blancos críticos tendrán implicaciones en el entorno de seguridad y defensa del Ecuador.

Palabras claves: Ciberdefensa, ciberseguridad, ciberataques, objetivos, activos críticos.

ABSTRACT

The present research work is intended to determine current and future critical challenges and targets in Ecuador's cyberspace, it starts with the development of an exploratory analysis of cyberspace, cyberattacks and cyberdefense through the use of primary sources and statistical data, an introductory environment is developed, the progress of cyberspace with its contribution and inadequate employment to society, defines an approach to the conceptualization of cyberdefense, the translation of conflicts into cyberspace, statistics of incidents are identified to be treated with a quantitative methodology, using predictive analytics using machine learning computing tools, the results of which will give the current and future identification of critical resources in cyberspace; critical targets will have implications for Ecuador's security and defense environment.

Key words: Cyberdefense, cybersecurity, cyberattacks, targets, critical information assets.

1 waabadp@ejercito.mil.ec
ACADEMIA DE GUERRA

Artículo enviado: 10/02/2020 - Aceptado: 28/02/2020 - Publicado: Abril 2020.
Revista de la Academia de Guerra del Ejército Ecuatoriano, Volumen 13. Núm. 1 Abril 2020. pp. 116-128
e-ISSN: 2600-5697 – ISSN: 2600-5689 – DOI: https://dx.doi.org/10.24133/age.n13.2020.11

1. Introducción

La creciente y vertiginosa expansión de las TICs[2], ha influenciado directamente en la exponencial difusión de información y datos a través de redes, medios de información y diferentes tecnologías de comunicación, en especial por la utilización del internet y el protocolo abierto IP[3], cuyo tráfico global para el 2022 se proyecta alcanzará los 4.8 ZB[4] a nivel global (Cisco Systems, 2019), este uso acelerado incrementa el riesgo y afectación de activos críticos de las organizaciones o Estados, como son sus datos e infraestructura tecnológica en general.

La afectación se enfoca en la integridad[5], confidencialidad[6] y disponibilidad[7] de los datos, información e infraestructura tecnológica, por medio de ataques de TICs, originados por intrusiones no autorizadas, los cuales se presentan en forma continua y se incrementa a la par del mismo desarrollo tecnológico, impactando a sectores que administran aplicaciones de TICs, como servicios financieros, entidades gubernamentales, proveedores de servicios de salud, entre otros de no menor importancia.

La información se compone de un conjunto organizado de datos, los cuales constituyen actualmente uno de los principales activos de las organizaciones en general y su seguridad se convierte en crítica (Dixon, President, & Outsourcing, 2014), las cuales se encuentran inmersas en el ciberespacio. El ciberespacio presenta una naturaleza transaccional entre los diferentes actores respecto a la transaccional de datos e información.

El ciberespacio representa a un entorno virtual, fuera de la naturaleza física, su aporte es indiscutible en el desarrollo de las sociedades y el mal uso actual es evidente, en la cual se involucra a la hoy denominada ciberdefensa que implica a la seguridad y defensa de activos críticos de una Estado en el ciberespacio, en el cual se derivan ciberdelitos que representan el cometimiento de ilícitos, mediante actividades o actos contra individuos, instituciones públicas o gubernamentales en general, desarrollados o cometidos en el ciberespacio, conjuntamente estos aspectos y otros, pueden desencadenar conflictos en este entorno.

Entre los objetivos principales de los ataques a nivel mundial se identifican perfiles de blancos de organizaciones y agencias militares, destacándose los de inteligencia (Emm & Chebyshev, 2018), por lo cual se define como una principal amenaza global a los ciberataques, ciberdelincuencia o ciberterrorismo. A nivel internacional los Estados y organizaciones, han desarrollado estructuras de Ciberdefensa para la seguridad y defensa de la información e infraestructura de TICs, pero a pesar de estos esfuerzos, más del 50 % de los ataques que se desarrollan causan daños y su recuperación puede tardar meses o incluso años (Cisco Systems, 2018).

El presente trabajo aporta fundamentalmente con la conceptualización de ciberdefensa, determinación de los desafíos y blancos criticos en el ciberespacio del Ecuador actuales y futuros, la investigación se encuentra estructurada con el desarrollo de un estado del arte mediante el ciberespacio y desarrollo, su uso inadecuado, la aproximación de la conceptualización de ciberdefensa, una descripción de la traslación de los conflictos al ciberespacio, riesgos de la ciberdefensa, se desarrolla un análisis exploratorio de datos y estadísticos de ciberataques de la región y Ecuador, se utiliza una metodología de análisis cuantitativa mediante la aplicación de análisis predictivo con el uso de herramientas informáticas de aprendizaje automático o machine learning, en cuyos resultados determinaran los desafios, blancos u objetivos críticos actuales y futuros del ciberespacio del Ecuador.

2. Estado del Arte

Ciberespacio y desarrollo

Es imprescindible para una adecuada comprensión del entorno de la presente investigación, determinar definiciones básicas en el entorno de la Ciberdefensa, las cuales se describen a continuación.

A nivel global se inicia con la utilización de la terminología cibernética o cybernetic, de origen griego κυβερνητική[8], cuyo significado comprende la acción de conducir una nave, este término es asimilado por el matemático Norbert Wiener, que la define como la tecnología de los sistemas de control, de este se desprende como prefijo el termino ciber o cyber, el cual indica relación con las redes informáticas (Real Academia Española, 2019).

La conceptualización de ciberespacio es difundida por primera ocasión a través del libro Neuromance de William Gibbson, quién la describe como el entorno virtual de sus escritos y la Real Academia Española define al ciberespacio como el "Ámbito virtual creado por medios informáticos" (Real Academia Española, 2019).

2 TICs, Tecnologías de la Información y de las Comunicaciones.

3 IP, Internet Protocol, Protocolo de Internet.

4 Zettabyte = 1000 Exabytes.

5 Integridad, datos o información libre de modificaciones no autorizadas.

6 Confidencialidad, acceso a datos o información a personal únicamente autorizados.

7 Disponibilidad, condición de datos o información de estar a disposición de usuarios o aplicaciones autorizados.

8 κυβερνητική, cibernético, ca.

El ciberespacio se fundamenta en la infraestructura tecnológica de hardware y software de la red de redes a nivel global, la cual por su naturaleza establece un sin número de transacciones de datos e información correspondiente a todos los sectores de la sociedad (educación, financiero, energético, etc.), generando una interacción exponencial entre personas, lo cual ha permitido una creciente satisfacción de las necesidades de los ciudadanos permitiendo romper fronteras, distancias e idiomas, proporcionando un sin número de beneficios a la sociedad.

Como elementos fundamentales del ciberespacio se puede describir a los siguientes:

- Datos e información.
- Tecnologías de Equipos Informáticos, hardware, software, redes, virtualización y almacenamientos.
- Tecnologías de Información, gestión y análisis.

El sector privado y público, cada vez más se encuentran inmersos en esta nueva dimensión, lo cual ha favorecido al crecimiento económico y comercial, suponiendo oportunidades de negocio, difusión cultural, entre otros, pero al mismo tiempo se identifica la evolución significativa de nuevas amenazas y riesgos informáticos.

El uso del ciberespacio e internet se ha convertido en elemento clave para el crecimiento económico, constituyéndose como un recurso crítico del que dependen sectores económicos y de la producción en general, esta dependencia directa del ciberespacio, internet y TICs, genera una debilidad ante fallos en la red del ciberespacio, misma que puede desencadenar vulnerabilidades en el área de la seguridad y defensa del ciberespacio, siendo necesario desarrollar acciones activas y pasivas como parte de estrategias de ciberdefensa y ciberseguridad.

Ciberespacio y su uso inadecuado

La seguridad y defensa del ciberespacio se convierte en un tema de relevancia, a medida que se incrementa la dependencia en el uso de medios cibernéticos, la rapidez de la evolución tecnológica y la expansión constante del ciberespacio, no han permitido desarrollar medios, procesos y/o mecanismos adecuados para prevenir amenazas de TICs y ataques cibernéticos.

