



**CONSEJO DE DEFENSA NACIONAL
INSTITUTO DE ALTOS ESTUDIOS ESTRATÉGICOS
PROGRAMA DE ESPECIALIZACIÓN EN
CIBERDEFENSA Y CIBERSEGURIDAD ESTRATÉGICA**



TRABAJO PRÁCTICO GRUPAL

**“APLICABILIDAD DE UN PLAN NACIONAL
DE CIBERDEFENSA EN EL PARAGUAY”**

**Lic. A. Sist. Edgar Wilfrido Ortiz Arza
Ing. Electrónico Jorge Daniel Orué Cuevas
Lic. A. Sist. Diana Liz Jané Otazú
Abogado Federico Manuel Peña Giménez
Lic. Informática Nicolás Pereyra Molinas
Lic. A. Sist. Julio Cesar Planás Montiel
Lic. A. Sist. Gustavo Adolfo Riquelme Medina
Lic. A. Sist. Marcos Darío Rivarola Lebrón
Ana. Sist. Marcos Antonio Riveros Coronel**

**CONSEJO DE DEFENSA NACIONAL
INSTITUTO DE ALTOS ESTUDIOS ESTRATÉGICOS
PROGRAMA DE ESPECIALIZACIÓN EN
CIBERDEFENSA Y CIBERSEGURIDAD ESTRATÉGICA**

TRABAJO PRÁCTICO GRUPAL

**“APLICABILIDAD DE UN PLAN NACIONAL
DE CIBERDEFENSA EN EL PARAGUAY”**

**Lic. A. Sist. Edgar Wilfrido Ortiz Arza
Ing. Electrónico Jorge Daniel Orué Cuevas
Lic. A. Sist. Diana Liz Jané Otazú
Abogado Federico Manuel Peña Giménez
Lic. Informática Nicolás Pereyra Molinas
Lic. A. Sist. Julio Cesar Planás Montiel
Lic. A. Sist. Gustavo Adolfo Riquelme Medina
Lic. A. Sist. Marcos Darío Rivarola Lebrón
Ana. Sist. Marcos Antonio Riveros Coronel**

Asunción, Paraguay

Abril 2019

TABLA DE CONTENIDO

	Página
INTRODUCCIÓN	8
DESARROLLO	11
1. Plan Nacional de Ciberseguridad.....	11
1.1. ¿Qué es el Plan Nacional de Ciberseguridad?	11
1.2. ¿Por qué un Plan Nacional?	11
1.3. ¿Cómo se trabajó en la elaboración del Plan Nacional?	12
1.4. Legislación en Materia de Ciberseguridad y Ciberdefensa en Paraguay:	13
1.5. Análisis del Plan Nacional de Ciberseguridad	17
1.6. Los 7 ejes del Plan Nacional de Ciberseguridad	19
1.7. Plan del MITIC Ciberseguridad.....	21
1.8. Avances de Implementación del Plan Nacional de Ciberseguridad	22
2. Situación actual del Paraguay en materia de Ciberdefensa y Ciberseguridad..	24
2.1. Concepto de la Ciberseguridad	24
2.1.1. ¿Cuál es el problema de tener múltiples definiciones?	25
2.1.2. ¿Es posible operar en un mundo con muchas definiciones del ciberespacio, posiblemente dispares?.....	26
2.2. Instituciones Públicas vinculadas con la Ciberdefensa en Paraguay	28
2.3. Situación actual del Paraguay en materia de Ciberdefensa.	31
2.4. Situación actual del Paraguay en materia de Ciberseguridad	33
3. Situación a nivel regional de los compromisos nacionales en Ciberseguridad	37
3.1. Argentina	39
3.2. Colombia.....	40
3.3. Chile.....	41
3.4. Brasil.....	42

4. Propuesta organizativa.....	43
CONCLUSIÓN	47
BIBLIOGRAFÍA	49

LISTA DE ABREVIATURAS

Administración Pública Federal - APF

Agenda Digital - AD

Central Inteligent Agency o Agencia Central de Inteligencia - CIA

Centro de Defensa Cibernética - CDCIBER

Centro de Respuestas ante Incidentes Cibernéticos - Paraguay. - CERT - PY

Centro Nacional de Ciberseguridad - CNC

Comando Conjunto Cibernético - CCOC

Comisión Nacional de Telecomunicaciones - CONATEL

Consejo Nacional de Política Económica y Social - CONPES

Denial of Service o Ataque de Denegación de Servicio - DoS

Departamento de Seguridad de Información y Comunicación - DSIC - GSI

Distributed Denial of Service o Ataque de Negación de Servicio Distribuido - DDoS

Ejército del Pueblo Paraguayo - EPP

Estrategia Nacional de Seguridad Ciudadana - ENSC

Fuerzas Armadas - FF.AA.

Global Cybersecurity Agenda o Agenda Global de Ciberseguridad - GCA

Global Cybersecurity Index o Índice Global de Ciberseguridad - GCI

Grupo de Acción Digital - GAD

Grupo de Respuesta a Emergencias Cibernéticas de Colombia - ColCERT

Instituto de Altos Estudios Estratégicos - IAEE

International Organization for Standardization u Organización Internacional de Normalización - ISO

International Telecommunication Union o Unión Internacional de Telecomunicaciones - ITU

Internet Service Provider o Proveedor de Servicios de Internet - ISP

Ministerio de Relaciones Exteriores - MRE

Ministerio de Tecnologías de la Información y Comunicación - MITIC

National Center for Missing and Exploited Children o Centro Nacional de Niños Desaparecidos y Explotados - NCMEC

National Institute of Standard and Technology o Instituto Nacional de Estándares y Tecnología - NIST

National Security Agency o Agencia Nacional de Seguridad - NSA
Organismos y Entidades del Estado - OEE
Organización de Estados Americanos - OEA
Organización de Tratado del Atlántico Norte - OTAN
Plan Nacional de Ciberseguridad - PNC
Secretaria de Tecnologías de la Información y Comunicación - SETIC
Secretaria Nacional de Tecnologías de la Información y Comunicación - SENATIC
Tecnologías de Información - TI
Tecnologías de Información y Comunicación - TICs
Unión de Naciones Sudamericanas - UNASUR

LISTA DE FIGURAS

Figuras	Página
1 Esquema del PNC	11
2 Comparativo Índices Globales de Ciberseguridad.....	38
3 Cuadro de calor de los índices globales de Ciberseguridad.....	39
4 Línea de tiempo PNC en Chile	42

INTRODUCCIÓN

La utilización masiva de teléfonos celulares inteligentes o smartphones, posibilita la penetración de internet en el país, más del 43% de la población paraguaya tiene acceso a la red de redes desde el 2017.¹ Este crecimiento alcanza a todos los ámbitos de la sociedad y plantea un nuevo escenario de actividades a la que denominamos ciberespacio, no limitado por fronteras físicas con amplias posibilidades de alcance global. En este contexto, es proclive la aparición de nuevas amenazas, conflictos y agresiones que pueden atentar contra el patrimonio de particulares, el normal funcionamiento de la sociedad, de las administraciones públicas, llegando inclusive a afectar el estado de derecho y la seguridad nacional.

El Desarrollo del presente trabajo de investigación denominado “Aplicabilidad de un Plan Nacional de Ciberdefensa en el Paraguay” propone realizar un estudio exhaustivo de la situación local en la materia, y a la par comparar los distintos enfoques que se tienen con relación a la defensa nacional en el ciberespacio de los principales actores de la región, describiendo brevemente la línea de acción que aplican en sus respectivos países.

El Paraguay cuenta con un Plan Nacional de Ciberseguridad, cuyo objetivo es acompañar el avance de las Tecnologías de Información y Comunicación (TIC), bajo ese contexto adquiere fundamental trascendencia la incorporación de medidas que posibiliten la utilización correcta de las tecnologías disponibles y la adopción de disposiciones que garanticen el uso seguro de las mismas para todos los ciudadanos, sea desde el ámbito civil, académico, de las funciones públicas y la relación de todas éstas con el mundo globalizado.

La ciberdefensa, por consiguiente, adquiere trascendencia mundial, en estas últimas décadas se han incrementado las amenazas cibernéticas por parte de atacantes generalmente protegidos por el anonimato que, movidos por factores diversos, pueden atentar contra objetivos comerciales, académicos y en muchos casos contra infraestructuras críticas de los países, con un alcance de hasta millones de personas afectadas.

¹ Secretaria Nacional de Tecnologías de la Información y Comunicación 2017. Encuesta sobre Acceso y Uso de Internet en Paraguay (en línea). Asunción. Paraguay. Consultado 25 de abril. 2019. Disponible en <http://gestordocumental.senatics.gov.py/share/s/ntjnuNLeT8u3gbAHC6WeVw>.

Algunos casos emblemáticos ocurridos son los ataques informáticos contra sitios web de Estonia en el año 2007 (prensa, ministerios, entidades económicas), lo sucedido en Natanz-Irán con la propagación de una aplicación informática maliciosa (malware), denominado Stuxnet, que en el 2010 afectó el funcionamiento de una central nuclear; filtraciones realizadas por la organización mediática internacional Wikileaks, filtraciones sobre ciberespionaje global realizado por Edward Snowden, consultor tecnológico estadounidense y ex empleado de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos de América, en el 2013 y el ataque realizado por la aplicación informática maliciosa (ransomware) que solicita un rescate monetario por los dispositivos y/o archivos bloqueados, denominada “WannaCry”, en el 2017 afectando a más de 150 países (EEUU, Rusia, Reino Unido, China, etc.).

Los intereses nacionales, podrían verse afectados, sea por la importancia de los blancos elegidos, por las consecuencias imprevisibles sobre los mismos, la dificultad que se tiene para identificar y sancionar a los autores de estos hechos y, por consiguiente, las falencias de legislaciones vigentes adecuadas al avance tecnológico.

Como objetivo del gobierno, se tiene la protección de todos los tipos de infraestructuras críticas como ser redes, servicios públicos, recursos naturales, cuyo ataque podría causar un gran impacto en la seguridad de la población, a la par del diseño de políticas orientadas a fortalecer la integridad y confiabilidad de la información en el ciberespacio y el funcionamiento eficiente del estado en sus áreas administrativas y jurídicas-políticas.

El trabajo de investigación es analizado desde el punto de vista de la legislación local vigente, también se verifica la situación actual del Paraguay en materia de ciberdefensa a partir del Plan Nacional de Ciberseguridad aprobado, se comparan las situaciones de otros países a nivel regional y se realiza una propuesta organizativa de la aplicabilidad de un plan de Ciberdefensa para el país.

Cómo propósito final, el trabajo de investigación pretende demostrar que la ciberdefensa es un tema clave a nivel mundial ya que desde la red de redes se puede atentar contra la defensa nacional y regional, al avance considerable científico y tecnológico se deben adecuar las reglas tradicionales de protección de la soberanía

con el establecimiento de políticas y normas orientado al desarrollo de capacidades ante las nuevas amenazas.

Así mismo orientar los esfuerzos para la adecuación de los marcos jurídicos y la relación entre los objetivos, competencias y funciones de los diferentes organismos del Estado. En conjunto estas acciones contribuirán al diseño y ejecución de planes que regulen tanto el sector público y las actividades del sector privado.

