UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN DERECHO: MENCIÓN: DERECHO DIGITAL Y SOCIEDAD DE LA INFORMACIÓN

RPC-SO-26-No.425-2018

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:

Aplicabilidad del manual de Tallin en la Legislación Ecuatoriana como respuesta a transgresiones de ciberseguridad

Línea de Investigación:

Sociedad contemporánea y análisis del comportamiento en el marco de la modernidad y la interdisciplinaridad. Sublínea Derecho Digital

Campo amplio de conocimiento:

UNESCO (CINE) 38. DERECHO

Autor:

Rueda Martínez Hugo Fernando

Tutor:

PhD. Miguel García Jiménez

Quito – Ecuador
2020

Resumen

El presente trabajo de investigación, analiza las transgresiones a la ciberseguridad en Ecuador, el crecimiento del ciberespacio y su evolución en el contexto actual, que, a causa de la pandemia la sociedad está obligada a emplear herramientas tecnológicas de uso ocasional hasta hace unos meses. En este corto tiempo se disparó el uso de la videoconferencia, portales de compras, redes sociales, banca web, en fin, el confinamiento empujó hacia la tecnología a la población. Bajo este contexto, usando la hermenéutica se realizó una comparación de las acciones políticas, legales y gubernamentales en Argentina, México y España, en función de ciberseguridad respecto al Ecuador, así como también se analizaron las reglas compatibles o aplicables a la legislación ecuatoriana del Manual de Tallin, como herramienta concebida bajo la necesidad de responder a transgresiones de ciberseguridad, en el marco del Derecho Internacional y fruto del trabajo de un grupo heterogéneo de profesionales convocados por la OTAN, precisando que las reglas plasmadas en el manual expresan el criterio de sus autores, más no de la OTAN. El resultado de esta investigación, sugiere que aplicar las reglas compatibles con la legislación ecuatoriana evita un análisis ya realizado por expertos, y retroalimenta las incidencias experimentadas por naciones que poblaron el ciberespacio mucho antes que el Ecuador.
Palabras clave: tecnología, ciberespacio, ciberseguridad, Tallin, OTAN

Abstract

This investigation analyzes the transgressions to cybersecurity in Ecuador, also the increase of cyberspace's citizens because of technological revolution and COVID-19 pandemic. This abnormal situation has forced to society use technological tools, generally used by TIC's workers until a few months ago. The population are increasing video conferencing communication, web shopping, social networks, web banking use. So, I worked hermeneutic method to compare political, law, and governmental actions in Argentina, Mexico, and Spain with Ecuador's cybersecurity. I analyzed Tallinn Manual's rules compatible or applicable to Ecuadorian legislation, this manual was created by needs that respond to cybersecurity transgressions within International Law. NATO hired a Professional workgroup to create Tallinn Manual, specified that the rules are not criteria NATO. The answer show that applying the rules compatible with Ecuadorian legislation avoids an expert analysis, and feeds back on the incident resolution by nations that arrived to cyberspace long before Ecuador.

Key words: technology, cyberspace, cybersecurity, Tallinn, NATO

Índice

Lista de Figuras

Introducción

La interconexión que se vive en la actualidad, ha ido generando una marcada dependencia de las tecnologías de la información, tanto de Estados como de la sociedad en general; esto ha provocado la aparición de nuevas vulnerabilidades que amenazan la seguridad en un escenario denominado Ciberespacio, el mismo que tiene cada vez más integrantes. En 1996, en Davos, Suiza, John Perry Barlow declaraba la *Independencia del Ciberespacio* (Barlow, 1996), de acuerdo a su enfoque se trataba de un nuevo territorio libre y soberano en donde se crearía una "sociedad de la mente". Pronto pudo verse que ese nuevo campo social no era específicamente espacio para intelectuales, de la mano con la evolución tecnológica, el aparecimiento de nuevos servicios, productos y mercados en el ciberespacio también se integraban personas de dudoso proceder y aparecieron nuevas formas de vulnerar los derechos personales.

Los gobiernos alrededor del mundo han tomado muy en serio la ciberseguridad, pues al tratarse el ciberespacio de un vasto escenario que puede contemplar inclusive hostilidades militares entre estados y actos subversivos, no puede desarrollarse en anarquía.

En el año 2007, *Estonia experimentó una serie de ataques cibernéticos al parlamento, bancos, ministerios, periódicos y medios de comunicación*. Ataques de una sofisticación nunca antes vista y atribuidos al ruso Konstantin Goloskokov, funcionario del Kremlin (Martínez, 2017). Antes de su adhesión oficial a la OTAN, había propuesto la creación de un Centro de Excelencia para que se encargase de estos temas, su propuesta tuvo apoyo luego del mencionado incidente, dando lugar a la *creación del CCDCOE (Centro de Excelencia Cooperativa de Ciberdefensa de la OTAN)* (Artiles, 2011), que fue establecido y acreditado por la OTAN como "Centro de Excelencia" en 2008, su sede fue establecida en la ciudad Tallin. A finales del año 2009 el CCDCOE invita a un "Grupo Internacional de Expertos" independientes a crear un manual que aborde la ciberseguridad bajo aristas legales, humanitarias y militares.

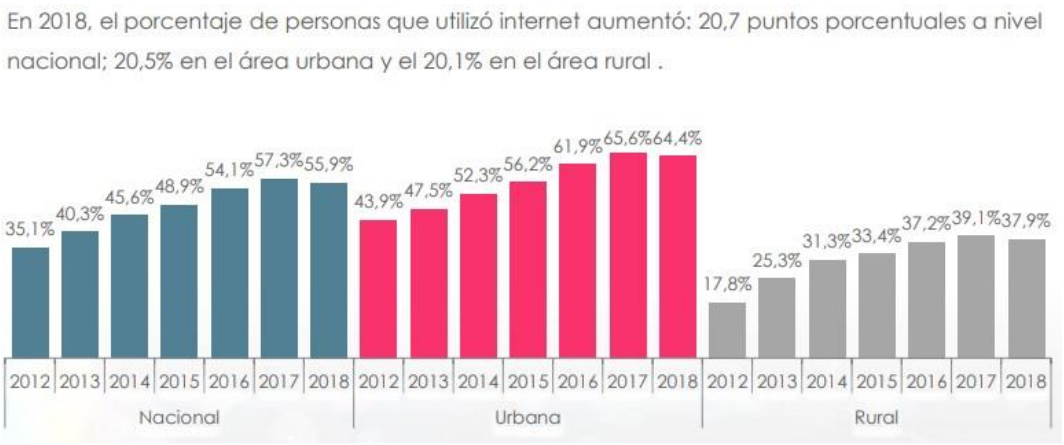
Cabe recalcar que su producto final, el Manual de Tallin, expresa el pensamiento y juicio del grupo de expertos y no es la voz oficial de la OTAN.

El mencionado documento, aportará con ciertas reglas aplicables a la Legislación del Ecuador.

El Crecimiento del Ciberespacio y las Ciberamenazas

El vertiginoso avance tecnológico, y la automatización incesante de servicios, mercados, procesos, además del uso obligatorio de las TICs en entornos públicos y privados, dio lugar al inminente crecimiento del ciberespacio, y con él la necesidad de salvaguardar en dicho escenario la integridad de personas e instituciones. En el ciberespacio, la ciberseguridad se volvió necesaria, vital. Algunos estados se han visto en la obligación de integrar en sus debates estos temas, ya que en cierta medida han sufrido algún incidente o han experimentado una transgresión de su seguridad en el ciberespacio, como sucedió con los ataques a Estonia en 2007 por parte de Rusia, o el *ataque a una planta nuclear en la ciudad iraní de Natanz en 2010, por medio del virus StuxNet*, que ordenó prácticamente autodestruirse a 1000 máquinas centrifugadoras de Uranio (BBC, 2015). Los ejemplos anteriores han sido detonantes para que los afectados tomen cartas en el asunto. El Ecuador no puede excluirse del avance tecnológico, y también ha sufrido las consecuencias que trae consigo la automatización.

Figura 1. *Crecimiento del Uso del Internet en el Ecuador*



Fuente: *Las cifras del 2008 al 2017 son fuente de la Encuesta Nacional de Empleo, Desempleo y Subempleo (ENEMDU) (dic) y del 2018 es de la Encuesta Multipropósito (dic.).* ***Elaboración:*** *Instituto Ecuatoriano de Estadísticas y Censos*

De acuerdo al INEC, el uso del internet en el Ecuador en 2018 creció en aproximadamente 20 puntos con relación a 2012.

Si bien se ha actuado con reformas a la ley, hace falta ser específico en lo referente al entorno donde se producen y las acciones que se deben tomar; para este caso puntual el ciberespacio y la ciberseguridad. Existe bibliografía que aborda temas de ciberseguridad, seguridad de la información, ciberespacio y que pueden ser de ayuda para responder a este tipo de problemas, pero no habido un trabajo colaborativo que haya reunido profesionales de diversas ramas donde unifiquen experiencias y diversidad de criterios para generar un producto terminado como es el Manual de Tallin; es necesario entonces determinar su aplicabilidad en la Legislación ecuatoriana para responder a transgresiones de ciberseguridad, este manual contiene interesantes interrogantes de ámbito penal tales como:

¿Un equipo informático puede ser considerado un arma?

La respuesta es sí, ya que en las manos equivocadas es posible causar daños o vulnerar derechos a terceros, pudiendo afectar a un estado, institución, empresa o población en general.

¿Cambiaron las amenazas en la ciberguerra o guerra cibernética?

Rotundamente sí, una amenaza no necesariamente proviene de un sector específico, ya sea estado, grupo terrorista, grupos delictivos o individuos particulares (Experts, 2017).

Uno de los ataques de importancia a nivel mundial, en donde se vio afectado como es lógico el Ecuador, es el suscitado en el mes de mayo de 2017, se experimentaba un *ataque a escala global del RansomWare WannaCry*, un tipo de virus que de acuerdo al sitio web gotelgest.net, se expandía a través de correo electrónico, una vez alojado en un equipo, fue capaz de encriptar la información, la misma que dejaba de ser accesible por el propietario y para poder recuperar el acceso a la misma debería pagar un rescate en bitcoins, de esta forma recibiría la llave o medio para desencriptar la información secuestrada (Gotelgest.Net, 2017).

La noticia del ataque del mencionado virus, se replicaba en todo el mundo, y en el Ecuador se informaba a través de medios de comunicación que la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), *por medio del sitio web de su Centro de*

Respuesta a Incidentes Informáticos EcuCERT, se encontraba receptando las denuncias de los afectados, con el fin de estudiar y contabilizar los casos perpetrados en el país, además se temía que no solamente exista secuestro de información, sino que se comercialice las bases de datos capturadas en mercados ilegales. *A pesar de las medidas adoptadas la fiscalía no receptó ninguna denuncia hasta la publicación del artículo*, de acuerdo a la fiscal general subrogante en ese momento, Thania Moreno, (El Comercio, 2017).

A pesar de lo expuesto, empresas como Telefónica en sus portales comunicaban la afectación de algunos equipos sin embargo la oportuna acción de sus departamentos de TI, garantizaron la disponibilidad de sus servicios, y el incidente no pasó de realizar la restauración de sus backups o respaldos de la información afectada. Además de los organismos gubernamentales como el EcuCERT, existen los CSIRT (Computer Incident Response Team), en español Equipo de Respuesta a Incidentes de Seguridad Informática, son equipos que forman parte de empresas privadas, instituciones públicas, militares o académicas. Los CSIRTs que operan en el Ecuador se han tratado de agrupar por medio del proyecto CSIRT-CEDIA (CEDIA, 2020).