Como ataque, se describe a " una agresión a la seguridad de un sistema fruto de un acto intencionado y deliberado que viola la política de seguridad de un sistema" (Arribas, 2011). En referencia a ciberataque, se la define como una "acciones hostiles desarrolladas en el ciberespacio con el objetivo de irrumpir, explotar, denegar, degradar o destruir la infraestructura tecnológica, componente lógico o interacciones de éste y pueden tener distintos niveles según su duración, frecuencia y daño generado" (Ministerio de Defensa Nacional Chileno, 2015).

Es importante comprender en el contexto del ciberespacio la conceptualización de vulnerabilidad de seguridad, como "un fallo o debilidad en el diseño, la implementación, la operación o la gestión de un sistema, que puede ser explotado con el propósito de violar la política de seguridad del sistema" (Arribas, 2011), a la Política de seguridad, se puede entender como "el conjunto de reglas y prácticas que definen y regulan los servicios de seguridad de una organización o sistema con el propósito de proteger sus recursos críticos y sensibles" (Arribas, 2011).

Como amenaza, en seguridad de TICs se puede describir como "una violación de la seguridad en potencia, que existe a partir de unas circunstancias, capacidad, acción o evento que pueda llegar a causar una infracción de la seguridad y/o causar algún daño en el sistema" (Arribas, 2011). Se debe considerar también que la garantía de las propiedades de la información o datos en el ciberespacio deben cumplir ciertas propiedades que incluyen a la disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; y confidencialidad (UIT, 2010).

Tanto el sector público como privado, a medida que estos adoptan cada vez más el ciberespacio y nuevas TICs, estos sectores son cada vez más difíciles de defender, por la tendencia del uso del ciberespacio y uso de servicios en la nube, incremento de la colaboración en tiempo real, la I+D+i[9], impactos en las organizaciones y la globalización, estos componentes, impulsan más aún la inseguridad actual que puede presentar el ciberespacio y al mismo tiempo el empleo del ciberespacio será adoptado por las organizaciones criminales, determinándose los nuevos delitos más sofisticados en el ciberespacio, los cuales se denomina como ciberdelitos.

El ciberespacio actualmente presenta como un dominio complejo, dinámico e incierto, lo cual configura las condiciones para ataques cibernéticos, incidentes, actividades maliciosas y un mal uso de esta dimensión contra la infraestructura de TICs, los derechos de la sociedad y Estado en general necesitan ser protegidos en esta dimensión.

Ciberdefensa

La seguridad en el ciberespacio, esta definiendo nuevos matices que son relevantes en un Estado u organización, siendo los usuario cada vez más dependientes de los sistemas de información, esta relevancia se encuentra ligada al desarrollo tecnológico como la actual cuarta revolución industrial y específicamente la indus-

9 I+D+i, Investigación, Desarrollo, Innovación

tria 4.0[10], esta seguridad en el entorno del ciberespacio define a la ciberdefensa, para lo cual es necesario determinar a la Ciberseguridad, que según el organismo internacional ITU[11].

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno (UIT, 2010, p. 20).

También se puede citar al Ministerio de Defensa de España a través de la Escuela de Altos Estudios de la Defensa, en la publicación de Documentos de Seguridad y Defensa, describe la definición de Ciberdefensa.

Ciberdefensa, como aplicación de medidas de seguridad para la protección y reacción frente a ataques cibernéticos contra las infraestructuras de las tic, requiere una capacidad de preparación, prevención, detección, respuesta, recuperación y extracción de lecciones aprendidas de los ataques que podrían afectar a la confidencialidad, integridad y disponibilidad de la información, así como a los recursos y servicios de los sistemas de las tic que la procesan (Escuela de Altos Estudios de la Defensa de España, 2014, p.41)

El Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile, en su publicación define a la Ciberdefensa como la "capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional … conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio" (CEEAG, 2018).

Desde el enfoque militar la Ciberdefensa "se centra en las medidas técnicas, políticas y organizativas que protegen los sistemas y redes militares de ciberataques, e incluye las capacidades de reacción y ataque propias de un conflicto armado" (Batanero, 2013).

Es adecuado distinguir o diferenciar entre las conceptualizaciones de Ciberseguridad y Ciberdefensa, mientras que la Ciberseguridad en general se enfoca en la protección, la Ciberdefensa engloba a la Ciberseguridad, Ciberinteligencia y las diferentes acciones ofensivas contra los ataques o ciberataques.

La conceptualización de Ciberdefensa a nivel global y regional, se describe a continuación citando a algunos investigadores.

Claus (2015), en su trabajo respecto a la Guardia Nacional de los Estados Unidos de Norteamérica y USCYBERCOM [12], concluye que la Ciberdefensa requiere un trabajo fuerte entre los sectores públicos y privados, proponiendo y validando al final un modelo público-privado para la Ciberdefensa eficaz de infraestructuras críticas.

Wells (2017), en su obra determina que las operaciones en el ciberespacio deben integrarse con otras y apoyados con la inteligencia, así como que ninguna organización civil o militar por si sola está preparada para hacer frente a fuerzas en el ciberespacio.

Nielsen (2016), en su investigación establece que el ejército de los Estados Unidos de Norteamérica tiene un papel importante en el dominio cibernético, requiriendo que los militares innoven y realicen una colaboración con actores internacionales, de gobierno y privados.

A nivel regional se pueden citar a trabajos como de Cabral (2015), quien en su investigación define que Argentina y Brasil en seguimiento de la tendencia mundial, respecto a la protección del ciberespacio es responsabilidad de la Defensa Nacional y coordinada por Fuerzas Armadas.

Moreno (2015), en su trabajo identifica a la Ciberdefensa militar de Colombia, las implicaciones del uso del ciberespacio y los convenios o coordinaciones necesarias con entidades públicas y privadas.

En función de situarnos en el contexto de la Ciberdefensa en Ecuador, la literatura es escasa pero se ha identificado las siguientes investigaciones en el entorno nacional.

Castro (2015), en su trabajo de investigación determina los factores fundamentales relacionados para el estudio prospectivo de la Ciberdefensa en las Fuerzas Armadas del Ecuador para el año 2017, presenta escenarios y las estrategias para la Ciberdefensa para el Ecuador.

Vargas (2017), en su estudio trata sobre la Ciberdefensa y Ciberseguridad en el Ecuador, realiza un examen analítico conceptual de seguridad y defensa,

10 Industria 4.0, es la industria de dispositivos inteligentes que se encuentran interconectados entre si.

11 ITU, International Telecommunication Union

12 USCYBERCOM, United States Cyber Command

proponiendo un modelo de gobernanza en Ciberdefensa del Ecuador, sus hallazgos demuestran una incipiente reflexión respecto a esfuerzos Interagenciales para su institucionalización.

En función de lo descrito, a nivel nacional no se define su conceptualización, proponiendo que la Ciberdefensa debe comprender la colaboración estrecha entre entidades públicas y privadas, en coordinación y liderazgo de Fuerzas Armadas, conceptualizándola como la seguridad y defensa de los activos críticos del Estado en el entorno del ciberespacio, que constituye un nuevo dominio con implicaciones geopolíticos entre Estados y antagonistas.

Traslación de los conflictos al ciberespacio

El traslado de los conflictos al ciberespacio se fundamenta en la rentabilidad económica que esta representa, en el cual un arma de bajo costo puede ser un teléfono inteligente, un ordenador, entre otros, comparado con las armas convencionales, determinando que se pueda interferir en actividades o dinámicas de gobierno, económicas, financieras, médicas, infraestructura, etc.

Como una segunda causa se puede describir a la gran capacidad y flexibilidad del ciberespacio, pero al mismo tiempo puede penetrar mas incidentes, ataques, interferencias en TICs, en un tiempo relativamente corto, esta nueva dimensión constituye un espacio convencional.

