UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES ESCUELA DE RELACIONES INTERNACIONALES

LA CIBERSEGURIDAD: UNA VISIÓN NACIONAL Y REGIONAL FRENTE A LAS CIBERAMENAZAS EN EL SIGLO XXI

CURSO DE ESPECIALIZACIÓN EN INSTRUMENTOS JURÍDICOS NACIONALES E INTERNACIONALES SOBRE SEGURIDAD DIGITAL EN EL SALVADOR

PARA OBTENER EL TÍTULO DE LICENCIADA EN RELACIONES INTERNACIONALES

PRESENTADO POR:

ADRIANA DANIELA GONZÁLEZ PORTILLO

DOCENTE ASESOR:

JORGE ALBERTO ARANDA

CIUDAD UNIVERSITARIA, SAN SALVADOR, OCTUBRE DE 2021

LA CIBERSEGURIDAD: UNA VISIÓN NACIONAL Y REGIONAL FRENTE A LAS CIBERAMENAZAS EN EL SIGLO XXI

RESUMEN

La ciberseguridad y ciberamenazas representan en la actualidad un nuevo tema de agenda a nivel nacional, regional e internacional que afecta a todos los países del mundo. Sin embargo, la capacidad de los Estados de enfrentar estos nuevos retos depende de condicionantes políticas, económicas y sociales.

A nivel nacional, El Salvador presenta serias debilidades en enfrentar las ciberamenazas provenientes del ciberespacio y en el desarrollo de marcos de acción legales de ciberseguridad. Esto genera que la securitización de la agenda nacional en lo referido a las tecnologías de información sea un marco de acción débil. A nivel regional, América Latina se ubica en las últimas posiciones en los indicadores internacionales de ciberseguridad, lo cual demuestra el déficit que existe como región en la construcción de cibercapacidades y en la regulación del ciberespacio como un nuevo escenario de lucha de intereses.

A nivel estatal todos los países de la región tienen que hacer frente a las ciberamenazas tanto a nivel interno como regional, promoviendo la cooperación y el fortalecimiento de las capacidades a nivel de país, con el objetivo de modernizarse y adaptarse a los nuevos cambios surgidos en el escenario internacional como producto de los procesos globalizadores. El Salvador y la región de América Latina tendrán que mantenerse en constante dinamismo para ir a la vanguardia de los cambios producidos en un sistema internacional cambiante y dinámico.

INTRODUCCIÓN

El presente ensayo tiene como objeto de estudio la ciberseguridad desde una perspectiva nacional y regional ante las amenazas que emergen del ciberespacio como nuevo medio de lucha de poderes. Desdé la década de los 90 y el auge que tuvo la informática moderna se dio una transformación en las estructuras de seguridad de los Estados. Con los nuevos retos identificados por los procesos globalizadores y el surgimiento de nuevas tecnologías, la protección del ciberespacio se ha vuelto un tema prioritario en las agendas nacionales,

regionales e internacionales.

La ciberseguridad es en la actualidad un tema de vanguardia en la agenda de los Estados, sin embargo, este reto no es enfrentado con las mismas posibilidades por parte de los actores del sistema, pues al ser considerado un problema global, cada Estado posee sus estrategias de seguridad. Sin embargo, es evidente la disparidad que existe en el tema de la ciberseguridad, al presentarse una brecha bien marcada entre los países más desarrollados y los subdesarrollados. Aspectos como el acceso a nuevas tecnologías, factores económicos, políticos y sociales son condicionantes que reflejan la capacidad de los Estados en enfrentar las amenazas del ciberespacio.

Las ciberamenazas generan pérdidas económicas masivas, afectan el bienestar de los individuos y generan un desbalance en todas las estructuras de seguridad de los Estados. Con el propósito de conocer el panorama nacional y regional de las ciberamenazas, el ensayo a presentar tiene como principal objeto de estudio la ciberseguridad, partiendo de un análisis a nivel nacional y la carencia de marcos de acción en materia de ciberseguridad hasta analizar el panorama regional, donde América Latina ha sido una región considerada como un eslabón fácil para los diferentes ataques en el marco de las tecnologías de la información.

DEFINICIONES CONCEPTUALES

El complejo mundo del ciberespacio ha adquirido relevancia al determinarse que este también es un medio para la búsqueda y consecución del poder de los Estados frente a otros actores del sistema internacional. El ciberespacio puede definirse como un espacio virtual en el que interactúan sistemas informáticos, redes y todo medio cibernético en el cual no se conocen límites y no tiene una regulación. Es por eso que es considerado como instrumento de poder para los Estados. Joseph Nye politólogo estadounidense creó el término ciberpoder que se define como: "*la habilidad de obtener resultados privilegiados, crear ventajas, o influenciar en eventos a través del uso de recursos electrónicos interconectados en el ciberdominio"*.[1] Esta definición deja en evidencia que el mundo del ciberespacio es considerado como un campo de lucha de poderes.

[1] Juan Manuel Aguilar Antonio, *Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior*. Instituto de Estudios Internacionales Universidad de Chile, (2021). doi:10.5354/0719-3769.2021.57067

El término ciberseguridad se ha vuelto fundamental en las agendas nacionales y en la política internacional. El mismo puede ser definido como la capacidad de proteger dispositivos móviles, computadoras, servidores, redes, sistemas electrónicos y todo equipo informático de diferentes ataques. Como una definición más específica se puede decir que la ciberseguridad hace referencia a la capacidad de los gobiernos, organizaciones y empresas de proteger sus sistemas de seguridad donde se resguarda la información de Estado, datos de los individuos, datos de empresas, entre otra información clasificada a través de la creación de leyes, marcos de acción y cooperación internacional. Es importante decir que la ciberseguridad se ha vuelto uno de los conflictos latentes del siglo XXI y una nueva forma de ejercer poder en el sistema internacional.

Por otro lado, las ciberamenazas son productos de los procesos de modernización de las tecnologías y puede ser definido como el ingenio de hackear u obtener beneficios y cumplimiento de objetivos ilícitos a través de recursos electrónicos, es por ello que siempre que se produce un ciberataque es para el cumplimiento de un objetivo estratégico previamente definido. Lo anterior permite evidenciar la relación que existe entre los tres términos, en el sentido que en el ciberespacio es donde tienen lugar las ciberamenazas y producto de estas surge la ciberseguridad como respuesta a los retos que se enfrentan en el ciberespacio por lo que existe una estrecha relación en estos conceptos y la alteración de uno provocaría la alteración de todos.