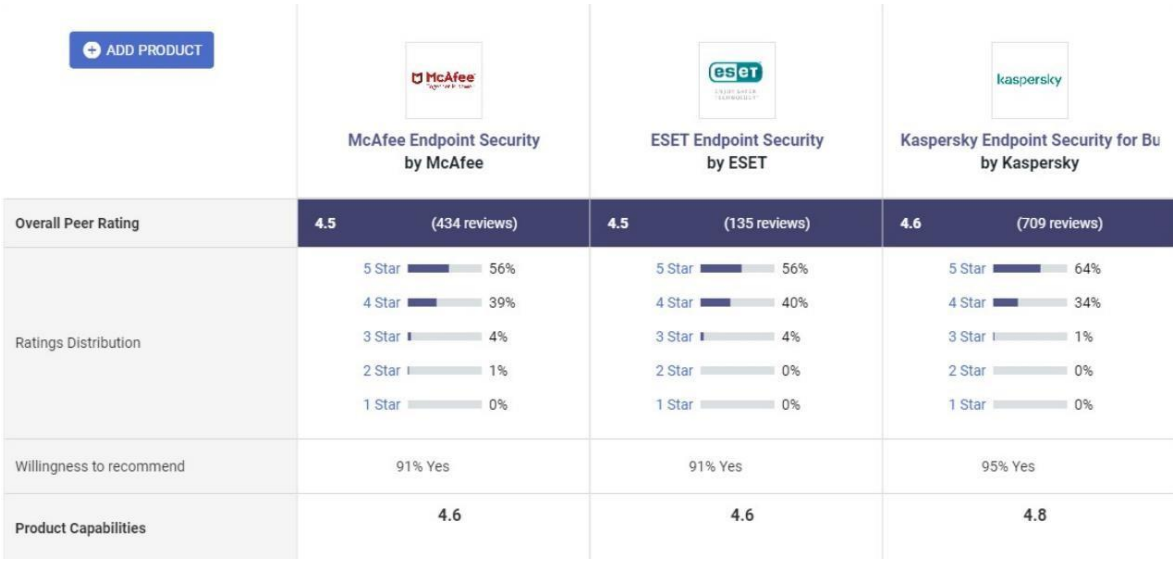
En el contexto actual, en el que el mundo atraviesa un problema a gran escala como es la pandemia COVID-19, producida por el virus SARS-CoV-2, responsable de miles de muertes y millones de contagiados; ha traído consigo además problemas sociales y económicos que cambiaron la dinámica del mundo; como consecuencia se potencian plataformas digitales para la atención médica, el teletrabajo, las ventas, la educación, etc; es decir la sociedad está incrementando rápidamente su presencia en el ciberespacio, y como es de fácil deducción no solamente personas de bien transitan en este escenario.

El CSIRT de la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA), mencionó el mes pasado que *en el Ecuador se dispararon los ataques a RDP a causa del teletrabajo*. Antes ya había lanzado la alerta de posibles estafas por internet, razón por la que aconsejaba estar preparados (CSIRT-CEDIA, 2020).

Instituciones y personas, básicamente protegen su información por medio de herramientas tales como antivirus, antispam, firewalls; obviamente esto a escala de la infraestructura que utilizan. Existen varias empresas que ofrecen productos de

ciberseguridad, podemos mencionar entre ellas a NortonLifeLock Inc, ESET, Kaspersky y McAffee Inc entre otras.

Figura 2. *Herramienta de Seguridad más usada*



ADD PRODUCT	McAfee Endpoint Security by McAfee	ESET Endpoint Security by ESET	Kaspersky Endpoint Security for Bu by Kaspersky
Overall Peer Rating	4.5 (434 reviews)	4.5 (135 reviews)	4.6 (709 reviews)
Ratings Distribution	5 Star 56% 4 Star 39% 3 Star 4% 2 Star 1% 1 Star 0%	5 Star 56% 4 Star 40% 3 Star 4% 2 Star 0% 1 Star 0%	5 Star 64% 4 Star 34% 3 Star 1% 2 Star 0% 1 Star 0%
Willingness to recommend	91% Yes	91% Yes	95% Yes
Product Capabilities	4.6	4.6	4.8

Fuente: *Gartner Inc*

Obtenido de: *https://www.gartner.com/reviews/market/endpoint-protection-platforms*

De acuerdo a la consultora Gartner Inc, empresa de investigación de las Tecnologías de Investigación y Comunicación TICs, que se ha convertido en un referente por su reputación, la presencia de Kasersky predomina en América y Europa como herramienta de protección, con una calificación de 4.6 estrellas.

Figura 3*. Compañía de TI con mejor reputación.*

Gartner, Inc. provides information technology, research and consulting services.

Industry	Management Consulting	Founded	1979
Country/Territory	United States	CEO	Eugene A. Hall
Employees	8,802	Headquarters	Stamford, Connecticut

As of Mar 17, 2020

ON FORBES LISTS

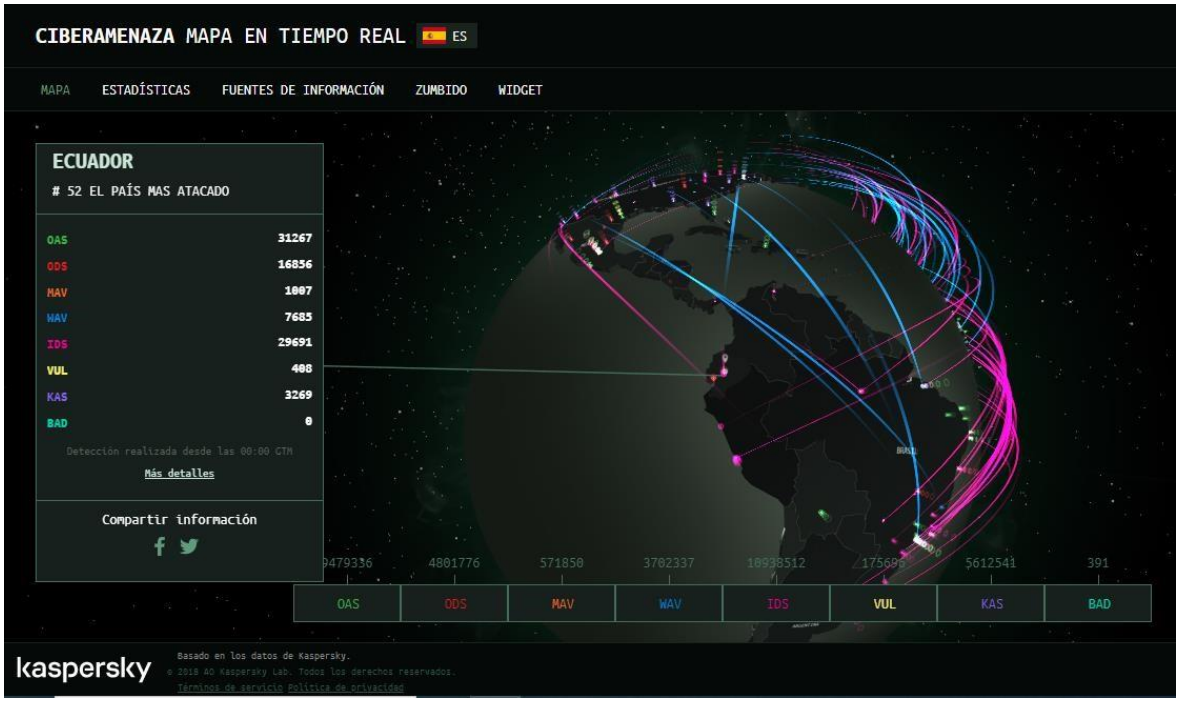
Best Management Consulting Firms 2020

Fuente: *Revista Forbes*

Obtenido de: *https://www.forbes.com/companies/gartner/#75edfa607faf*

Kaspersky brinda al público en general, estadísticas en tiempo real de ciberataques, esta información se encuentra dividida por región, país, tipo de herramienta (*WAV, IDS, KAS, BAD, VUL*), nombre de la amenaza y conserva datos de hasta un mes atrás.

Figura 4*. Ciberamenazas en tiempo real*



Fuente: *Kaspersky*
Obtenido de: *https://cybermap.kaspersky.com/es*

En el caso del Ecuador, al mes de mayo se encontraba en la posición 52 de los países con más ciberataques. Las herramientas usadas por Kaspersky para detectar y eliminar amenazas son:

a) ***WAV.-*** Web Anti Virus, muestra el flujo de detección de malware durante el análisis web cuando la página html de un sitio web se abre o un archivo es descargado.

b) ***IDS.-*** Intrusion Detection Scan, muestra el flujo de detección de los ataques a las redes.

c) ***KAS.-*** Kaspersky Anti Spam, muestra el tráfico sospechoso y no deseado.

d) ***BAD.-*** Botnet Activity Detection, muestra estadísticas sobre direcciones IP de víctimas de ataques de denegación de servicios DDoS y servidores botnet C&C.

e) ***VUL.-*** Vulnerability Scan, muestra el flujo de la detección de vulnerabilidades.

El Ecuador, está incrementando su presencia en el ciberespacio de forma acelerada, y precisa de un instrumento de Ciberseguridad para uso en instituciones Públicas y Privadas, el mismo que en conjunto con la Legislación vigente y Planes Nacionales tales como Gobierno Electrónico, Seguridad Pública y Ciudadana, Sectorial de Defensa y Específico de Inteligencia, conformen una guía de actuación en respuesta a las transgresiones de la ciberseguridad.

Actualmente existe desconfianza por parte de los actores del ciberespacio de nuestro país, en relación a las herramientas que, en este momento a causa de la pandemia nos vemos obligados a usar, en sectores como el económico, laboral, salud, educación, comercio, distracción e incluso socialización; desconfianza hasta cierto punto justificada, porque se mantiene la idea de que el ciberespacio es un escenario inseguro, dónde la vulneración de derechos no está penada.

La coyuntura actual en el Ecuador es sin duda propicia para enfocarnos en la seguridad del ciberespacio y a responder en el marco legal a sus transgresores.

Conceptos de Interés

Bajo el contexto de la presente investigación, es necesario mantener en mente el significado o conceptos de palabras que se mencionan con frecuencia, y son fundamentales para su comprensión.

Derecho

De acuerdo a González y Carvajal, etimológicamente proviene del vocablo directum, que significa “seguir el sendero señalado por la ley”, de manera general es el conjunto de normas jurídicas que un estado crea para regular el comportamiento externo de las personas, y se produce una sanción en caso de incumplimiento (González & Moreno, 2002).

Otros autores como Pereznieto y Ledesma, definen al Derecho como *“el conjunto de normas que imponen deberes y normas que confieren facultades, que establecen las bases de convivencia social y cuyo fin es dotar a todos los miembros de la sociedad de los mínimos de*

seguridad, certeza, igualdad, libertad y justicia" (Pereznieto Castro & Ledesma Mondragón, 1992)

Sociedad de la Información

Se volvió habitual hablar de ella en la última década, consecuencia obviamente de la evolución tecnológica. No todas las personas estamos conscientes de su significado, o lo que representa específicamente, se tiene la idea de que implica tecnología, computadores, incluso modernidad. Para algunos autores es ambiguo el término "Sociedad de la Información", y se prefiere usar términos como Sociedad del Conocimiento, Sociedad de Red, e incluso Cibersociedad, pero son términos que a la larga de alguna manera resultan sinónimos.

El Gobierno Español, a través del Real Decreto 1289/1999, (publicado en el Boletín Oficial del Estado Nro 178 de 27 de julio de 1999), creó la Comisión Interministerial de la Sociedad de la Información y de las nuevas tecnologías de España. El texto original del decreto mencionaba un concepto claro y simple de Sociedad de la Información: *"engloba un conjunto de actividades industriales y económicas, comportamientos sociales, actitudes individuales y formas de organización política y administrativa, de importancia creciente en las naciones situadas en la vanguardia económica y cultural, a lo que no pueden sustraerse los poderes públicos."* (España, Real Decreto 1289/1999, 1999).

EGA (e-Governance Academy)

Es una organización de consultoría sin fines de lucro, que fuera una iniciativa del gobierno de Estonia en conjunto con el Open Society Institute (OSI) y el Programa de las Naciones Unidas para el Desarrollo (PNUD). Se encarga de crear y transferir conocimiento, así como también difundir las mejores prácticas en cuánto a transformación digital se refiere: gobierno electrónico, democracia electrónica y ciberseguridad nacional.

NCSI (National Cyber Security Index)

Es un índice desarrollado por la Academia de Gobierno Electrónico (EGA), mide en los países el nivel de ciberseguridad y en qué campos prioritarios debe tomar acción. Muestra el top de los países mejores preparados para enfrentar o manejar ciberataques.

Ciberespacio

Este término fue introducido por William Gibson en su novela de ciencia ficción Neuromante, publicada en 1984 por la editorial Ace Books, aquí lo califica como una "alucinación consensual". No existe un concepto único de Ciberespacio, pero una mayoría apunta a calificarlo como un espacio creado gracias a la interconexión de computadores. Esto nos lleva a precisar que el ciberespacio es tan grande como el Internet, es decir cualquier dispositivo que tenga capacidad de conectarse al internet como computadores, teléfonos inteligentes, dispositivos electrónicos, etc.; forman parte del ciberespacio.