El alcance de este dominio presenta en el contexto global como ilimitado, este se caracteriza por el anonimato, ineficiencia de procesos de detección e identificación, facilidad del acceso a la red de redes por parte de cualquier individuo, trayendo como consecuencia la dificultad de la capacidad de realizar ataques o contraofensivas en el ciberespacio por parte de los actores afectados.

Una de las razones más importantes se presenta, la falta de una normativa a nivel nacional, regional o global, esta falta de normativa en el ámbito jurisdiccional que tenga competencias en materia del derecho de los delitos informativos o de TICs, siendo estos origen de conflictos actuales o futuros, por ejemplo se puede desarrollar delitos desde un Estado diferente a que se encuentra la victima/objetivo/blanco, siendo difícil determinar la legislación del delito, diferentes regulaciones, complicando la definición de los actos punibles según la legislación de los Estados.

Riesgos de la Ciberdefensa

En referencia a la Política de la Defensa Nacional del Ecuador "Libro Blanco", esta determina como un fenómeno social a los ciberataques e identifica que el desarrollo de las TICs debe identificar al desarrollo de políticas y estrategias para la ciberseguridad y ciberdefensa, determinando a los ciberataques como amenazas globales (Ministerio de Defensa Nacional del Ecuador, 2018).

Principalmente se define como principales riesgos del Estado ecuatoriano en el campo tecnológico a los ciberataques que actuarán en el ciberespacio en el cual operarán organizaciones criminales, originando las denominaciones de ciberterrorismo, ciberdelito, cibercrimen, ciberespionaje, infiltración de los sistemas de TICs, entre otros, los cuales se constituyen en instrumentos de agresión contra la infraestructura de un Estado, que tendrá consecuencias o efectos en la seguridad nacional de un país.

Los ciberataques utilizan las vulnerabilidades o brechas de seguridad tecnológica en sistema o equipos de TICs, con el propósito de copiar, borrar, secuestrar o reescribir datos o información, accionar equipos o maquinaria conectada de objetivos o blancos siendo del sector privado o público, incluso hasta el individuo. En función de lo cual se puede dar un listado de los principales ciberataques como Código dañino o Malware (para dañar el funcionamiento correcto de cualquier equipo o maquinaria), Gusanos (estos pueden reproducirse a sí mismos, replicándose), Virus (se copian a sí mismo con el propósito de infectar otros programas o archivo), Troyanos (su objetivo es el robo o destrucción de datos), Botnet (el cual tiene como objetivo ataques de denegación de servicio, fraudes, robos de información, la inutilización), Bomba Lógica (su objetivo es actuar en un momento determinado para dañar o destruir a un equipo, sistema o maquinaria conectada), entre los más importantes.

Como origen de los ciberataques, se tiene a los países, empresas, organizaciones terroristas, organizaciones delincuenciales, individuos, etc. Es el origen de la guerra cibernética en la cual se irrumpe en las leyes o códigos geopolíticos, se puede citar como ejemplo al incidente sucedido en Estonia en el 2007, siendo esta una exrepública de la URSS[13], el gobierno central retiro una estatua de bronce que conmemora la liberación del ejército rojo de Tallin en la Segunda Guerra Mundial, esta actividad genero una serie de disturbios en la población y específicamente en el sector de origen ruso, al día siguiente del retiro de la estatua, se inició múltiples ataques informáticos o ciberataques hacia los diferentes sistema o equipos de TICs, que afectaron al normal desenvolvimiento del gobierno central, sistemas de comunicaciones, medios de comunicación, sistemas bancarios y financieros, entre otros, con el empleo principalmente con ciberataques de DOS[14] y ciberataques

13 URSS, Unión de Repúblicas Socialistas Soviéticas.

14 DOS, denegación de servicio

coordinados de DDOS[15] con el empleo de botnets alojadas en varios países de la región (Flint, 2016).

La referencia del ciberespacio, en el cual se genera ciberataques y origina la conceptualización de la ciberdefensa y ciberseguridad, ya implica a la narrativa de la geopolítica e impactos en la seguridad nacional de un país, en la cual se debe analizar a un país dentro del contexto o entorno del ciberespacio, por ejemplo:

Estonia, como país pequeño, moderno y experto en tecnología, era un campo de pruebas ideal para los ciberatacantes con motivaciones políticas. . . . Estonia pasó a experimentar los primeros ataques a gran escala, pero. . . Las vulnerabilidades están creciendo tanto en el mundo desarrollado como en el mundo en desarrollo. (Tiirmaa-Klaar, 2011, págs. 1-2; citado en Kaiser, 2015, pág. 13)

En general se han desarrollado incidentes en el ciberespacio que configuran a una nueva red geopolítica de la guerra cibernética o ciberguerra, en el contexto de las relaciones internacionales y así como en la ciencia de seguridad y defensa, incrementando las preocupaciones de los países respecto al territorio, poder, fronteras, economía, etc. Siendo de importancia que los Estados en función de las vulnerabilidades se convierte para los ciberataques o ciberguerra, como la parte central para el inicio o configuración de estos (Kaiser, 2015).

Actualmente estas vulnerabilidades representan apagones de redes eléctricas, daños en sistemas industriales importantes, como el caso del Stuxnet constituido como un ciberataque al sistema nuclear de Irán, en el cual se detuvo un sistema informático y específicamente al equipo PLC[16] que detuvo el sistema nuclear.

Se han desarrollado deferentes incidentes en el ciberespacio que afectan e inciden en sectores de importancia en la economía de los países, el ciberespacio presenta un potencial escenario de conflictos altamente complejos por estar en una constante evolución.

La combinación de acciones bélicas con ciberataques, podrá determinar una coordinación para la paralización de infraestructuras críticas de un país, los ejemplos citados determinan que los ciberataques son mecanismos o armas que pueden afectar a un país y que estos requieren pocos recursos relativamente comparado con el daño que puede causar.

En el WEF[17], en su edición 14, describe los principales riesgos a nivel mundial categorizando desde los sectores económicos, ambiental, geopolítica, sociedad y tecnológico, identificando a los ciberataques y daños a la infraestructura crítica de información entre los 10 riesgos que más impacto han tenido en el 2019, así como los riesgos mas probables a los fraudes o robo de datos y ciberataques, en el 2019. El desarrollo de este análisis ubica a los riesgos tecnológicos entre los principales a nivel mundial.

Por lo cual, se evidencia que el riesgo de ciberataque constituye y confluyen como el principal y de mayor impacto, como de probabilidad a nivel global en el sector tecnológico, sin dejar de mencionar a los riesgos de fraude o robo de datos y los daños a infraestructura crítica de TICs, como los que actualmente irrumpen en el ciberespacio y que afectan no solo a las diferentes instituciones públicas o privadas, sino a ser humano.

Es innegable que la tecnología continua teniendo un rol importante a nivel global en los riesgos latentes de una sociedad, pero en función de que los seres humanos en general se encuentran interconectados actualmente, esta afectación tiene su incidencia mayor en cada individuo de la misma, los ciberataques sin dudarlo afectan directamente a las instituciones gubernamentales, financiera y de la banca, principalmente como instituciones o entidades, pero en los últimos años se ha incrementado casi exponencialmente la afectación se dirige también a nivel individual, con incremento en los casos de afectación a personas en las cuales sobresalen principalmente el robo o fraude de datos, como por ejemplo los datos de cuentas bancarias, claves transaccionarías, claves y cuentas de ahorro y crédito, correo electrónico, el cifrado de la información con fines monetarios, entre otros.

Es importante resaltar que actualmente nos encontramos en el desarrollo de la cuarta revolución industrial y de esta se deriva la Industria Conectada 4.0 que funcionalmente es la interconexión entre las cosas denomina también IoT[18], que comprende el sin número de equipos, sistemas de procesamiento industrial, maquinaria, entre otros, que se encuentran conectados a la red de redes. En referencia a lo descrito es de vital importancia se incluyan también a los equipos, maquinaria y sistemas médicos - farmacéuticos, que cuya afectación producirán problemas complejos para todas las sociedades y sus impactos pueden ser críticos.