CIBERSEGURIDAD Y CIBERAMENAZAS ¿CÓMO ENFRENTA EL SALVADOR ESTE RETO GLOBAL?

Según un estudio realizado en 2017 por Kaspersky Lab la empresa de ciberseguridad global, *El Salvador es el segundo país de Latinoamérica más vulnerable a sufrir un ciberataque.*[2] Esto se debe a varias razones: en primer lugar, El Salvador no posee una ley de ciberseguridad, esto limita el accionar del propio Estado salvadoreño para salvaguardar sus sistemas informáticos y sus estructuras cibernéticas, agregando que el país no tiene una estrategia nacional de ciberseguridad, esto sumado a la limitada capacidad de acción a nivel de país ante

[2] "La ciberseguridad, componente clave la transformación digital", Industria El Salvador, reporte de comunicaciones y telecomunicaciones (El Salvador, 2018). http://industriaelsalvador.com/wp-content/uploads/2019/07/3.-CIBERSEGURIDAD-INDUSTRIAL.-Jos%C3%BAe-G%C3%B3mez.-TIGO.pdf

ciberamenazas.

Pero ante lo expuesto y ante la carencia de normativa legal surge la pregunta ¿cómo enfrenta El Salvador este reto?

Entre los primeros esfuerzos a nivel de país que se realizaron en materia de ciberseguridad, se puede mencionar el papel de la Policía Nacional Civil como parte de la administración pública salvadoreña, la cual es considerada de las primeras instituciones que priorizaron el impulso de la ciberseguridad. Esto gracias al convenio de cooperación técnica y financiera con la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC) donde se brindaron procesos de formación al personal técnico que conformaría la Unidad de Cibercrimen en El Salvador en la cual se reforzaron aspectos como el marco jurídico penal contra las ciberamenazas en El Salvador, la detección de ciberataques y protección de los ordenadores informáticos. Así mismo en el marco del convenio celebrado con la UNODC en el año de 2011, tuvo lugar la creación del grupo de investigación de delitos cibernéticos conformado por el equipo técnico capacitado, este grupo sería la antesala para la creación de la unidad de investigación de delitos informáticos que empieza su accionar en el año 2015.

Estos eran de los primeros esfuerzos a nivel de país en un tema en el que el Estado carecía de conocimientos, de prevención y de control. Esta deficiencia provocó que esta unidad de investigación desde sus inicios careciera de cooperación técnica y financiera. En la actualidad esto ha limitado su accionar y su capacidad de investigación y análisis ante casos de ciberamenazas.

La ciberseguridad iba colocándose como punto de agenda a nivel nacional y ante el limitado desarrollo a nivel de país en estrategias nacionales y medidas legales y técnicas para la detección de ciberamenazas, en el año 2015 con apoyo técnico de la OEA a través de sus comisiones especializadas, se logró crear el Centro de Respuesta ante Incidentes de Seguridad Informática en El Salvador conocido como SAL Cert. Esta institución tiene como objetivo la prevención de ciberamenazas y vulnerabilidades a las estructuras de seguridad del Estado, así mismo ser la organización que coordine con las instituciones públicas y privadas para la detección de amenazas a los sistemas informáticos. Sin embargo, aunque la creación de este centro sí representó un esfuerzo significativo para la prevención y respuesta a incidentes de ciberamenazas; su trabajo no es visibilizado, es decir, no existe un seguimiento y visibilidad

de los resultados del centro, esto limita que se conozca su accionar, sus casos de éxito y qué medidas se implementan para la prevención de ciberataques. Es por ello que a nivel de país no se conoce mayor información sobre el SAL Cert debido a la falta de apoyo técnico operativo y poca rendición de resultados que el mismo centro posee.

Hasta el año 2015 no se contaba con ningún marco jurídico en materia de seguridad cibernética, sin embargo, es menester mencionar que en octubre de 2015 la Asamblea Legislativa aprobó la ley de firma electrónica. Esta ley tuvo un impacto significativo para impulsar el comercio electrónico y las iniciativas de gobierno electrónico en el país. Con esta ley, la firma electrónica, otorgaba validez legal a todos los documentos y mensajes enviados de forma electrónica.

No obstante, tras la aprobación de esta ley surge algo cuestionable, ¿estaba la sociedad civil preparada en materia de educación cibernética para la promulgación e implementación de la misma? La respuesta es no. Y es que al ser una ley donde otorgaba validez jurídica a documentos electrónicos, la autenticidad de los datos y la integridad de los documentos firmados es fundamental, de manera que, al no tener la orientación en el marco del uso de la firma electrónica, el riesgo que representa la exposición a ataques de robo de datos o transferencia inapropiada de datos es sumamente alto.

Aún más en un país donde no existe una ley de ciberseguridad que regule este tipo de relaciones cibernéticas en el marco de lo penal, pues si bien la ley de firma electrónica establece las obligaciones de los proveedores de servicios de certificación, solo se limita a decir “notificar” o “informar” a la unidad de firma electrónica sobre incidentes en materia de ciberseguridad, lo cual en gran medida limita el proceso ante un ataque cibernético. Esto resulta ser muy cuestionable, ya que, al ser conscientes de la vulnerabilidad de los sistemas de la información en el país, haber aprobado la ley de firma electrónica sin una correcta educación a la sociedad civil, regulación, líneas de acción y marcos legales de implementación, por muy novedosa que esta sea representa un riesgo.

Las acciones anteriormente mencionadas si bien tenían sus limitantes representaban un gran esfuerzo a nivel de país. Sin embargo, uno de los esfuerzos más significativos tuvo lugar en el año 2016 cuando se crea la primera ley en el marco de la ciberseguridad. Se trata de la Ley Especial contra Delitos Informáticos y Conexos que representaba la primera ley que integraba

un marco normativo sobre delitos cibernéticos. Esta ley integra 36 artículos, divididos en 5 capítulos, los cuales regulan delitos contra los sistemas tecnológicos de la información, delitos informáticos, delitos informáticos relacionados con el contenido de los datos, delitos informáticos contra niñas y personas discapacitadas y delitos contra el orden económico. En cada uno de estos se establece la sanción penal si este llegará a ejecutarse. Sin embargo, a pesar de que existe un marco regulatorio, 5 años después de esta ley aún no cuenta con un reglamento, esto limita su operatividad y alcance de resultados.