Ciberdelito

Se refiere a cualquier acto que vulnere la legalidad en el ciberespacio.

Ciberoperaciones

Son las acciones militares que un estado puede ejecutar como medio defensivo, así como también ofensivo hacia otra nación o naciones por medio del ciberespacio (Cabrera, 2019).

Ciberseguridad

Se considera de acuerdo a la ISACA (Information Systems Audit and Control Association) como *"la protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, se almacena y se transporta mediante los sistemas de información que se encuentran interconectados"* (ISACA, 2015).

Ciberdefensa

Se define de acuerdo al Consejo Argentino de las Relaciones Internacionales (CARI) como *"el conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición."* (CARI, 2013).

Cibernauta

De acuerdo a la Real Academia Española, es una persona que navega por el ciberespacio.

IoT (Internet of Things)

De acuerdo a SAP Latinoamérica, el internet de las cosas se trata de *"una red de objetos físicos –vehículos, máquinas, electrodomésticos y más, que utiliza sensores y APIs para conectarse e intercambiar datos por internet."* (SAP, 2020).

API (Application Programming Interface)

Las interfaces de programación de aplicaciones son aplicaciones (software) disponibles, pueden ser de código abierto o de pago, que ayudan aportando mejoras en la creación o desarrollo de aplicaciones (nuevo software).

Materiales y Métodos

El proceso de investigación se ha sostenido en el *método hermenéutico*, dado que permite la interpretación de los significados del objeto de estudio partiendo de una triple perspectiva: el fenómeno propiamente dicho, la sinergia sistémico – cultural y su interconexión en el contexto histórico – social. En las ciencias jurídicas tiene validez cuando las normas jurídicas constituyen el centro de estudio (Villabella Argamenol, 2006). La normativa jurídica relativa a delitos informáticos y derechos intelectuales, es la fuente principal que aborda el presente trabajo.

En cuanto a los instrumentos o técnicas empleados, en primer lugar, se ha usado la técnica documental, ya que este estudio se basa en el análisis de documentos como el Manual de Tallín, así como de leyes, libros, artículos e internet, en donde se puede demostrar la realidad del problema que se investiga

En segundo lugar, otro instrumento usado para la recopilación de información ha sido la entrevista, que para el presente caso se realizó a dos especialistas, Dr. Christian Fierro, Especialista en Derecho Penal y Abg. Jairo Jarrín, Especialista en Propiedad Intelectual, las entrevistas se encuentran en el Anexo 2, los dos profesionales manifiestan que conocen del ciberespacio y sus amenazas. El Dr. Christian Fierro, experto en Derecho Penal, recalca que la legislación vigente no es eficiente y clara en cómo actuar ante transgresiones a la ciberseguridad, pues considera que en materia penal no se ha caminado de la mano con el

avance tecnológico y que "*el ordenamiento jurídico legista, no jurisprudencial ni casuístico, depende absolutamente del principio de tipicidad, lo cual hace que, si una norma penal se redacta de manera tal, que restringe los presupuestos que configuran un tipo penal a una situación muy en específica, dicha norma resulta insuficiente para enmarcar nuevas conductas que van acordes al avance tecnológico",* lo que puede culminar en impunidad. En cambio, considera que en el escenario actual en el que se está desenvolviendo el mundo, sí existirá un crecimiento acelerado de presencia delictiva en el ciberespacio ecuatoriano. Y la preocupación radica en que los afectados no denuncian, o las denuncias no logran resultado alguno, de acuerdo a su perspectiva entre otras razones por los altos costos de la materialización notarial o pericial, además de la falta de procesos penales expeditos. El Dr. Fierro, enfatiza que los esfuerzos gubernamentales relacionados con el tema de investigación, han derivado en acciones meramente administrativas. Por su parte el Abg. Jairo Jarrín, relata que la normativa vigente ampara los derechos de autor, aunque menciona que la piratería es un serio problema que prácticamente no inmuta a la sociedad ecuatoriana, más que al afectado. Un ejemplo claro es que, en el Ecuador la mayor parte de personas e incluso ciertas empresas usan software de manera ilegal, el software es crackeado para poder usarse, es decir se vulnera la seguridad del mismo, se lo altera con el fin de no pagar por su uso. También comparte la preocupación de que, en la situación actual, en la que la sociedad se ha visto obligada a servirse de la tecnología en diversos campos, existirá un crecimiento acelerado de transgresiones a la ciberseguridad. Cree además que las autoridades han realizado y se están realizando un trabajo loable en temas de derechos intelectuales.

En cuanto a acciones gubernamentales, enfocadas a la ciberseguridad, se observaron investigaciones realizadas en Argentina, México y España, países que han sido referentes en incluir de forma temprana en su legislación delitos informáticos, protección de datos personales, además de adoptar políticas institucionales en el marco de la ciberseguridad. En el caso del Ecuador, la creación del Código Integral Penal, Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, Ley de Comercio Electrónico, Firmas y Mensajes de Datos, representó un primer paso para la regulación del ciberespacio y voltear la mirada a la ciberseguridad. Por último, se analizó el Manual de Tallin, como producto resultante de una investigación colaborativa entre profesionales

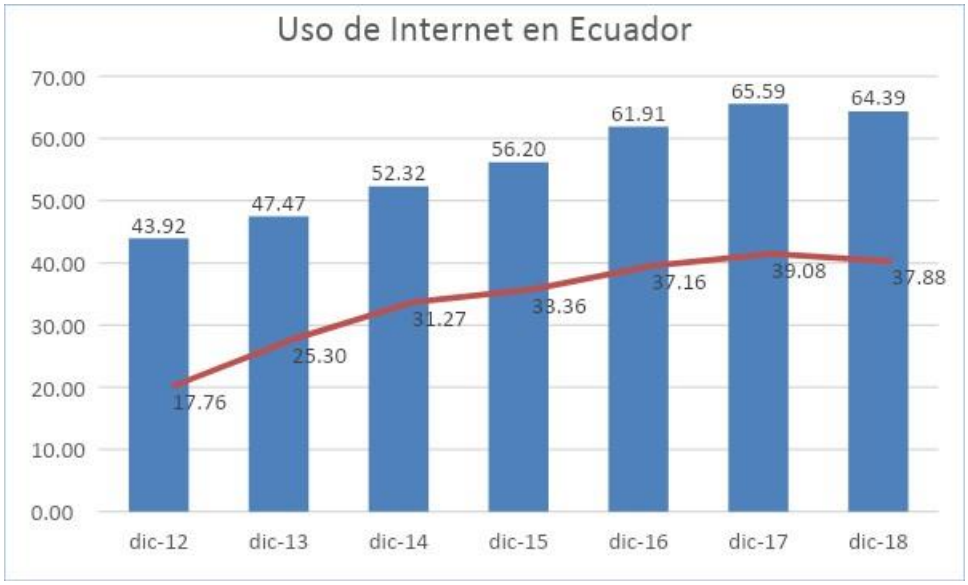
expertos de diversas ramas convocados por la OTAN, su origen y generación, partiendo de la necesidad de minimizar la anarquía en ese vasto escenario conocido como ciberespacio.

Resultados

La transgresión a la ciberseguridad, no escapa a ningún estado, y se ha convertido en un problema importante a resolver. Si bien existen naciones que presentan un alto nivel de madurez en su ciberseguridad y han reforzado su ámbito legal, como el caso de España; otras han ralentizado su paso como el caso de México y Argentina.

El desarrollo tecnológico, y la tendencia creciente del uso del internet en Ecuador a partir de 2012, como se puede ver en la siguiente figura, ocasionó que se el país se adhiera a la misión de salvaguardar el ciberespacio.

Figura 5. *Tendencia del Uso de Internet en Ecuador*



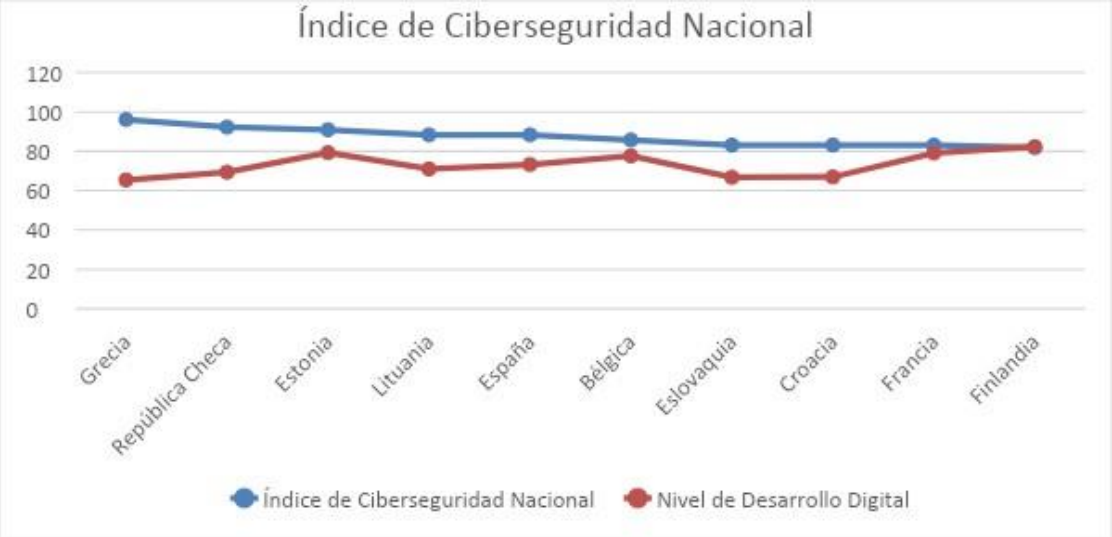
Fuente: *Las cifras del 2008 al 2017 son fuente ENEMDU (dic) y del 2018 es de la Encuesta Multipropósito (dic.).*

Elaboracion: *Instituto Nacional de Estadística y Censos - INEC*

Los cambios realizados en la legislación vigente sobre temas penales, derechos intelectuales, telecomunicaciones, gobierno electrónico, defensa nacional y registro de datos públicos, son muestra de la voluntad gubernamental de ir en sentido de la modernización tecnológica de las instituciones, sin embargo, una vez iniciado este camino no es posible retroceder o detenerse, la evolución debe ser constante y no enfocarse únicamente en cambios administrativos.

La experiencia acumulada por países que llevan la delantera en ciberseguridad al Ecuador, debe ser el punto referencial para marcar un camino a seguir y monitorear.

Figura 6. *Ciberseguridad Nacional vs Nivel de Desarrollo Digital*



Fuente*: NCSI*

Obtenido de *https://ncsi.ega.ee/ncsi-index/?order=rank*

El camino adoptado por España, lo lleva a estar en la posición 5 en el NCSI, en el Ecuador es importante el incremento de los actores en el ciberespacio, y aunque se trata de un sitio global, común, diferente al territorio, no está exento de regulación. Luego de ser víctima la sociedad ecuatoriana, de un robo masivo de datos personales en 2019, de enfrentarse a incidentes de índole mundial como el ransomware WannaCry en 2017, accesos no consentidos a sistemas informáticos, suplantación de identidad, entre otros, es necesario concientizar a la población sobre la ciberseguridad, así como también se requiere de un cambio de mentalidad en relación al uso de software original. El Ecuador se encuentra en la posición 79 en lo que se refiere a Ciberseguridad de acuerdo al Índice de Ciberseguridad Nacional (NCSI, 2020), y en la posición 52 entre los países más atacados de acuerdo a Kaspersky Labs. Indicador que a simple vista nos da la idea del bajo nivel de madurez de la ciberseguridad que tiene el país. En un escenario óptimo el ciberespacio no debería tener vacíos legales, que se presten a la ejecución de acciones dolosas que queden en la impunidad, esto en función de las acciones delictivas comunes, ya que acciones o amenazas de tipo militar o más evolucionadas como las que ejecutan estados, grupos terroristas no se analizan en esta investigación.

Al tomar acciones en respuesta a ciberamenazas como lo ha hecho España, Argentina y México, se puede observar que su nivel de madurez en ciberseguridad ha aumentado, y de manera marcada España pues ocupa la posición número 5 en el Índice de Ciberseguridad Nacional. Obviamente debemos recordar que en Europa se discutieron estos temas hace aproximadamente dos décadas y que Estonia solicitó el apoyo a la OTAN por la ofensiva sufrida en 2007 y como respuesta, la entidad solicitó a un grupo de profesionales expertos la elaboración de un documento que sirviera de guía para responder a estas ofensivas, concibiéndose así el Manual de Tallin.

