PLAN NACIONAL DE CIBERSEGURIDAD

RETOS, ROLES Y COMPROMISOS

SECRETARÍA
NACIONAL DE TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

TETÃ REKUÁI
GOBIERNO NACIONAL
Jajapo ñande raperã ko'ãga guive
Construyendo el futuro hoy

ACRÓNIMOS

ADEFI – Asociación de Entidades Financieras del Paraguay
ADSL – Línea de Abono Digital Asimétrica
ANDE – Administración Nacional de Electricidad
APP – Alianza Público-Privada
ASOBAN – Asociación de Bancos de Paraguay
BID – Banco Interamericano de Desarrollo
BNF – Banco Nacional de Fomento
ccTLD – Dominio de Nivel Superior de País
CEPAL – Comisión Económica para América Latina y el Caribe
CERT-PY – Centro de Respuesta ante Incidentes Cibernéticos de Paraguay
CNC – Centro Nacional de Computación
CONACYT – Consejo Nacional de Ciencia y Tecnología
CONATEL – Comisión Nacional de Telecomunicaciones
COPACO – Compañía Paraguaya de Comunicaciones S.A.
DCS – Sistema de Control Distribuido
DoS – Ataque de Denegación de Servicio
ENSC – Estrategia Nacional de Seguridad Ciudadana 2013-2016
ESSAP – Empresa de Servicios Sanitarios del Paraguay S.A.
FEEI – Fondo para la Excelencia de la Educación y la Investigación
FONACIDE – Fondo Nacional de Inversión Pública y Desarrollo
FSU – Fondo de Servicios Universales
IP – Protocolo de Internet
ISO – Organización Internacional de Normalización
IXP – Punto de Intercambio de Internet
LED – Laboratorio de Electrónica Digital
MIC – Ministerio de la Industria y Comercio
MIPYMES – Micro, Pequeñas y Medianas Empresas
MRE – Ministerio de Relaciones Exteriores
NCMEC – Centro Nacional para Niños Desaparecidos y Explotados
NIC.PY – Network Information Center of Paraguay
OEA – Organización de los Estados Americanos
ONG – Organizaciones No Gubernamentales
ORBA – Observatorio Regional de Banda Ancha de la CEPAL
PETROPAR – Petróleos Paraguayos
PIB – Producto Interno Bruto
ProCiencia – Programa Paraguayo para el Desarrollo de la Ciencia y Tecnología
PRONII – Programa Nacional de Incentivo a los Investigadores
RedClara – Cooperación Latino Americana de Redes Avanzadas
SCADA – Supervisión Control y Adquisición de Datos
SENATICs – Secretaría Nacional de Tecnologías de la Información y Comunicación
TIC – Tecnologías de la Información y Comunicación
UNA – Universidad Nacional de Asunción
UNICEF – Fondo para la Infancia de las Naciones Unidas

PRESENTACIÓN

Este Plan Nacional de Ciberseguridad es un documento estratégico que sirve como fundamento para la coordinación de las políticas públicas de ciberseguridad, integrando a todos los sectores en el desarrollo de las tecnologías de la información y comunicación (TIC) en un ambiente cibernético confiable y resiliente. Bajo el liderazgo de la Presidencia de la República del Paraguay, a través de la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs), y en coordinación con el Ministerio de Relaciones Exteriores (MRE), se produjo este Plan Nacional 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).

El resultado de este intenso trabajo de recolección y recopilación de información, combinado con el diálogo y debate con el sector privado y la sociedad civil, es este documento, que no sólo refleja el compromiso del Estado con el desarrollo seguro de las TIC como la mayor de las prioridades, sino que también 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.

ÍNDICE

INTRODUCCIÓN

Ante la creciente importancia de las TIC para la economía y la sociedad, la Presidencia de la República del Paraguay, a través de la SENATICs, ha tomado la decisión de impulsar el desarrollo de un plan estratégico de ciberseguridad. Ningún otro país de América Latina y del Caribe ha tenido un incremento tan vigoroso de número de usuarios de Internet como Paraguay. En términos porcentuales, Paraguay es el país con mayor incremento en la penetración de Internet en la región desde 2012, dado que aumentó de un 29,34 por ciento en 2012 a un 43 por ciento en 2014 – o sea, más de 13,6 puntos porcentuales[1].