15 DDOS, denegación de servicio distribuido

16 PLC, Controlador Lógico Programable

17 WEF, Word Econmic Forum

18 IoT, Internet of things, Internet de las Cosas

El impacto de los ataques en el ciberespacio, también se trasladará ya no solo a los seres humanos, instituciones públicas o privadas y sociedades o países, esta afectación o incidencia llegará a todas las cosas que se encuentren conectadas, lo cual eleva aun más el riesgo que puede afectar a una sociedad o comunidad, que en función de las vulnerabilidades que presente a nivel institucional, su gestión de solución a estos ataques se encuentra en desarrollo a pesar que esta relegada en función del avance de los ciberataques, pero lo crítico será el profundo impacto que causará los ataques cuando se generalicen hacia el componente mas importante de una sociedad, que es la familia, que a través de su hogar o casa tiene o tendrá un sin numero de cosas interconectadas, lo cual puede incluir a un nuevo o potencial blanco para las organizaciones criminales que usan el ciberespacio para el cometimiento de sus delitos.

3. Diseño

Análisis de Ciberataques a la Región y Ecuador

La percepción de seguridad de TICs en Latinoamérica ante los incidentes y amenazas, determina la mayor preocupación respecto al acceso indebido, robo de información y la privacidad de la información, como se ilustra en la figura 2. Respecto a medidas para la seguridad y defensa de ciberataques, en la región se encuentra atrasada y más del 50 % (ESET SECURITY REPORT Latinoamerica, 2019) de las organizaciones no cuentan con controles o políticas de seguridad implementadas, evidenciándose al sector de gobierno como el menos desarrollado y actualmente el más vulnerable en la región, con una menor tendencia para adoptar o desarrollar sistemas, arquitecturas, plataformas, herramientas o tecnologías de seguridad y defensa, al contrario el sector financiero se presenta como el más desarrollado en comparación con los demás, en la figura 3 se observa los controles de seguridad (cifrado, 2FA[19] y EDR[20]) implementados por sector en Latinoamérica.

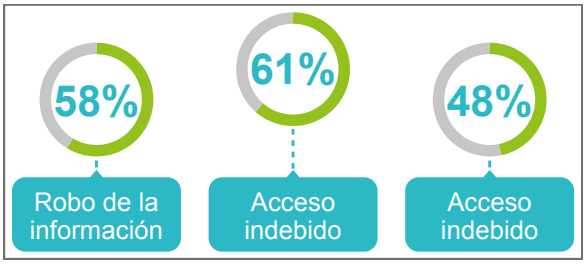

Figura 1. Preocupaciones de seguridad en Latinoamérica.
(Fuente: ESET SECURITY REPORT Latinoamerica, 2019)

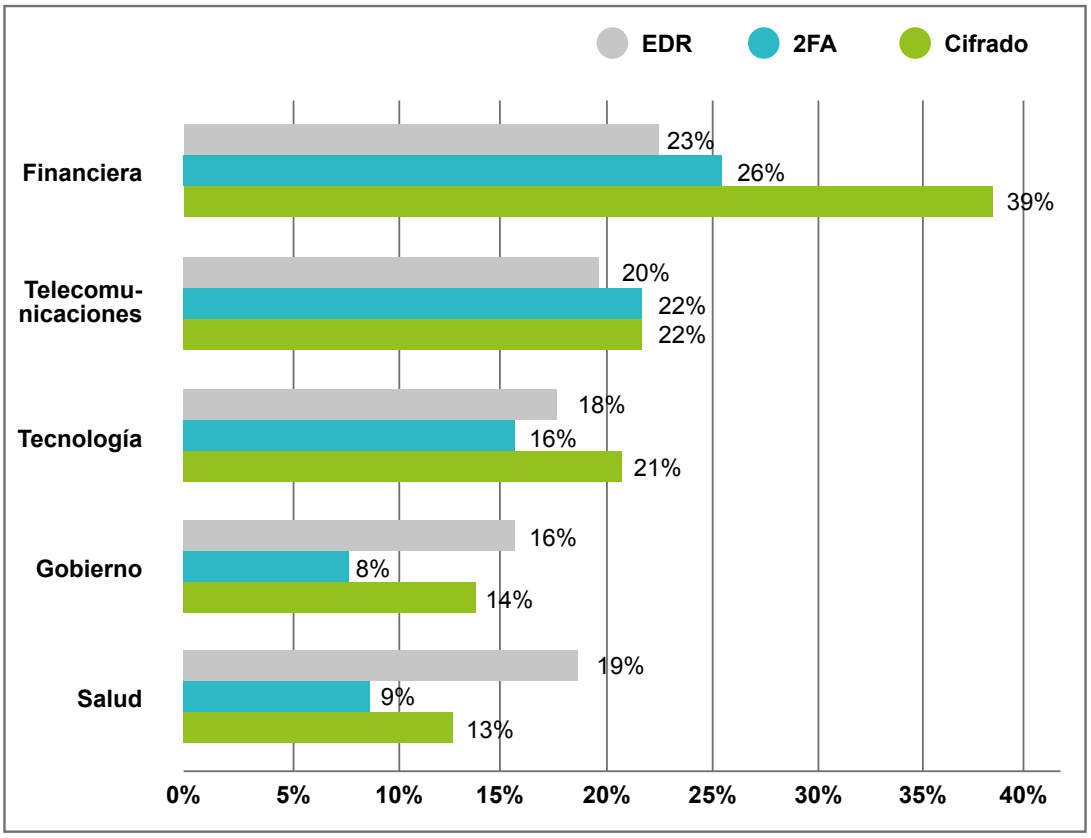

Figura 2. Implementación de controles de seguridad
(Fuente: ESET SECURITY REPORT Latinoamerica, 2019)

19 2FA, Two Factor Authentication, Autenticación de dos factores.

20 EDR, Endpoint Protection Platforms, protección de plataformas de puntos finales

A nivel nacional en el Ecuador hace pocos años se ha iniciado un desarrollo lento de la adopción de tecnologías de seguridad y defensa respecto a los datos, información e infraestructura de TICs del Estado, evidenciándose que se encuentra relegada respecto al desarrollo e implementación principalmente de políticas de seguridad, planes de continuidad y clasificación de la información, aspectos fundamentales de la Ciberdefensa, en la figura 4 se ilustra los niveles de implementación de prácticas de gestión para la seguridad por país en Latinoamérica.