Sintetizar las reglas del Manual de Tallin que pueden ser aplicadas a la Legislación del Ecuador en el ámbito Penal y Derechos Intelectuales, supondría un atajo en la unificación de criterios profesionales para la toma de acciones, modificación o adición de elementos legales, en virtud de que las naciones que sugirieron la elaboración del documento ya sufrieron y resolvieron problemas similares. Es importante indicar que el enfoque no solamente está direccionado a las instituciones gubernamentales, sino que también apunta a las empresas privadas.

El Manual de Tallin 2.0 se divide en cuatro partes que se detallan a continuación:

Parte I: Derecho Internacional General y Ciberespacio

La Soberanía

Regla 1 – Soberanía (principios generales). El principio de la Soberanía territorial de un Estado se puede aplicar al ciberespacio.

Regla 2 – Soberanía interna. Un Estado goza de autoridad soberana con respecto a la infraestructura cibernética, las personas y las actividades ubicadas dentro de su territorio, sujeto a sus obligaciones legales internacionales.

Regla 3 – Soberanía externa. Un Estado es libre de realizar actividades cibernéticas en sus relaciones internacionales, sometiéndose a cualquier norma que vaya en contra del Derecho Internacional.

Regla 4 – Violación de la soberanía. Un Estado no debe realizar operaciones cibernéticas que violen la soberanía de otro Estado.

Las reglas anteriores, tratan a la Soberanía como un principio cimental del Derecho Internacional, resaltando la autoridad suprema del Estado, reconoce además que varios

aspectos del ciberespacio y actividades que en él se desarrollan, no van más allá del alcance del principio de soberanía.

Los estados pueden ejercer soberanía sobre la infraestructura cibernética que se encuentre en otro territorio, un ejemplo es la infraestructura que se monta en "la nube", aunque el servicio se brinda en el Ecuador, los proveedores y la infraestructura se encuentran en el extranjero, sin embargo, Ecuador puede ejercer la soberanía en ese ciberespacio. Se debe entender también que el "otro territorio" puede imponer restricciones, inclusive paralizar el servicio si se constata que se está dando uso doloso, el hecho que se preste un servicio internacional no implica que se pierda soberanía. La naturaleza virtual del ciberespacio no implica que carece de fiscalidad, se sugirió en algún momento que el ciberespacio se asimila a alta mar o al espacio aéreo internacional, nada más alejado de la realidad, aunque se realice un ciberataque desde otro estado, aguas internacionales o espacio aéreo internacional, es realizado por una persona o entidad, quienes están sujetos a la jurisdicción de uno o más estados.

Los artículos 1 y 3 de la Constitución Ecuatoriana, responden a la soberanía (Constitución de Ecuador, 2008, Artículos 1 y 3).

La Debida Diligencia

Regla 6 – Debida diligencia (principios generales). Un Estado debe ejercer la debida diligencia para no permitir que su territorio, o infraestructura cibernética bajo su control, se utilicen para operaciones cibernéticas que afecten los derechos y produzcan graves consecuencias a otros Estados.

Regla 7 – Cumplimiento del principio de la debida diligencia. El principio de la debida diligencia requiere que un Estado tome todas las medidas que sean factibles para poner fin a las operaciones cibernéticas que afectan el derecho de otros Estados y producen consecuencias graves.

En esta parte se habla de que exista eficiencia en procesos legales, y en el caso de que se identifiquen acciones indebidas de índole cibernético, no exista obstrucción, negligencia o ausencia de justicia.

La Jurisdicción

Regla 8 – Jurisdicción (principios generales). Sujeto a las limitaciones establecidas en el derecho internacional, un Estado puede ejercer jurisdicción territorial y extraterritorial sobre actividades cibernéticas.

Regla 9 – Jurisdicción territorial. Un estado puede ejercer jurisdicción territorial sobre:

a) La infraestructura cibernética y personas involucradas en ciberataques en su territorio.

b) Los ciberataques originados, o culminados en su territorio

Regla 10 – Jurisdicción prescriptiva extraterritorial. Un estado puede ejercer jurisdicción prescriptiva extraterritorial con respecto a ciberataques, cuando:

a) Ha sido efectuado por sus ciudadanos
b) Ha sido efectuado a bordo de buques y aeronaves que posean su nacionalidad;
c) Ha sido efectuado por ciudadanos extranjeros contra su población,
d) Constituyan delitos según el derecho internacional sujetos al principio de universalidad.

Regla 11 – Jurisdicción extraterritorial obligatoria. Un Estado solo puede ejercer jurisdicción extraterritorial obligatorio en relación con personas, objetos y actividades cibernéticas en función de:

a) Una asignación específica de autoridad bajo el derecho internacional
b) Consentimiento válido de un gobierno extranjero para ejercer jurisdicción en su territorio.

Regla 12 – Inmunidad de los Estados frente a la jurisdicción. Un Estado no puede ejercer la jurisdicción ejecutoria o judicial en relación con personas involucradas en ciberataques o infraestructura cibernética que gozan de inmunidad bajo el derecho internacional

Regla 13 – Cooperación internacional en la aplicación de la ley. Aunque generalmente, los Estados no están obligados a cooperar en la investigación y el enjuiciamiento de delitos cibernéticos, tal cooperación puede ser requerida por los términos de un tratado aplicable u otra obligación de derecho internacional.

El conjunto de reglas sobre la jurisdicción involucra la infraestructura en relación al estado, personas involucradas en ciberataques, define la competencia legal nacional y transfronteriza. En el COIP, puede incluir como jurisdicción adicional al ciberespacio, ejemplo en su artículo 14.

Ley de Responsabilidad Internacional

Este segmento del manual, los autores lo han divido en cuatro secciones que abordan la no ejecución de ofensivas cibernéticas contra otros estados y la reparación cuando se hayan producido. La investigación supone al Ecuador como víctima y no como actor por lo que no es tema de análisis.

Ciberoperaciones no Reguladas Per Se por el Derecho Internacional

Este capítulo se direcciona a ciberoperaciones preparadas por y contra estados, además se unifica en esta sección a grupos que se encuentran al margen de la ley y que

representan un peligro a la integridad de los ciudadanos más allá de la delincuencia común, pudiéndose convertir en objetivo militar, por lo que no corresponde su análisis.

Parte II: Regímenes Especializados de Derecho Internacional y Ciberespacio

Derecho Internacional de Derechos Humanos

Regla 34 – Aplicabilidad.

Regla 35 – Derechos que disfrutan las personas.

Regla 36 – Compromiso de respeto y protección a los derechos humanos internacionales.

Regla 37 – Limitantes.

Regla 38 – Ausencia de justicia.

El enfoque que los autores le dan a esta sección, está en relación a que las personas "conectadas" y "no conectadas" coexisten, así como en su igualdad de derechos y el reconocimiento y protección por parte del estado, razón por la que no es parte del análisis, así como no se analizan los temas relacionados a:

a) Derecho Diplomático y Consular
b) Derecho del Mar
c) Derecho Aeronáutico
d) Derecho Espacial

Derecho Internacional de Telecomunicaciones

Regla 62 – Suspensión o detención de las telecomunicaciones. Se refiere a que el Estado puede suspender parcial o completamente las telecomunicaciones, cuando se amenaza a la seguridad nacional.

Parte III: Paz y Seguridad Internacional y Ciberactividades

Solución Pacífica de Disputas

Prohibición de Intervención

El Uso de la Fuerza

Seguridad Colectiva

Parte IV: La Ley en Conflictos Ciber Armados en General

La Ley en Conflictos Armados en General

Conducción de Hostilidades

Algunas Personas, Objetos y Actividades

Invasión

Neutralidad

Las partes III y IV se refieren a conflictos armados, razón por la que no son temas de esta investigación.

Discusión

Siguiendo el método hermenéutico, y con la técnica del análisis documental, seguidamente se van a tomar en consideración varios sistemas jurídicos internacionales para, en el ámbito del derecho comparado, establecer un precedente aplicable a la República del Ecuador.

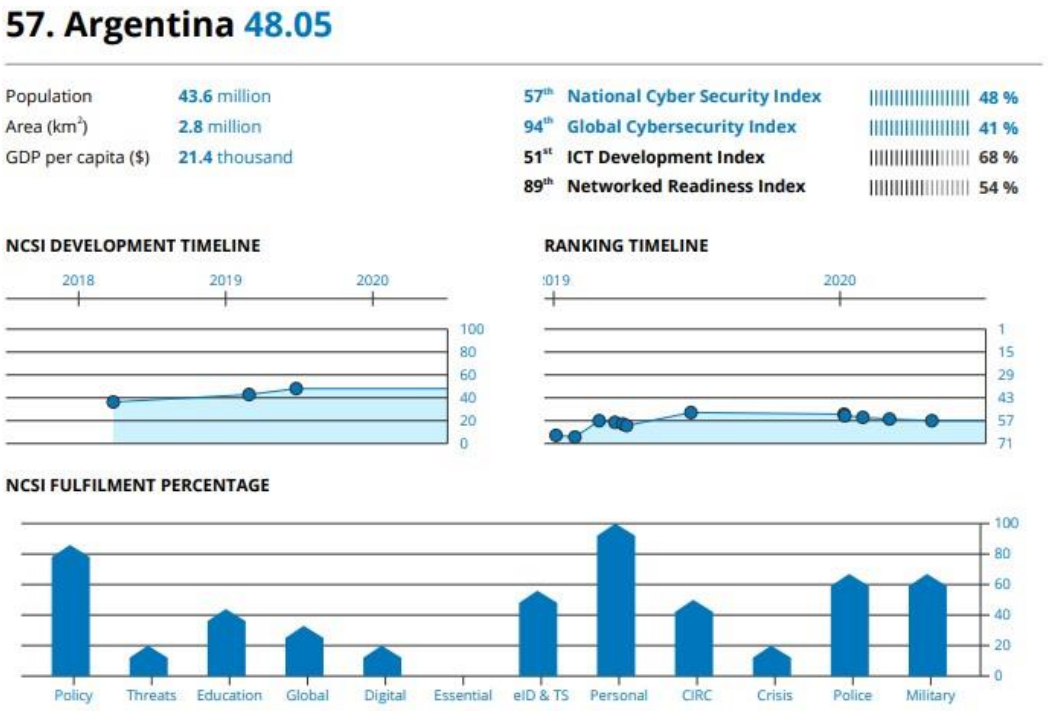
Ciberseguridad en Argentina

En 2013, en el Simposio Argentino de Informática y Derecho (SID 2013), Christian Borghello y Marcelo Temperini (Borghello & Temperini, 2013), abordaron el tema de *Ciberseguridad Nacional Argentina*, a consecuencia de una serie de ataques que se dieron sobre la infraestructura de instituciones públicas, los delincuentes vulneraban seguridades e inhabilitaban por algunas horas los servicios electrónicos que brindaban esos portales, en otros casos modificaron el contenido de los sitios y bases de datos a los que lograron penetrar, situación que se agravó con el hurto de información de datos personales. Los autores mencionaron que la solución no era la prohibición de acceso a la información de la Administración Pública, sino fortalecer el conocimiento y destrezas en cuanto a ciberseguridad se refiere. Solicitaban la respuesta del personal responsable de los sistemas vulnerados y más aún del mismo estado argentino que aparentemente no le daba la importancia suficiente a lo sucedido o no sabía cómo responder a los hechos mencionados, consecuentemente proponían la planeación y aplicación de un verdadero SGSI (Sistema de Gestión de la Seguridad de la Información).

Cabe mencionar que lo expuesto sucedía a pesar de que en Argentina ya se había reformado el código integral penal en 2008, dónde se incluyeron delitos de tipo informático, a partir del año 2000 en Argentina ya se contaba con la Ley de Protección de los Datos

Personales y estaban en funcionamiento los CSIRT y el ICIC (ex ArCERT); aun así, no fue posible procesar a los responsables de los ataques, no existió sentencia condenatoria alguna. De acuerdo a (Cornaglia & Vercelli, 2017), se pude identificar una gran cantidad de *normativa,* así como acciones que se han orientado a mejorar la *capacidad de respuesta en ciberdefensa*.

