**Importancia de un mecanismo centroamericano homologado en materia de ciberseguridad y la conformación de una ciberdefensa armoniosa**

Lic. José Daniel Desayes Herrera

**Resumen**

Las estrategias estatales de ciberseguridad en la actualidad son de especial relevancia para la supervivencia del Estado y como pilar fundamental de las políticas de seguridad nacional, a nivel internacional se han establecidos planes de acción para mitigar el impacto y afectaciones de la ciberdelincuencia y lo ciberataques teniendo como principal objetivo guarda la información a un nivel micro de los ciudadanos y empresas dentro del territorio nacional, a nivel macro evitar filtraciones de gran relevancia para las instituciones públicas, tales como la información sobre recursos estratégicos y tácticos, a nivel centroamericano no se ha establecido a la fecha un mecanismo avalado regionalmente que trate este tipo de amenazas, pese a ser de especial relevancia en el contexto actual de globalización y era digital donde a diario existen múltiples fugas y filtraciones de información, el establecimiento de un mecanismo y una estrategia de ciberdefensa a nivel centroamericano solidificaría en gran medida los proceso de integración regionales.

**Palabras claves**: Estrategia, ciberseguridad, ciberdefensa, Centroamérica, ciberdelincuencia.

**Introducción**

La ciberseguridad y las medidas que toma el Estado como actor encargado de la seguridad nacional y de los ciudadanos ha tomado en los últimos años un papel sumamente relevante en cuanto al establecimiento de los mecanismo jurídico estratégicos se han adoptado en harás de disminuir la ciberdelincuencia y las afectaciones que esta ocasiona a pequeña y gran escala. Cada día son más populares a nivel internacional las filtraciones de información gubernamental clasificada, robos de cuentas de banco y hacking a importantes instituciones de orden social, civil y económico, en el contexto de una era digital y globalizada que tan vulnerables somos como individuos, país y región

El presente ensayo pretende destacar la importancia de la ciberseguridad y la institucionalización de la misma a través de un mecanismo centroamericano que permita de manera armoniosa y en aras de lograr la integración regional tratar, monitorear y dar solución a esta nueva problemática naciente.

El presente ensayo científico se llevó a cabo en base a la metodología cualitativa, la cual según Sampieri, (2014) consiste en analizar, comparar y describir acontecimientos o sucesos en un contexto natural, de igual forma abarcar los tipos de datos estadísticos o números, pero bajo el estudio de la calidad de actividades.

En esta investigación se llevó a cabo mediante el uso o aplicación de técnicas como revisión de documentos relacionados a la presente temática, páginas web de las organizaciones regionales, entrevistas a expertos relacionados al tema, y análisis de estudios especializados en seguridad, defensa y cibernética conteniendo datos cualitativos y cuantitativos, que conduzcan objetivos relacionados a esta investigación.

Se utilizó técnicas de recopilación y selección de documentos especializados en el tema de seguridad regional centroamericana, ciberseguridad, ciberdefensa y ciberdelincuencia. De igual forma técnicas de registro, análisis y sistematización de la información.

La entrevista en esta investigación se utilizó como mecanismo prioritario para recopilar información por parte de individuos o personas capacitadas o que tengan relación con el tema investigativo, fortaleciendo el contenido del mismo.

En este estudio investigativo se utilizará el método inductivo el cual según Sampieri, (2014) consiste en la formación de una evidencia singular y que sugiere una posibilidad de una conclusión universal, lo cual se expresaría en términos de probabilidades o posibilidades. Por lo que el propio análisis y la recopilación documental nos permitirán delimitar y estimar la convalidación de conceptos en la información para que se pueda obtener un juicio sobre ella.

Así mismo para la realización de este ensayo definiremos conceptos clases para mayor entendimiento de la temática abordada

La seguridad regional según Snedden, (2018) es un sistema donde los Estados articulan normas, relaciones y prácticas con el fin de garantizar su seguridad. Por lo tanto es toda aquella iniciativa que contiene una agenda en común para la estabilidad y desarrollo de sus países como la región en general, optando mecanismos como la homologación de sus intereses en materia de seguridad y defensa. Permitiendo identificar a su vez, los riesgos o amenazas de alto peligro que afecte de manera sistemática a todos los Estados que geográficamente están delimitados en esa región.

