“ESTRATEGIA NACIONAL DE CIBERDEFENSA Y CIBERSEGURIDAD EN BOLIVIA”

Victor Hugo Cuevas Bustamante
Carrera de Ingeniería en Sistemas Electrónicos, Escuela Militar de Ingeniera
La Paz, Bolivia

“NATIONAL CYBER DEFENSE AND CYBER SECURITY STRATEGY IN BOLIVIA”

Resumen - Los innumerables incidentes informáticos de inseguridad que ocurrieron en el mundo y en nuestro país fueron a causa del crecimiento exponencial de la digitalización de la información, por un lado, con facilidades y beneficios y por otro con riesgo de vulneración y manipuleo; esta realidad proyectada en la dimensión nacional significa que como país estamos expuestos a muchos peligros derivados del uso de la tecnología, en el presente trabajo proponer los elementos componentes de una Estrategia Nacional de ciberseguridad permitirá enfrentar, neutralizar y defender al Estado Plurinacional de Bolivia de las amenazas y ataques provenientes del ciberespacio, la metodología empleada fue mixta cuali-cuanti (cualitativa - cuantitativa), a fin de exponer los diferentes aspectos que se requieren en el tema en cuestión, los resultados obtenidos fueron determinantes para elaborar las propuestas a implementar iniciando con un diagnóstico de la situación actual de Bolivia en el área de la ciberseguridad, luego se identificó principalmente las ausencias de la normativa legal, la organización encargada de realizar actividades de ciberseguridad y ciberdefensa y por último la falta de cultura cibernética en todos los niveles de educación de nuestro país; se establecieron ámbitos de acción en los cuales se necesita una directriz del estado que permita articular y coordinar los esfuerzos de diferentes organismos nacionales, complementados con el apoyo de organismos internacionales, por lo que este trabajo se constituye en un aporte desde la óptica netamente académica, conscientes de las limitantes principalmente económicas para que pudiera implementarse en el mediano plazo.

Palabras Claves— Estrategia Nacional, Ciberseguridad, Ciberdefensa, Seguridad Nacional

Abstract - The innumerable computer insecurity incidents that occurred in the world and in our country were due to the exponential growth of the digitalization of information, on the one hand, with facilities and benefits and on the other with the risk of violation and manipulation; this reality projected in the national dimension means that as a country we are exposed to many dangers derived from the use of technology, in the present work proposing the component elements of a National Cybersecurity Strategy will allow confronting, neutralizing and defending the Plurinational State of Bolivia from the threats and attacks from cyberspace, the methodology used was mixed qualitative-quantitative (qualitative - quantitative), in order to expose the different aspects that are required in the subject in question, the results obtained were decisive to elaborate the proposals to be implemented, starting with a diagnosis of the current situation in Bolivia in the area of cybersecurity, then mainly the absences of legal regulations were identified, the organization in charge of carrying out cybersecurity and cyberdefense activities and finally the lack of cyber culture at all levels of education of our country; spheres of action were established in which a state guideline is needed that allows articulating and coordinating the efforts of different national organizations, complemented with the support of international organizations, for which this work constitutes a contribution from the purely academic perspective, aware of the mainly economic limitations so that it could be implemented in the medium term.

Keywords— National Strategy, Cybersecurity, Cyberdefense, National Security

I. INTRODUCCION

El exponencial empleo de nuevas tecnologías de información y comunicaciones como son los sistemas celulares 4G, 5G, el Internet, las redes sociales y la convergencia tecnológica, ha desembocado en una dependencia total de los sistemas de información, sin embargo, los usuarios no son conscientes de los riesgos que conlleva una digitalización de la comunicación, en la que los servicios en los que se basa el funcionamiento de las sociedades modernas, están expuestos a la manipulación y los resultados serían inciertos e inimaginables si fueran alterados, pudiendo ocasionar pérdidas no solo económicas sino incluso de vidas humanas.