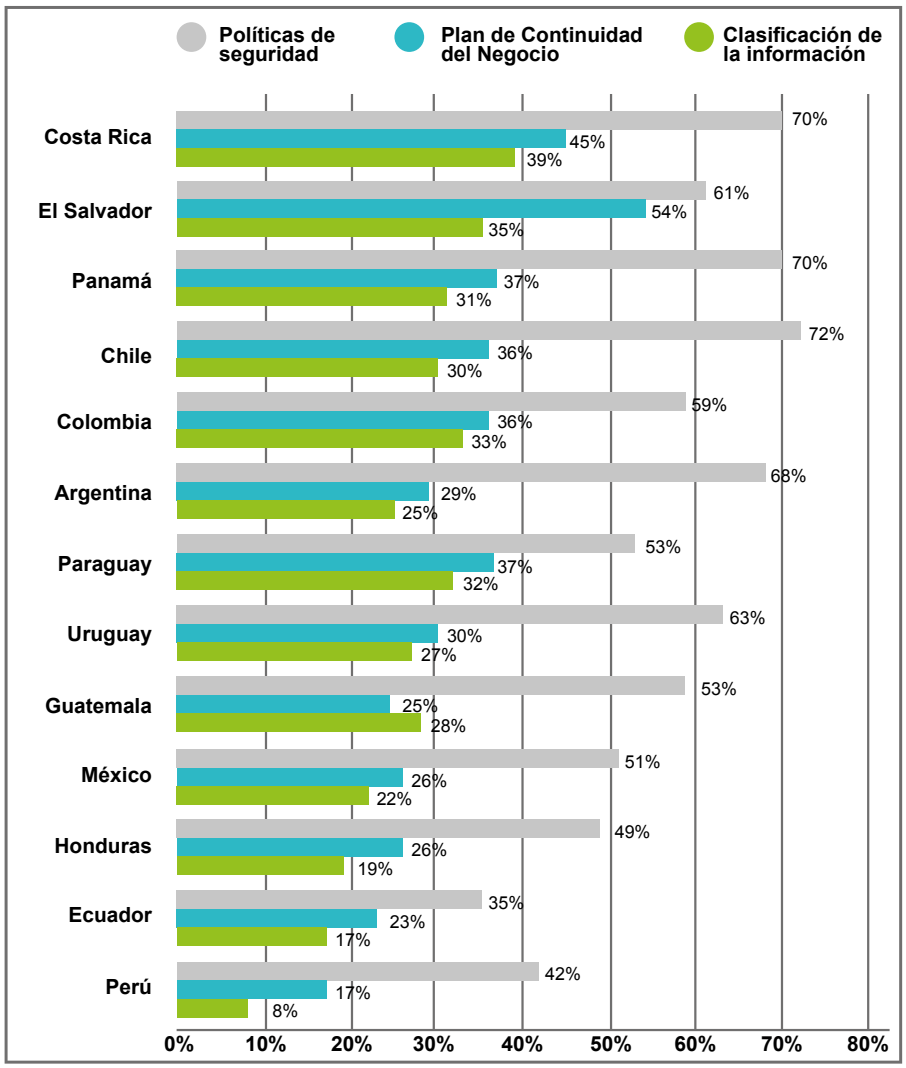

Figura 3. Prácticas de gestión para la seguridad por país
(Fuente: ESET SECURITY REPORT Latinoamerica, 2019)

Para una adecuada Ciberdefensa a más de los recursos tecnológicos es fundamental complementarlos con una apropiada gestión e integración de la misma, en el Ecuador los niveles de adopción de políticas de seguridad de TICs, planes de continuidad y clasificación de la información son inadecuados (ESET SECURITY REPORT Latinoamerica, 2019) actualmente.

La adopción de una Ciberdefensa completa para el Ecuador es de vital importancia, en función que los ataques o ciberataques a plataformas de TICs, se han incrementado en los últimos años, en la figura 5 se observa los países con la tasa más alta de computadoras infectadas con malware[21] en el año 2016 (Statista, 2019b) y aún más preocupante que el Ecuador se ha convertido en uno de los principales países de origen del tráfico de ciberataques a nivel internacional (Statista, 2019a), por ejemplo se ilustra en la figura 6, el tráfico de origen de ataques DDoS[22] a nivel mundial.

21 Malware, del inglés malicious software, software malicioso.

22 DDoS, Distributed Denial of Service, ataque de Denegación de Servicio Distribuido.

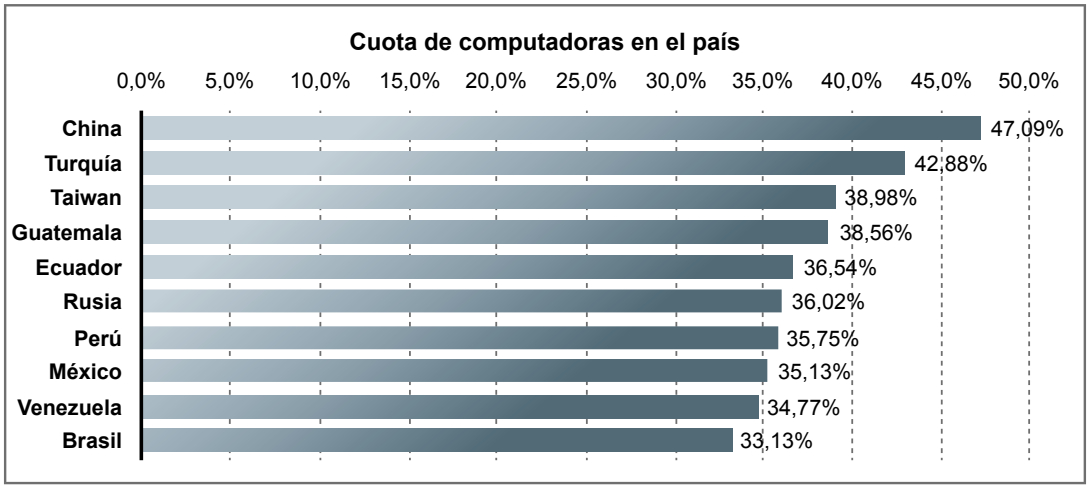

Figura 4. Países con la mayor tasa de infección de malware 2016
(Fuente: Phishing Activity Trends Report 4th Quarter 2016, page 13)

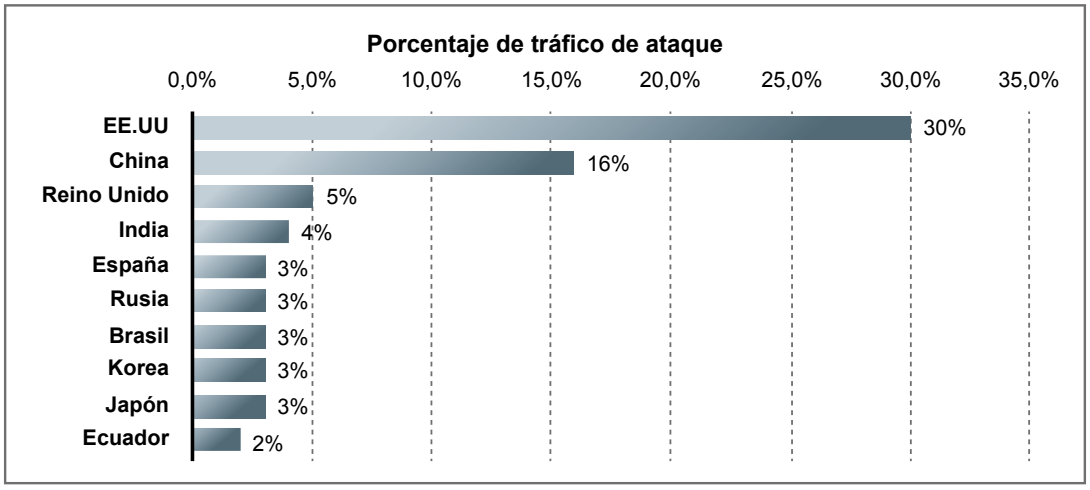

Figura 5. Principales países de origen del tráfico de ataques DDoS
(Fuente: Akamai - The State of the Internet - Security Report Summer 2018)

En Latinoamérica el desarrollo de la ciberdefensa, se encuentra retrasada y en Ecuador su adopción es incipiente colocándolo entre los últimos países de la región respecto a la adopción de la gestión de seguridad de TICs.

Se evidencia la crítica situación respecto a ciberataques en contra del Ecuador, lo cual compromete su seguridad y defensa, en la figura 7 se ilustra el número de ciberataques a aplicaciones web gubernamentales por países de Latinoamérica, en un período de siete días del 18 al 25 de junio de 2019, identificando al Ecuador con 5542 ataques desarrollados (Statista, 2019c).