DESARROLLO

1. Plan Nacional de Ciberseguridad

1.1. ¿Qué es el Plan Nacional de Ciberseguridad?

Es la base de políticas gubernamentales y nacionales que establece las líneas de acción a ser adoptadas por un país para fortalecer la seguridad de sus activos críticos y lograr un ciberespacio seguro, confiable y resiliente, y sirve como guía para la ejecución de políticas públicas en ciberseguridad. Más específicamente, este documento define los ejes, los objetivos y un plan de acción para la ejecución de la política nacional de ciberseguridad, de la cual participarán en el proceso de implementación varias entidades gubernamentales, el sector privado, la academia y la sociedad civil.



Figura 1 Esquema del PNC

1.2. ¿Por qué un Plan Nacional?

- La evolución de la sofisticación de los ciberataques debe ser respondida de manera dinámica y proporcional.
- Sin una respuesta estratégica coordinada, los esfuerzos nacionales en materia de ciberseguridad serán insostenibles, esporádicos, duplicados e ineficientes.
- Existe una creciente dependencia de las TICs y el ciberespacio en los gobiernos.

- Un Plan nacional construido participativamente aumenta los niveles de compromiso, trabajo conjunto y posibilidades de coordinar medidas concretas.

1.3. ¿Cómo se trabajó en la elaboración del Plan Nacional? ²

El Plan Nacional de Ciberseguridad es producto de un esfuerzo conjunto y coordinado, que involucró directamente a más de 120 personas representantes de todos los sectores que tienen roles e intereses en el ciberespacio.

En mayo de 2015 se iniciaron los trabajos con el lanzamiento oficial realizado en el Hotel Granados Park. Estuvieron presentes representantes del gobierno, del sector privado, Proveedores de Servicios de Internet (ISPs por sus siglas en inglés), sector educativo, sociedad civil, así como también actores internacionales. El apoyo de la Organización de Estados Americanos -OEA y sus países miembros fue fundamental en todo el proceso.

La metodología adoptada para la elaboración del Plan Nacional de Ciberseguridad fue a través de mesas de trabajo por sector (gobierno, financiero, educativo, justicia, sociedad civil, infraestructura crítica, etc.) en las cuales se debatieron los problemas específicos de cada sector, así como las posibles líneas de acción a ser adoptadas.

Dichas líneas de acción fueron plasmadas de forma consensuada en un documento, el cual fue el 1er Borrador.

En el mes de julio del 2015 se convocó por segunda vez al grupo de trabajo, de modo a presentar este borrador y ponerlo a consideración. Nuevamente se trabajó por temas, con mesas de trabajos sectoriales específicas, en un proceso colaborativo de revisión y corrección. Se finalizó con una plenaria, donde los involucrados aportaron comentarios, ideas y sugerencias globales y transversales.

² Secretaria Nacional de Tecnologías de la Información y Comunicación. Plan Nacional de Ciberseguridad. ¿Cómo se trabajó? Asunción. Paraguay Consultado 25 de abril 2019. Disponible en <https://www.senatics.gov.py/plan-nacional-de-ciberseguridad/como-se-trabajo>

Finalmente, en marzo de 2016 se terminaron todas las correcciones, lográndose así el Borrador Final del Plan Nacional de Ciberseguridad. El proceso y sus discusiones principales fueron presentados en Segurinfo Paraguay 2016, en el Banco Central del Paraguay.

Posteriormente, se procedió a la aprobación del Decreto N° 7052/2017 *“Por el cual se aprueba el Plan Nacional de Ciberseguridad y se integra la Comisión Nacional de Ciberseguridad”*, en fecha 24 de abril de 2017.

1.4. Legislación en Materia de Ciberseguridad y Ciberdefensa en Paraguay:

El desarrollo normativo en el marco regulatorio vigente en la República del Paraguay, en materia de Ciberseguridad y Ciberdefensa, ha ido evolucionando pausadamente, desde los primeros esfuerzos atendiendo los múltiples problemas nacionales e internacionales ocurridos en ese contexto, además de la preocupación mundial. A raíz de los hechos mencionados, y como consecuencia de ellos, países de Europa se reúnen en el Convenio de Budapest contra la Ciberdelincuencia, y elaboran un instrumento mediante el cual se dio inicio a la regulación de la estructura y la legislación en lo concerniente a la Ciberdefensa y Ciberseguridad en el campo internacional. Luego en nuestro país, atendiendo la creciente ola de ataques locales e internacionales, como así también de la constante innovación tecnología para tales efectos, se dan los primeros pasos para contrarrestarlos o prevenirlos. Posteriormente y luego de aunar esfuerzos entre entes privados y públicos de nuestro país, se pudo realizar un Plan Nacional de Ciberseguridad, el cual fue sancionado a través del Decreto N° 7052/2017 *“Por el cual se aprueba el Plan Nacional de Ciberseguridad y se integra la Comisión Nacional de Ciberseguridad”*. Como consecuencia de todo lo referido más arriba, se puede señalar que nuestro país también ha realizado un ajuste en su normativa penal respecto a varios Ciberdelitos que generaban un caos social. En la actualidad se puede notar que el avance respecto a la Ciberdefensa, es muy notorio y que ha motivado en nuestro país, la unión de las empresas estatales y privadas, y que la misma siga firme y continúe logrando objetivos propuestos, a la espera de que pronto nuestro Plan de Ciberdefensa pueda llegar a su conclusión y así

estar adecuados respecto a los estándares de los otros países que ya se encuentran en etapa totalmente operativa.

A continuación se presentan dentro de un orden cronológico, los instrumentos normativos que han dado inicio y forma a la legislación nacional en materia de Ciberseguridad y Ciberdefensa, que es como sigue:

- Ley N° 642/1995 “De Telecomunicaciones”. Se crea la Comisión Nacional de Telecomunicaciones (CONATEL). Fecha: 29/12/1995.
- Ley N° 1337/1999 “De Defensa Nacional y Seguridad Interna”. Se establecen las bases jurídicas respecto a la Defensa Nacional y la Seguridad Interna. Fecha 14/04/1999. Fue modificada y ampliada posteriormente por Ley N° 5036/2013.
- Ley N° 4017/2010 “De Validez Jurídica de la Firma Electrónica, la Firma Digital, los Mensajes de Textos y el Expediente Electrónico”. Validación Jurídica y regulación de la utilización de la firma electrónica, la firma digital, los mensajes de textos y el expediente electrónico. Fecha 03/06/2010. Fue modificada por Ley N° 4610/2012.
- Resoluciones 3459/2010 y 4408/11 del Ministerio Público, mediante las cuales se crea la Unidad Especializada de Delitos Económicos y se delimitan su competencia.
- Ley N° 4439/2011 “Que Modifica y Amplia varios Artículos de la Ley N° 1160/97 Código Penal”. Modifica varios artículos del Código Penal Paraguayo referente a delitos informáticos. Fecha 03/10/2011.
- Decreto N° 7706/2011 “Por la cual se aprueba el Plan Director de Tecnologías de la Información y Comunicación (TICs) del Poder Ejecutivo”. Hoja de ruta que permite desarrollar estrategia para que las TICs en un eje estratégico para alcanzar el desarrollo sostenible a largo plazo en el Paraguay. Fecha 15/11/2011.

- Decreto N° 8716/2012 “Por la cual se crea y reglamenta la Secretaria de Tecnologías de la Información y Comunicación (SETICs). Derogada por la Ley de Creación de la SENATIC.
- Decreto N° 10.517/2013 “Por la cual se autoriza a la Secretaria de Tecnologías de la Información y Comunicación (SETICs), a desarrollar, implementar y monitorear el Sistema de Intercambio de Información entre Instituciones Públicas”. Fecha 16/01/2013.
- Ley N° 4868/2013 “Comercio Electrónico”. Marco regulatorio respecto al comercio y la contratación a través de medios electrónicos o tecnología equivalente. Fecha 26/02/2013.
- Ley N° 4.989/2013 “Que crea el marco de aplicación de las tecnologías de la información y comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)”. Creación de la SENATIC. Fecha 09/08/2013. Derogada por la Ley N° 6207/2018 de Creación del Ministerio de Tecnología de la Información y Comunicación (MITIC).
- Decreto N° 11.624/2013 “Por el cual se reglamenta la Ley N° 4.989/2013 del 9 de agosto de 2013, “Que crea el marco de aplicación de las tecnologías de la información y comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)” y establece la estructura orgánica y funcional de la citada Secretaría Nacional”. Fecha 12/08/2013.
- Ley N° 5036/2013 “Que modifica y amplía los artículos 2°, 3° y 56 de la ley n° 1337/99 “De Defensa Nacional y Seguridad Interna””. Fecha 22/08/2013.
- Decreto N° 1.165/2014 “Por el cual se aprueba el reglamento de la Ley N° 4.868 del 26 de febrero de 2013 de “Comercio Electrónico””. Fecha 27/01/2014.

- Decreto N° 1.306/2014 “Por el cual se modifican los artículos 6° y 7° del Decreto N° 11624/2013 que reglamenta la Ley N° 4989/2013 “Que crea el marco de aplicación de las tecnologías de la información y comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)”. Fecha 27/02/2014.
- Ley N° 5282/2014 “De libre acceso ciudadano a la Información Pública y Transparencia Gubernamental”. Fecha 18/09/2014.
- Decreto N° 6234/2016 Por el cual se declara de interés nacional la aplicación y el uso de las Tecnologías de la Información y Comunicación (TICs) en la gestión pública, se define la Estructura Mínima con la que deberá contar y se establecen otras disposiciones para su efectivo funcionamiento. Fecha 08/11/2016.
- Decreto N° 5323/2016 Por el cual se reglamentan los artículos 20 y 21 de la Ley N° 4989/2013 “que crea el marco de aplicación de las Tecnologías de la Información y la Comunicación en el sector público y crea la SENATICs” y se establece la instancia de coordinación de las Unidades Especializadas TIC de las Instituciones del Poder Ejecutivo.”. Fecha 23/05/2016.
- Ley N° 5653/2016 “De protección de Niños, Niñas y Adolescentes contra contenidos nocivos de Internet”. Fecha 24/08/2016.
- Decreto N° 7052/2017 “Por el cual se aprueba el Plan Nacional de Ciberseguridad y se integra la Comisión Nacional de Ciberseguridad” Fecha 24/04/2017.
- Ley N° 6207/2018 “Que crea el Ministerio de Tecnologías de la Información y Comunicación y establece su Carta Orgánica.

- Decreto N° 1260/2019 “Por la cual se aprueba la Estructura Orgánica del Ministerio de Tecnologías de la Información y Comunicación (MITIC)”. Fecha 11/02/2019.