Un aspecto importante es que la ley en sus artículos deja plasmado de forma implícita las infraestructuras críticas que el país prioriza. Entre estas se encuentran: la prestación de servicios de salud, de comunicaciones, sistemas bancarios, entidades financieras, de provisión y transporte de energía y de medios de transporte. Si bien la ley regula la protección de estos servicios, no se cuenta con una legislación específica en el marco de infraestructuras críticas, pues es importante mencionar que esta ley representa el marco regulatorio más integrado sobre ciberseguridad en el país y si bien hace mención de estas infraestructuras aún representa un marco normativo débil.

La ley de delitos informáticos y conexos si representa un avance a nivel de país, sin embargo la forma en que esta ley integra los tipos penales en el ámbito de ciberseguridad, es un reto, por el desafío que presenta el tema en una sociedad donde los conocimientos en el marco de la ciberseguridad son mínimos, generando en los operadores de justicia una limitante para su correcta aplicación penal principalmente en su parte técnica operativa de la investigación del delito, los cuales están condicionadas a la aplicación de actividades técnicas y periciales.

Esta ley pone en punto de discusión que El Salvador por el escaso desarrollo de la investigación en materia de delitos informáticos, se ha limitado de manera significativa práctica de esta ley en lo referido al procesamiento de casos. Por otro lado, debido a la misma falta de concientización y escasa educación en materia de ciberseguridad por parte de la sociedad civil, no se han penalizado delitos por la falta de denuncia por parte de la población. Al menos en los primeros años de vigencia por parte de esta ley e incluso 5 años luego de su aprobación, el poder jurídico de esta ley aun es cuestionable ante la falta de rendición de resultados ante la sociedad civil.

¿QUÉ REGULAN OTRAS LEYES?

Es importante mencionar que a nivel de país la Ley Especial contra Delitos Informáticos y Conexos, es el marco legal más integrado en materia de ciberseguridad. Sin embargo, el Código Penal, en el Capítulo II y desde el artículo 184 regula los delitos relativos a la intimidad. Entre estos se menciona la palabra "soporte informático", lo cual implica que en caso de reportarse una violación de comunicaciones privadas y se dañe o se perjudique la intimidad de un individuo, este artículo regula la violación de comunicaciones privadas. Así mismo en el artículo 216 se menciona la estafa agravada en lo referido a la "transmisión informática de datos" y la manipulación de estos mismos para desarrollar una estafa. Por otro lado, en el artículo 222 hace mención de la manipulación informática de datos bajo intención de daño el cual es penalizado en el orden jurídico salvadoreño, y por último en el artículo 230 sobre apoderarse de soportes informáticos.

En lo referido al código procesal penal, se menciona la obtención y resguardo de información electrónica en su artículo 201 en lo referido a *"cuando se tenga razones fundadas para inferir que una persona posee información constitutiva de delito o útil para la investigación, almacenada en equipos o instrumentos tecnológicos*".[3]

Lo anterior, muestra de forma general que en la normativa penal salvadoreña no se menciona de manera directa la palabra "delito cibernético" cuando debería tener una regulación exacta donde se tipifiquen los delitos cibernéticos y la regulación penal a cada uno de estos. Así mismo se hace caso omiso de la mención de ciberamenazas a infraestructuras críticas, las cuales representan el aparato administrativo del propio Estado y por tanto la seguridad de estas en un mundo cada vez más digitalizado y propenso a caer en riesgos cibernéticos, debería ser regulado penalmente.

Las leyes mencionadas anteriormente, desde el Código Penal hasta la Ley de Delitos Informáticos y Conexos, representan un avance significativo pues de manera general se han aprobado directrices en el marco de la ciberseguridad y regulación del ciberespacio, sin embargo, el análisis radica en que El Salvador no tiene un marco integrado de ciberseguridad, sino que su regulación se basa en varias disposiciones establecidas en diferentes leyes o documentos secundarios. Al respecto, se cuenta con la Estrategia de Gobierno Digital, desarrollada en el año de 2018, que abarca un trabajo continuo hasta el año 2022. Esta

[3] Código Procesal Penal (El Salvador: Asamblea Legislativa de EL Salvador, 1983), articulo 201.

estrategia tiene por objetivo aprovechar el desarrollo de las nuevas tecnologías para la modernización de la administración pública. Sin embargo, en este proceso de modernización se presentan retos nacionales que no se tienen presentes como las ciberamenazas, por lo que aún la aprobación de esta estrategia dejó de lado la creación de marcos de protección y recurso humano preparado para accionar ante casos de ciberamenazas. Aún más importante se pasó por alto la creación de una política de ciberseguridad nacional que hiciera partícipe de forma integral el sector público y privado para fomentar la cooperación nacional en el ámbito de ciberseguridad.

DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE CIBERSEGURIDAD EN AMÉRICA LATINA

Luego de estudiar a nivel general el panorama nacional relativo a las ciberamenazas, a partir de ahora el estudio estará centrado en América Latina. Al respecto, puede mencionarse que el problema principal radica en la brecha de ciberseguridad que existe en la forma en que se enfrentan las ciberamenazas en países de América Latina. Para realizar un análisis a nivel regional es necesario hacerlo con base en mediciones internacionales como el Índice Global de Ciberseguridad (GCI) realizado por la Unión Internacional de Telecomunicaciones (ITU) y el Índice Nacional de Ciberseguridad de la E- Governance Academy o National Cyber Security Index (NCSI) por sus siglas en inglés. Ambos realizan su diagnóstico basándose en una serie de indicadores de cumplimiento.