Las principales características que posee la seguridad regional según Evans, (2013) se destaca por ser un mecanismo de prevención, gestión y reducción de conflictos o amenazas que puedan incidir o perjudicar la seguridad interna de los Estados y la región. Asimismo, el mismo autor plantea que la seguridad regional, es un reto en materia de integración, durabilidad y eficiencia ya que al momento de plantear una estrategia común para beneficiar a los Estados, surge un conflicto de intereses, que de no tener una mediación o un diálogo constante, la iniciativa no logrará concretarse. Por ende, la seguridad regional debe llevarse a cabo mediante la armonización de mecanismos que ayuden no solamente a obtener los ejes de seguridad deseados, también que los Estados que forman parte de ello se mantengan bajo los lineamientos establecidos.

Por su parte La conceptualización del término de ciberseguridad ha variado de acuerdo a los avances tecnológicos y los riesgos que esta presenta al ser vulnerable ante ciberamenazas o ataques a través del ciberespacio. La Unión Internacional de Telecomunicaciones (ITU) define ciberseguridad como el conjunto de herramientas, políticas, métodos de gestión de riesgos y de seguridad tecnológica que puedan utilizarse para proteger los medios informáticos y los usuarios en el ciberentorno.

Del mismo modo, la Junta Interamericana de Defensa (JID) adjudica el término de ciberseguridad, a todo fundamento que tiene por objetivo la aplicación de medidas de seguridad para la protección y la libertad de acción en el ciberespacio. Agregando a su vez que todo medio informático o bien que forma parte de las Tecnologías de la Información y Comunicación (TIC) tenga condiciones efectivas en su aseguramiento para evitar afectaciones o ataques a sus componentes.

El término de ciberdefensa actualmente se define por sus componentes y áreas de acción cibernética las cuales están estrechamente vinculadas con asuntos de seguridad y defensa de un Estado, además que tradicionalmente este concepto ha sido acogido por organizaciones de carácter militar o dedicado a la seguridad de un Estado. En base a la Junta Interamericana de Defensa, en su Guía de Ciberdefensa (2020) delimita el termino ciberdefensa a toda capacidad de proteger y defender los intereses nacionales frente a ciberamenazas de gran magnitud. De igual forma añade elementos fundamentales o principales características que definen su modo de operación, como la defensiva y ofensiva, manteniendo lazos de cooperación con otras instituciones, principalmente de origen estatal.

El Ministerio de Defensa de Chile enfatiza que la ciberdefensa está delimitada para brindar una repuesta eficiente hacia aquellas áreas que son de vital importancia para el funcionamiento y existencia de un Estado, principalmente aquellas relacionadas a infraestructuras críticas, componentes logísticos y la propia ciudadanía. A su vez, la ciberdefensa por su rol que desempeña en cuidar y proteger los recursos esenciales de un Estado, está estrechamente vinculada a asuntos de seguridad nacional o bien es parte de una política de defensa, por lo tanto, la ciberdefensa debe de caracterizarse por ser un instrumento de constante adaptabilidad hacia los nuevos desafíos y gozar de una capacidad eficiente en su cobertura de defensa hacia los ejes vulnerables de un país ante cualquier ciberamenazas

Aunque no se encuentre una definición concreta en cuanto al término de ciberdelincuencia, podemos partir de acuerdo a la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC) la cual indica que la ciberdelincuencia es aquella acción que ataca principalmente los sistemas, datos y redes, ya sea mediante el uso o contra las Tecnologías de la Información y Comunicación, conocidas como (TIC); del mismo modo, la Comisión Europea desde la Dirección General de Migración y Asuntos de Interior, agrega que la ciberdelincuencia se relaciona con otros delitos como el terrorismo y el crimen organizado, por lo que sus acciones pueden estar comprendidas no solo por un individuo, también por grupos, Estados u organizaciones de alto perfil delictivo.