Un ejemplo real es el de Estonia, de como una potencia del mundo, digitalmente hablando, con altos niveles de gobierno electrónico, en el año 2007 sufrió uno de los primeros ciberataques por parte de un grupo de piratas informáticos presumiblemente provenientes de Rusia. Dicho ataque dejó fuera de servicios las páginas web del Gobierno llevando al país casi a su paralización total, para superar la crisis de comunicaciones utilizaron nuevamente el fax y el teléfono.

El filtraje de información de hacktivistas a nivel mundial en el conocido WikiLeaks (de Assange) y la publicación de información secreta del pentágono son otros ejemplos que a nivel mundial consternaron a la sociedad.

En nuestro continente, ataques cibernéticos sofisticados no son frecuentes en comparación con el resto del mundo, sin embargo, de los pocos reportados tenemos el ejemplo de México, donde a mediados de 2018 algunos Bancos reportaron haber sido blanco de grupos de ciberdelincuentes, que ejecutaron ataques de tipo Amenaza Persistente Avanzada (APT, por sus siglas en inglés) los cuales habrían sido ejecutados o al menos respaldados por actores estatales [1].

De acuerdo con la noticia que dio el periódico El Diario: Un ataque cibernético por día se registra en Bolivia, según el reporte del representante del colectivo ciudadano "Más y mejor internet para Bolivia", Mario Durán, fundamentado en mapas de ciberataques diseminados por la red.

Fue bien replicado que la página web de un medio estatal fue "hackeada" por un grupo autodenominado "Chilean hackers", que posteó una noticia falsa en la que se mencionaba un supuesto accidente de tránsito en el que habría estado inmerso el presidente Evo Morales. Minutos después la información fue desmentida.

Estos y otros sucesos ocurren y ocurrirán en nuestra sociedad si no tomamos cartas en el asunto y no coordinamos acciones serias para organizarnos, fundamentarnos legalmente, capacitarnos y proponer estrategias de seguridad y defensa.

Entonces, ¿Cuáles son los elementos componentes de una Estrategia Nacional de ciberdefensa y ciberseguridad que permita enfrentar, neutralizar y defender al Estado Plurinacional de Bolivia de las amenazas y ataques provenientes del ciberespacio?

En Bolivia hablar de una Estrategia Nacional de Ciberseguridad y Ciberdefensa es aún ficción, falta una coordinación institucional a nivel nacional y una cooperación gubernamental e internacional, falta una norma legal de la cual se desprenda una estrategia nacional, programas y posibles proyectos.

Esta pregunta dio al autor del presente artículo, la inquietud de poder investigar al respecto, asimismo, al crear y dirigir una Dirección de Ciberdefensa en una institución pública nacional bastante importante, se logró analizar y comparar estructuras nacionales de ciberdefensa de diferentes países entre los cuales se estudió a Ecuador, Colombia, España y Argentina logrando extractar interesantes conceptos que se pueden aplicar al modelo propio y exclusivo para Bolivia.

Por lo tanto, proponer los elementos componentes de una Estrategia Nacional de ciberseguridad permitirá enfrentar, neutralizar y defender al Estado Plurinacional de Bolivia de las amenazas y ataques provenientes del ciberespacio.

II. MATERIAL

La seguridad del ciberespacio no solo es responsabilidad propia individual, sino que también es un asunto de seguridad y soberanía nacional que influye en la gobernanza nacional, en la política nacional e internacional en diferentes grados en la integridad de la economía y en la protección de la información de sus ciudadanos.

La doctrina de seguridad y defensa reconoce la protección de la territorialidad de un estado como componentes: el espacio aéreo, naval y el terrestre, debiendo considerarse ahora el espacio cibernético, construido por el ser humano sobre las bases del espectro electromagnético y las infraestructuras tecnológicas de información y comunicaciones que debe ser protegido de ciertos riesgos y amenazas [3].