***Figura 7**. Índice Nacional de Ciberseguridad (Argentina)*



***Fuente:** NCSI*
***Obtenido de:** https://ncsi.ega.ee/country/ar/*

En la actualidad de acuerdo al NCSI Argentina se encuentra en la posición número 57 de los países mejores preparados para prevenir y combatir ciberataques.

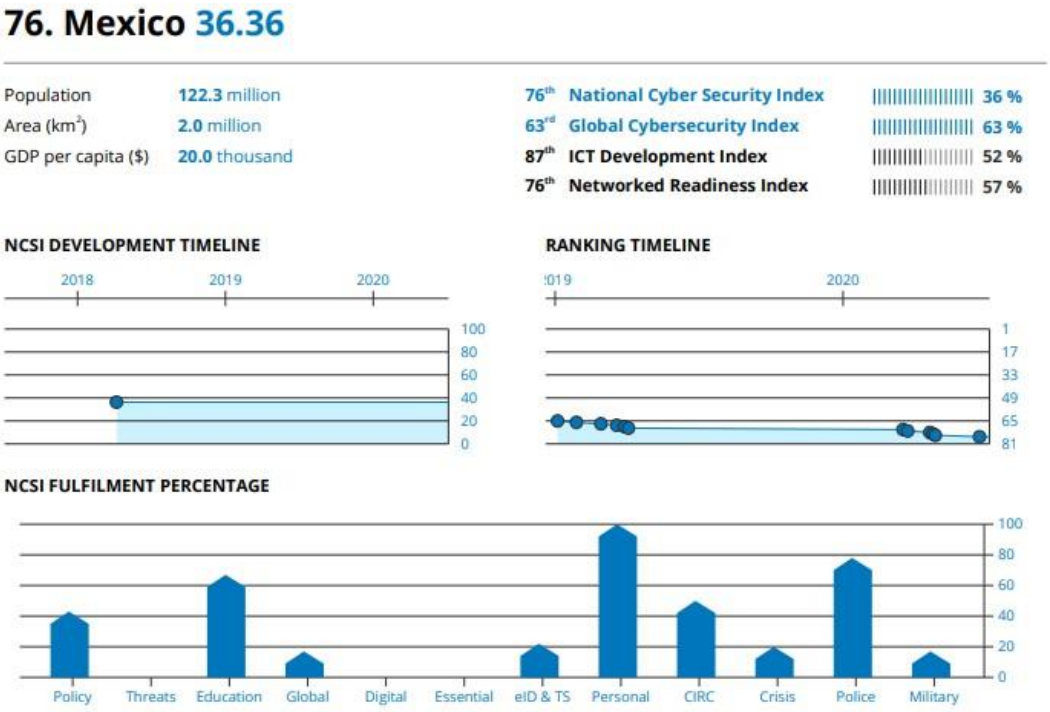
Ciberseguridad en México

Por lo que a México refiere, en al año 2015 de acuerdo Iván Espinosa, en un artículo publicado en la Revista del Centro de Estudios Superiores Navales (Espinosa, 2013), mencionaba que existía una crisis relacionada con la *ciberseguridad*, argumentando que no existía una política unificada para coordinar esfuerzos entre las entidades gubernamentales y la iniciativa privada. Se enfrentaban principalmente a tres amenazas: ciberdelincuencia (fraude, robo y pornografía infantil), espionaje y acceso indebido a sistemas de

organizaciones gubernamentales. Esta nación años atrás había tomado acción en cuanto a ciberseguridad, principalmente se puede recalcar la implementación de la Estrategia Nacional de Seguridad de la Información (ENSI) y la Estrategia de Ciberseguridad de la Policía Federal; inicialmente con grandes miras hacia el fortalecimiento de la ciberseguridad pero que lamentablemente en el caso de ENSI tras su adopción, no se publicó ni se difundió. En lo que respecta a la Policía Federal se concentró en la ciberdelincuencia a nivel federal y no a nivel Estatal, tampoco existía cooperación con las Fuerzas Armadas. En el sector privado por su parte el 10% de las empresas había experimentado un ciberataque, en mayor proporción existieron fraudes, modificación de estados contables, financieros y robo de datos personales. En respuesta a este auge delictivo el gobierno mexicano propició la creación de un CERT especializado, impulsó la educación en cuanto a buenas prácticas de ciberseguridad, fortaleció la academia en lo referente a formación y especialización en ciberseguridad, motivó la creación de la Ley de Protección de Datos Personales, la que vería la luz unos años más adelante. Se hablaba también en ese momento sobre modificar su código penal para especificar la tipificación de ciberdelitos. Es importante destacar que México incluyó en su legislación los *delitos de tipo informático* a partir de mayo de 1999 (Jiménez Rojas, 2016).

La ciberseguridad no es competencia solamente del gobierno central, debe ser cooperativa con el sector privado, que necesariamente ante el auge delictivo debe realizar inversiones para contener las amenazas latentes y salvaguardar un bien valioso, la información, que en algunos casos por su naturaleza contiene datos personales que pueden usarse con fines dolosos.

***Figura 8**. Índice Nacional de Ciberseguridad (México)*



***Fuente:** NCSI*

***Obtenido de:** https://ncsi.ega.ee/country/mx/*

De acuerdo al NCSI, México ocupa el puesto número 76 entre los países mejores preparados para el manejo y respuesta de ciberataques.

Ciberseguridad en España

En el caso de España, ha sido objetivo prioritario garantizar la integridad, confidencialidad y disponibilidad de los sistemas que soportan la infraestructura crítica de sus instituciones, empresas y ciudadanía en general; así lo demuestran la evolución de su legislación, que incluyó por ejemplo artículos en su Código Penal referentes a Delitos Informáticos en 1995 (España, Ley Orgánica 10/1995, 1995), así como también la Ley Orgánica de Protección de Datos de Carácter Personal de 1999 y se reforma en 2018 como Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales; otro ejemplo es lo acordado por el Consejo de Ministros en enero del año 2006, donde se

constituyó el Instituto Nacional de Tecnologías de la Comunicación (INTECO) con la predisposición de cooperar en el ámbito de la sociedad de la información en Europa. De acuerdo a Alberto Hernández Moreno ex Director de INCIBE, inicialmente el INTECO apoyó a la movilidad, administración digital y la accesibilidad; en razón al incremento nacional e internacional de ciberataques y su impacto, INTECO se reorientó específicamente hacia la ciberseguridad, en diciembre de 2013 se implementa la Estrategia de Ciberseguridad Nacional (ECSN) en sincronía a la atención prestada por Europa a los temas de Ciberseguridad, que buscaba desarrollar los valores europeos de democracia y libertad, persiguiendo un crecimiento sostenible y seguro de la economía digital a través de las siguientes estrategias: ciberresiliencia, reducción de los ciberdelitos, desarrollo de políticas de ciberdefensa, ciberseguridad y ciberespacio. La ECSN tenía como objetivo global, lograr que España fortaleciera su capacidad de prevención, detección, defensa y respuesta a los ciberataques, para conseguirlo se plantearon los siguientes objetivos específicos:

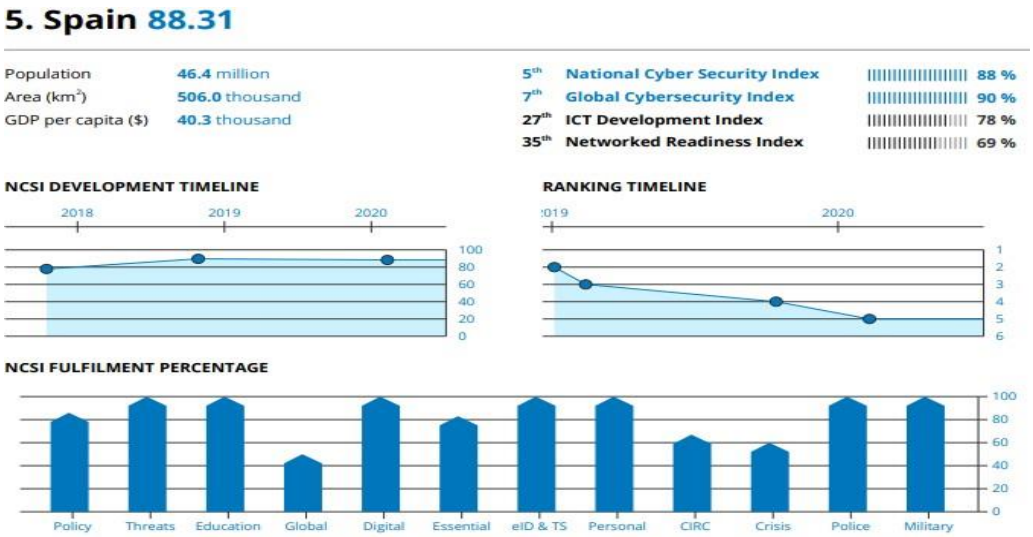
- *"Garantizar que los sistemas de información y telecomunicaciones que utilizan las Administraciones Públicas posean el adecuado nivel de ciberseguridad y resiliencia.*
- *Impulsar la seguridad y resiliencia de los sistemas de información y telecomunicaciones usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular.*
- *Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio.*
- *Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio.*
- *Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad.*
- *Contribuir a la mejora de la ciberseguridad en el ámbito internacional."* (Moreno, 2018)

Una vez aprobada la ECSN y con el proceso de transformación de INTECO, el mismo que culmina en 2014, nace el INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA

(INCIBE) con el fin de dar respuestas rápidas y eficientes a las necesidades producto de nuevas ciberamenazas o posibles crisis. Actualmente el INCIBE es una institución referente en ciberseguridad que aborda los sectores públicos y privados.

El esfuerzo realizado por España ha logrado fortalecer la ciberseguridad en su territorio, pues como se vio anteriormente, las reformas jurídicas acompañaron de cerca al crecimiento tecnológico.

***Figura 9**. Índice Nacional de Ciberseguridad (España)*



***Fuente:** NCSI*
***Obtenido de:** https://ncsi.ega.ee/country/es/*

De acuerdo al NCSI, España ocupa el puesto número 5 entre los países mejores preparados para el manejo y respuesta de ciberataques.

Es concluyente que todas las naciones sufren transgresiones a su ciberseguridad, para la presente investigación se encuentran los reportes del NCSI adjuntos en el Anexo 1. La diferencia en el nivel de madurez de la ciberseguridad entre una y otra nación, radica en las políticas implementadas por sus autoridades, cooperación entre sectores de la sociedad, capacitación, educación y culturización de la sociedad en temas de ciberseguridad.

El avance de la tecnología se da a pasos agigantados, y con él, se desarrollan también nuevas amenazas que detener y combatir, por lo que resulta imperante estar preparado ante potenciales transgresiones a la ciberseguridad.

El Manual de Tallin 2.0

Las amenazas que se han perpetrado en el ciberespacio han empujado a las naciones a buscar soluciones para mejorar su ciberseguridad y tener una referencia práctica de respuesta en caso de enfrentar estas situaciones. Un ejemplo de lo expuesto es el *Manual de Tallin*, considerado una guía completa para asesores políticos, expertos legales y tecnológicos de cómo interpretar que el Derecho de la era anterior a la cibernética, puede aplicarse a las ofensivas cibernéticas, tanto ejecutadas por los estados como dirigidas en contra de los estados, puesto que este tipo de eventos no se desarrollan en un vacío legal, los estados responden a derechos y obligaciones bajo el derecho internacional. *El Manual de Tallin 2.0*, realiza un análisis legal de los eventos cibernéticos más comunes, aquellos a los que los estados se enfrentan día a día, cabe mencionar que el manual no es un documento oficial y se recalca que representa la opinión de sus autores, más no de la OTAN (CCDCOE, 2017). El espectro abarcado por el Manual de Tallin, es muy amplio, se refiere desde las ofensivas ejecutadas en tiempo de paz, hasta la ley de conflictos armados, situación que no concierne a esta investigación y puede ser observado en investigaciones posteriores. Las 14 reglas analizadas se pueden acoplar a la legislación ecuatoriana, son resultado de la experiencia de resolver y enfrentar ciberataques en un entorno al que llegaron antes que el Ecuador.