Haciendo el primer diagnóstico sobre la base del Índice Global de Ciberseguridad, sus mediciones se basan en dar cumplimiento a la Agenda Global de Ciberseguridad creada por la ITU, donde América Latina en los años *2018-2019 del 0 al 100% tuvo una calificación de 28.8% solo por debajo de los continentes de África y Oceanía, en los siguientes años se ha mantenido en el mismo rango, con algunos cambios positivos en el 2020. Con respecto al Índice Nacional de Ciberseguridad que va siempre en promedio del 0 al 100% y corresponde a la construcción de cibercapacidades de defensa nacional, los países de América Latina se encuentran en el rango de medición de 27.7 para el año 2019 poniendo a la región en la quinta posición ubicándose en los últimos puestos*.[4] Estos indicadores internacionales de

[4] Juan Manuel Aguilar Antonio, *La brecha de ciberseguridad en América frente al contexto global de ciberamenazas*, Revista de Estudios en Seguridad Internacional, (México: Universidad Nacional Autónoma de México, 2020) ,30-40 Comparativo regional y global entre ponderaciones del GCI (2018) y el NCSI (2019).

medición permiten evidenciar los retos que enfrenta la región en el contexto de las ciberamenazas. El problema radica en que América Latina enfrenta problemas estructurales como marcos políticos débiles, poca modernización del aparato estatal, atraso tecnológico, menor desarrollo económico y sobre todo carece de marcos de acción regulatorios en el marco de la ciberseguridad.

ACCIONAR DE PAÍSES MEJORES EVALUADOS EN EL 2020: INSTRUMENTOS NACIONALES E INTERNACIONALES DE CIBERSEGURIDAD, ESTRATEGIAS Y ESFUERZOS

En el 2020 los países mejores evaluados de América Latina en el Índice Global de Ciberseguridad fueron Brasil, México, Uruguay, República Dominicana y Chile.[5] Según las mediciones de indicadores internacionales, Brasil fue el país mejor evaluado en América Latina ocupando el puesto número 18 en el año 2020 en el ranking respaldado por la Unión Internacional de Telecomunicaciones. Ante esto es necesario conocer la hoja de ruta que ha logrado que ascienda 53 puestos en el Índice Global de Ciberseguridad. Como parte de sus iniciativas, en el año 2020 se aprobó su estrategia nacional de ciberseguridad estableciendo un consejo nacional de Ciberseguridad.

Consecuentemente, el Equipo de Respuesta ante Emergencias Informáticas CERT ha logrado tener un trabajo articulado con la empresa privada y organismos nacionales logrando una coordinación para proteger y detectar ciberamenazas. Asimismo, la cultura de ciberseguridad que tienen los habitantes y la promoción de educación en materia de seguridad cibernética, cursos especializados y la inversión en proteger las infraestructuras críticas han logrado que la lucha contra las ciberamenazas pueda ser un trabajo respaldado política, social y económicamente.

Otro país que ha logrado un avance en las mediciones internacionales ha sido México el cual logró ascender de forma significativa ubicándose en el lugar 52 en el ranking gracias a iniciativas como la creación de una estrategia nacional de seguridad y contar con un equipo de respuesta ante emergencias cibernéticas que ha logrado una buena articulación de esfuerzos

https://revistaei.uchile.cl/index.php/REI/article/view/57067

[5] Latinamerica Tech: ¿Cómo se coloca América Latina en el índice global de Ciberseguridad 2020?, acceso 20 de agosto de 2021, http://www.latinamerica.tech/es/2021/07/26/como-se-coloca-america-latina-en- el-indice-global-de-ciberseguridad-2020/.

para hacer frente a las ciberamenazas. Sin embargo, en México no se cuenta con leyes específicas para hacer frente a algunas amenazas como el delito informático y no se posee el respaldo político de las acciones tomadas y un marco coercitivo que ayude a controlar las amenazas surgidas del ciberespacio. Estas y otras deficiencias principalmente en el manejo de crisis en casos de ataques informáticos referente a la organización y coordinación entre instituciones involucradas, el carecer de marcos legales y un sistema de justicia penal preparado, tuvo como consecuencia que México solo ascendiera al puesto 52 en el ranking global.

En el caso de Uruguay, al ser el tercer país mejor evaluado de América Latina, como estrategia país cuenta con un plan de gobierno electrónico 2020 y con algunos marcos legales regulatorios referente al delito cibernético. En ese sentido, *el país cuenta con legislación sobre la protección de datos personales y privacidad, cifrada en la Ley Nº 18.331, que se aplica a las bases de datos de los sectores público y privado*.[6] Sin embargo, la estrategia que ha tenido mayor relevancia es la creación del proyecto "Fortalecimiento de la ciberseguridad en Uruguay" y el Marco de Ciberseguridad de Uruguay (MCU) que ha logrado cooperación técnica y financiera en lo relacionado con ciberseguridad nacional convirtiéndose en el primer país de Latinoamérica en apostarle a proyectos que refuercen las estructuras de ciberseguridad del Estado.

También se debe hablar de República Dominicana que ha logrado un avance significativo en las mediciones realizadas con la puesta en marcha de la estrategia nacional de ciberseguridad dando énfasis en la protección de infraestructuras críticas nacionales y al crear legislaciones específicas que aborden algunas ciberamenazas tales como *la Ley N° 53-07301 sobre Crímenes y Delitos de Alta Tecnología y la Ley N° 172- 13,302 cuyo objetivo es "la protección integral de los datos personales*".[7]

En el caso de Chile, es considerado como el último país mejor evaluado de la región por haber establecido su estrategia nacional de ciberseguridad y su política de ciberseguridad, lo cual lo coloca en buenos niveles de desarrollo en la creación de cibercapacidades así como en el establecimiento de marcos legales que protejan los datos personales la penalización de los

[6] "*Ciberseguridad: Riesgos avances y el camino a seguir en América Latina y El Caribe*", OEA & BID, Reporte ciberseguridad, (2020):171. www.observatoriociberseguridad.com
[7] Ibid. 146-149.

delitos informáticos y la protección de la propiedad intelectual como una de sus estrategias prioritarias.