Por lo que podemos asumir que el aprovechamiento con fines delictivos y perjudicar a la vez los medios relacionados a las TIC, representa una de las principales características que posee la ciberdelincuencia. Asimismo, por los avances tecnológicos de la globalización, se destaca por tener un rápido y continuo desarrollo como amenaza emergente a la seguridad nacional como afirma el Servicio de Seguridad Central de la Agencia de Seguridad Nacional Norteamericana (NSA-CSS) al evaluar su alcance y gravedad de impacto.

La región centroamericana desde el final de los conflictos que ocurrieron en la década de los años 80, han realizado esfuerzos por mantener la paz, la estabilidad y afrontar todo tipo de amenaza que socave la seguridad de los Estados por medio de los principios establecidos en el marco normativo de integración como es el Protocolo de Tegucigalpa. No obstante Centroamérica no se encuentra exenta de tensiones políticas internas que prevalecen en ella actualmente, con el posicionamiento de directrices ideológicas tradicionales como las vertientes ideológicas de izquierda o derecha sumando conflictos externos, como la guerra de las 5G entre EEUU y China, la cual tiene importancia en el desarrollo de nuevas redes móviles de quinta generación y su impacto en la configuración de la internacionalización del internet de las cosas.

La región centroamericana lleva un proceso de modernización en sus diferentes áreas, especialmente cuando se trata de las propias capacidades que posee un Estado. Sin embargo, estas acciones de actualización tecnológica son llevadas a cabo sin el respaldo de una sólida seguridad cibernética lo que conlleva a crear niveles de vulnerabilidad altos y la región puede estar propensa ante un ciberataque por parte de la ciberdelincuencia lo que causaría la perdida de los niveles de seguridad y estabilidad en la región, así como para los propios Estados.

Para que la región centroamericana evite este tipo de escenario necesita contar con instrumentos eficaces en materia de ciberseguridad y ciberdefensa, especialmente con un mecanismo que sea homologado por los Estados y permita la coordinación, articulación y desarrollo de políticas de seguridad cibernética al nivel centroamericano.

Sin embargo, lo único referente a instrumentos de seguridad cibernética son los de orden jurídicos e institucional que posee cada Estado, pero surge el cuestionamiento de que tan eficaces son los instrumentos que tienen los Estados centroamericanos en materia de ciberseguridad o ciberdefensa, sobre todo si estos en realidad son factibles para proteger y neutralizar un ciberataque dirigido hacia un recurso de alto valor estratégico

Los instrumentos de ciberseguridad o ciberdefensa que posee cada Estado centroamericano se adecua con los recursos que estos disponen para emplearlos, creando como resultado una disparidad en seguridad cibernética lo que en algunos casos resta la efectividad, debido que unos Estados poseen mejores capacidades que otros para contar una ciberseguridad y ciberdefensa más factible y en constante actualización, mientras que otros priorizan áreas esenciales para evitar un desgaste en su capacidad económica e institucional como lo expone el MSc. Barberena al explicar que

*“Algunos Estados o bien gobiernos delimitan una guía o programa nacional de cómo abordar la ciberseguridad desde diversos puntos, ya sea de seguridad o protección al individuo, de seguridad económica y política, o bien de seguridad en las infraestructuras críticas lo que a veces resulta en parte bien para los países que lo realizan, pero no eficientemente para hablar de una seguridad concreta en la región”. (Barberena,2021)*

En general los Estados cuentan con instrumentos de ciberseguridad y ciberdefensa, pero se estructuran en base a las condiciones que estos tienen internamente, y mediante sus propios intereses y no colectivamente. Por ende, Centroamérica no cuenta con un mecanismo homologado que ayude a proteger y defender de manera coordinada y armonizada a la región ante un ciberataque.

La falta de un mecanismo homologado al nivel regional se puede abordar en diferentes perspectivas, pero se destaca una variable que constantemente ha permanecido en Centroamérica, sobre todo cuando se trata en temas de integración, y es la falta de una voluntad política.