Para ello se hace necesario y fundamental contar con una organización o institución responsable, que establezca y aplique las políticas, estrategias, planes y medidas proactivas y reactivas de seguridad que permitan contar con barreras defensivas y ofensivas orientadas a mitigar efectivamente los diferentes tipos de amenazas y ataques cibernéticos.

En Bolivia las nuevas tecnologías se implementan con esmero y en forma acelerada por el retraso frente a las economías de la región, en el caso gubernamental está en ejecución dos programas a manera de soberanía tecnológica, la implementación de software libre y el Gobierno electrónico, aprovechando cada vez más los medios digitales para ofrecer servicios a la ciudadanía, sin embargo la falta de decisión política y la limitación de recursos no permiten promover una conciencia plena de prevención y mitigación de los riesgos provenientes de la actividad ilícita con los medios digitales, por lo tanto, es vulnerable a sufrir ataques cibernéticos potencialmente devastadores, al no contar con estrategias en el ámbito de ciberseguridad, planes que protejan la infraestructura critica o un organismo que asuma el comando y control de seguridad cibernética, más aún con una legislación completamente olvidada al respecto.

Según la recomendación UIT-T X.1205 de abril de 2008 de la Unión Internacional de Telecomunicaciones, la Ciberseguridad es el conjunto

de herramientas, políticas, estrategias, directrices, métodos de gestión de riesgos, conceptos de seguridad, salvaguardas de seguridad, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciber entorno.

La ciberdefensa, como parte de la ciberseguridad, enfrenta el exigente desafío de esforzarse por conseguir libertad de acción en un dominio como el ciberespacio, donde el adversario puede ejercer algún grado de control. Esto es tremendamente difícil y requiere alta disponibilidad de tecnología avanzada de mando y control, para asegurar la obtención y entrega de información y para apoyar el control directivo de los esfuerzos, conforme a las exigencias que los escenarios políticos y estratégicos actuales imponen considerando, además, que los nuevos escenarios podrían exigir mayores capacidades en el futuro [2].

En el campo militar ciberdefensa es el conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticos de la defensa, a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos a la vez que se impide que fuerzas enemigas los utilicen para cumplir sus cometidos.

Una de las definiciones que mejor describe un incidente de seguridad informática se le atribuye a las acciones o hechos que perjudiquen la connotación de confidencialidad, integridad o disponibilidad de la información de una organización. Este proceso de administración coordinada de los incidentes de seguridad que pueden presentarse a nivel nacional es controlado a través de las estructuras denominadas CSIRT Equipos de Respuesta ante Incidentes de seguridad computacional, acrónimo del inglés Computer Security Incident Response Team.

Un CSIRT es un equipo para minimizar y controlar los daños ante un ciberataque, que además asesora, responde y recupera la normalidad en las operaciones, así como previene que ocurran futuros incidentes, para lo cual los equipos intervienen como coordinadores en todas aéreas, individuos o procesos que intervienen en el hecho.

El resguardo, vigilancia y control de la información personal, de empresas, instituciones públicas y privadas y del propio Estado debe regirse a normas claramente definidas que deben empezar en leyes, estrategias, programas y planes para que personal técnico pueda realizar su trabajo.

Al respecto de la legislación, en nuestro País se han elaborado diferentes Leyes y Decretos que asignan a la innovación y al desarrollo tecnológico un papel fundamental para el incremento de la productividad y la competitividad del Estado.

En la nueva Constitución Política del Estado Plurinacional de Bolivia, en su Art. 244 misiona a las Fuerzas Armadas a defender y conservar la independencia, seguridad y estabilidad del Estado, su honor y la soberanía del país.