Esta descripción de manera general permite analizar que los países mejor evaluados en el Índice Global de Ciberseguridad del año 2020 tienen en común aspectos tales como: cuentan con una estrategia nacional de ciberseguridad a excepción de Uruguay, sin embargo, todos poseen un marco de regulación para las infraestructuras críticas junto al establecimiento de marcos legales para ciberamenazas específicas y regulación en las leyes nacionales y marcos penales para los ciberdelitos. No obstante, se observa una deficiencia y es que de estos países mejores evaluados solo República Dominicana pertenece al único tratado internacional de ciberseguridad que es el Convenio de Budapest, de manera que, si bien han desarrollado estrategias nacionales, no han tomado como prioridad la cooperación regional e internacional como una visión y compromiso compartido para hacer frente a las ciberamenazas.

COOPERACIÓN REGIONAL: EL PAPEL DE LA ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA) EN MATERIA DE CIBERSEGURIDAD Y PREVENCIÓN DE CIBERAMENAZAS EN AMÉRICA LATINA

La Organización de Estados Americanos (OEA), representa uno de los principales foros políticos para la región, por lo cual, ha priorizado su estrategia de ciberseguridad aproximadamente desde el año 2002. Pues desde entonces se han establecido iniciativas tales como conformar un grupo de expertos gubernamentales sobre delitos cibernéticos, crear instancias como la Comisión Interamericana de Telecomunicaciones (CITEL) y el Comité Interamericano contra el Terrorismo (CICTE) y el compromiso de desarrollar una estrategia Interamericana Integral para combatir las ciberamenazas en el ciberespacio.

El papel de la CITEL, ha sido significativo para promover la cooperación en materia de ciberseguridad y protección de estructuras críticas tales como telecomunicaciones, sistemas de suministro eléctrico, transporte, bancos, sistemas financieros, servicios gubernamentales y judiciales, entre otros, de los que depende el funcionamiento del aparato estatal. Por lo que la CITEL se encarga de formulación de políticas y regulaciones bajo la emisión de guías y mejores prácticas nacionales y regionales en materia de ciberseguridad. También es importante mencionar que desde la CITEL se crean carpetas técnicas para el desarrollo de tecnologías para la prevención y preparación de las infraestructuras críticas. Sin duda alguna

el papel de la CITEL es estratégico para el aumento de la sinergia entre todos los organismos regionales, nacionales e internacionales para impulsar el desarrollo de políticas de ciberseguridad, principalmente para la protección de estructuras críticas a nivel interno de los países latinoamericanos y para la elaboración de estrategias nacionales que tienen como objetivo hacer frente a las ciberamenazas.

En lo que al Comité Interamericano contra el Terrorismo (CICTE) respecta, se tiene que *se cuenta con un programa de ciberseguridad el cual está consolidado como líder regional en la provisión de iniciativas de investigación, fortalecimiento de la capacidad técnica y desarrollo de políticas de ciberseguridad en las Américas*.[8] De manera articulada con la CITEL, reconocen que el ciberespacio representa un nuevo lugar para el desarrollo de intereses y juegos de poderes entre los Estados y se convierte en un constante reto para salvaguardar la seguridad del Estado-Nación. Es por ello que el CICTE ha acompañado la conformación de Equipos de Respuesta para Emergencias Informáticas por sus siglas (CERTS) en países como *Colombia, Costa Rica, Guatemala, República Dominicana, Chile, Belice, Uruguay, Perú, El Salvador, Venezuela, Trinidad y Tobago*.[9] Estos representan algunos de los países que han logrado contar con un equipo técnico especializado para respuestas informáticas.

Por otro lado, a través de la CICTE se han desarrollado Equipos de Respuestas a Incidentes de Seguridad Informática CSIRT Américas, una plataforma que permite la cooperación regional y la interacción con todos los países que poseen un CSIRT con el objetivo de intercambiar buenas prácticas e información. Al respecto, son acerca de 22 centros los que interactúan en esta plataforma para identificar posibles puntos de riesgo y ciberamenazas en la región, principalmente de grupos que actúan a través de métodos como el malware y ciberespionaje. Un logro importante fue que durante el cuarto periodo de sesiones en el año de *2004 se adoptó la Declaración de Montevideo con el objetivo de tener un compromiso político para combatir las amenazas terroristas de todo tipo e identificar amenazas a la seguridad cibernética de los Estados.*[10]

[8] "Programa de ciberseguridad del CICTE", Organización de Estados Americanos OEA. acceso el 23 de agosto de 2021, http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp.
[9] Ibid.
[10] *Una Estrategia Interamericana Integral de Seguridad Cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética*, Resolución y Anexo A. Asamblea General de la OEA, (2004).

También la CICTE ha destacado por apoyar en la creación de capacidades de estos equipos nacionales brindando apoyo técnico para desarrollar cibercapacidades, y en el establecimiento de políticas o estrategias nacionales de ciberseguridad. Esto ha sido uno de los resultados más evidentes ya que a principios de 2020, *12 países habían aprobado estrategias nacionales de ciberseguridad, incluidos Colombia (2011 y 2016), Panamá (2013), Trinidad y Tobago (2013), Jamaica (2015), Paraguay (2017), Chile (2017), Costa Rica (2017), México (2017), Guatemala (2018), República Dominicana (2018), Argentina (2019) y Brasil (2020*),[11] entre otros en progreso, lo cual ha representado un avance significativo para algunos países de la región. Si bien existen retos como establecer en sus legislaciones nacionales la tipificación y penalización de los delitos de ciberamenazas, hasta la fecha se ha logrado que algunos países puedan aumentar sus capacidades de ciberdefensas a través de la CICTE.

Otro esfuerzo significativo en materia de ciberseguridad es que a través de la CITEL y el CICTE en coordinación con los ministros de justicia de las Américas (REMJA), lograron que en el año 2004 los Estados Miembros de la OEA dieran su visto bueno al aprobar en la Asamblea General el documento Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética. Al respecto se estableció que, los Estados miembros de la OEA *están comprometidos, en el marco de este proyecto a fomentar una cultura de seguridad cibernética que disuada el uso indebido de la Internet y los sistemas de información asociados e impulse el desarrollo de redes de información que sean de confianza y fiables*.[12] Esto se logró gracias a los estudios especializados por la CITEL, CICTE y REMJA que son los entes encargados de coordinar las acciones de esta estrategia.