1.5. Análisis del Plan Nacional de Ciberseguridad

Analizando el PNC, se mencionan y transcriben algunas cuestiones urgentes de atender:

- Se menciona sobre la posibilidad de la adhesión al Convenio de Budapest sobre Ciberdelincuencia, acotando que entre los años 2010-2011 se realizaron cambios importantes en la legislación penal del país, adecuándola a los estándares mínimos que dispone dicho convenio (pág. 17 del PNC)
- Se señala en el Plan que *“cabe destacar que el Ministerio del Interior aprobó la “Estrategia Nacional de Seguridad Ciudadana 2013-2016” (ENSC)³⁴ por medio de la Resolución N°211/2013 que apunta esencialmente a proveer y mejorar la seguridad de la ciudadanía en general, proporcionando la infraestructura tecnológica a la Policía Nacional y al Ministerio Público. La ENSC viene a consolidar la Política Nacional de Seguridad Ciudadana estructurada en 2010. Sin embargo, dicha estrategia aún no contempla propuestas específicas para ofrecer seguridad a la ciudadanía en cuestiones de ciberdelincuencia.”* (pág. 18 del PNC)
- Sobre el Decreto N°6234/2016, éste dice que *“ordena que las instituciones dependientes del Poder Ejecutivo, tanto la Administración Central como las entidades y organismos descentralizados, cuenten con Unidades Especializadas en TIC con el objetivo de promover la implementación, acrecentamiento y acceso a la infraestructura y a las tecnologías de la información y comunicación, bajo supervisión directa de la máxima autoridad de*

cada institución. Sin embargo, estas Unidades Especializadas no han sido implementadas por completo en toda la Administración Pública.

En este sentido, es fundamental establecer una mejor coordinación para la implementación de mecanismos de seguridad en los sistemas de TI de la Administración Pública, con el respaldo suficiente en las unidades especializadas.” (pág. 18 del PNC)

- *Se reconoce que “la situación de las empresas públicas en términos de ciberseguridad es muy incipiente. Existe la necesidad de desarrollar una reglamentación coordinada y centralizada en ciberseguridad para las empresas públicas, con una definición de estándares mínimos para el funcionamiento de las infraestructuras críticas en el país.” (pág. 18 del PNC)*
- *En términos de ciberseguridad, no hay aún en el sector privado empresas certificadas por el ISO 2700138, y se estima que un alto porcentaje de las empresas no cumplen con los registros de seguridad en TIC para manejos de documentos (pág. 19 del PNC)*
- *Se advierte que no existe una obligación legal para que las entidades del sector privado compartan información sobre incidentes cibernéticos con el CERT-PY, ni los vínculos y mecanismos necesarios para cooperación y colaboración (pág. 19 del PNC)*
- *Respecto a la sensibilidad y educación, se reconoce que las acciones realizadas por el gobierno, el sector privado y organizaciones internacionales es de manera descoordinada y no se realizan mediciones de la efectividad alcanzada (pág. 19-20 del PNC)*

- Y finalmente, respecto a la capacitación sobre Ciberseguridad, debe incluirse en la enseñanza básica desde los primeros niveles y en los niveles más técnicos como materias específicas.

Estos son algunos de los puntos generales de más urgente atención a nivel nacional según lo mencionado en el Plan promulgado en el año 2017.

1.6. Los 7 ejes del Plan Nacional de Ciberseguridad

1. **Sensibilización y Cultura:** sensibilizar y capacitar a la ciudadanía en general para lograr una cultura cibernética con enfoque en la prevención de los riesgos asociados al uso de las TIC's. Los mecanismos sugeridos son las campañas para el usuario final de las TIC's, la inclusión de la enseñanza sobre ciberseguridad desde los primeros niveles educativos y el compromiso de los más altos niveles dentro de las entidades públicas y privadas.

La cultura incluye la visión de mantener la confianza del consumidor como base para el crecimiento de la economía digital.

2. **Investigación, Desarrollo e Innovación:** incluir la enseñanza sobre ciberseguridad desde los primeros niveles de enseñanza, estimulando la investigación e implantando un enfoque de inversión mínima para la formación de docentes.

El desarrollo implica la coordinación gobierno-sociedad civil-empresas-academia para impulsar proyectos de interés general, que cumplan con estándares mínimos de ciberseguridad. El incentivo al sector privado debe aplicar para cumplir reglas de ciberseguridad.

3. **Protección de Infraestructuras Críticas:** tanto físicas como lógicas, sin afectar su eficiencia y efectividad, mediante la identificación de las mismas y la aplicación de medidas de seguridad adecuadas estableciendo normas claras, protocolos y un plan de comunicación nacional para proteger la infraestructura

crítica en el caso de un ataque cibernético. La capacidad de resiliencia y la gestión de los riesgos es fundamental para ese tipo de infraestructuras.

4. **Capacidad de Respuesta ante Incidentes Cibernéticos:** proveer al CERT-PY de talentos humanos suficientes, infraestructura adecuada y asignación presupuestaria que garantice su adecuada operación.

El CERT-PY debe ser el gestor centralizado nacional de los eventos cibernéticos, un facilitador actualizado de los tipos de amenazas vigentes, a través de convenios y leyes que garanticen el logro de sus fines.

5. **Capacidad de Investigación y Persecución de la Ciberdelincuencia:** Se deben proveer recursos y herramientas adecuadas para las entidades abocadas a la investigación de delitos informáticos, incluyendo programas de capacitación nacional e internacional para agentes fiscales, policiales y jueces.

Es importante adecuar la legislación con un marco regulatorio actualizado y capacidades operativas que aumenten la posibilidad de identificar a los responsables. La legislación debe complementar las documentaciones legales internacionales que el país reconozca.

La Cooperación internacional en materia policial y judicial deberá fortalecerse.

6. **Administración Pública:** se deberán establecer directrices para la adquisición de productos y servicios TICS y la estandarización de especificaciones mínimas de seguridad, así como la precalificación de proveedores que ofrecen estos servicios y productos, que permitan la prevención de incidentes. Igualmente deberá establecerse autoridades para implementar el PNC.

7. **Sistema Nacional de Ciberseguridad:** se deberá designar un Coordinador Nacional de Ciberseguridad, con la responsabilidad de monitorear y evaluar la implementación del Plan Nacional de Ciberseguridad, en cooperación entre las distintas partes

Cada eje tiene definido sus propios objetivos y estos sus líneas de acción que a su vez deben desplegarse en acciones específicas que deriven en el cumplimiento efectivo de las líneas de acción, que puedan ser temporales y medibles, para poder evaluar efectivamente el nivel de cumplimiento de esas acciones del PNC y los productos logrados con esas acciones.

1.7. Plan del MITIC Ciberseguridad

Paraguay cuenta con un Plan Nacional de Ciberseguridad, producto de un trabajo multi-stakeholder de varios años, y de un proceso que involucró representantes de más de 120 organizaciones, entre ellas instituciones públicas, sector privado, academia, sociedad civil, gremios profesionales y organismos internacionales, entre otros.

Este Plan ha identificado, entre otras cosas, la necesidad de fortalecer los roles y atribuciones referentes a ciberseguridad y protección de la información, no sólo en cuanto a capacidad de respuesta a incidentes, sino también en cuanto a formación y concienciación, protección de infraestructuras críticas, seguridad en la administración pública, capacidad de investigación y persecución de la ciberdelincuencia y coordinación nacional.

Este camino recorrido condujo a la inclusión de la Ciberseguridad y la protección de la información como un eje misional del MITIC, a través de una Dirección General de Ciberseguridad y Protección de la Información, con atribuciones y un organigrama acorde a los desafíos a los que se enfrente.

Su objetivo principal es promover iniciativas que contribuyan a la construcción de un ecosistema digital seguro, confiable y resiliente, incluyendo el sector público, privado, academia y ciudadanía, a través de políticas, planes, proyectos y servicios de ciberseguridad, tanto preventivos como reactivos.

1.7.1. Roles y responsabilidades

1. Implementar mecanismos de gestión, coordinación, respuesta e investigación de incidentes cibernéticos que pongan en riesgo el ecosistema digital nacional.
2. Establecer e incentivar mecanismos de intercambio de información relacionado a incidentes cibernéticos y amenazas, entre el sector gubernamental, privado, regional e internacional.
3. Implementar mecanismos y desarrollar actividades conducentes a la protección de sistemas, redes, procesos e información de los organismos y entidades del Estado, así como también las infraestructuras tecnológicas críticas, con un enfoque preventivo.
4. Promover iniciativas de concienciación y planes de capacitación en materia de ciberseguridad y protección de la información, en coordinación con las instituciones públicas, el sector privado, instituciones educativas y organismos internacionales.
5. Establecer, gestionar y promover la adopción de políticas, estándares, lineamientos, guías y marcos de protección de la información para los organismos y entidades del Estado.
6. Proponer y promover la adopción de guías de buenas prácticas de ciberseguridad y protección de la información en todo el ecosistema nacional.
7. Proponer, coordinar, gestionar y monitorear los planes y estrategias de ciberseguridad a nivel nacional.

1.8. Avances de Implementación del Plan Nacional de Ciberseguridad

Según consulta realizada a la Senatic's en fecha 24/04/2019, los avances en la implementación del plan logrados hasta la fecha son los siguientes:

“En el contexto de las responsabilidades, es desde la Dirección General de Ciberseguridad y Protección a la Información, que funciona a partir de la creación del MITIC, desde donde se impulsa la implementación del PNC. Antes del Ministerio lo hacía la SENATIC’s, a través del CERT-PY.”³

Tenemos como hoja de ruta en este nuevo gobierno, impulsar desde el MITIC la implementación de dicho plan, junto con la Comisión Nacional de Ciberseguridad, conformada por las instituciones más representativas del sector público, privado y la academia.

Sobre los avances, este año el 26/03 se realizó la segunda reunión de la Comisión Nacional de Ciberseguridad CNC, a fin de presentar a los miembros un desglose de las acciones requeridas y responsables por ejes, objetivos y líneas de acción. En la misma se asignaron a los actores con responsabilidad directa en cada una de las líneas de acción; así también las actividades o iniciativas ya existentes a nivel país, que son todos aquellos proyectos, iniciativas o actividades que ya fueron realizados y/o se encuentran realizando actualmente respecto a cada línea de acción.

Una vez validada por la CNC, se prevé realizar reuniones de seguimiento con los actores asignados para cada línea de acción. Por cuestiones presupuestarias se priorizan aquellas líneas de acciones que tengan costos de implementación bajos

Se están analizando las opciones de financiación de aquellas líneas que requieran un presupuesto, así como recursos humanos dedicados de forma exclusiva.

También desde el MITIC, se prevé la contratación de una persona dedicada 100% del tiempo a las actividades relacionadas al PNC, su implementación y mantenimiento.

³ Ministerio de Tecnologías de la Información y Comunicación. Viceministerio de Tecnologías de la Información y Comunicación. Ciberseguridad y protección a la información. Asunción. Paraguay Consultado 25 de abril 2019 Disponible en <https://www.mitic.gov.py/viceministerios/tecnologias-de-la-informacion-y-comunicacion/ciberseguridad-y-proteccion-a-la-informacion>

De forma básica es el estado actual.”⁴

Analizando el mail recibido en fecha 25/04/2019, los principales inconvenientes que han impedido tener mejores resultados son la falta de organización adecuada desde la promulgación del PNC y creación de la Comisión Nacional de Ciberseguridad, directamente influidos por falta de recursos humanos esenciales y del bajísimo presupuesto asignado para el logro de los fines propuestos.

Asimismo, y buscando más detalles de lo realizado hasta la fecha, consultando el sitio web de la Senatic’s, el mismo se encuentra desactualizado respecto a informaciones sobre la versión oficial del Plan y los avances realizados hasta la fecha. Sobre el Plan, la web menciona solamente la versión del borrador.