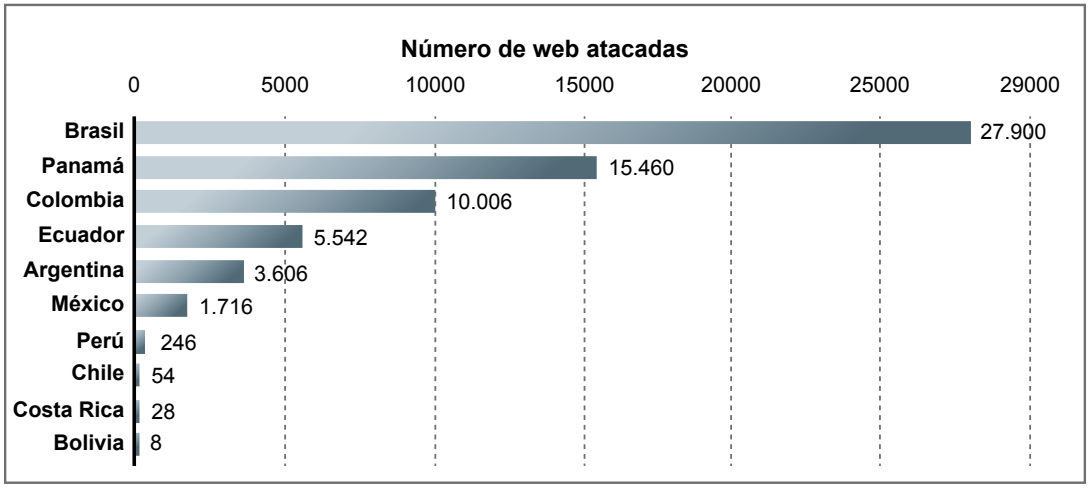

Figura 6. Ciberataques a web gubernamentales por países de Latinoamérica
(Fuente: Akamai Technologies, 2019)

En el mismo período como se ilustra en la figura 8, es relevante señalar que el Ecuador es el principal país que ha recibido ciberataques en la industria del juego, estos se dirigen principalmente a las cuentas del juego en el país, en la figura 9 se observa que el Ecuador ha recibido 237.000 ciberataques a aplicaciones web en el sector de alta tecnología (Statista, 2019c), lo cual corrobora el estado crítico de su Ciberdefensa.

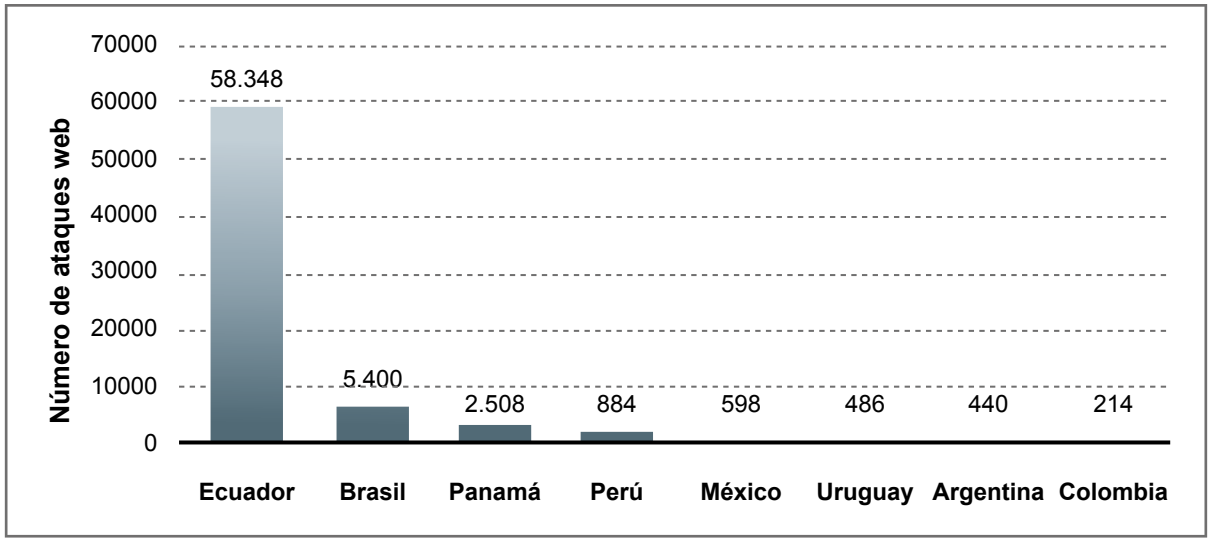

Figura 7. Ciberataques a cuentas de juego por países de Latinoamérica
(Fuente: Akamai Technologies, 2019)

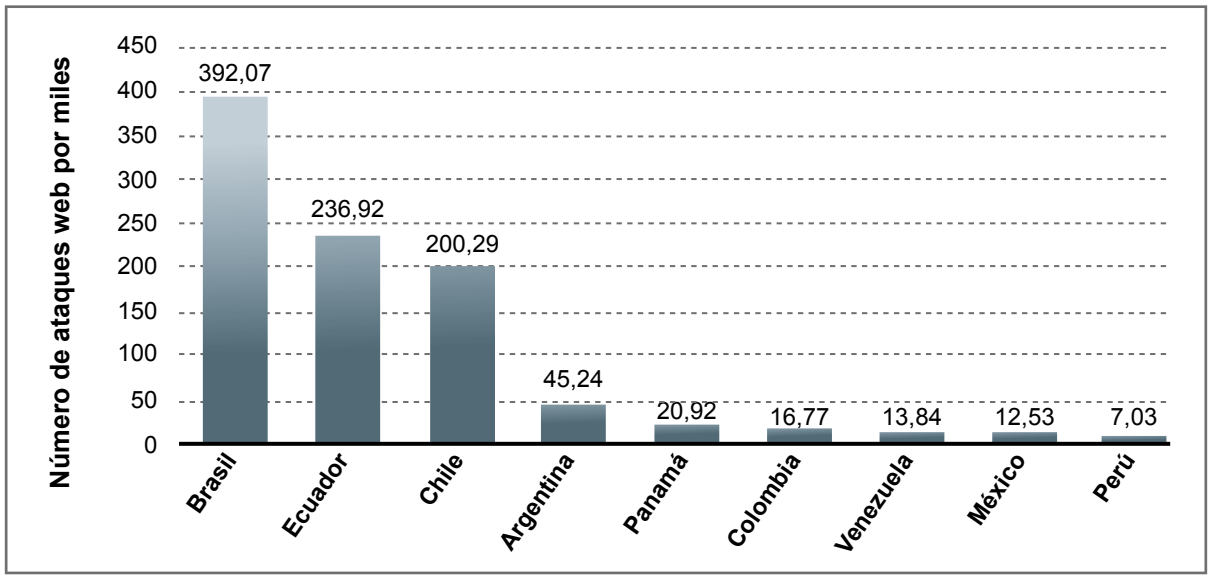

Figura 8. Ciberataques a web de alta tecnología por países de Latinoamérica
(Fuente: Akamai Technologies, 2019)

Como alta tecnología se define a sectores relacionados con la informática, telemática, robótica, biotecnología, industria de la defensa, domótica , entre otras.

Se incluyen en la figura 10, los países con más número de ataques a aplicaciones en el sector de servicios financiero en el mismo período, ubicando a Ecuador en el tercer lugar a nivel de Latinoamérica con 33350 ataques y en la figura 11, se ilustra a los países latinoamericanos con mayor número de ataques a aplicaciones web de entretenimiento, con 264910 ciberataques Ecuador se ubica en segundo lugar de la escala (Statista, 2019c).