 La falta de una voluntad política entre los Estados desarticula las posibilidades de establecer una ciberresiliencia centroamericana de manera consensuada, lo que repercute en un aumento de los niveles de inseguridad cibernética para la región al no disponer de una iniciativa que ayude a aumentar las capacidades de protección y defensa ante un ciberataque. La voluntad política es la que define el rumbo de la región como lo expresa el MSc. Padilla

*“Lo primordial es la existencia de una voluntad política y confianza entre los Estados miembros, voluntad que les permita negociar, consensuar y ejecutar estrategias, planes y programas regionales que les permita prevenir y contrarrestar tipo de actividades”. (Padilla, 2021)*

Por lo tanto, la homologación de una ciberseguridad centroamericana representa un reto para los Estados de la región, puesto que se necesita de la voluntad y confianza de todos los Estados para disminuir la brecha de seguridad cibernética, a su vez que permita crear mecanismos eficiente para contrarrestar eficientemente las acciones de la ciberdelincuencia, debido que Centroamérica esta propensa a ataques cibernéticos o bien presentar una mayor vulnerabilidad para aquellos entes que ya han sido víctimas de un ciberataque tal como lo plantea el MSc. Padilla en la entrevista realizada al destacar que

 *“En casos como las organizaciones que se han visto afectadas muchas veces toman la decisión de mantener estos sucesos en secreto; siempre y cuando estos eventos no sean obviados a los usuarios y se mantenga en estricta discreción, y así prevenir repercusiones que comprometan seriamente la organización, es decir el posible flujo de sus usuarios (cuentahabientes) en el caso de bancos; por perder confiabilidad al admitir que sus sistemas fueron burlados y generar desconfianza debido a su exposición a vulnerabilidades de ciberseguridad”. (Padilla, 2021)*

Asimismo, tanto la ciberseguridad como la ciberdefensa requieren de todo un programa completo para lograr sus objetivos de mantener seguro las capacidades tecnológicas de un área estratégica, esto implica el tener condiciones eficientes como los mecanismos institucionales, así como los recursos para sustentar y desarrollar las acciones de respuesta cuando se presente una eventual amenaza cibernética.

Puesto que al implementar una ciberseguridad se está creando una espacio o ambiente de resiliencia o dicho de otra manera una administración del riesgo mediante un sistema de prevención. Lo mismo sucede en el caso de la ciberdefensa, para que esta tenga una buena efectividad necesita disponer de capacidades que le permitan actuar, la ciberdefensa radica comúnmente en las políticas de defensa y está articulada para defender, neutralizar y adaptarse ante cualquier hecho perjudicial del ciberespacio.

Centroamérica por su actualización tecnológica y las nuevas amenazas que operan en la actualidad por medio del ciberespacio, se presenta la necesidad de homologar un mecanismo de ciberseguridad y ciberdefensa, el cual deba ser articulado con las instituciones correspondientes en materia de seguridad nacional y medios tecnológicos. Esto se puede lograr de manera factible puesto que los Estados de la región cuentan con los instrumentos necesarios para consensuar una estrategia en común, tomando énfasis en los mecanismos de orden jurídico, conformado por las constituciones, leyes, códigos, decretos e instituciones gubernamentales que abordan el campo de la ciberseguridad y ciberdefensa.

A manera de ejemplo de una convalidación de estos mecanismos podemos tomar primeramente que los Estados definan y consensen la aceptación de una amenaza para Centroamérica como es la ciberdelincuencia, posterior a ello plantear una repuesta hacia esta problemática demostrándolo en un solo programa regional que abarque de manera unánime los instrumentos que tienen los Estados, los cuales en la actualidad no tienen un solo parámetro que homologue una sola acción tal como hace referencia el MSc. Padilla

*“En los países del SICA solo Panamá, Guatemala, Costa Rica y República Dominicana cuentan con una estrategia de ciberseguridad. En el caso de la Estrategia Nacional de Seguridad Cibernética de Guatemala muestra un panorama global, en el cual evalúa el estado de la seguridad cibernética del país, involucrando a todos los sectores de manera directa o indirectamente”. (Padilla, 2021)*

De igual forma, haciendo énfasis a la convalidación de instrumentos, podemos resaltar que la mayoría de los Estados de la región centroamericana cuentan con un marco legal que les permite de cierta forma actuar y desarrollar iniciativas en seguridad cibernética, como las disposiciones generales y elementos conceptuales de la constitución, y las leyes de ciberdelito que la mayoría de los Estados de la región poseen los cuales a su vez están presentes en esta tesis. También los Estados estos cuentan con ministerios, comandos, direcciones y unidades especializadas en tecnología y seguridad informática, lo que permitiría la habilitación de una cooperación y coordinación de acciones regionales para fortalecer las capacidades de prevención y repuesta ante un ciberataque por medio del ciberespacio.