2. Situación actual del Paraguay en materia de Ciberdefensa y Ciberseguridad

2.1. Concepto de la Ciberseguridad

La red de información electrónica conectada se ha convertido en una parte integral de nuestra vida cotidiana. Todos los tipos de organizaciones, como instituciones médicas, financieras y educativas, utilizan esta red para funcionar de manera eficaz.

Utilizan la red para recopilar, procesar, almacenar y compartir grandes cantidades de información digital. A medida que se recopila y se comparte más información digital, la protección de esta información se vuelve incluso más importante para nuestra seguridad nacional y estabilidad económica.

La ciberseguridad es el esfuerzo constante por proteger estos sistemas de red y todos los datos contra el uso no autorizado o los daños.

⁴ Mail recibido de la **Lic. Diana L. Valdez Tullo**.
Dirección General de Ciberseguridad y Protección de la Información
Departamento de Políticas y Gobernanza de Ciberseguridad
Vice-Ministerio de Tecnologías de la Información y Comunicación (MITIC)

A nivel personal, debe proteger su identidad, sus datos y sus dispositivos informáticos. A nivel corporativo, es responsabilidad de todos proteger la reputación, los datos y los clientes de la organización.

A nivel del estado, la seguridad nacional, y la seguridad y el bienestar de los ciudadanos están en juego.⁵

Hoy día la palabra “cyberseguridad” es utilizada en muchos contextos, pero no es totalmente clara en los términos conceptuales y a lo que realmente se refiere.

Las fuentes son entidades relevantes como el gobierno nacional o regional, los organismos de normalización y el diccionario.

La razón por la que se elige el término "ciberespacio" es que todos los demás términos (por ejemplo, seguridad cibernética o ciberseguridad, ciberdelincuencia, ciberguerra, ciberterrorismo, etc.) se basan o derivan del ciberespacio. Por lo tanto, la seguridad cibernética es la seguridad del ciberespacio.

La ciberdelincuencia es un delito cometido dentro del ciberespacio o donde se utilizan elementos del ciberespacio como vehículo para cometer un delito, y así sucesivamente para otros términos derivados.

2.1.1. ¿Cuál es el problema de tener múltiples definiciones? ⁶

Si se usan definiciones dispares en una discusión, es a priori imposible llegar a una conclusión que sea significativa, correcta y completa para las partes involucradas. Por ejemplo, si una definición se enfoca solo en hardware (por ejemplo, computadoras, teléfonos móviles, dispositivos de red, etc.) pero ignora los datos y otra definición hace lo contrario, entonces cualquier conclusión de un lado tendría poco sentido para el otro. Y las cosas pueden empeorar, ya que muchos documentos simplemente usan la expresión del ciberespacio sin definirlo realmente. Un ejemplo de tal documento es la "*Estrategia de seguridad de la información para*

⁵ Ref. Bibliográfica: Cisco NetAcad, un programa de responsabilidad social corporativa de Cisco.

⁶ Damir Rajnovic, July 26, 2012

proteger a la nación" por el Consejo de Política de Seguridad de la Información, Japón, que desafortunadamente no es el único de su tipo. Este uso laxo de los términos deja demasiado espacio abierto para la interpretación y el malentendido.

2.1.2. ¿Es posible operar en un mundo con muchas definiciones del ciberespacio, posiblemente dispares?

Es posible, pero es más difícil de lo que debería ser. Es un poco más fácil si las partes involucradas son conscientes de que las definiciones utilizadas por ambos lados no son idénticas y si tienen en cuenta estas diferencias.

Para que una definición se considere tal, debe cumplir dos condiciones: debe tener una definición oficial y debe ser realizada por una entidad respetable.

Para este propósito, definimos "oficial" como presentado en un documento de alto nivel que se utiliza como base para el desarrollo de políticas y prevalece en una organización / región determinada. Entidades como los gobiernos y los organismos de normalización se consideran respetables en el sentido de que influyen en el pensamiento y el comportamiento de una multitud de organizaciones.

Dada la cantidad de material relacionado con el ciberespacio debería ser relativamente fácil encontrar definiciones de qué es el ciberespacio, pero ese no es necesariamente el caso.

Lo que se debe enfatizar es que si una definición oficial de un ciberespacio no se ubicó para un país determinado, eso no significa necesariamente que la definición no existe.

Otro problema es cómo se escribe el término ciberespacio. El diccionario de Oxford dice que es una sola palabra, el ciberespacio, pero no todos lo siguen. Algunos usan dos palabras "ciber espacio" o colocan un guión entre las palabras "ciber-espacio". La capitalización del término también varía. A veces, el ciberespacio se escribe en minúsculas y, a veces, se escribe con una "C" mayúscula.

Una nota de interés es que no todos los países parecen tener una definición oficial de ciberespacio. China y Japón son tales ejemplos. Aparentemente,

no tienen una definición predominante de qué es el ciberespacio, pero cada parte del gobierno usa su propia definición.

En general, parece que muy pocos gobiernos tienen una definición oficial del ciberespacio. También se debe tener en cuenta que, en algunos casos, la definición de ciberespacio se deriva del término "seguridad cibernética". En estos casos, se consideró que "ciberseguridad" significa "seguridad del ciberespacio".⁷

La ciberseguridad es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.

El término es amplio y se aplica a numerosos elementos, desde seguridad informática hasta recuperación ante desastres y educación del usuario final.

El gobierno de Estados Unidos invierte USD 13 000 millones al año en ciberseguridad, pero advierte que los ciberataques siguen evolucionando con gran rapidez. Para contrarrestar la proliferación de código malicioso y ayudar en la detección temprana, el Instituto Nacional de Estándares y Tecnología (NIST) recomienda el monitoreo continuo y en tiempo real de todos los recursos electrónicos.

Las amenazas que contrarrestan la ciberseguridad son tres: **el cibercrimen**, que incluye actores individuales o grupos que dirigen ataques a sistemas para obtener ganancias financieras; **la ciberguerra**, que a menudo involucra recopilación de información con motivaciones políticas; y **el ciberterrorismo**, cuyo propósito es comprometer los sistemas electrónicos y causar pánico o temor. Los métodos comunes que usan los ciberatacantes para controlar las computadoras o redes incluyen virus, gusanos, spyware y troyanos.

⁷ Ref. Bibliográfica: Damir Rajnovic July 26, 2012 Cisco Blog Security – Disponible en <https://blogs.cisco.com/security/cyberspace-what-is-it>

Los virus y los gusanos se pueden autorreplicar y dañar archivos o sistemas, en tanto que el spyware y los troyanos a menudo se utilizan para la recopilación subrepticia de datos.

En general, un usuario promedio entra en contacto con código malicioso a través del archivo adjunto de un correo electrónico no solicitado o cuando descarga programas que parecen legítimos, pero de hecho contienen una carga de malware.⁸

2.2. Instituciones Públicas vinculadas con la Ciberdefensa en Paraguay

El Estado paraguayo viene realizando tareas de orden estructural para considerar las implicancias del ciberespacio en el país, y en especial la defensa nacional que se denominará ciberdefensa.

“La defensa nacional es el sistema de políticas, procedimientos y acciones desarrollado exclusivamente por el Estado para enfrentar cualquier forma de agresión externa e interna que ponga en peligro la soberanía, la independencia y la integridad territorial de la República, o el ordenamiento constitucional democrático vigente.”⁹

Es un deber y atribución del Presidente de la República declarar el Estado de Defensa Nacional (Art 238 inciso 7 de la Constitución Nacional), adopta las medidas necesarias para defensa nacional (Art 238 inciso 9 de la Constitución Nacional).

Por otra parte, la defensa nacional es un derecho y un deber de todos los paraguayos (Art. 4 Ley 1337/99). Por lo expuesto anteriormente, la defensa nacional está liderado por el Presidente de la República.

En la Ley 1337/99 se establece el marco de la defensa nacional, donde el Presidente de la República cuenta con el Consejo de Defensa Nacional como órgano asesor y

⁸ Kaspersky. ¿Qué es la Ciberseguridad? 2019. Consultado el 23 de abril 2019. Disponible en <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>

⁹ Art. 1 Ley 1337/99

consultivo en materia de defensa nacional (Art. 8 Ley 1337/99). El Consejo de Defensa Nacional está conformado por:

- a) el Presidente de la República, quien lo presidirá;
- b) el Ministro de Defensa Nacional;
- c) el Ministro de Relaciones Exteriores;
- d) el Ministro del Interior;
- e) el Oficial General que ejerza el cargo más elevado dentro de las Fuerzas Armadas de la Nación;
- f) el Jefe del Estado Mayor Conjunto de las Fuerzas Armadas de la Nación;
- g) el Funcionario a cargo del organismo de inteligencia del Estado; y,
- h) el Secretario Permanente del Consejo de Defensa Nacional.

Entre las funciones de la Secretaría Permanente del Consejo de Defensa Nacional (Art. 14 Ley 1337/99) se encuentran:

- a) acopiar información y documentación de interés para la defensa nacional;
- b) elaborar y proponer el programa de estudios e investigaciones de carácter científico-técnico que se vinculen con los fines y objetivos de la defensa nacional;
- c) elaborar borradores y formular sugerencias para la elaboración del plan y la política nacionales de la defensa, y los correspondientes planes sectoriales que se deriven del mismo, para discutirlos en el seno del Consejo de Defensa Nacional;

Las funciones del Consejo de Defensa Nacional anteriormente indicadas constituyen la base para abordar la planificación básica para la defensa nacional.

Por otra parte, el Ministerio de Tecnologías de la Información y Comunicación - MITIC (Art. 7 Ley 6207/2018) tiene como competencias:

- Promover iniciativas que contribuyan a la construcción de un ecosistema digital seguro, confiable y resiliente, incluyendo el sector público, privado, academia y ciudadanía.
- Coordinar la ejecución de acciones conjuntas e integradas entre las distintas reparticiones públicas, de actividades relacionadas con la integración de los servicios públicos, ciberseguridad, el desarrollo de la normalización y la sistematización y difusión de la información de acciones relacionadas con la gestión pública por medios electrónicos.
- Propiciar y emitir directrices para la optimización de los trámites y procesos, y la interoperabilidad entre los distintos Organismos y Entidades del Estado (OEE), a su vez diseñar, coordinar, y monitorear las políticas públicas, planes y estrategias a ser ejecutadas por los mismos, en el marco del Gobierno Electrónico y de Ciberseguridad.
- Dictar, asesorar y participar en la formulación de las políticas nacionales en todas aquellas materias relacionadas con la protección de la información personal y gubernamental; el uso de tecnologías en la educación, en materia de ciberseguridad, innovación productiva, economía digital y demás sectores convergentes de las Tecnologías de la información y Comunicación (TIC).
- Ejercer como Autoridad de Ciberseguridad, y de prevención, gestión y control de incidentes cibernéticos que pongan en riesgo el ecosistema digital nacional.

- Definir y designar los sistemas, procesos y tecnologías de información que serán considerados infraestructura TICs crítica para el funcionamiento del Estado paraguayo.
- Salvaguardar la efectiva capacidad de gestión de la infraestructura TICs crítica para el funcionamiento del Estado paraguayo.