La Ley Orgánica de las FF.AA. Nº 1405 (30 de diciembre de 1992), establece: en su artículo primero que las Fuerzas Armadas de la Nación, son la Institución Armada Fundamental y permanente del Estado Boliviano, y sustentan como principios referidos a la Seguridad y Defensa del Estado, en el artículo tercero indica: El Estado mediante las Fuerzas Armadas organizará la Seguridad y Defensa Nacional, como un Sistema integrado con el objeto de neutralizar, rechazar o destruir cualquier acción tendente a vulnerarlas. Su acción será ejercida por los mandos militares de acuerdo a la Constitución Política del Estado, y al ordenamiento jurídico vigente. Sin embargo, desde la cabeza de sector que vendría a ser el Ministerio de Defensa no existen estrategias a nivel nacional para la ciberdefensa [4].

El DS 29272: Plan Nacional de Desarrollo dentro lo que es Bolivia productiva, cuenta con el Plan de Innovación y Desarrollo Tecnológico, pero no contempla una Bolivia segura ciberespacial.

La Ley general de telecomunicaciones, tecnologías de información y comunicación Nº 164 (2011). Garantizar el desarrollo y la convergencia de redes de telecomunicaciones y tecnologías de información y comunicación, crea consejos plurinacionales para el desarrollo de las TIC’s, pero no especifica la seguridad en el ciberespacio.

La Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicaciones AGETIC., creada por Ley Nº 2514 como la entidad gubernamental ha incorporado dentro de su estructura al Centro de Gestión de Incidentes Informáticos CGII., con la finalidad de gestionar los diferentes ataques cibernéticos recibidos en las instituciones públicas y privadas del país; sin embargo, en el contexto mundial, la Ciberdefensa es una atribución de las Fuerzas Armadas, derivada como resultado de la elaboración multilateral de una Estrategia Nacional de Ciberdefensa y Ciberseguridad.

El delito de amenazas en Bolivia queda tipificado en el Código Penal Nº 1970, en el artículo 293 como una conducta basada en la advertencia a otra persona de un mal grave. La sanción será la prestación de trabajo de un mes a un año y multa hasta de sesenta días.

En el caso de que la amenaza se haga con arma o por tres o más personas, la pena será de reclusión de tres a diez y ocho meses.

En el Artículo 363 bis, referente a la Manipulación Informática, indica que el que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a

un resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio a tercero, será sancionado con reclusión de uno a cinco años y con multa de setenta a doscientos días.

En el artículo 363 ter., referente a la Alteración, acceso y uso indebido de datos informático indica que el que sin autorización se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.
Sin embargo, ambos artículos no precisan que se trata de ciberataque, que vendría a ser un mal peor.

Por otra parte, la "Agenda Patriótica 2025": presentan 13 pilares para el fortalecimiento de un país con dignidad y soberanía, (Agenda Patriótica, 2014) y en el cuarto pilar de la Agenda, denominado "Soberanía Científica y Tecnológica con Identidad Propia", tiene por objetivo romper con las cadenas globales de valor del capitalismo avanzado en las naciones industrializadas, a las que Bolivia actualmente se incorpora mediante la venta de materias primas. El desarrollo de tecnologías propias se presenta como la solución a este problema, con la misión de industrializar y transformar los recursos estratégicos con los que cuenta el país para el fortalecimiento de la economía nacional. Sin embargo, en esta agenda no incluye una directriz de seguridad y defensa ante las amenazas del ciberespacio.

En ninguno de los casos se observa la presencia de actores no gubernamentales (como ser la academia, la sociedad civil o la comunidad técnica), a pesar de que es necesario un control social fuerte por parte de todos los implicados y un proceso transparente en la implementación debido a la sensibilidad de la información que se está tratando y/o las implicaciones futuras de la puesta en marcha de las dos políticas.

III. MÉTODOS

Considerando que la propuesta de identificación de elementos componentes de una Estrategia Nacional requiere de una investigación muy completa del fenómeno social, este tema en particular empleó una investigación científica mixta, en la que el tratamiento de la información cuali-cuanti (cualitativa - cuantitativa), presenta resultados confiables y válidos, con sustento en el contexto teórico y metodológico [5].