Sin embargo, el uso de las TIC trae consigo desafíos permanentes, no sólo en lo que se refiere a sus cambios tecnológicos constantes, sino también al aumento del riesgo de delitos informáticos[2], 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.

Asimismo, los delitos en el ámbito cibernético no se restringen a las acciones contra un sistema informático. Entre febrero del 2014 y abril del 2015, se identificaron más de 797 imágenes de pornografía infantil en las redes sociales subidas desde nuestro país, detectadas como resultado del convenio firmado entre el Ministerio Público y el Centro Nacional para Niños Desaparecidos y Explotados (NCMEC, por sus siglas en inglés)[3]. 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.

Paraguay no está ajeno a estos riesgos; es por ello que el Estado de forma conjunta con el sector privado, la academia y la sociedad civil, ha desarrollado este Plan Nacional para coordinar las políticas públicas de ciberseguridad e integrar a todos los actores interesados en esta tarea. Este Plan complementa y fortalece otras iniciativas actualmente en desarrollo por parte del Estado como lo son los proyectos de Gobierno Electrónico[4], TIC en la educación e inclusión digital, despliegue de fibra óptica, firma digital, comercio electrónico, del Centro de Respuesta ante

---

[1] Ref. ITU https://www.google.com/url?q=http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2016/Individuals_Internet_2000-2015.xls&sa=D&ust=1475240869824000&usg=AFQjCNFVFakzPhpdl4p5o5p9UHGLAsfEjQ

[2] Delito informático: actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito.

[3] Disponible en: http://www.ministeriopublico.gov.py/pornografia-infantil-fiscal-general-conforma-equipo-de-trabajo-y-se-abre-investigacion-de-oficio-n389. Recuperado el 24 de noviembre de 2015.

[4] Disponible en: http://www.senatics.gov.py/servicios-senatics. Recuperado el 24 de noviembre de 2015.

Incidentes Cibernéticos (CERT-PY)[5], de la Unidad Especializada de Delitos Informáticos del Ministerio Público y de la División Especializada contra Delitos informáticos de la Policía Nacional, entre otros.

Este instrumento está compuesto por un diagnóstico sobre la ciberseguridad en el país, el cual sirve de fundamento para los siete ejes estructurales de este Plan Nacional: (i) Sensibilización y Cultura; (ii) Investigación, Desarrollo e Innovación; (iii) Protección de Infraestructuras Críticas; (iv) Capacidad de Respuesta ante Incidentes Cibernéticos; (v) Capacidad de Investigación y Persecución de la Ciberdelincuencia; (vi) Administración Pública y (vii) Sistema Nacional de Ciberseguridad.

1. METODOLOGÍA DE ELABORACIÓN

En el 2015 se desarrollaron mesas de discusión con representantes de todos los sectores de la sociedad paraguaya, afectados directa e indirectamente por el estado actual de la ciberseguridad en el país, con el propósito de recolectar datos e información para la elaboración de este Plan, de manera a que el mismo represente las necesidades específicas de cada sector. Las consultas con los interesados se realizaron siguiendo un estilo de entrevista y se animó a cada grupo de interés a compartir su punto de vista y sus recomendaciones para el proceso. Después de reuniones con los diferentes actores y grupos de interés, se prepararon sucesivos borradores del Plan Nacional de Ciberseguridad que, a su vez, fueron revisados en consultas conjuntas entre el Gobierno y grupos de interés (sociedad civil y sector empresarial) con el propósito de incluir los distintos puntos de vista.

2. DIAGNÓSTICO SOBRE LA CIBERSEGURIDAD EN PARAGUAY

Paraguay posee la población de usuarios y usuarias de Internet de más rápido crecimiento en la región considerando los años 2010 - 2014, con lo cual el fortalecimiento de la ciberseguridad se identifica como urgente y prioritario. 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[6] contra sitios web gubernamentales.