El enfoque principal de esta estrategia es poder crear una cultura de seguridad cibernética en todos los países miembros de la OEA. Asimismo, la estrategia reconoce que tanto a nivel individual como estructural es necesario establecer marcos eficaces de protección de redes y sistemas de información en equipos informáticos. Además, promueve de forma activa la formulación de políticas y adopción de legislación sobre ciberamenazas para la protección efectiva de las estructuras críticas de los Estados como una prioridad en el tema de ciberseguridad. También la estrategia busca fomentar en los países la detección y eliminación

[11] OEA & BID, Reporte Ciberseguridad, 13.
[12] Asamblea General de la OEA, Una Estrategia Interamericana Integral de Seguridad Cibernética, Resolución y Anexo A, (2004).

de diferentes delitos informáticos que ponen en jaque las estructuras de seguridad de los Estados y la de sus habitantes. Esta estrategia dispone de todas estas acciones, pero haciendo un llamado para respetar la privacidad de los derechos individuales de los usuarios de Internet.

Así mismo la CITEL se compromete en la adopción de normas y brindar asistencia técnica a los países, con el objetivo de mejorar las capacidades de estos en tecnologías de la información y prevención de ciberamenazas. Como resultado de esto *hasta el 2019 se había logrado adoptar 309 propuestas interamericanas (IAPs) que fueron expuestas en la Conferencia Mundial de Radiocomunicaciones, y tuvieron una aceptación del 98%.*[13] Todas estas propuestas representan los intereses de los Estados de la OEA en lo relacionado con ciberseguridad y protección de las telecomunicaciones. Así mismo la CITEL logró establecer un proyecto llamado aulas digitales para reducir la brecha existente en Latinoamérica en acceso y manejo de las tecnologías de la información.

Lo anteriormente descrito deja en evidencia que a través de la OEA y las instancias creadas en materia de ciberseguridad y protección de ciberamenazas se han logrado avances significativos que ayudan a mejorar las capacidades de la región. La OEA ha tenido como objetivo que los países puedan comprometerse en lo relacionado con la ciberseguridad. Sin embargo, persisten las diferencias entre la prioridad que le dan al ciberespacio los diferentes países, eso queda reflejado en los indicadores y ranking internacionales. Por otra parte, el papel que la OEA ha desempeñado como organismo regional ha sido determinante para potenciar diferentes iniciativas que comprometan a todos los países miembros a impulsar la cooperación regional en materia de ciberseguridad coordinando diferentes acciones que contribuyan a la creación de cibercapacidades en la región Latinoamericana.

INSTRUMENTOS JURÍDICOS INTERNACIONALES: EL PAPEL DEL CONVENIO DE BUDAPEST UN RETO PARA LOS PAÍSES DE AMÉRICA LATINA

El surgimiento de las ciberamenazas ha ocasionado que el derecho internacional emita responsabilidades legales para regular estas nuevas amenazas en el marco de las TIC, adaptándose a los cambios producidos por las nuevas tecnologías en las relaciones entre los Estados y sus nacionales y entre otros sujetos que interactúan en el escenario internacional.

[13] Graciela Piedras, *Promoviendo cooperación en materia de ciberseguridad y protección de la infraestructura crítica*, especialista senior de telecomunicaciones CITEL (Foro Regional de la UIT para las Américas sobre Ciberseguridad).

Desde el derecho internacional se han emitido disposiciones legales que regulan el accionar de los Estados en el mundo digital. De igual manera, las organizaciones internacionales y regionales han tenido un papel importante en la emisión de resoluciones y declaraciones que son elementos de derecho internacional que regulan el ciberespacio como ejemplo la OEA. Sin embargo, en lo relacionado a normativa internacional, como único referente se tiene el caso de la Convención de Budapest del año 2001 que fue impulsado por el Consejo de Europa. La Convención de Budapest es a la fecha el único tratado internacional en lo referente al tema de ciberseguridad que persigue incrementar la cooperación y compromiso de los Estados para que puedan adoptar en sus legislaciones nacionales disposiciones penales y regulatorias en lo referido a las ciberamenazas para que los países puedan tener jurisdicción en los delitos cibernéticos en sus territorios.

A nivel de América Latina solamente 8 países se han adherido a dicha Convención según el reporte de ciberseguridad 2020. En ese sentido, los Estados latinoamericanos parte de la Convención son República Dominicana, Panamá, Costa Rica, Colombia, Perú, Chile, Argentina y Paraguay. Este dato resulta preocupante pues esta Convención constituye el único tratado internacional en materia de ciberseguridad razón por la cual, adquiere una relevancia a nivel mundial por su contenido fundamentado en tres ejes estratégicos. Al respecto, el primero es: los delitos informáticos y su penalización según sus tipos; el segundo la creación de normas procesales en lo referido a penalizar cualquier delito que sea cometido en medios informáticos de cualquier tipo, y por último, el fomento a la cooperación internacional en lo referido a compartir información y en la creación de buenas prácticas.

Hacer un análisis a nivel regional permite reflexionar sobre la situación de ciberseguridad en América Latina y es que si bien la región ha tenido avances significativos sigue ostentando los últimos puestos en las mediaciones internacionales de cibercapacidades, esto deja en evidencia la brecha regional que presenta la región en la construcción de cibercapacidades, esto principalmente por cuestiones estructurales como la falta de voluntad política por parte de los gobernantes en establecer marcos efectivos de regulación y acción a las estructuras informáticas las cuales inciden de manera directa en la seguridad nacional de los países de América Latina.

Un notable avance en esta materia lo ha impulsado la OEA a través de sus comisiones especializadas que han sido fundamentales en apoyo técnico operativo y financiero a

diferentes países, esto deja en evidencia que la cooperación regional ha impulsado la creación de cibercapacidades teniendo un papel directo en el fortalecimiento a la ciberseguridad. Sin embargo, esto no es suficiente pues se necesita un trabajo articulado entre todos los actores, desde gobierno, sector privado y sociedad civil, esto a fin de fortalecer a nivel regional los marcos legales de ciberseguridad principalmente legislación especializada en protección de las infraestructuras críticas, promover educación especializada en materia de ciberseguridad y contar con líneas de acción para prevención y alerta de ciberamenazas, ante los retos que se desarrollan en el ciberespacio.