Esta investigación evidencia la aplicación de un diseño experimental, puesto que se tuvo la experiencia de crear una estructura básica de una dirección de ciberdefensa, incluyendo un CSIRT, en una institución encargada de la Seguridad y Defensa Nacional.

Sobre la base de la experiencia realizada, fue pertinente el empleo de la investigación aplicada, especialmente al área técnica, donde el análisis del caso se particularizó a la construcción inicial del diagnóstico específico de la ciberdefensa y ciberseguridad de Bolivia.

En base al objeto de estudio y sus características, se empleó la investigación aplicada e investigación exploratoria, considerando para el efecto la información obtenida de las fuentes primarias y secundarias, mediante encuestas y entrevistas a personal especialista y técnico de ciertas instituciones públicas y privadas del Estado y para las fuentes secundarias se aplicó un tipo de revisión bibliográfica.

Para esta investigación se empleó la técnica de muestreo no probabilístico intencional ya que permitió seleccionar personal de alto rango administrativo y técnico para la elaboración de la propuesta.

Asimismo, se empleó el Método Hipotético Deductivo, ya que su procedimiento lógico y ordenado lo convierten una práctica científica que parte con varios pasos esenciales que son: observación del fenómeno a estudiar, creación de una hipótesis para explicar el fenómeno, deducción de consecuencias o proposiciones y finalmente la verificación o comprobación de la verdad de los enunciados deducidos.

Una vez finalizado el proceso de recolección de datos, inicia el proceso de análisis, no obstante, considerando que el análisis de datos en esta parte del estudio está enfocado a la combinación de estrategias cuantitativas y cualitativas, se proponen diferentes acciones que deberán ser tomadas en cuenta por quienes corresponda.

IV. RESULTADOS

Se llegó a diagnosticar cuál es la situación actual de la ciberseguridad y ciberdefensa en Bolivia, concluyendo que la nueva Constitución Política del Estado garantiza la seguridad nacional a través de sus fuerzas Armadas, pero, no existe una entidad legalmente organizada que tome el mando para realizar actividades de ciberdefensa ni ciberseguridad.

Se determinó que no existe una Ley de Defensa Nacional que involucre al ciberespacio como un quinto elemento geopolítico, no existe un Libro Blanco de defensa actualizado en el Ministerio de Defensa, por lo tanto, tampoco existen políticas, estrategias, planes ni programas de ciberdefensa en las Fuerzas Armadas.

Se analizó las instituciones encargadas de la seguridad nacional, observando que no existe estructuras destinadas a la ciberdefensa. Existe una unidad que se encarga del cibercrimen, pero aplica

sanciones en forma aislada.

Se logro identificar que en la legislación boliviana no se encuentra tipificado y sujeto a sanción las acciones ilícitas en el ciberespacio.

Existe poco conocimiento de lo que es la ciberseguridad en nuestras universidades, por lo tanto, es necesario reconducir la educación, desde primaria, respecto a las nuevas tecnologías de información y comunicación y su seguridad.

Se identificó que no existe una lista de Infraestructuras críticas digitales estratégicas del Estado para su protección y defensa ante posibles ciberataques.mo se pudo obseSrvar en el desarrollo del presente artículo, existen varios pasos a seguir, de acuerdo con la metodología CSLI, la misma nos orienta y nos incentiva a desarrollar estos proyectos espaciales que a simple vista parecen ser demasiado costosos y bastante largos en su desarrollo. Si se cumple con todos los requerimientos, que por cierto son dependientes de nosotros mismos y posibles de cumplir, el lanzamiento de nuestro primer EMI-CubeSat estaría rondando los primeros meses de 2024.