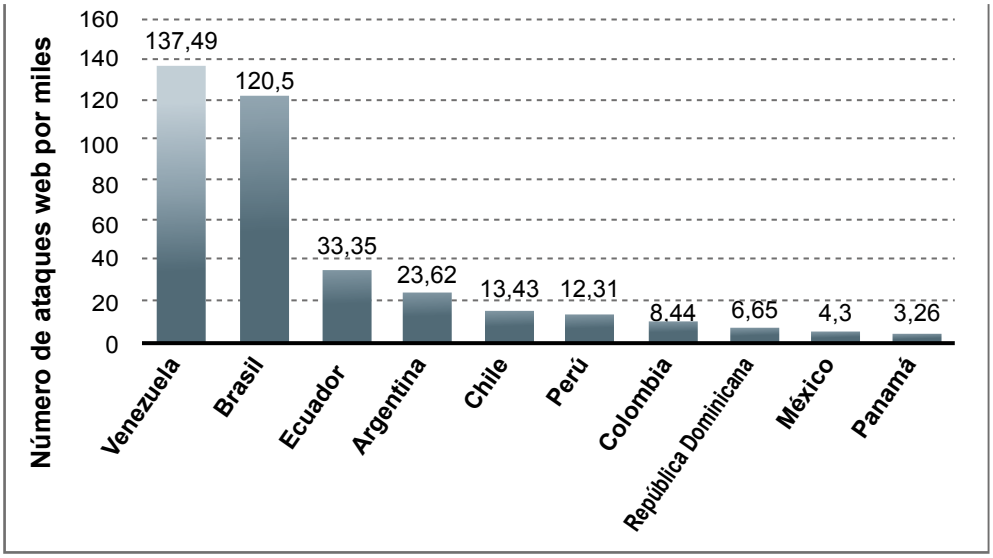

Figura 9. Países con más ataques web en servicios financieros
(Fuente: Akamai Technologies, 2019)

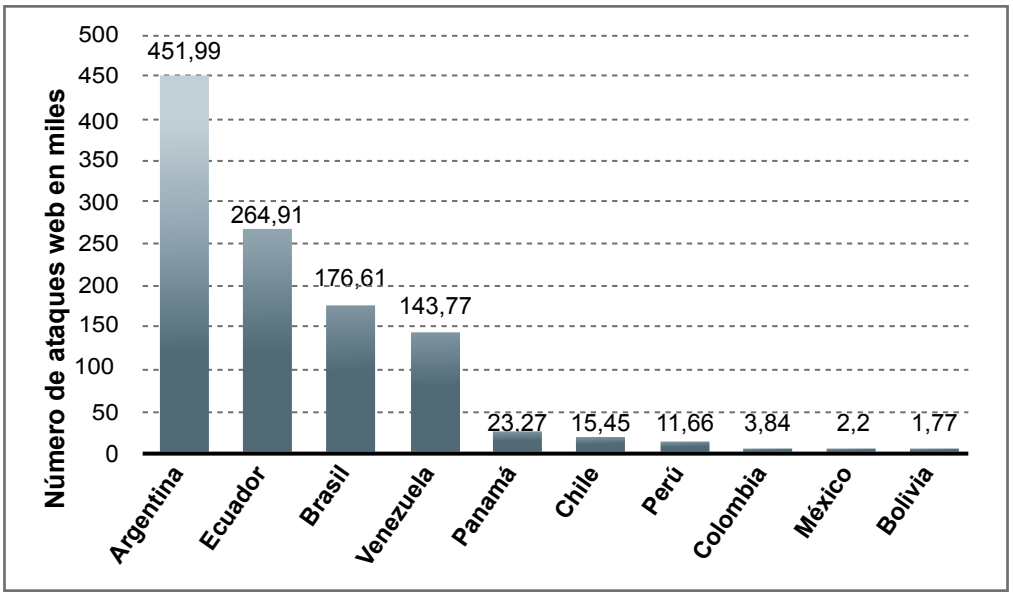

Figura 10. Países con más ataques web de entretenimiento multimedia
(Fuente: Akamai Technologies, 2019)

Sobre la base de la literatura expuesta y el análisis desarrollado, se identifican que actualmente el Ecuador está expuesto a un gran número de ciberataques y que comparado con otros países de la región, se ubica como uno de los principales objetivos de los atacantes a nivel global y entre los países más afectados a nivel Latinoamericano.

Metodología de Análisis

La metodología empleada para el presente trabajo de investigación es la cuantitativa, en función que esta permite el tratamiento numérico de los datos. Para los datos se desarrolla un análisis predictivo, que consiste en la extracción de información de los datos que se han descritos anteriormente empleando una estadística de modelización, aprendizaje automático y minería de datos, para el tratamiento de tendencias y patrones de comportamiento futuro.

El Análisis Predictivo, se fundamenta en las relaciones entre variables de eventos o incidentes que han sucedido, a partir de los datos descritos se define un modelo predictivo para que este sea aplicado a una característica individual, que dará un resultado predictivo.

El propósito del modelo es evaluar la probabilidad de algo especifico, se desarrolla la técnica de árbol de clasificación, que se define como una técnica de aprendizaje de árboles de decisión no paramétrica que da como resultado árboles de clasificación.

Como herramientas de análisis predictivo se utiliza la herramienta Orange Data Mining[23], que es un software de código abierto de aprendizaje automático o machine learning, que permite desarrollar análisis predictivos utilizando diferentes técnicas y que permite una programación visual simple y sencilla.

En la figura 12, se ilustra la configuración de la herramienta Orange Data Mining de los datos recopilados para la proyección del comportamiento de las variable identificadas, en la cual predominan las variables de Ciberataques a cuentas de juego en línea y web de alta tecnología en referencia a la variable objetivo de Ciberataques a web gubernamentales; al cambiar la variable objetivo a cuentas de juego en línea las que predominan son en este orden Ciberataques a web de alta tecnología y a web gubernamentales.

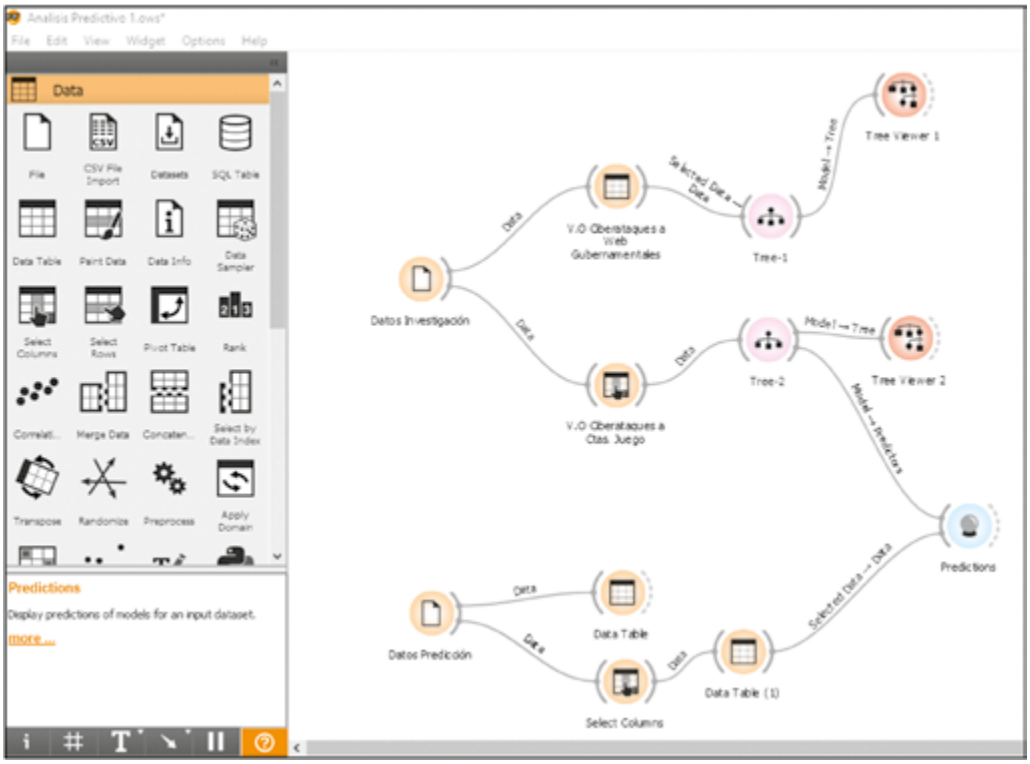

Figura 11. Analítica Predictiva con Orange
(Fuente: Elaboración Propia)

Como resultado de la analítica actual se determina a las variables de *Políticas de Seguridad, Ciberataques a web de entretenimiento multimedia y a web de alta tecnología,* son los sectores que más son impactados, en los resultados del análisis predictivo se configura que los sectores o blancos críticos en el ciberespacio del Ecuador serán de mayor impacto para el Ecuador son los Ciberataques a web gubernamentales, web de alta tecnología y web de cuentas de juegos.