En resumen, el MITIC tiene varias competencias que contribuyen a establecer las condiciones en términos de políticas, planes y acciones para establecer el ecosistema digital seguro y la Ciberseguridad. El área operativa de las acciones de Ciberseguridad se encuentra en la Dirección General de Ciberseguridad y Protección de la información del Viceministerio de Tecnologías de la Información y Comunicación del MITIC. Trabajar coordinadamente con el MITIC es clave para poder abordar la Ciberdefensa.

Por lo anteriormente expuesto, el Presidente del Consejo de Defensa Nacional tiene la atribución (Art. 8 Ley 1337/99) para que representantes del MITIC vinculados con ciberseguridad puedan participar en las deliberaciones que permitan abordar el plan de ciberdefensa.

2.3. Situación actual del Paraguay en materia de Ciberdefensa.

La defensa nacional es una de las funciones básicas del estado, la Ciberdefensa se define como el conjunto de acciones de defensa activas-pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio, mitigar y neutralizar al enemigo o a otras inteligencias en oposición.

De acuerdo con artículos referentes a la Ciberdefensa y Ciberseguridad a nivel regional¹⁰, los países como Brasil, Chile, Colombia, Argentina, Perú, Venezuela y otros países componentes del llamado UNASUR (Unión De Naciones Sudamericanas) cuentan con programas referentes a la ciberdefensa como un bloque unido para fortalecer la defensa regional, este bloque en agosto del 2013 ha emitido

¹⁰ Consejo de Defensa Sudamericano- UNASUR. Ministerio de Defensa Nacional del Ecuador. Mecanismos de Defensa. 2014. Consultado el 26 de abril 2019. Disponible en http://www.imaginar.org/taller/ciberdefensa/D2_09_mecanismos_cdsmidena_mfiol.pdf

una declaración firme para el rechazo sobre la interceptación de las telecomunicaciones y las acciones de espionaje por parte de la agencia nacional de seguridad del gobierno de los Estados Unidos, las cuales constituyen una amenaza a la seguridad y graves violaciones de los derechos humanos, civiles y políticos del derecho internacional y de las soberanías, y que propiamente dañan las relaciones entre naciones, a partir de este hecho estos países han empezado a invertir y desarrollar mecanismos, políticas y otros componentes necesarios para la Ciberdefensa y Ciberseguridad.

En este sentido Paraguay ha empezado a mancomunar esfuerzos para la elaboración del Plan Nacional de Ciberseguridad liderando la Presidencia de la República del Paraguay, por medio de aquel entonces la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs) actualmente Ministerio de Tecnologías de la Información y Comunicación (MITIC), y en coordinación con el Ministerio de Relaciones Exteriores (MRE). Este Plan Nacional se produjo con la participación de los diversos sectores involucrados en el tema de la ciberseguridad en Paraguay, bajo el apoyo y facilitación de la Organización de los Estados Americanos (OEA). En cuanto a Ciberdefensa se han realizado seminarios internacionales en el que fuerzas militares y policiales son instruidos por disertantes expertos de Israel, España, Brasil y de Estados Unidos, donde se ha dado principal énfasis en la Protección de la información estatal sensible, el Plan Nacional de Ciberseguridad, Seguridad de la Información y Auditoría de Sistemas, una visión desde la óptica de la Ciberdefensa¹¹.

Además, el Ministerio de Tecnologías de la Información y Comunicación y el Ministerio de Defensa Nacional en convenio de cooperación en base al delineamiento de una agenda digital que tiene como hoja de ruta el Estado paraguayo, la Ciberdefensa se encuentra dentro de los ejes estratégicos de la misma, mediante este acuerdo se ha llevado a cabo la Primera especialización en Ciberdefensa y Ciberseguridad Estratégica en el Instituto de Altos Estudios

¹¹ Agencia de Información Paraguaya. Ministerio de Tecnologías de la Información y Comunicación. Unidad Especializada Tics. Militares y policías fueron instruidos en Ciberdefensa. 2016. Asunción. Paraguay Consultado 25 de abril 2019 Disponible en <https://www.ip.gov.py/ip/este-viernes-culmina-el-segundo-seminario-internacional-de-ciberdefensa/>

Estratégicos (IAEE) para formar recursos humanos calificados en materia de Ciberdefensa.

2.4. Situación actual del Paraguay en materia de Ciberseguridad

Dado que el ciberespacio se ha convertido en un ámbito de impensada importancia para el sistema comunicacional y operacional del ser humano, a tal punto de que prácticamente toda forma de interrelación y de operaciones van migrando a este ámbito, cada vez a mayor ritmo de aceleración.

Podemos citar que *“el ciberespacio puede ser pensado como la interconexión de los seres humanos a través de las telecomunicaciones, sin tener en cuenta la geografía física”*¹², cuyos elementos deben ser mantenidos en un ambiente de mayor seguridad posible de forma a impedir el acceso indebido de las informaciones o la manipulación indebida de los procesos que suceden en ella, recayendo en los gobiernos nacionales o en las asociaciones de ellos la responsabilidad de garantizar el normal y correcto funcionamiento del ciberespacio, en colaboración con el sector no público como actor interesado en los beneficios que brinda el uso seguro de la tecnología.

El escenario sugiere la difuminación de los límites nacionales y el aumento de fenómenos globales de beneficios y/o de delincuencia cibernética que afectan de igual modo a distintos actores independientemente de la ubicación física en que se encuentren, lo que lleva a iniciar nuevos mecanismos de cooperación internacional, enfocados en la previsión y/o tratamientos de eventos consumados para paliar los efectos de la ciberdelincuencia.

La relación de las altas probabilidades de beneficios y el bajo coste de las herramientas para delinquir en el ciberespacio hacen de la misma un punto atractivo para los ciberdelincuentes, unidos a la independencia de la ubicación geográfica para el atacante, y las altas posibilidades de mantener el anonimato y de estar alcanzados por leyes que no le son aplicables.

¹² Revista UNISCI N° 42. octubre 2016. La ciberseguridad como factor crítico en la Seguridad de la Unión Europea. Consultado 25 de abril 2019 Disponible en <https://www.ucm.es/data/cont/media/www/pag-89564/UNISCIDP42-2NIEVA-MANUEL.pdf>

En el contexto de los avances tecnológicos globales, el Paraguay como país inserto en el contexto internacional ha experimentado el auge tecnológico en las comunicaciones, en el tratamiento de la información y la incorporación de las mismas en los distintos campos del quehacer estatal, académico, industrial, comercial y de servicios, por lo que se hizo necesario desde el gobierno enfocarse en una política nacional de Ciberseguridad, que si bien es cierto ha llegado con bastante retraso en comparación con otros países del mundo y de la región, es importante acelerar su implementación efectiva en base a un orden de necesidades y prioridades, debiendo realizarse las adecuaciones periódicas que sean necesarias para que sea una herramienta realmente útil a nivel estratégico nacional.

Otras cuestiones relacionadas son las instituciones encargadas de llevar a cabo la persecución de la delincuencia cibernética, como la creación en el año 2010 de la Unidad Especializada de Delitos Informáticos de la Fiscalía General, que trabaja con la Unidad Especializada en la Lucha contra la Trata de Personas y la Explotación Sexual de Niños, Niñas y Adolescentes. Esta unidad firmó un importante acuerdo en enero de 2014 con el Centro Nacional de Niños Desaparecidos y Explotados (NCMEC, por sus siglas en inglés).

El Ministerio Público también trabaja en coordinación con la Policía Nacional, en particular con la División Especializada contra Delitos Informáticos, dependiente del Departamento contra Delitos Económicos y Financieros, que está encargada de la investigación de hechos punibles de carácter informático.

En Paraguay se ha tenido un incremento muy vigoroso en el número de usuarios de Internet. Esto merece un llamado de atención en cuanto a los mecanismos de Ciberseguridad que se le puede ofrecer a la ciudadanía.

Sin embargo, el uso de las TIC trajo consigo desafíos permanentes, no sólo en lo que se refiere a sus cambios tecnológicos constantes, sino también al aumento del riesgo de delitos informáticos, es decir, aquellos que se realizan utilizando como herramienta principal las TIC y/o suelen implicar la violación de sistemas informáticos.

La facilidad de las transacciones financieras por Internet y el flujo de información aumentan el riesgo de explotación y abuso a través de los delitos informáticos con los que se obtiene acceso a la información personal y sensible.

Las características intrínsecas de los delitos informáticos, tales como el costo reducido de los ataques y su facilidad de ejecución, pueden causar graves dificultades en el desarrollo de las TIC, en los servicios prestados por la Administración Pública, en el buen funcionamiento de las infraestructuras críticas y en las actividades de las empresas y ciudadanos.

La ciberseguridad es así una necesidad para el avance confiable de los sistemas de información y comunicación, así como para la protección de los ciudadanos, particularmente los más vulnerables.

El PNC complementa y fortalece otras iniciativas actualmente en desarrollo por parte del Estado como lo son los proyectos de Gobierno Electrónico, TIC en la Educación e Inclusión Digital, despliegue de fibra óptica, Firma Digital, Comercio Electrónico, del Centro de Respuesta ante Incidentes (CERT-PY), de la Unidad Especializada de Delitos Informáticos del Ministerio Público y de la División Especializada contra Delitos informáticos de la Policía Nacional, entre otros.

Asimismo, se ha observado en Paraguay un aumento de los ataques cibernéticos, como los ataques de denegación de servicios (DoS), incluidos incidentes dirigidos a los portales web de diversos organismos gubernamentales. En 2012, hubo una serie de ataques contra sitios web gubernamentales.^{13 14}

Entre otros ciberataques vivenciados en Paraguay se encontró el Internet de numeraciones de tarjetas de créditos (actividad conocida como carding) entre agosto de 2002 y octubre de 2004. Asimismo, hubo casos de apología del delito a través de la red, así como delitos, estafa. En el ámbito de las redes sociales, se denuncia casi diariamente la creación de perfiles falsos, los cuales serían utilizados

¹³ Centro de Respuestas ante incidentes cibernéticos CERT-PY Disponible en: <http://www.cert.gov.py/index.php>

¹⁴ ABC Color. Admiten debilidad de webs. 21 julio 2012. Consultado 23 abril 2019. Disponible en <http://www.abc.com.py/nacionales/admiten-vulnerabilidad-de-webs-428866.html>

como medio para la captación de posibles víctimas de trata de personas, extorsiones, grooming o ciberbullying.

La explotación sexual infantil también forma parte de los delitos que se encuentran más frecuentemente citados en las estadísticas. El Ministerio Público, conjuntamente con la División Especializada contra Delitos Informáticos de la Policía Nacional, investiga casos en que se utilizan las redes sociales para exhibir imágenes y ofertar a menores de edad.

En base a la cooperación internacional con el Centro Nacional para Niños Desaparecidos y Explotados (NCMEC, por sus siglas en inglés) desde enero de 2014, se pudieron detectar más de 797 casos, entre fotos y videos de pornografía infantil, que fueron subidos a la red desde Paraguay entre febrero del 2014 y abril del 2015.

En el 2012, el reporte de NCMEC identificó 408 casos de pornografía infantil en el país, sin embargo, se realizaron solamente 13 denuncias al Ministerio Público.

Estos datos no sólo revelan la importancia de establecer mecanismos para impedir la proliferación de delitos cometidos a través de medios tecnológicos, sino también la necesidad de establecer mecanismos que posibiliten la denuncia, la investigación y el enjuiciamiento de estos delitos.