Igualmente, Centroamérica cuenta con mecanismos de integración que pueden emplear una mayor cooperación y coordinación, como el SICA, teniendo la capacidad de ampliar iniciativas en materia de acuerdos y adopción de compromisos que beneficien a la región, destacándose áreas económicas, políticas y sociales. Por lo que representaría una base sólida para que los Estados logren acercar una homologación en materia de ciberseguridad, sobre todo lo considerable que pueden ser los protocolos y tratados que este dispone como el Protocolo de Tegucigalpa, el Tratado Marco de Seguridad Democrática y las Estrategias de Seguridad regional y Digital, que, a pesar de no contar tangiblemente con el desarrollo de una ciberseguridad, pueden servir para consensuar una iniciativa nueva o que actualice los anteriores mencionados.

También otro de los organismos que se encuentran constituidos para la coordinación e integración regional es la CFAC, la cual impulsa esfuerzos a fin de proporcionar un nivel óptimo de defensa contra aquellas amenazas que perjudiquen a los Estados, lo que resultaría factible para la constitución de una iniciativa en materia de ciberdefensa mutua. Es necesario que la región centroamericana utilice los mecanismos disponibles para lograr un acercamiento y armonización de sus intereses, debido que la ciberseguridad y ciberdefensa representa un reto no solamente en temas de acuerdo y homologación, también en cuanto a las capacidades de los recursos que poseen los Estados, especialmente en la adquisición de medios materiales tecnológicos y el sostenimiento económico, por lo que si llegase a haber una unanimidad en esta materia, resultaría beneficioso para la ampliación de las capacidades en todos los Estados.

Podemos asumir que la región centroamericana posee vulnerabilidades en cuanto a una seguridad cibernética eficiente, debido a que los Estados de la región han realizado algunos esfuerzos en materia de ciberseguridad y ciberdefensa pero de manera propia y no coordinada al nivel regional que los beneficie mutuamente. Sumado a la creciente demanda en la modernización tecnológica de sectores vitales que contribuyen al desarrollo de los Estados ya sea en materia económica, social, institucional y de seguridad, sin que estos cuenten con un mecanismo de ciberseguridad y ciberdefensa que garantice su bienestar.

Ante esto, se presenta la necesidad de una iniciativa regional en materia de ciberseguridad y ciberdefensa la cual establezca mecanismos de coordinación, cooperación, y armonización, que ayude a proteger las capacidades críticas de los Estados y consigo mismo el ciberespacio de las ciberamenazas o de ataques provocados por parte de la ciberdelincuencia. De igual forma se resalta la importancia de la presente investigación para evaluar y estudiar a mayor profundidad esta problemática actual, sobre todo en el contexto actual en cual dependemos cada día más de los avances tecnológicos, representando no solamente ámbitos positivos, también repercusiones graves si no se toman las acciones correctas en materia de seguridad.

Es considerable mencionar que por la operatividad que tiene la ciberdelincuencia, y sus respectivos impactos altamente perjudiciales, el campo de la ciberseguridad y ciberdefensa se aborda principalmente en términos de seguridad nacional y seguridad regional, en este caso se abarca ambos conforme a los instrumentos que tienen los Estados como son sus áreas jurídicas e institucionales y que estos brindan seguridad a los Estados.

No obstante, Centroamérica al no contar con un mecanismo homologado que fortalezca las capacidades de repuesta ante la ciberdelincuencia, se presenta una alta vulnerabilidad o un riesgo ante un ciberataque que degrade los niveles de seguridad y provoque daño a los medios como las comunicaciones interconectadas, los medios digitales o informáticos y los sistemas de servicios básicos.