Conclusiones

La transgresión a la ciberseguridad, no escapa a ningún estado, y se ha convertido en un problema importante a resolver. Si bien existen naciones que presentan un alto nivel de madurez en su ciberseguridad y han reforzado su ámbito legal, como el caso de España; otras han ralentizado su paso como el caso de México y Argentina. La experiencia acumulada por países que llevan la delantera en ciberseguridad al Ecuador, debe ser el punto referencial para marcar un camino a seguir y monitorear. Debemos recordar que en Europa se discutieron estos temas hace aproximadamente dos décadas, que Estonia solicitó el apoyo a la OTAN por la ofensiva sufrida en 2007 y como respuesta, la entidad solicitó a un grupo de profesionales expertos la elaboración de un documento que sirviera de guía para responder a estas ofensivas, concibiéndose así el Manual de Tallin. Tras el análisis de las reglas del Manual de Tallin que pueden ser aplicadas a la Legislación del Ecuador, se encuentran 14 reglas relacionadas con la soberanía que pueden ser aplicadas, y acoplar la

idea de soberanía geográfica y jurisdicción al ciberespacio. Situación que implicaría tomar el control progresivamente de un escenario en el que aún existe la impunidad y se presta para vulnerar derechos. El uso del Manual de Tallin supondría un atajo en la unificación de criterios profesionales para la toma de acciones, modificación o adición de elementos legales, en virtud de que las naciones que sugirieron la elaboración del documento ya sufrieron y resolvieron problemas similares. Es importante indicar que el enfoque no solamente está direccionado a las instituciones gubernamentales, sino que también apunta a las empresas privadas, pues son sectores que idealmente deberían apoyarse.

Referencias Bibliográficas

Artiles, N. G. (2011). Situación de la Ciberseguridad en el ámbito internacional y en la OTAN. *Cuadernos de estrategia*, 165-214.

Barlow, J. P. (8 de Febrero de 1996). *Declaración de independencia del ciberespacio*. Obtenido de https://www.eff.org/cyberspace-independence

BBC. (11 de Octubre de 2015). *El virus que tomó control de mil máquinas y les ordenó autodestruirse*. Obtenido de https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

Borghello, C., & Temperini, M. G. (2013). XI Simposio Argentino de Informática y Derecho (SID) - JAIIO 42 (2013). *Ciberseguridad nacional argentina: cracking de servidores de la administración pública*, (págs. 28-43). Córdoba - Argentina.

Cabrera, C. I. (Diciembre de 2019). *Empleo de las redes informáticas en ciberoperaciones en el marco de la Gran Unidad de Batalla*. Obtenido de http://190.12.101.91/bitstream/1847939/1435/1/TFI%20ECS%20C1E4_249.pdf

CARI. (Noviembre de 2013). *Ciberdefensa-Ciberseguridad Riesgos y Amenazas*. Obtenido de http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

CEDIA. (2020). *LISTADO CSIRTS EC*. Obtenido de https://csirt.ec/csirts-en-ecuador/listados/

Cornaglia, S., & Vercelli, A. (2017). La ciberdefensa y su regulación legal en Argentina (2006 - 2015). *Revista Latinoamericana de Estudios de Seguridad*, 46-62.

CSIRT-CEDIA. (2020). *Equipo de Respuesta a Incidentes de Seguridad Informática*. Obtenido de https://csirt.cedia.edu.ec/

Ecuador, A. N. (2008). Constitución del Ecuador. Quito: Registro Oficial.

El Comercio, D. (17 de Mayo de 2017). *El ciberataque global impactó en Ecuador*. Obtenido de https://www.elcomercio.com/actualidad/ciberataque-wannacry-impactoecuador-hackeo.html

España, G. d. (23 de Noviembre de 1995). *Ley Orgánica 10/1995*. Obtenido de https://www.boe.es/eli/es/lo/1995/11/23/10

España, G. d. (27 de Julio de 1999). *Real Decreto 1289/1999*. Obtenido de https://www.boe.es/eli/es/rd/1999/07/23/1289

Espinosa, E. I. (2013). Hacia una estrategia nacional de ciberseguridad en México. *Revista del Centro de Estudios Superiores Navales (CESNAV)*, 453-481.

Experts, G. (2017). *Manual de Tallin.* Tallin: Cambridge University Press.

González, F. F., & Moreno, G. C. (2002). *Nociones de Derecho Positivo Mexicano.* México : PEARSON.

Gotelgest.Net. (16 de 05 de 2017). *Ataque RansomWare a escala global: Cómo prevenirlo en tu empresa.* Obtenido de https://www.gotelgest.net/ataque-ransomware-aescala-global-como-prevenirlo-en-tu-empresa/

ISACA. (30 de Junio de 2015). *ISOTools Excellence*. Obtenido de https://www.pmgssi.com/2015/06/iso-27001-diferencia-entre-ciberseguridad-y-seguridad-de-lainformacion/

Jiménez Rojas, J. R. (2016). Delitos informáticos en México. *Revista Seguridad UNAM*, 207236.

Martínez, R. (17 de Mayo de 2017). *Los Ciberataques a Estonia desde Rusia desatan la alarma en la OTAN y la UE*. Obtenido de https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html

Moreno, A. H. (2018). Moreno, A. H. (2018). De INTECO a INCIBE: un proceso de transformación para el fortalecimiento de la ciberseguridad de los ciudadanos y empresas en España. *Economía industrial*, 71-80.

Pereznieto Castro, L., & Ledesma Mondragón, A. (1992). *Introducción al Estudio del Derecho.* México: Harla.

sadasd. (sdas). *asdas.* sdas: asdsad.

SAP. (2020). *Definición de internet de las cosas*. Obtenido de https://www.sap.com/latinamerica/trends/internet-of-things.html

Villabella Argamenol, C. M. (2006). *Los Métodos en la Investigación Jurídica. Algunas Precisiones.* Mexico D.F.: Instituto de Investigaciones Jurídicas.

Anexo 1. Reportes NCSI National Cyber Security Index

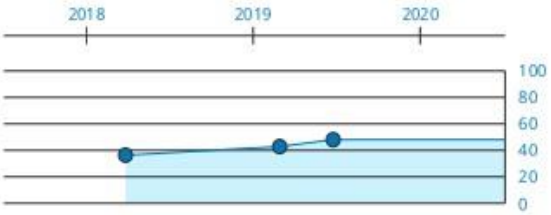
NCSI
national cyber security index

57. Argentina 48.05

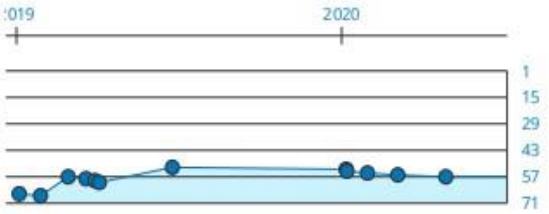
Population	43.6 million
Area (km²)	2.8 million
GDP per capita ($)	21.4 thousand

57th	National Cyber Security Index	48 %
94th	Global Cybersecurity Index	41 %
51st	ICT Development Index	68 %
89th	Networked Readiness Index	54 %

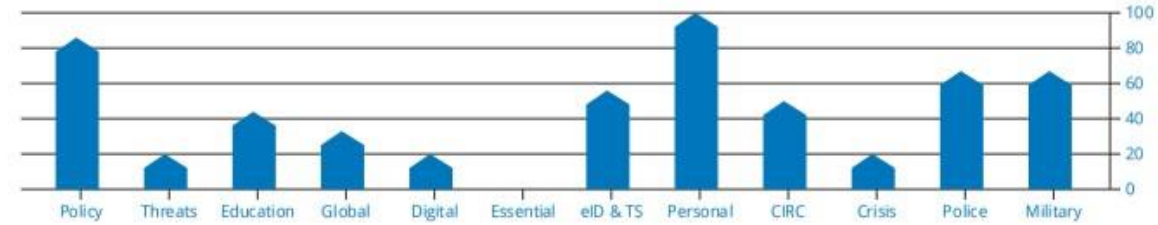
NCSI DEVELOPMENT TIMELINE



RANKING TIMELINE



NCSI FULFILMENT PERCENTAGE



GENERAL CYBER SECURITY INDICATORS

1. Cyber security policy development	6	7	(86%)
1.1. Cyber security policy unit		3	
1.2. Cyber security policy coordination format		2	
1.3. Cyber security strategy		1	
1.4. Cyber security strategy implementation plan	0	1	
2. Cyber threat analysis and information	1	5	(20%)
2.1. Cyber threats analysis unit	0	3	
2.2. Public cyber threat reports are published annually	0	1	
2.3. Cyber safety and security website		1	
3. Education and professional development	4	9	(44%)
3.1. Cyber safety competencies in primary or secondary education	0	1	
3.2. Bachelor's level cyber security programme	0	2	
3.3. Master's level cyber security programme		2	
3.4. PhD level cyber security programme	0	2	
3.5. Cyber security professional association		2	
4. Contribution to global cyber security	2	6	(33%)
4.1. Convention on Cybercrime		1	
4.2. Representation in international cooperation formats		1	
4.3. International cyber security organisation hosted by the country	0	3	
4.4. Cyber security capacity building for other countries	0	1	

BASELINE CYBER SECURITY INDICATORS

5. Protection of digital services	1	5	(20%)
5.1. Cyber security responsibility for digital service providers	0	1	
5.2. Cyber security standard for the public sector		1	
5.3. Competent supervisory authority	0	3	
6. Protection of essential services	0	6	(0%)
6.1. Operators of essential services are identified	0	1	
6.2. Cyber security requirements for operators of essential services	0	1	
6.3. Competent supervisory authority	0	3	
6.4. Regular monitoring of security measures	0	1	
7. E-identification and trust services	5	9	(56%)
7.1. Unique persistent identifier		1	
7.2. Requirements for cryptosystems	0	1	
7.3. Electronic identification	0	1	
7.4. Electronic signature		1	
7.5. Timestamping	0	1	
7.6. Electronic registered delivery service	0	1	
7.7. Competent supervisory authority		3	
8. Protection of personal data	4		(100%)
8.1. Personal data protection legislation		1	
8.2. Personal data protection authority		3	

INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Cyber incidents response	3	6	(50%)
9.1. Cyber incidents response unit		3	
9.2. Reporting responsibility	0	1	
9.3. Single point of contact for international coordination	0	2	
10. Cyber crisis management	1	5	(20%)
10.1. Cyber crisis management plan	0	1	
10.2. National-level cyber crisis management exercise	0	2	
10.3. Participation in international cyber crisis exercises		1	
10.4. Operational support of volunteers in cyber crises	0	1	
11. Fight against cybercrime	6	9	(67%)
11.1. Cybercrimes are criminalised		1	
11.2. Cybercrime unit		3	
11.3. Digital forensics unit	0	3	
11.4. 24/7 contact point for international cybercrime		2	
12. Military cyber operations	4	6	(67%)
12.1. Cyber operations unit		3	
12.2. Cyber operations exercise	0	2	
12.3. Participation in international cyber exercises		1	

NCSI
national cyber security index

76. Mexico 36.36

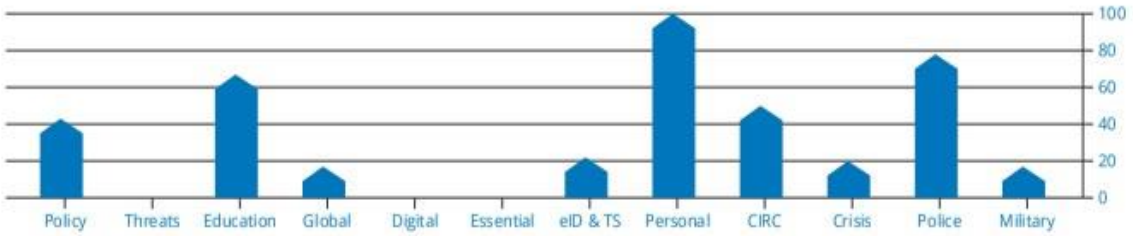
Population	**122.3** million
Area (km²)	**2.0** million
GDP per capita ($)	**20.0** thousand

76th	National Cyber Security Index	36 %
63rd	Global Cybersecurity Index	63 %
87th	ICT Development Index	52 %
76th	Networked Readiness Index	57 %