CONSIDERACIONES FINALES Y RECOMENDACIONES

El estudio presentado ha permitido identificar que la ciberseguridad y el riesgo de las ciberamenazas son retos globales. Es por ello que, se debe fomentar una mayor cooperación a nivel internacional y regional, involucrando a todos los actores del sistema, así como estableciendo mecanismos de monitoreo y evaluaciones para el cumplimiento de objetivos. La Seguridad internacional ha tomado nuevos desafíos en el marco de la Revolución Tecnológica que se ha suscitado desde la década de los 90. Sumado a los procesos globalizadores, la agenda de seguridad a nivel internacional ahora involucra el mundo del ciberespacio dejando a nivel estatal un nuevo reto frente a fenómenos como el cibercrimen o el ciberespionaje que son parte de las ciberamenazas, por lo que el nivel de respuesta y acción de los Estados a nivel internacional y regional frente a estos nuevos desafíos dependerá de cuestiones tales como: equipos de respuesta ante incidentes informáticos, estrategias nacionales de ciberseguridad, marcos de regulación a los sistemas informáticos de los Estados, equipos capacitados y líneas de acción a nivel estatal que trabajen el tema de ciberseguridad de forma eficiente e integral abarcando al Estado, el sector privado e impulsando la cooperación regional e internacional.

A nivel regional, América Latina se ubica en las últimas posiciones de los principales indicadores internacionales en materia de ciberseguridad, esto demuestra que si bien la región ha avanzado en la creación de su Estrategia Interamericana para Combatir las Amenazas de la Ciberseguridad, establecimiento de marcos legales y cooperación regional a través de la OEA, aún enfrenta un reto grande en lograr resultados eficaces y optimizar las capacidades a nivel regional, esto implica una mayor cooperación a nivel estatal y construcción de alianzas para enfrentar los retos del ciberespacio.

El análisis final a nivel nacional permite evaluar cómo se está enfrentando esta situación a nivel de país. La recopilación y el estudio de información permiten identificar que el país se encuentra en un déficit en lo relacionado con la creación de cibercapacidades, marcos de acción, equipos de respuesta debidamente capacitados, marcos legales débiles y lo más importante una ausencia de marcos regulatorios integrados sobre ciberamenazas y penalización de las mismas.

El Salvador durante el año 2020 ocupó el puesto *111 en el ranking del National Cyber security Index (NCSI) y con un nivel de desarrollo digital del 19.48 de 100, esto representó un número preocupante, sumado que en el ranking del Índice Global de Ciberseguridad (GCI) se posicionó en el número 152. Estos números según los indicadores internacionales de ciberseguridad demuestran que tuvo un retroceso del -18.28 según el NCSI.*[14]

Esta posición a nivel de país en el año 2020 creó una situación de alerta en el marco de la creación de estrategias de ciberseguridad, es por eso que en el mes de abril de 2021 se creó la primera política de ciberseguridad aprobada ese mismo mes, la cual tiene como objetivo sentar las bases para crear un plan nacional de ciberseguridad presentando una serie de estrategias inmersas en la política, entre las cuales se encuentra *la búsqueda y generación de capacidades en ciberseguridad para la persecución del delito en el ciberespacio y la cibercriminalidad, contribuir a la ciberseguridad en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable en apoyo a los intereses nacionales*.[15]

La política pretende desarrollar una estrategia nacional de ciberseguridad con el tiempo, pero ante esto es menester preguntarse, ¿qué mecanismos de resultados y seguimientos tiene esta política? Desde su aprobación en abril de 2021 no se ha presentado ningún mecanismo de seguimiento a las acciones que plantea, no obstante, la propuesta es comprometedora y ambiciosa. Ante esto el Gobierno tiene la obligación y presión de ejecutar cada una de estas acciones y de disponer de financiamiento para cada una de estas. Sin embargo aún no se conoce un mayor avance, pues si bien la política se aprobó a penas en el mes de abril dependerá de la voluntad política de las autoridades centrales en brindar un seguimiento a cada una de las acciones programadas.

[14] Ranking National Cyber Security Index (NCSI), https://ncsi.ega.ee/ncsi-index/
[15] Política de Ciberseguridad. Estrategias. Secretaria de Innovación de la Presidencia, (2021). 6.

El estudio presentado también permitió identificar que es de suma importancia que a nivel del Órgano Ejecutivo y autoridades legislativas se dote de un reglamento a la Ley Especial contra Delitos Informáticos y Conexos, que hasta ahora es la única ley integrada sobre ciberseguridad en el país y al carecer de un reglamento limita su capacidad operativa. Es por eso que hasta este momento, la ley se ha visto limitada en su cometido, lo cual es preocupante debido a que al ser el único marco legal integrado sobre esta materia, las autoridades centrales han dejado un claro vacío al no disponer de un reglamento para la misma y que por la materia sobre la que legisla como lo es los tipos penales relacionados con las ciberamenazas, es fundamental.

Otro punto importante a tener en cuenta es que, hasta este tiempo, El Salvador no forma parte del Convenio de BUDAPEST, ni ha sido invitado a incorporarse, lo cual limita el compromiso de los propios gobiernos, ya que el tratado de Budapest es fundamental como un marco de referencia para la implementación de leyes en materia de ciberseguridad, principalmente en el ámbito penal. En este sentido el Código Penal de El Salvador no menciona los delitos informáticos, únicamente se hacen mención de la palabra "informática" esto limita en gran medida que en el ámbito de lo penal no se defina claramente las ciberamenazas.

Tampoco define de forma clara el procedimiento a seguir en caso de amenazas a sistemas informáticos o ataques informáticos en contra del Estado, por lo que *las disposiciones de estos ordenamientos se aplicarían dejando a la consideración de las autoridades ministeriales y judiciales la valoración de los elementos informáticos involucrados en los injustos penales*,[16] ante la ausencia de regulación clara e integrada en la legislación penal de El Salvador. El llamado es a las autoridades centrales, desde el Órgano Ejecutivo hasta el Legislativo a priorizar y ser parte del único tratado a nivel internacional sobre ciberseguridad el cual se caracteriza por ser el marco de referencia global para la adopción de leyes internas.