V. CONCLUSIONES

Proponer elementos componentes para implementar una Estrategia Nacional de ciberseguridad en Bolivia permitirá prevenir, detectar, proteger, recuperar y defendernos como Estado ante incidentes en el ciberespacio. La redacción de una Guía para la elaboración de la Estrategia Nacional de Ciberdefensa y Seguridad del Estado Plurinacional de Bolivia, enmarcada en los parámetros fijados por organizaciones internacionales como la ITU y la OEA, constituye el primer paso para lograr que nuestro país tome conciencia de los peligros propios del ciberespacio y las enormes consecuencias que puede tener el recibir un ciberataque en alguna institución pública o privada y no estar preparados para ello.

El diagnóstico realizado nos hace dar cuenta que no existe una Política Nacional ante incidentes cibernéticos, por lo tanto, es necesario diseñar e implementar una norma o Política de Estado que dé prioridad la ciberseguridad y ciberdefensa.

La falta de una Ley de Seguridad y Defensa en el Ministerio cabeza de sector revela el poco interés de trabajo con respecto al tema discutido, por lo tanto, es necesario reformular los conceptos de seguridad y defensa tomando en cuenta al ciberespacio. De ahí se desprenderán las respectivas políticas y estrategias para el sector.

Las Fuerzas Armadas, al no tener directrices concretas, se queda atada de manos y pies en el cumplimiento de su misión al respecto de la ciberdefensa, por lo que es necesario que adopte el rol que le corresponde en aspectos de ciberataques y organizar, en coordinación con los más altos niveles, un modelo estructural boliviano de ciberdefensa y ciberseguridad.

El código penal data de muchos años atrás, por lo tanto, es necesario la actualización de la normativa jurídica nacional y desarrollo de normas técnicas necesarias para la ciberseguridad nacional.

Este trabajo investigativo toma especial relevancia porque busca aportar en forma práctica en la organización e implementación de directrices necesarias para que el estado boliviano cuente con una estructura encargada de la organización, planificación, ejecución y supervisión de todas las actividades relacionadas al campo de la ciberseguridad, los sistemas y las tecnologías de la información para mantener la seguridad en los procesos que desarrollan las instituciones tanto del estado como privadas, con especial interés a la infraestructura crítica y áreas que son vitales para el desarrollo del país.

En el campo de la educación es necesario que se implemente nuevas materias en la currícula de primaria, secundaria y reforzar a nivel universitario, esto mediante una reformulación de la Ley de Educación Avelino Siñani.

Por último, al no contar con una relación de Infraestructuras críticas digitales estratégicas, es deber de la entidad a organizar elabore un documento donde identifique estas infraestructuras.

REFERENCIAS

[1] Bloomberg (29 de May de 2018). Bloomberg cybersecurity. Obtenido de Mexico Foiled Million Bank Heist, Then Kept It a Secret: https://www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret.

[2] Instituto Ciberseguridad Española. (2013). Estrategia de Ciberseguridad Nacional. Madrid: Presidencial del Gobierno.

[3] Ministerio Defensa Nacional. (2004). Política de Defensa Nacional, Libro Blanco 2004. La Paz: MDN.

[4] Gaceta Oficial, (2009), Constitución Política del Estado Plurinacional de Bolivia. octubre 2015.

[5] Hernández, R. (2010). Metodología de la Investigación. México: Mc Graw Hill Educación.

Biografía Autor

Victor Hugo Cuevas Bustamante, docente de la materia Comunicaciones Satelitales de la carrera de Ingeniería en Telecomunicaciones de la Escuela Militar de Ingeniería.
Ingeniero en Sistemas Electrónicos – Escuela Militar de Ingeniería 1999. Diplomado en Educación Superior por competencias – EMI 2006, Magister Sciantiarum en Ingeniería de Redes de Comunicación – Universidad Mayor de San Andrés 2009, Especialización en Control, Operación y Diseño de satélites de Comunicación, Beigin – China 2013.

Fecha de Envió del Articulo: La Paz, 17 de octubre de 2022.

Fecha de Recepción de artículo: La Paz, 30 de octubre de 2022.