En efecto, es fundamental o importante que la región centroamericana disponga de un mecanismo homologado en materia de ciberseguridad y ciberdefensa para brindar resiliencia a las capacidades de los Estados y prevenir cualquier incidente que pueda darse en el ciberespacio, lo que también beneficia a la estabilidad nacional y regional y permita adaptarse y hacer frente a la problemática de la ciberdelincuencia en la actualidad y el futuro. Debido que la tecnología con el tiempo avanza en proporciones altas y es a través de ella que el mundo actual ya sea bajo áreas políticas, económicas, sociales y de seguridad, establecen sus interacciones, lo que conlleva a que Centroamérica acople sus necesidades a estas nuevas formas de desarrollo e interconexión.

Lo cual aportaría beneficiosamente a la región si se poseen los mecanismos adecuados para crear iniciativas en estas materias, pero de lo contrario, solamente se mostrará un aumento de la vulnerabilidad si bien recordamos las capacidades que tiene la región y su rol no solamente para Centroamérica también para el resto del continente y el propio mundo. Por ende, considero que los Estados tienen la viabilidad con sus instrumentos que tienen para lograr establecer una iniciativa que los homologue, ya sea estableciendo un nuevo marco regional o bien actualizar los ya existentes, repercutiendo en una mejoría de las capacidades y estas puedan ser acopladas a los sectores estratégicos.

Por otro lado, en cuanto a mecanismos vigentes de integración regional desde el SICA y a través de sus diversas instancias se ha buscado la integración de la perspectiva multidimensional de la misma, en ese sentido se adoptado como plan macro de integración la implementación de los Objetivos de Desarrollo sostenible enmarcados en la Agenda 2030 de Naciones Unidas para el lineamiento de los esfuerzos conjuntos realizados en la región.

Dentro de la agenda 2030 y su implementación en la región, la importancia de un mecanismo regional de ciberseguridad se encontraría en pleno cumplimiento de los objetivos de desarrollo número 9, 11, 15 y 17 mismos que relacionamos a continuación.

En cuanto al objetivo de desarrollo numero 9 mismo que trata sobre la industria, innovación e infraestructura, el mecanismo de ciberseguridad regional sería altamente beneficioso por cuanto la modernización de los esquemas de producción industrial, así mismo brindando protección a los proyectos de innovación en un contexto donde la información es vulnerable todo el tiempo. Por su parte para el objetivo de desarrollo numero 10 mismo que hace referencia a la construcción de sociedades y ciudades sostenibles, el establecimiento de una zona ideal y segura a nivel físico como digital permitiría una mayor apertura en cuanto a la atracción de inversión extranjera directa a la región. Así mismo el establecimiento del sistema permitirá una mayor paz y esfuerzos conjuntos en cumplimiento de los objetivos 16 y 17.

**Bibliografía**

 Chile, M. d. (2021). Ciberdefensa. Obtenido de https://www.defensa.cl/temas-de-contenido/ciberdefensa/

Comisión Europea, D. G. (2021). *ec.europa.eu*. Obtenido de https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime\_enCortés, A. F. (2017). Amenazas Persistentes Avanzadas (APT): Modelo de Funcionamiento y Análisis al caso de Estudio Projectsauron. *Universidad Pil*

Antonio, J. M. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de amenazas. *Revista de Estudios en Seguridad Internacional, 6*(2). Obtenido de http://dx.doi.org/10.18847/1.12.2

Linares, H. (2003). Las Nuevas Amenazas a la Seguridad Nacional. *NACAO DEFESA*, 02-10. Obtenido de https://comum.rcaap.pt/bitstream/10400.26/1771/1/NeD\_ExtraAbril03\_HelbertLinares.pdf

Martinez, L. M., Ceceñas, P. E., & Ontiveros, v. C. (2014). Virtualidad, Ciberespacio y Comunidades Virtuales. *Universidad Juárez del Estado de Durango*, 02-144. Obtenido de http://www.upd.edu.mx/PDF/Libros/Ciberespacio.pdf

Ministerio de Defensa, C. S. (2014). *Documentos de Seguridad y Defensa-Estrategia de la información y seguridad en el ciberespacio.* Madrid: Ministerio de Defensa. Obtenido de https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF494.pdf

Organización de las Naciones Unidas, 2015, Resolución - A/RES/70/1 “Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible” Disponible en: https://unctad.org/system/files/official-document/ares70d1\_es.pdf