Por último y una de las principales debilidades identificadas es que con la aprobación de la Ley Bitcoin la madrugada del 9 de junio de 2021, ante las ciberamenazas, el país se encuentra en una posición muy vulnerable, pues dicha ley constituye el primer reglamento legal para una moneda virtual la cual es considerada de curso legal a nivel nacional a partir del 7 de septiembre según disposiciones por parte del Ejecutivo. En consecuencia, El Salvador se ha

[16] Fiscalía General de la Republica de El Salvador; Oficina de las Naciones Unidas contra la Droga y el Delito para Centroamérica y el Caribe, *Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexo*, (2017).

convertido en el primer país de Latinoamérica y del mundo en considerar el Bitcoin como moneda de curso legal.

Esto representa una amenaza latente para el país por varias razones: la primera, el nivel de desarrollo tecnológico no está en condiciones de poder adquirir una moneda y billetera virtual, pues este influye de manera directa en las estructuras de seguridad de los Estados. En segundo aspecto la legislación en materia de ciberseguridad a nivel de país es mínima, teniendo como marco más integrado la ley de delitos informáticos y conexos la cual no incorpora la penalización de delitos en lo relacionado con el bitcoin, la única regulación existente de la misma es la Ley Bitcoin la cual deja un vacío legal en torno a métodos de ciberseguridad aplicados a las monedas virtuales, a las billeteras digitales y al uso de aplicaciones para el funcionamiento de esta moneda. Por último, la poca conciencia a nivel de las autoridades centrales de los riesgos que representan las criptomonedas como una de las mayores amenazas de ciberseguridad por el vacío legal y por la falta de control estatal que estas presentan.

Lo anterior deja en evidencia que a nivel de país se enfrentan grandes retos en materia de ciberseguridad que van desde crear políticas y estrategias de ciberseguridad, protección de estructuras críticas, ratificación del Convenio de Budapest y buscar cooperación internacional y regional a través de la adopción de tratados, convenios u acuerdos internacionales sobre ciberseguridad y respuesta a ciberamenazas.

Por último y algo fundamental, crear una cultura cibernética, partiendo desde los funcionarios públicos, entidades privadas y la sociedad civil, pues ante las nuevas dinámicas a enfrentar a nivel de país en lo referido a adoptar una moneda digital para curso legal que solo dispone de una ley que aún no tiene reglamento para la autorización del bitcoin a nivel estatal, pone al país en una situación alarmante. Ante esto la capacidad del Estado de hacer frente a esta nueva realidad y de crear marcos de acción en materia de ciberseguridad es fundamental para definir el rumbo que a nivel de país se tomara en la protección del ciberespacio. Sin duda alguna ante un mundo cada vez más globalizado la capacidad de los Estados de modernizarse y adaptarse a las amenazas del ciberespacio será el aspecto fundamental que regirá las relaciones en un sistema internacional dinámico y cambiante.

BIBLIOGRAFÍA

- Aguilar Antonio, Juan Manuel.” “Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior”. (México: Universidad Autónoma de México). 173. https://revistaei.uchile.cl/index.php/REI/article/view/57067
- Aguilar Antonio, Juan Manuel, La brecha de ciberseguridad en América frente al contexto global de ciberamenazas, (México: Universidad Nacional Autónoma de México, 2020). https://revistaei.uchile.cl/index.php/REI/article/view/57067
- Banco Interamericano de Desarrollo (2016). Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe? Washington D.C. Banco Interamericano de Desarrollo. https://observatoriociberseguridad.org/#/home
- Ciberseguridad. Análisis de Latinoamérica. https://ciberseguridad.com/normativa/latinoamerica/#Estrategia_Interamericana_Integral_para_combatir_las_Amenazas_a_la_Seguridad_Cibernetica. Acceso el 25 de agosto de 2021
- Constitución de la República de El Salvador. El Salvador: Asamblea Legislativa de El Salvador, 1983.
- Código Penal de El Salvador. El Salvador: Asamblea Legislativa de El Salvador, 1997.
- Código Procesal Penal de El Salvador. El Salvador: Asamblea Legislativa de El Salvador, 1998
- Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética. Organización de Estados Americanos (2003).
- Estrategia Interamericana de Seguridad Cibernética: Un Enfoque Multidimensional y Multidisciplinario para la creación de una Cultura de Seguridad Cibernética. Organización de Estados Americanos (2004).
- Fiscalía General de la Republica de El Salvador. Oficina de las Naciones Unidas contra la Droga y el Delito para Centroamérica y el Caribe. *Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexo*, 2017.
- Gómez, Josué. “La ciberseguridad, componente clave la transformación digital”. Industria El Salvador, Reporte de comunicaciones TIGO El Salvador. (2018).

- Ley Especial Contra Delitos Informáticos y Conexos de El Salvador. El Salvador: Asamblea Legislativa, El Salvador 2016.
- Latinamerica Tech: ¿Cómo se coloca América Latina en el índice global de Ciberseguridad 2020? Acceso el 20 de agosto de 2021. http://www.latinamerica.tech/es/2021/07/26/como-se-coloca-america-latina-en-el-indice-global-de-ciberseguridad-2020
- Programa de ciberseguridad del CICTE. Organización de Estados Americanos OEA. Acceso el 23 de agosto de 2021. http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp.
- Reporte ciberseguridad 2020 "Ciberseguridad: Riesgos avances y el camino a seguir en América Latina y El Caribe". OEA & BID. (2020). 171. www.observatoriociberseguridad.com
- Tendencias en la Seguridad Cibernética en América Latina y el Caribe y Respuestas de los Gobiernos. Organización de Estados Americanos y Trend Micro (2013).
- Política de Ciberseguridad (El Salvador: Secretaria de Innovación de la Presidencia, 2021). Estrategias. 6.
- Piedras Graciela. "Promoviendo cooperación en materia de ciberseguridad y protección de la infraestructura crítica". Especialista senior de telecomunicaciones. CITEL (Foro Regional de la UIT para las Américas sobre Ciberseguridad).
- Ranking National Cyber Security Index (NCSI). https://ncsi.ega.ee/ncsi-index/
- Serrano Seguro, Antonio. "Ciberseguridad y Derecho Internacional". Revista Española de Derecho Internacional, Universidad de Granada, (2017). 291-299. http://dx.doi.org/10.17103/redi.69.2.2017.2.02