La única forma de avanzar de manera efectiva con la ciberseguridad en el país es mediante la identificación de la situación actual y de los principales desafíos a enfrentar para trascenderla.¹⁵

¹⁵ Detenido por pedir en Facebook al EPP que secuestren a hijos de congresistas y maten policías”. Disponible en: <http://ea.com.py/v2/detenido-por-pedir-en-facebook-al-epp-que-secuestren-a-hijos-de-congresistas-y-maten-policias/>.

Bancarios van a 3 años a cárcel por estafa de 400 mil dólares”. Disponible en: <http://www.ultimahora.com/bancarios-van-3-anos-carcel-estafa-400-mil-dolares-n705027.html>.

Cae proxeneta que utilizaba perfiles falsos en internet para extorsionar”. Disponible en: <http://www.abc.com.py/edicion-impresa/judiciales-y-policiales/cae-proxeneta-que-utilizaba-perfiles-falsos-en-internet-para-extorsionar-1363524.html>.

Fiscalía investigará caso de pornografía infantil”. Disponible en: <http://www.paraguay.com/nacionales/fiscalia-investigara-caso-de-pornografia-infantil-126212>

3. Situación a nivel regional de los compromisos nacionales en Ciberseguridad

Latinoamérica, como región, sintió la necesidad de sumarse al trabajo de normar, proyectar, legislar y cooperar entre sí para enfrentar muchas situaciones y prevenir otras, productos de ciberataques.

En Latinoamérica se empezó a trabajar con la normativa de los países en cuanto a lo que le exigen a las empresas para cuidar su información.

Las experiencias adquiridas en la región han ayudado también al Paraguay a encaminar los proyectos a nivel nacional reestructurando desde lo referente a establecer las entidades responsables hasta actualizar la legislación que apoye la gestión.

Un análisis comparativo de los índices de ciberseguridad presentado por la International Telecommunication Union (ITU) en los últimos años nos demuestra el trabajo que viene realizando cada país en el tema.

El Índice de Ciberseguridad Global (GCI) es una iniciativa de la Unión Internacional de Telecomunicaciones (ITU) que involucra a expertos de diferentes organizaciones, está compuesto, producido, analizado y publicado para medir el compromiso de los Estados miembros. Esta marcado en la Agenda de Ciberseguridad Global (GCA) de la ITU que se lanzó en 2007, y refleja sus 5 pilares: legal, técnico, organizativo, desarrollo de capacidades y cooperación.

El GCI combina 25 indicadores en una medida de referencia para monitorear el compromiso de ciberseguridad de 194 Estados Miembros recopilados a través de una encuesta online.

Para cada pilar, se han desarrollado preguntas para evaluar el compromiso. A través de la consulta con un grupo de expertos, las preguntas se ponderan con una puntuación global GCI.

Según datos obtenidas junto a la CONATEL en la mesa de discusión conducida el 6 de mayo de 2015 y en el “Plan Nacional de Telecomunicaciones Paraguay 2011-2015”, disponible en: <http://www.conatel.gov.py/files/MANUAL%20PLAN%20NACIONAL.pdf>.

El resultado general muestra la mejora y el fortalecimiento de los cinco pilares en varios países de todas las regiones. Además de proporcionar la puntuación GCI, este índice también proporciona información sobre las prácticas en cada país miembro que dan una idea del progreso logrado.

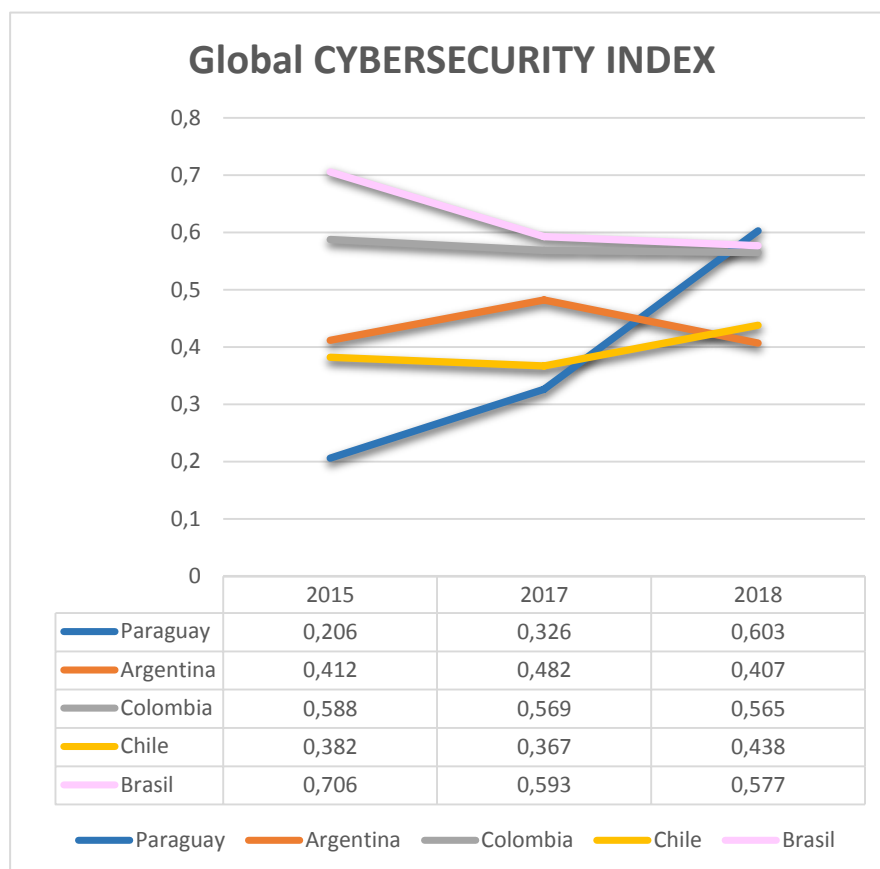


Figura 2 Comparativo Índices Globales de Ciberseguridad

En el análisis comparativo de los valores de los índices presentados por la ITU se visualiza el estado en el que esta cada uno de los países seleccionados en esta investigación.

Este gráfico nos permite visualizar rápidamente el nivel de compromiso y los esfuerzos que se está haciendo en la región al respecto de la Ciberseguridad y Ciberdefensa.

De acuerdo al informe 2018 de la ITU a nivel global se puede observar la situación regional en América del Sur representando entre la mayoría de los países miembros de esa región valores similares en sus índices de compromiso.

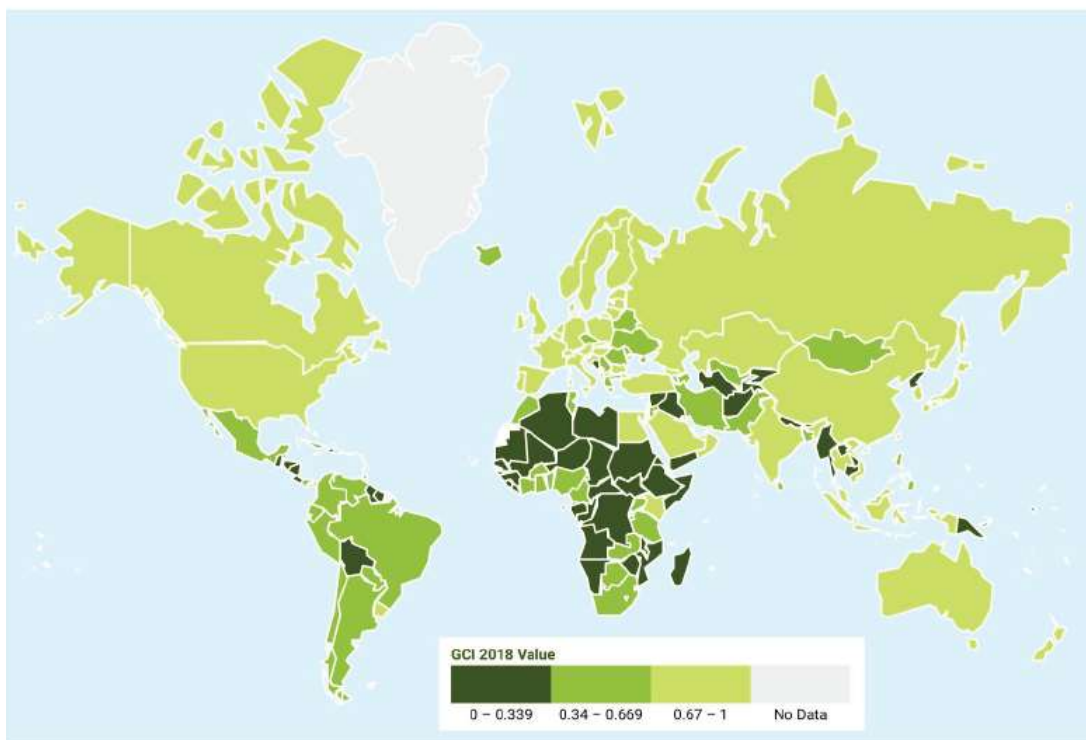


Figura 3 Cuadro de calor de los índices globales de Ciberseguridad

Entre los países destacados en la región hemos seleccionado Argentina, Brasil, Chile y Colombia para mencionar el proceso desde sus inicios y su situación actual en cuanto al manejo de la Ciberseguridad y Ciberdefensa.

3.1. Argentina

En Argentina para el ámbito de la Ciberdefensa la Subsecretaría de Ciberdefensa del Ministerio de Defensa y el Comando Conjunto de Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas son los organismos encargados de dar respuesta ante las amenazas cibernéticas o agresiones que afectan la defensa nacional. El Comando Conjunto de Ciberdefensa cuenta con un Comandante y depende del Estado Mayor, y contiene dos áreas que son el Centro de Ingeniería y el Centro de Operaciones.

El concepto de Ciberdefensa de la República Argentina conforme al sistema de defensa nacional sigue un modelo de carácter defensivo y está orientado al desarrollo de capacidades. En la legislación argentina existe una definición específica de Ciberdefensa en la Actualización de la Directiva de Política de Defensa Nacional, donde se observó que desde el 2006 al 2015 se tuvo un aumento de

regulaciones sobre el tema, pero dicho crecimiento normativo también tiene ambigüedades e interpretaciones diversas en los criterios jurídicos al momento de la aplicación. Es posible destacar las normativa del Poder Ejecutivo Nacional (decretos) y se suman normativas vinculadas a seguridad de la información, infraestructuras críticas y regulaciones de Internet (por ejemplo, la Ley N° 27.078 de Argentina Digital).¹⁶

El Comando Conjunto de Ciberdefensa, participo en el II Ciberolimpiadas Militares 2018 realizado en Colombia en agosto del 2018.

3.2. Colombia

En el 2011 el gobierno colombiano expidió el primer documento CONPES (Consejo Nacional de Política Económica y Social) para establecer la institucionalidad en Ciberseguridad y Ciberdefensa. Con esto se da inicio al ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) y el CCOC (Comando Conjunto Cibernético). También cada fuerza militar desarrolló su capacidad de ciberdefensa y ciberseguridad, y la Policía se suma con el Centro Cibernético Policial.