Desafíos en el Ciberespacio del Ecuador

En referencia a la revisión bibliográficas, de datos y al análisis de los ciberataques, se determina que las siguientes líneas generales de desafíos en el ciberespacio para el Ecuador:

- Formulación y posterior aplicación de Políticas Públicas de Seguridad de TICs:
  - Desarrollo de trabajo colaborativo entre entidades públicos y privados, a nivel nacional y local.
  - Generación de cultura de seguridad de TICs en la sociedad ecuatoriana.
- Desarrollo de capacidades de Ciberdefensa:
  - Estado.
  - Gobiernos locales.
  - Instituciones u organismos privados.

4. Conclusiones

El ciberespacio, se presenta como un escenario de conflictos complejos, en función del avance tecnológico mundial. Ninguna organización o país, se encuentra 100% seguro o protegido de ciberataques en el entorno del ciberespacio, por lo cual es necesario la colaboración entre organismos sean públicos-privados, así como entre paises a nivel regional o internacional.

23 Orange Data Mining, software desarrollado por la Universidad de Liubliana de Eslovenia

La conceptualización de Ciberdefensa, personalmente concluyo que esta se refiere a la *Seguridad y Defensa* de los activos críticos del Estado en el entorno del ciberespacio, que constituye un nuevo dominio con implicaciones geopolíticos entre Estados y antagonistas.

En función del análisis descrito, se identifica al conjunto de computadores personales, aplicativos web gubernamentales, cuentas de juegos en línea, web de alta tecnología, aplicaciones web de servicios financieros y web de entrenamiento multimedia, como los principales objetivos o blancos de los ciberataques que se dirige al Ecuador.

Los principales desafíos que se enfrenta el Ecuador se definen en una *Formulación y posterior aplicación de Políticas Públicas de Seguridad de TICs,* complementada con un adecuado *Desarrollo de capacidades de Ciberdefensa*, a futuro se proyecta como impactos potenciales Ciberataques *a cuentas de juego en línea, a web de alta tecnología y a web gubernamentales.*

REFERENCIAS

[1] Arribas, G. N. (2011). Introducción a las vulnerabilidades (S. FUOC Eureca Media, Ed.). Barcelona: FUOC.

[2] Cabral, V. J. Q. (2015). La estrategia de Argentina y Brasil para la Defensa Cibernética , una análisis por los niveles de la conducción. Retrieved from http://190.12.101.91:80/jspui/handle/1847939/462

[3] Castro Peralvo, E. J. (2015). Estudio prospectivo de la Ciberdefensa en las Fuerzas Armadas del Ecuador (UFA ESPE). Retrieved from http://repositorio.espe.edu.ec/bitstream/21000/7426/2/T-ESPE-047514.pdf

[4] CEEAG. (2018). LA CIBERGUERRA: SUS IMPACTOS Y DESAFÍOS (Andros Impresores, Ed.). Retrieved from http://www.ceeag.cl/wp-content/uploads/2018/07/LA-CIBERGUERRA-SUS-IMPACTOS-Y-DESAFIOS.pdf

[5] Cisco Systems. (2018). Reporte Anual de Ciberseguridad de Cisco 2018. In Reporte Anual de Ciberseguridad de Cisco 2018 (Vol. 1). Retrieved from https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

[6] Cisco Systems. (2019). Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. In Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. Retrieved from http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html

[7] Claus, B., Gandhi, R. A., Rawnsley, J., & Crowe, J. (2015). Using the oldest military force for the newest national defense. Journal of Strategic Security, 8(4), 1–22. https://doi.org/10.5038/1944-0472.8.4.1441

[8] Dixon, B. Y. D. O. N., President, S. V., & Outsourcing, G. D. (2014). Protecting an Organization's Most Important Asset: (June). Retrieved from https://search-proquest-com.biblioteca-uoc.idm.oclc.orgdocview/1535257890?accountid=15299

[9] Emm, D., & Chebyshev, V. (2018). Kaspersky: Boletín de seguridad PRINCIPALES HISTORIAS DE SEGURIDAD EN 2018. Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/63/2018/12/14040903/KSB2018_Review-of-the-year_final_SP.pdf

[10] Escuela de Altos Estudios de la Defensa de España. (2014). Documentos de Seguridad y Defensa 60. Estrategia de La Información y Seguridad En El Ciberespacio, p. 125. Retrieved from http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/docSegyDef/ficheros/060_ESTRATEGIA_DE_LA_INFORMACION_Y_SEGURIDAD_EN_EL_CIBERESPACIO.pdf

[11] ESET SECURITY REPORT Latinoamerica 2019. (2019). Retrieved from https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf

[12] Flint, C. (2016). Introduction to geopolitics. Retrieved from https://ebookcentral.proquest.com

[13] Kaiser, R. (2015) "The Birth of Cyberwar," Political Geography 46: 11–20.

[14] Ministerio de Defensa Nacional Chileno. (2015). BASES PARA UNA POLÍTICA NACIONAL DE CIBERSEGURIDAD. BASES PARA UNA POLÍTICA NACIONAL DE CIBERSEGURIDAD, pp. 1–15. Retrieved from https://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Política-Nacional-sobre-Ciberseguridad.pdf

[15] Ministerio de Defensa Nacional del Ecuador. (2018). POLÍTICA DE LA DEFENSA NACIONAL DEL ECUADOR "LIBRO BLANCO" (Instituto Geográfico Militar, Ed.). Retrieved from https://www.defensa.gob.ec/wp-content/uploads/2019/01/Política-de-Defensa-Nacional-Libro-Blanco-2018-web.pdf

[16] Moreno, W. C. (2015). Ciberdefensa Y Ciberseguridad En El Sector Defensa De Colombia Palabras Clave. Retrieved from http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2849/00002590.pdf?sequence=1

[17] Nielsen, S. (2016). The Role of the U . S . Military in Cyberspace. Journal of Information Warfare, 15(2), 27–38. Retrieved from https://search-proquest-com.biblioteca-uoc.idm.oclc.org/docview/1968022194?accountid=15299

[18] Real Academia Española. (2019). Diccionario de la lengua española | Edición | RAE - ASALE. Retrieved January 2, 2020, from Real Academia Española website: https://dle.rae.es

[19] Statista. (2019b). Security Software. Retrieved from https://www-statista-com.biblioteca-uoc.idm.oclc.org/study/22270/security-software-statista-dossier/

[20] Statista. (2019c). Cyber Crime. Retrieved from https://www-statista-com.biblioteca-uoc.idm.oclc.org/markets/424/topic/1065/cyber-crime/

[21] UIT. (2010). Ciberseguridad Definiciones y terminología relativas a la creación de confianza y seguridad. 20–22. Retrieved from https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

[22] Vargas Borbúa, R., Reyes Chicango, R. P., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en Ciberdefensa/ Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance. URVIO - Revista Latinoamericana de Estudios de Seguridad, (20), 31. https://doi.org/10.17141/urvio.20.2017.2571

[23] Batanero, J. C. (2013). CIBERDEFENSA. Ciberdefensa, pp. 1–40. Retrieved from http://www.criptored.upm.es/descarga/ConfrenciaJuanCarlosBatanero TASSI2013.pdf

[24] Statista. (2019a). IT Security. In IT Security. Retrieved from https://www-statista-com.biblioteca-uoc.idm.oclc.org/study/15503/information-security-statista-dossier/

[25] Wells, L. (2017). Cognitive-Emotional Conflict. Prism, 7(2), 4–17. Retrieved from http://www.jstor.org/stable/26470514

[26] WEF (2019). The Global Risks Report 2019, 14th Edition.