NCSI DEVELOPMENT TIMELINE

RANKING TIMELINE

NCSI FULFILMENT PERCENTAGE



GENERAL CYBER SECURITY INDICATORS

1. Cyber security policy development	3	7	(43%)
1.1. Cyber security policy unit	0	3	
1.2. Cyber security policy coordination format		2	
1.3. Cyber security strategy		1	
1.4. Cyber security strategy implementation plan	0	1	
2. Cyber threat analysis and information	0	5	(0%)
2.1. Cyber threats analysis unit	0	3	
2.2. Public cyber threat reports are published annually	0	1	
2.3. Cyber safety and security website	0	1	
3. Education and professional development	6	9	(67%)
3.1. Cyber safety competencies in primary or secondary education	0	1	
3.2. Bachelor's level cyber security programme		2	
3.3. Master's level cyber security programme		2	
3.4. PhD level cyber security programme	0	2	
3.5. Cyber security professional association		2	
4. Contribution to global cyber security	1	6	(17%)
4.1. Convention on Cybercrime	0	1	
4.2. Representation in international cooperation formats		1	
4.3. International cyber security organisation hosted by the country	0	3	
4.4. Cyber security capacity building for other countries	0	1	

BASELINE CYBER SECURITY INDICATORS

5. Protection of digital services	0 / 5	(0%)
5.1. Cyber security responsibility for digital service providers	0 / 1	
5.2. Cyber security standard for the public sector	0 / 1	
5.3. Competent supervisory authority	0 / 3	
6. Protection of essential services	0 / 6	(0%)
6.1. Operators of essential services are identified	0 / 1	
6.2. Cyber security requirements for operators of essential services	0 / 1	
6.3. Competent supervisory authority	0 / 3	
6.4. Regular monitoring of security measures	0 / 1	
7. E-identification and trust services	2 / 9	(22%)
7.1. Unique persistent identifier	1	
7.2. Requirements for cryptosystems	0 / 1	
7.3. Electronic identification	0 / 1	
7.4. Electronic signature	1	
7.5. Timestamping	0 / 1	
7.6. Electronic registered delivery service	0 / 1	
7.7. Competent supervisory authority	0 / 3	
8. Protection of personal data	4	(100%)
8.1. Personal data protection legislation	1	
8.2. Personal data protection authority	3	

INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Cyber incidents response	3 / 6	(50%)
9.1. Cyber incidents response unit	3	
9.2. Reporting responsibility	0 / 1	
9.3. Single point of contact for international coordination	0 / 2	
10. Cyber crisis management	1 / 5	(20%)
10.1. Cyber crisis management plan	0 / 1	
10.2. National-level cyber crisis management exercise	0 / 2	
10.3. Participation in international cyber crisis exercises	1	
10.4. Operational support of volunteers in cyber crises	0 / 1	
11. Fight against cybercrime	7 / 9	(78%)
11.1. Cybercrimes are criminalised	1	
11.2. Cybercrime unit	3	
11.3. Digital forensics unit	3	
11.4. 24/7 contact point for international cybercrime	0 / 2	
12. Military cyber operations	1 / 6	(17%)
12.1. Cyber operations unit	0 / 3	
12.2. Cyber operations exercise	0 / 2	
12.3. Participation in international cyber exercises	1	

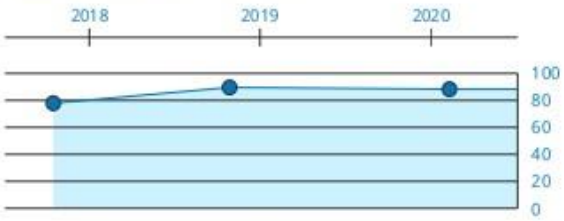
NCSI
national cyber security index

5. Spain 88.31

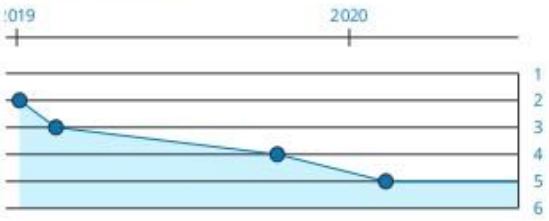
Population	**46.4** million
Area (km²)	**506.0** thousand
GDP per capita ($)	**40.3** thousand

5th	National Cyber Security Index	88 %
7th	Global Cybersecurity Index	90 %
27th	ICT Development Index	78 %
35th	Networked Readiness Index	69 %

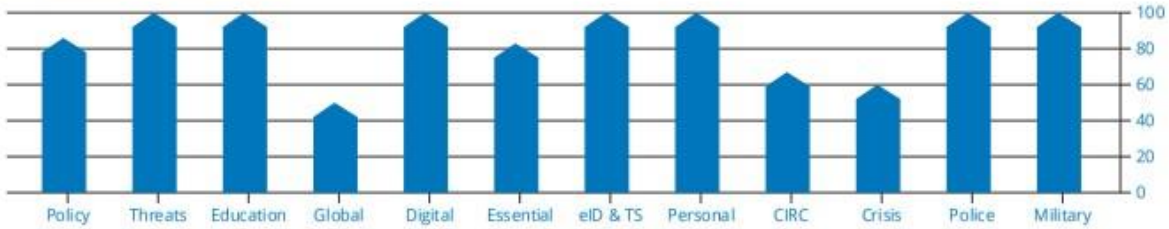
NCSI DEVELOPMENT TIMELINE



RANKING TIMELINE



NCSI FULFILMENT PERCENTAGE



GENERAL CYBER SECURITY INDICATORS

1. Cyber security policy development	6/7	(86%)
1.1. Cyber security policy unit	3	
1.2. Cyber security policy coordination format	2	
1.3. Cyber security strategy	1	
1.4. Cyber security strategy implementation plan	0/1	
2. Cyber threat analysis and information	5	(100%)
2.1. Cyber threats analysis unit	3	
2.2. Public cyber threat reports are published annually	1	
2.3. Cyber safety and security website	1	
3. Education and professional development	9	(100%)
3.1. Cyber safety competencies in primary or secondary education	1	
3.2. Bachelor's level cyber security programme	2	
3.3. Master's level cyber security programme	2	
3.4. PhD level cyber security programme	2	
3.5. Cyber security professional association	2	
4. Contribution to global cyber security	3/6	(50%)
4.1. Convention on Cybercrime	1	
4.2. Representation in international cooperation formats	1	
4.3. International cyber security organisation hosted by the country	0/3	
4.4. Cyber security capacity building for other countries	1	

BASELINE CYBER SECURITY INDICATORS

5. Protection of digital services	5	(100%)
5.1. Cyber security responsibility for digital service providers	1	
5.2. Cyber security standard for the public sector	1	
5.3. Competent supervisory authority	3	
6. Protection of essential services	5 / 6	(83%)
6.1. Operators of essential services are identified	1	
6.2. Cyber security requirements for operators of essential services	1	
6.3. Competent supervisory authority	3	
6.4. Regular monitoring of security measures	0 / 1	
7. E-identification and trust services	9	(100%)
7.1. Unique persistent identifier	1	
7.2. Requirements for cryptosystems	1	
7.3. Electronic identification	1	
7.4. Electronic signature	1	
7.5. Timestamping	1	
7.6. Electronic registered delivery service	1	
7.7. Competent supervisory authority	3	
8. Protection of personal data	4	(100%)
8.1. Personal data protection legislation	1	
8.2. Personal data protection authority	3	

INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Cyber incidents response	4 / 6	(67%)
9.1. Cyber incidents response unit	3	
9.2. Reporting responsibility	1	
9.3. Single point of contact for international coordination	0 / 2	
10. Cyber crisis management	3 / 5	(60%)
10.1. Cyber crisis management plan	0 / 1	
10.2. National-level cyber crisis management exercise	2	
10.3. Participation in international cyber crisis exercises	1	
10.4. Operational support of volunteers in cyber crises	0 / 1	
11. Fight against cybercrime	9	(100%)
11.1. Cybercrimes are criminalised	1	
11.2. Cybercrime unit	3	
11.3. Digital forensics unit	3	
11.4. 24/7 contact point for international cybercrime	2	
12. Military cyber operations	6	(100%)
12.1. Cyber operations unit	3	
12.2. Cyber operations exercise	2	
12.3. Participation in international cyber exercises	1	

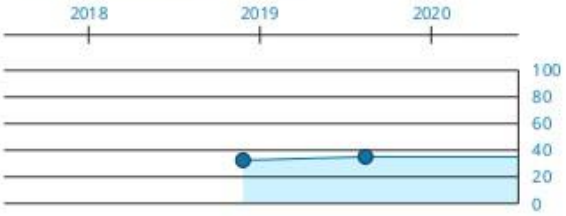
NCSI
national cyber security index

79. Ecuador 35.06

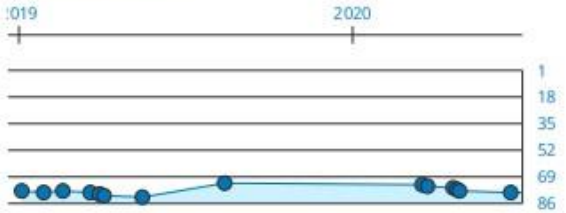
Population	**16.5** million
Area (km²)	**276.8** thousand
GDP per capita ($)	**11.8** thousand

79th	National Cyber Security Index	35 %
98th	Global Cybersecurity Index	37 %
97th	ICT Development Index	48 %
82nd	Networked Readiness Index	56 %

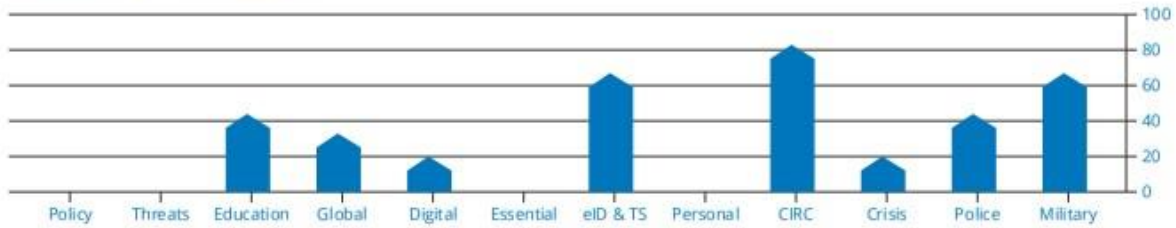
NCSI DEVELOPMENT TIMELINE



RANKING TIMELINE



NCSI FULFILMENT PERCENTAGE



GENERAL CYBER SECURITY INDICATORS

1. Cyber security policy development	0	7	(0%)
1.1. Cyber security policy unit	0	3	
1.2. Cyber security policy coordination format	0	2	
1.3. Cyber security strategy	0	1	
1.4. Cyber security strategy implementation plan	0	1	
2. Cyber threat analysis and information	0	5	(0%)
2.1. Cyber threats analysis unit	0	3	
2.2. Public cyber threat reports are published annually	0	1	
2.3. Cyber safety and security website	0	1	
3. Education and professional development	4	9	(44%)
3.1. Cyber safety competencies in primary or secondary education	0	1	
3.2. Bachelor's level cyber security programme	0	2	
3.3. Master's level cyber security programme		2	
3.4. PhD level cyber security programme	0	2	
3.5. Cyber security professional association		2	
4. Contribution to global cyber security	2	6	(33%)
4.1. Convention on Cybercrime	0	1	
4.2. Representation in international cooperation formats		1	
4.3. International cyber security organisation hosted by the country	0	3	
4.4. Cyber security capacity building for other countries		1	

BASELINE CYBER SECURITY INDICATORS

5. Protection of digital services	1 / 5	(20%)
5.1. Cyber security responsibility for digital service providers	0 / 1	
5.2. Cyber security standard for the public sector	1 / 1	
5.3. Competent supervisory authority	0 / 3	
6. Protection of essential services	0 / 6	(0%)
6.1. Operators of essential services are identified	0 / 1	
6.2. Cyber security requirements for operators of essential services	0 / 1	
6.3. Competent supervisory authority	0 / 3	
6.4. Regular monitoring of security measures	0 / 1	
7. E-identification and trust services	6 / 9	(67%)
7.1. Unique persistent identifier	1 / 1	
7.2. Requirements for cryptosystems	0 / 1	
7.3. Electronic identification	0 / 1	
7.4. Electronic signature	1 / 1	
7.5. Timestamping	1 / 1	
7.6. Electronic registered delivery service	0 / 1	
7.7. Competent supervisory authority	3 / 3	
8. Protection of personal data	0 / 4	(0%)
8.1. Personal data protection legislation	0 / 1	
8.2. Personal data protection authority	0 / 3	

INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Cyber incidents response	5 / 6	(83%)
9.1. Cyber incidents response unit	3 / 3	
9.2. Reporting responsibility	0 / 1	
9.3. Single point of contact for international coordination	2 / 2	
10. Cyber crisis management	1 / 5	(20%)
10.1. Cyber crisis management plan	0 / 1	
10.2. National-level cyber crisis management exercise	0 / 2	
10.3. Participation in international cyber crisis exercises	1 / 1	
10.4. Operational support of volunteers in cyber crises	0 / 1	
11. Fight against cybercrime	4 / 9	(44%)
11.1. Cybercrimes are criminalised	1 / 1	
11.2. Cybercrime unit	0 / 3	
11.3. Digital forensics unit	3 / 3	
11.4. 24/7 contact point for international cybercrime	0 / 2	
12. Military cyber operations	4 / 6	(67%)
12.1. Cyber operations unit	3 / 3	
12.2. Cyber operations exercise	0 / 2	
12.3. Participation in international cyber exercises	1 / 1	

Anexo 2. Entrevistas

Entrevistado: Dr. Christian Fierro García
Formación: Dr. en Jurisprudencia y experto en Derecho Penal
Nro. Cédula: 1707368344

Tema: El COIP como instrumento de ejecución punitiva en el Ciberespacio

1. **Estimado Dr. Fierro, ¿usted tiene conocimiento de qué es el Ciberespacio?**
    a. *Si Estimado Hugo.*

2. **¿Ha tenido la oportunidad de seguir o defender un caso sobre vulneración de derechos en el Ciberespacio?**
    a. *Si.*

3. **Dr. Fierro, ¿piensa usted que nuestra legislación vigente es eficiente y clara, acerca de cómo actuar sobre delitos que se efectúan en el Ciberespacio?**
    a. *No. Considero que nuestra legislación no ha caminado de la mano del avance tecnológico. Nuestro ordenamiento jurídico legalista, no jurisprudencial ni casuístico, tiene una dependencia absoluta al principio de tipicidad, lo cual hace que, si una norma penal se redacta de manera tal, que restringe los presupuestos que configuran un tipo penal a una situación muy en específica, dicha norma resulta insuficiente para enmarcar nuevas conductas que van acordes al avance tecnológico. Lo cual podría contribuir a la impunidad.*

4. **A su criterio, ¿los artículos del COIP, referentes a delitos informáticos, son suficientes para controlar a la delincuencia que actúa en el Ciberespacio?**
    a. *No. Puesto que, por su exagerada especificación de las conductas que se consideran antijurídicas, caen en el error de dejar por fuera nuevas conductas. Por ejemplo, si una norma, prevé que falsificar papel moneda es*

un delito, excluye la posibilidad de que, falsificar dinero electrónico sea una conducta penalmente relevante.

5. **De acuerdo a su experiencia en materia penal, ¿el Ciberespacio se encuentra lo suficientemente normado?**
    a. *No. Nuestra legislación está retrasada en esta materia. Al punto que ni siquiera existen normas claras y precisas respecto a cómo recabar y practicar la prueba digital, mucho menos cuenta con normas que prevean todas aquellas conductas que deben ser criminalizadas. Puesto que hay casos donde, por la redacción restringida del legislador, no basta un tipo general, sino que es necesario de tipos más específicos.*

6. **En el escenario actual del mundo, afectado por una pandemia que ha obligado de manera general, a cambiar la rutina de las personas de actividades presenciales a virtuales como por ejemplo teletrabajo, educación virtual, compras por internet, inclusive se habla de telemedicina, etc.; se debe esperar de acuerdo a su experiencia, un crecimiento acelerado de la delincuencia en el ciberespacio?**
    a. *Si. Porque los infractores si avanzan de la mano del avance tecnológico. Ellos si se adecúan con mayor facilidad a la situación. El infractor no se mantiene en una situación de robar viajeros a caballo, cuando ahora viajan en autos y ya no llevan consigo su dinero, sino que lo mantienen en cuentas electrónicas. La ley por el contrario si se mantiene anquilosada y petrificada. Mientras el delincuente está aprendiendo y adquiriendo experiencia en cómo romper la ciberseguridad, la ley hasta el 2014 aún legislaba el duelo.*

7. **¿Dr. Fierro, de acuerdo a la respuesta anterior, se puede enfrentar ese posible crecimiento?**
    a. *Hay ciertos tipos penales a los cuales se pueden subsumir esas conductas, pero no son suficientes.*

8. **¿En los casos de delitos ejecutados en el ciberespacio que usted conoce, han sido suficientes de acuerdo a su criterio los artículos presentes en la Legislación Ecuatoriana para su juzgamiento?**
    a. *No, precisamente, la tipicidad específica, ha provocado que, ciertas conductas que deberían merecer reproche no sean juzgadas ni sancionadas.*

9. **¿Dr. Fierro, cómo ha observado usted la sanción de ciberdelitos?**
    a. *Nuestra legislación en materia sancionadora es limitada, puesto que se enfoca en la imposición de penas, mas no en lo restaurativo. Por lo que, deberían preverse sanciones restaurativas, que eviten nuevos ilícitos.*

10. **¿Dr. Fierro usted cree que los afectados por ciberdelitos denuncian los casos, y éstos han sido resueltos, quedan en denuncia; o simplemente los afectados prefieren no denunciarlos?**
    a. *No. Porque como manifesté hay muchas deficiencias normativas en cuanto a cómo recopilar, recabar, conservar, presentar y practicar la prueba de este tipo de delitos. Lo cual, conjuntamente a los altos costos de la materialización notarial o pericial de estas evidencias, y, la falta de procesos penales expeditos, conllevan a que o no se denuncie o las denuncias no logren nada.*

11. **Dr. Fierro, el artículo 140 de la Ley Orgánica de Telecomunicaciones, otorga la rectoría del sector que nos encontramos tratando al MINTEL, cree usted que esta designación mejorará la seguridad en el Ciberespacio?**
    a. *No. Porque, dicha designación es meramente administrativa, y, para personas formales y reguladas. No para quien opera irregularmente ni para materia penal.*

12. **¿Conoce usted si actualmente se cuenta con un protocolo para la gestión de incidentes, o manual de Ciberseguridad que pueda usarse por instituciones públicas o privadas?**

a. *No. Hay un vacío normativo en esta materia.*

Entrevistado: Abg. Jairo Jarrín Farías

Formación: Abogado, experto en Derechos Intelectuales, ex Miembro Principal del Órgano Colegiado de Derechos Intelectuales - OCDI

Nro. Cédula: 1711736700

Tema: Transgresiones de Seguridad en el Ciberespacio

1. **Estimado Abg. Jarrín, ¿usted tiene conocimiento de qué es el Ciberespacio?**
    a. *Sí. Hugo lo conozco.*

2. **¿Ha tenido la oportunidad de seguir o defender un caso sobre vulneración de derechos en materia de propiedad intelectual en el Ciberespacio?** *a. Sí.*

3. **Abg. Jarrín, ¿piensa usted que nuestra legislación vigente es eficiente y clara, acerca de cómo actuar sobre delitos que se efectúan en el Ciberespacio?**
    a. *No es suficiente, aunque debo ser enfático en mencionar que se han realizado cambios en temas de derechos intelectuales a nivel institucional y normativo, como por ejemplo la creación del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, conocido como el Código Ingenios que mejoró sustancialmente el reconocimiento y la protección en derechos intelectuales, además del otorgamiento de nuevas atribuciones e implementación de mecanismos más eficientes para que la Autoridad competente en materia de derechos intelectuales de cumplimiento a sus objetivos y fines..*

4. **A su criterio, ¿la normativa vigente, en referencia a delitos informáticos, es suficiente para controlar los delitos que se efectúan en el Ciberespacio?**

a. *Se tienen herramientas como el código antes mencionado, además el COIP contempla sanciones a delitos de tipo informático. La dificultad o más bien, la complejidad en materia de protección y defensa contra infracciones y delitos en el Ciberespacio es la dinámica de la evolución, tanto en materia de desarrollo tecnológico, y su correlación con el también dinámico desarrollo de conductas antijurídicas.*

5. **De acuerdo a su experiencia en materia de derechos intelectuales, ¿el Ciberespacio se encuentra lo suficientemente normado como para responder a transgresiones que vulneren los derechos de sus integrantes?**

    a. *Los ciudadanos ecuatorianos tienen a su favor leyes que protegen sus derechos intelectuales, las cuales, sin perjuicio del carácter territorial del otorgamiento, reconocimiento y protección, van de la mano con los compromisos que como país tenemos a nivel internacional. No se puede hablar de que el ciberespacio ecuatoriano es un lugar seguro, en ninguna parte del mundo lo es, además y como te he comentado, en el camino de la evolución tecnológica, no van de la mano las transgresiones y la ley. Las leyes se crean en respuesta a las infracciones, la naturaleza misma del derecho penal, el principio de legalidad y la reserva de ley impiden una respuesta en muchos casos, oportuna.*

6. **En el escenario actual del mundo, afectado por una pandemia que ha obligado de manera general, a cambiar la rutina de las personas de actividades presenciales a virtuales como por ejemplo teletrabajo, educación virtual, compras por internet, inclusive se habla de telemedicina, etc.; se debe esperar de acuerdo a su experiencia, un crecimiento acelerado de actos que vulneren derechos en el ciberespacio?**

    a. *Definitivamente sí, el aumento del uso de herramientas tecnológicas, implica el crecimiento de la piratería, el phishing, entre otras. Es necesario también lograr un desarrollo sostenido de las herramientas de seguridad y protección informáticas, pues la capacidad de respuesta normativas no siempre será adecuada, especialmente eficientes, eficaces y oportunas.*

7. **¿Se tienen los instrumentos legales suficientes para enfrentar ese posible crecimiento?**

    a. *Tenemos instrumentos, pero únicamente un proceso de seguimiento y evaluación que establezca la relación entre la norma y la casuística, permitirá más adelante saber si fueron o no suficientes.*

8. **¿En los casos de delitos ejecutados en el ciberespacio que usted conoce, han sido suficientes de acuerdo a su criterio los artículos presentes en la Legislación Ecuatoriana para su juzgamiento?**

    a. *Como antes mencioné no siempre serán suficientes, la tecnología siempre va por delante y hay que notar que los infractores no son gente "improvisada" por así decirlo; son personas expertas y cuentan con herramientas sofisticadas para delinquir.*

9. **¿Abg. Jarrín, qué tan eficiente ha resultado la sanción de ciberdelitos en los que se ha vulnerado los derechos de autor?**

    a. *Puedo manifestar que los ciberdelitos se denuncian en muy poca medida, sin embargo, en los que han sido evidenciados, se ha actuado conforme a la ley; quizá a nivel estadístico, podría anotar que el porcentaje de infracciones accionados -en la vía administrativa- en materia de derechos de autor es inferior a lo que respecto de derechos de propiedad industrial se tramita.*

10. **¿Abg. Jarrín, usted cree que los afectados por ciberdelitos denuncian los casos, y éstos han sido resueltos, quedan en denuncia; o simplemente los afectados prefieren no denunciarlos?**

    a. *Personalmente creo que en general las personas tienen la percepción de que este tipo de infracciones o delitos no se sancionan y por esta razón prefieren no denunciarlos. Adicionalmente, la dinámica de la conducta antijurídica y el mínimo de rastros que deja, deja en mala posición al posible denunciante; en otros casos como el phishing, inclusive se genera "vergüenza" por haber caído en el engaño y la víctima prefiere no denunciar.*

11. **Abg. Jarrín, el artículo 140 de la Ley Orgánica de Telecomunicaciones, otorga la rectoría del sector que nos encontramos tratando al MINTEL, cree usted que esta designación mejorará la seguridad en el Ciberespacio?**

    a. *Creo que mejorará la organización institucional, la seguridad pienso que no. La complejidad del desarrollo del Ciberespacio requiere de coordinación interinstitucional, pues las aristas de este universo son múltiples.*

12. **¿Conoce usted si actualmente se cuenta con un protocolo para la gestión de incidentes, o manual de Ciberseguridad que pueda usarse por instituciones públicas o privadas?**

    a. *Del conocimiento que tengo, no existe. En este sentido, se requiere también concientizar sobre el beneficio del establecimiento de políticas, procesos y procedimientos internos para evitar o dar oportuna respuesta a las amenazas en el Ciberespacio, más aún con el aumento en la utilización de mecanismos virtuales que requieren presencia en el Ciberespacio, en esta nueva "normalidad". Tanto en los sectores público y privado, la protección de datos es fundamental, siendo imprescindible la implementación de estos mecanismos de prevención y respuesta oportuna.*