Posterior a esto en el 2016, otro CONPES actualizó la política con una perspectiva integral de Estado en seguridad digital, que incluyó al Ministerio de Tecnologías de la Información y Telecomunicaciones, y a los sectores financieros y de energías. Con la coordinación del consejero de Seguridad de Presidencia, Colombia adoptó las recomendaciones internacionales de la OTAN y hoy está como uno de los referentes de la región.

En el mismo año en Setiembre, durante el Simposio Internacional sobre Seguridad Cibernética y Equipos de Respuesta, Colombia procedió a la firma de un Memorando de Entendimiento con la Organización de Estados Americanos (OEA) para el establecimiento de un Centro de Conocimiento para la Seguridad Digital en

¹⁶ Silvina Cornaglia - Ariel Vercelli, 2017. La ciberdefensa y su regulación legal en Argentina 2006 – 2015 (en línea). URVIO. Consultado 25 abril 2019. Disponible en <http://dx.doi.org/10.17141/urvio.20.2017.2601>

Bogotá, para compartir las buenas prácticas, intercambiar información y fortalecer la cooperación¹⁷.

También en Marzo de 2019 Colombia y Chile suscribieron Memorando de Entendimiento de Cooperación en Ciberseguridad, Ciberdefensa y Cibercriminalidad para promover la cooperación recíproca en las áreas de interés común en materia de ciberseguridad, así como la coordinación entre las entidades participantes de ambos países¹⁸.

3.3. Chile

En Chile se empezó a trabajar en todo lo relacionado a las nuevas tecnologías desde el año 1998 con la conformación de una Comisión Presidencial "*Nuevas Tecnologías de Información y Comunicación*", constituida por Decreto Supremo el 1 de julio de 1998. Sus labores finalizaron el 26 de enero de 1999 con la entrega de un informe final.

La Agenda Digital (AD) es un trabajo iniciado en abril del año 2003 con la constitución del Grupo de Acción Digital (GAD) El resultado de este esfuerzo es un amplio acuerdo público-privado sobre una estrategia-país, mirando a la celebración del Bicentenario en 2010, y un Plan de Acción para el período 2004- 2006, que contempla 34 iniciativas.


En el marco de la Estrategia Digital elaborada para el periodo 2007-2012 se estableció como objetivo "*Contribuir al desarrollo económico y social del país a través del potencial que ofrece el uso de las tecnologías de información y comunicación para mejorar la calidad de la educación, incrementar la*

¹⁷ Escuela Suramericana de Defensa. Colombia contará con un Centro de Conocimiento de Seguridad Digital. Publicado 29 Setiembre 2016. Consultado 25 abril 2019. Disponible en <http://esude-cds.unasursg.org/index.php/noticias/141-colombia-contara-con-un-centro-de-conocimiento-de-seguridad-digital>

¹⁸ Cancillería de Colombia. Colombia y Chile suscribieron Memorando de Entendimiento de Cooperación en Ciberseguridad, Ciberdefensa y Cibercriminalidad. Publicado 21 marzo 2019. Consultado 25 abril 2019. Disponible en <https://www.cancilleria.gov.co/newsroom/news/colombia-chile-suscribieron-memorando-entendimiento-cooperacion-ciberseguridad>

transparencia, aumentar la productividad y competitividad, y hacer mejor gobierno, mediante mayor participación y compromiso ciudadano.”¹⁹

El programa de gobierno 2018-2022 considera el desarrollo de una estrategia de seguridad digital que tiene por misión la protección de los usuarios privados y públicos, junto con la protección de la privacidad de nuestros ciudadanos.²⁰



1999		2003	2006		2007	2012		2017	2022
<i>Comisión Presidencial "Nuevas Tecnologías de Información y Comunicación"</i>	...	<i>Agenda Digital (AD)</i>		...	<i>Estrategia Digital</i>		...	<i>Política Nacional de Ciberseguridad</i>	
		<i>Grupo de Acción Digital (GAD)</i>							

Figura 4 Línea de tiempo PNC en Chile

3.4. Brasil

Los esfuerzos de defensa y seguridad cibernéticas en Brasil suceden en un contexto de iniciativas de reestructuración interna y fortalecimiento de la capacidad de defensa nacional iniciada en 1999 con la creación del Ministerio de la Defensa.²¹

La coordinación de la ciberdefensa está a cargo del “Centro de Defensa Cibernética” (CDCiber), vinculado al Ejército brasileño y al Ministerio de la Defensa.

El CDCiber, creado en 2010, volviéndose operacional entre los años de 2011 y 2012. El centro se encuentra entre los niveles estratégico y operacional del gobierno, a vez que es subordinado al Ministerio de la Defensa.

La estrategia del CDCiber incluye actividades cibernéticas en las áreas de la inteligencia, ciencia y tecnología, habilidades operacionales, doctrina y recursos

¹⁹ Comité de Ministros. Desarrollo Digital. Estrategia Digital 2007 – 2012. Publicado diciembre 2007. Santiago, Chile. Consultado 23 abril 2019. Disponible en https://www.observatoriodigital.gob.cl/sites/default/files/estrategia_digital_2007-2012.pdf

²⁰ Comité Interministerial sobre Ciberseguridad. Programa de gobierno 2018-2022. Santiago, Chile. Consultado 23 abril 2019. Disponible en <https://www.ciberseguridad.gob.cl/el-cics/>

²¹ URVIO - Revista Latinoamericana de Estudios de Seguridad N° 20, junio 2017, pp. 16-30. Consultado 24 abril 2019. Disponible en <https://revistas.flacsoandes.edu.ec/urvio/article/view/2576/2104>

humanos; su misión consiste en la protección de las redes militares y gubernamentales de ciberataques.

El Departamento de Seguridad de Información y Comunicación (DSIC-GSI), órgano que compone el gabinete, es directamente responsable por la coordinación de acciones de seguridad cibernética, lo que incluye la operación y manutención de un centro de tratamiento de incidentes en las redes de la Administración Pública Federal (APF).

La Estrategia de Ciberseguridad estableció metas de mejoramiento de la seguridad y resiliencia de las infraestructuras críticas y servicios públicos nacionales para el período de 2015 a 2018.

4. Propuesta organizativa

Tomando en consideración lo mencionado, encontramos que ante estas amenazas, se deben delimitar políticas de Ciberdefensa.

Ciberdefensa se entiende como el conjunto de acciones defensivas, exploratorias y ofensivas, realizadas en el ciberespacio, en el contexto de una planificación nacional de nivel estratégico, coordinado e integrado por el Ministerio de Defensa Nacional, con la finalidad de proteger los sistemas de información relacionados a la defensa nacional, obtener datos para la producción de conocimientos de inteligencia y comprometer los sistemas de información del adversario.

El marco regulatorio relativo a las acciones de la defensa nacional, se encuentra delimitado por lo establecido en la Ley N° 1.337/99 “De la Defensa Nacional y de Seguridad Interna” y su modificatoria la Ley N° 5036/13 “Que modifica los Artículos 2°, 3° y 56° de la Ley N° 1337/99 de Defensa. Nacional y Seguridad Interna”.

El artículo 2 de la citada norma, establece “*La defensa nacional es el sistema de políticas, procedimientos y acciones desarrollado exclusivamente por el Estado para enfrentar cualquier forma de agresión externa e interna que ponga en peligro*

la soberanía, la independencia y la integridad territorial de la República, o el ordenamiento constitucional democrático vigente.”²².

En concordancia con el artículo precedente, el artículo 5 del mismo cuerpo legal determina que *“La política de defensa nacional, como parte integrante de la política general del Estado, definirá los objetivos de la defensa nacional y establecerá los recursos y acciones para dar cumplimiento a lo estipulado en el Artículo 2º”.*²³

El Consejo de Defensa Nacional, en uso de sus atribuciones legales y dando cumplimiento a lo establecido en la normativa, a través de la Resolución N° 33/13, aprueba la *“Directiva de Defensa Nacional”* con la finalidad de *“Establecer los lineamientos generales de la Política de Defensa y las directrices para su implementación, de tal forma a constituirse en la base del Planeamiento de la Defensa Nacional y de las capacidades que se precisan.”*²⁴.

Así también, en otro esfuerzo gubernamental de establecer políticas y lineamientos relativos a la Defensa Nacional, a través del Decreto N° 9804/12 *“Por el cual se designa al Ministerio de Defensa Nacional como ente coordinador y responsable de la elaboración del libro blanco de Defensa Nacional de la República del Paraguay”*., don se establece las políticas estatales en materia de defensa nacional, y distingue las acciones y procesos a realizarse a nivel del Estado, para la prosecución de las políticas establecidas.

Del análisis de los instrumentos normativos mencionados de manera precedente, se hace mención y reconocimiento a las amenazas existentes en el ciberespacio, en los siguientes puntos:

²² PARAGUAY. Ley N° 5036/13. 2013. Que modifica los Artículos 2º, 3º y 56º de la Ley N° 1337/99 de Defensa Nacional y Seguridad Interna.

²³ PARAGUAY. Ley N° 5036/13. 2013. Que modifica los Artículos 2º, 3º y 56º de la Ley N° 1337/99 de Defensa Nacional y Seguridad Interna.

²⁴ CONSEJO DE DEFENSA NACIONAL. 2013. Directiva de Defensa Nacional (en línea). Consejo de Defensa Nacional. Paraguay. Consultado 25 abril 2019. Disponible en http://www.mdn.gov.py/application/files/1214/4242/5025/Directiva_de_Defensa_2013_-_2018.pdf

1. Al integrarse al Comité Interamericano contra el Terrorismo, dependiente de la Organización de Estados Americanos, el cual emitió la AG/Res. 2004 que consagra la “ADOPCIÓN DE UNA ESTRATEGIA INTERAMERICANA INTEGRAL DE SEGURIDAD CIBERNÉTICA: UN ENFOQUE MULTIDIMENSIONAL Y MULTIDISCIPLINARIO PARA LA CREACIÓN DE UNA CULTURA DE SEGURIDAD CIBERNÉTICA”, mediante la cual se insta a los Estados miembros a:
 - a. Adoptar la Estrategia Interamericana Integral de Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética.
 - b. Instar a los Estados Miembros a implementar, según corresponda, las recomendaciones de la Reunión Inicial del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA (REMJA-V/doc.5/04) y las recomendaciones relativas a seguridad cibernética de la Quinta Reunión de la REMJA (REMJA-V/doc.7/04 rev. 4) como medio de crear un marco para promulgar leyes que protejan los sistemas de información, impidan el uso de computadoras para facilitar actividades ilícitas y sancionen el delito cibernético.²⁵
2. Reconocimiento a la globalización y las innovaciones tecnológicas como posibles fuentes de nuevas amenazas para la soberanía nacional, a través de ciberataques y cuyas consecuencias resultan poco predecibles.
3. Reconocimiento como Área de Operaciones de Ciberdefensa, identificando los posibles daños a ser causados por ciberataques. Este documento reza *“Los delitos cibernéticos tienen la posibilidad de dañar y causar perjuicios, atacando la infraestructura informática. Los virus informáticos y programas especiales pueden permear la seguridad de los*

²⁵ ORGANIZACIÓN DE ESTADOS AMERICANOS. 2004. Adopción de una estrategia interamericana integral de seguridad cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética (en línea). Estados Unidos de América. Consultado 25 abril 2019. Disponible en <https://www.sites.oas.org/cyber/Documents/Estrategia-seguridad-cibernetica-resolucion.pdf>

sistemas informáticos y afectar otros sistemas, tales como los financieros, bancarios, militares, de infraestructura, programas e investigaciones, tanto de entes gubernamentales como privados.”²⁶

Por tanto, es posible determinar que dentro de las políticas de Estado relativas a la defensa nacional, se identifican a las amenazas cibernéticas y se reconocen el daño que dichas amenazas pueden causar al Estado. Sin embargo, a modo de establecer una política rectora en Ciberdefensa, el Estado debe actualizar el marco normativo de la materia, para estar a la altura de los estándares internacionales y determinar claramente el marco de acción para el desarrollo de actividades de Ciberdefensa por parte de las instituciones designadas para ello.

Asignar los recursos humanos y financieros necesarios para implementar el PNC, además de las mejoras necesarias que se aluden en el apartado anterior donde se mencionan y transcriben algunas cuestiones urgentes de atender debido a la cada vez más alta necesidad de su puesta en marcha, considerando el vertiginoso avance de las innovaciones tecnológicas y el perfeccionamiento de las técnicas y tácticas de la ciberdelincuencia que expone a la sociedad a daños cada vez mayores.

²⁶ MINISTERIO DE DEFENSA NACIONAL. 2013. Primer Libro Blanco de la Defensa Nacional de la República del Paraguay (en línea). Paraguay. Consultado 25 abril 2019. Disponible en <http://providingforpeacekeeping.org/wp-content/uploads/2016/02/2013-Libro-Blanco-de-la-Defensa.compressed.compressed.pdf>

CONCLUSIÓN

En la actualidad, una de las principales amenazas para las organizaciones son los ciberataques, los cuales se materializan a través de los puntos vulnerables de los sistemas interconectados en el ciberespacio, que afectan y dañan de manera directa y sustancial a personas, empresas, organizaciones y en diversas ocasiones a infraestructura crítica del Estado o a servicios prestados por el mismo, en detrimento al bienestar nacional o a sus capacidades de defensa.

Constituyen ciberataques el conjunto de acciones ofensivas realizadas por un individuo o un grupo de individuos contra un sistema de información a través de medios tecnológicos para conseguir un objetivo.

Ante estas circunstancias, tanto las organizaciones civiles, corporaciones y, en especial el Estado deben contar con estrategias a modo de demostrar capacidad de defensa y resiliencia ante estos eventos, minimizando el impacto de los mismos.

Siendo esto así, el fin máximo de cada uno de los Estados es salvaguardar su soberanía, economía y sus infraestructuras críticas ante posibles amenazas y ataques, de parte de cibercriminales o de otros Estados.²⁷

La seguridad cibernética es una parte cada vez más importante de nuestra vida hoy en día, y el grado de interconexión de las redes implica que todo puede estar expuesto, y todo, desde la infraestructura crítica nacional hasta nuestros derechos humanos básicos, puede verse comprometido. Por lo tanto, se insta a los gobiernos a considerar políticas que apoyen el crecimiento continuo de la sofisticación, el acceso y la seguridad de la tecnología y, como primer paso crucial, adoptar una estrategia nacional de ciberseguridad.

Como aspectos generales a mejorar en el PNC, figuran la necesidad de ir mejorando el contexto de las cuestiones relativas a la protección de la privacidad y la libertad de expresión de las personas, la adhesión a convenios internacionales y el

²⁷ KOLINI, F. Y JANCZEWSKI, L. (2015), "Cyber Defense Capability Model: A Foundation Taxonomy" (en línea). Association for Information Systems. Australia. Consultado el 25 abril 2019. Disponible en <https://aisel.aisnet.org/confirm2015/32>

establecimiento de alianzas reales a nivel internacional para la persecución de delitos cibernéticos.

Por todo lo expuesto e investigado, consideramos que siendo el Plan Nacional de Ciberdefensa una cuestión de nivel estratégico, debería ser aplicado bajo la coordinación del Ministerio de Defensa Nacional utilizando para sus objetivos nacionales a las FF.AA. como la primera medida de acción; teniendo la colaboración del MITIC y profesionales civiles especializados en el tema.

BIBLIOGRAFÍA

- SENATICs. 2017. Plan Nacional de Ciberseguridad. Paraguay.
- PRESIDENCIA DE LA REPÚBLICA DEL PARAGUAY DECRETO 7052. 2017. Aprobación Plan Nacional de Ciberseguridad
- ITU. Guía para la elaboración de una Estrategia Nacional de Ciberseguridad. 2018. ISBN: 978-92-61-27793-2
- ITU. Global Cybersecurity Index (GCI) 2018 Suiza. ISBN: 978-92-61-28201-1
- ITU. Global Cybersecurity Index (GCI) 2017 Suiza. ISBN: 978-92-61-25071-3
- Biblioteca del congreso. Decretos.
- ITU. Committed to connecting the world.. Cybersecurity 2017. Consultado el 25 abril 2019. Disponible en <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx>
- Secretaria Nacional de Tecnologías de la Información y Comunicación 2017. Encuesta sobre Acceso y Uso de Internet en Paraguay (en línea). Asunción. Paraguay. Consultado 25 de abril. 2019. Disponible en <http://gestordocumental.senatics.gov.py/share/s/ntjnuNLeT8u3gbAHC6WeVw>.
- Secretaria Nacional de Tecnologías de la Información y Comunicación. Plan Nacional de Ciberseguridad. ¿Cómo se trabajó? Asunción. Paraguay Consultado 25 de abril 2019. Disponible en <https://www.senatics.gov.py/plan-nacional-de-ciberseguridad/como-se-trabajo>
- Ministerio de Tecnologías de la Información y Comunicación. Viceministerio de Tecnologías de la Información y Comunicación.

Ciberseguridad y protección a la información. Asunción. Paraguay
Consultado 25 de abril 2019 Disponible en
<https://www.mitic.gov.py/viceministerios/tecnologias-de-la-informacion-y-comunicacion/ciberseguridad-y-proteccion-a-la-informacion>

- *Cisco NetAcad, un programa de responsabilidad social corporativa de Cisco.*
- Damir Rajnovic, July 26, 2012
- Ref. Bibliográfica: Damir Rajnovic July 26, 2012 Cisco Blog Security – Disponible en <https://blogs.cisco.com/security/cyberspace-what-is-it>
- Kaspersky. ¿Qué es la Ciberseguridad? 2019. Consultado el 23 de abril 2019. Disponible en <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>
- Consejo de Defensa Sudamericano- UNASUR. Ministerio de Defensa Nacional del Ecuador. Mecanismos de Defensa. 2014. Consultado el 26 de abril 2019. Disponible en http://www.imaginar.org/taller/ciberdefensa/D2_09_mecanismos_cdsmidena_mfiol.pdf
- Agencia de Información Paraguaya. Ministerio de Tecnologías de la Información y Comunicación. Unidad Especializada Tics. Militares y policías fueron instruidos en Ciberdefensa. 2016. Asunción. Paraguay Consultado 25 de abril 2019 Disponible en <https://www.ip.gov.py/ip/este-viernes-culmina-el-segundo-seminario-internacional-de-ciberdefensa/>
- Revista UNISCI N° 42. octubre 2016. La ciberseguridad como factor crítico en la Seguridad de la Unión Europea. Consultado 25 de abril 2019 Disponible en <https://www.ucm.es/data/cont/media/www/pag-89564/UNISCIDP42-2NIEVA-MANUEL.pdf>

- Centro de Respuestas ante incidentes cibernéticos CERT-PY Disponible en: <http://www.cert.gov.py/index.php>
- ABC Color. Admiten debilidad de webs. 21 julio 2012. Consultado 23 abril 2019. Disponible en <http://www.abc.com.py/nacionales/admiten-vulnerabilidad-de-webs-428866.html>
- Silvina Cornaglia - Ariel Vercelli, 2017. La ciberdefensa y su regulación legal en Argentina 2006 – 2015 (en línea). URVIO. Consultado 25 abril 2019. Disponible en <http://dx.doi.org/10.17141/urvio.20.2017.2601>
- Escuela Suramericana de Defensa. Colombia contará con un Centro de Conocimiento de Seguridad Digital. Publicado 29 Setiembre 2016. Consultado 25 abril 2019. Disponible en <http://esude-cds.unasursg.org/index.php/noticias/141-colombia-contara-con-un-centro-de-conocimiento-de-seguridad-digital>
- Cancillería de Colombia. Colombia y Chile suscribieron Memorando de Entendimiento de Cooperación en Ciberseguridad, Ciberdefensa y Cibercriminalidad. Publicado 21 marzo 2019. Consultado 25 abril 2019. Disponible en <https://www.cancilleria.gov.co/newsroom/news/colombia-chile-suscribieron-memorando-entendimiento-cooperacion-ciberseguridad>
- Comité de Ministros. Desarrollo Digital. Estrategia Digital 2007 – 2012. Publicado diciembre 2007. Santiago, Chile. Consultado 23 abril 2019. Disponible en https://www.observatoriodigital.gob.cl/sites/default/files/estrategia_digital_2007-2012.pdf
- Comité Interministerial sobre Ciberseguridad. Programa de gobierno 2018-2022. Santiago, Chile. Consultado 23 abril 2019. Disponible en <https://www.ciberseguridad.gob.cl/el-cics/>

- URVIO - Revista Latinoamericana de Estudios de Seguridad N° 20, junio 2017, pp. 16-30. Consultado 24 abril 2019. Disponible en <https://revistas.flacsoandes.edu.ec/urvio/article/view/2576/2104>
- PARAGUAY. Ley N° 5036/13. 2013. Que modifica los Artículos 2°, 3° y 56° de la Ley N° 1337/99 de Defensa Nacional y Seguridad Interna.
- PARAGUAY. Ley N° 5036/13. 2013. Que modifica los Artículos 2°, 3° y 56° de la Ley N° 1337/99 de Defensa Nacional y Seguridad Interna.
- CONSEJO DE DEFENSA NACIONAL. 2013. Directiva de Defensa Nacional (en línea). Consejo de Defensa Nacional. Paraguay. Consultado 25 abril 2019. Disponible en http://www.mdn.gov.py/application/files/1214/4242/5025/Directiva_de_Defensa_2013_-_2018.pdf
- ORGANIZACIÓN DE ESTADOS AMERICANOS. 2004. Adopción de una estrategia interamericana integral de seguridad cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética (en línea). Estados Unidos de América. Consultado 25 abril 2019. Disponible en <https://www.sites.oas.org/cyber/Documents/Estrategia-seguridad-cibernetica-resolucion.pdf>
- MINISTERIO DE DEFENSA NACIONAL. 2013. Primer Libro Blanco de la Defensa Nacional de la República del Paraguay (en línea). Paraguay. Consultado 25 abril 2019. Disponible en <http://providingforpeacekeeping.org/wp-content/uploads/2016/02/2013-Libro-Blanco-de-la-Defensa.compressed.compressed.pdf>
- KOLINI, F. Y JANCZEWSKI, L. (2015), "Cyber Defense Capability Model: A Foundation Taxonomy" (en línea). Association for Information Systems. Australia. Consultado el 25 abril 2019. Disponible en <https://aisel.aisnet.org/confirm2015/32>