Los delitos en el ámbito cibernético también han estado relacionados a prácticas fraudulentas por el uso de tarjetas de créditos falsas y la explotación de otros mecanismos de pago electrónico. Entre los hechos más denunciados ante la Unidad Especializada de Delitos Informáticos del Ministerio Público y la División Especializada contra Delitos Informáticos de la Policía Nacional, figuran estafas a través de tarjetas de crédito, extorsiones y amenazas utilizando correo electrónico, mensajes de texto y redes sociales, así como alteración de datos en sistemas informáticos. También se menciona la clonación de tarjetas y el abuso de dispositivos electrónicos. Por ejemplo, en julio de 2013, un ciudadano búlgaro fue extraditado a los Estados Unidos desde Paraguay por haber pertenecido a la red *ShadowCrew* de venta por

[5] Disponible en: http://www.cert.gov.py/index.php Recuperado el 24 de noviembre de 2015.
[6] http://www.abc.com.py/nacionales/admiten-vulnerabilidad-de-webs-428866.html

Internet de numeraciones de tarjetas (actividad conocida como *carding*) entre agosto de 2002 y octubre de 2004. Asimismo, hubo casos de apología del delito a través de la red[7], así como delitos de estafa[8]. En el ámbito de las redes sociales, se denuncia casi diariamente la creación de perfiles falsos, los cuales serían utilizados como medio para la captación de posibles víctimas de trata de personas, extorsiones, *grooming* o *ciberbullying*[9].

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[10]. 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.

Asimismo, hubo una denuncia de compra de software de control remoto diseñado con fines de espionaje por parte de la institución estatal encargada de la lucha contra la producción y tráfico de drogas, la cual, si bien está facultada por ley a realizar escuchas en el marco de sus investigaciones con orden judicial, ha generado dudas con respecto a un posible mal uso del mismo.

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. Esta sección describe el estado del Internet y su infraestructura en Paraguay, de la aplicación de las TIC y de la ciberseguridad en las diferentes instituciones y sectores en el país.

Internet y su infraestructura

Internet de alta velocidad llega a los municipios paraguayos por medio de microondas o fibra óptica, mientras que la tecnología de Línea de Abono Digital Asimétrica (ADSL, por sus siglas en inglés) es incipiente en Paraguay[11]. En términos de uso de Internet, el porcentaje de penetración que se entiende como la cantidad de personas que han usado Internet (en cualquier lugar) dentro de un país en los últimos 12 meses, llegó al 43 por ciento en 2014 (Gráfico 1).

---

[7] 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/. Recuperado el 24 de noviembre de 2015.

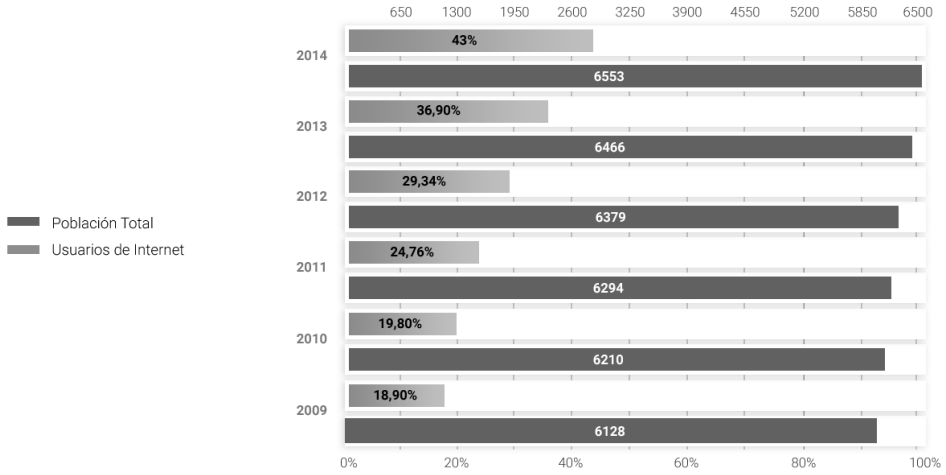
[8] Bancarios van a 3 años a cárcel por estafa de 400 mil dólares". Disponible en: http://www.ultimahora.com/bancarios-van-3-anos-carcel-estafa-400-mil-dolares-n705027.html. Recuperado el 24 de noviembre de 2015.

[9] 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. Recuperado el 24 de noviembre de 2015.

[10] Fiscalía investigará caso de pornografía infantil". Disponible en: http://www.paraguay.com/nacionales/fiscalia-investigara-caso-de-pornografia-infantil-126212. Recuperado el 24 de noviembre de 2015.

[11] 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. Recuperado el 24 de noviembre de 2015.

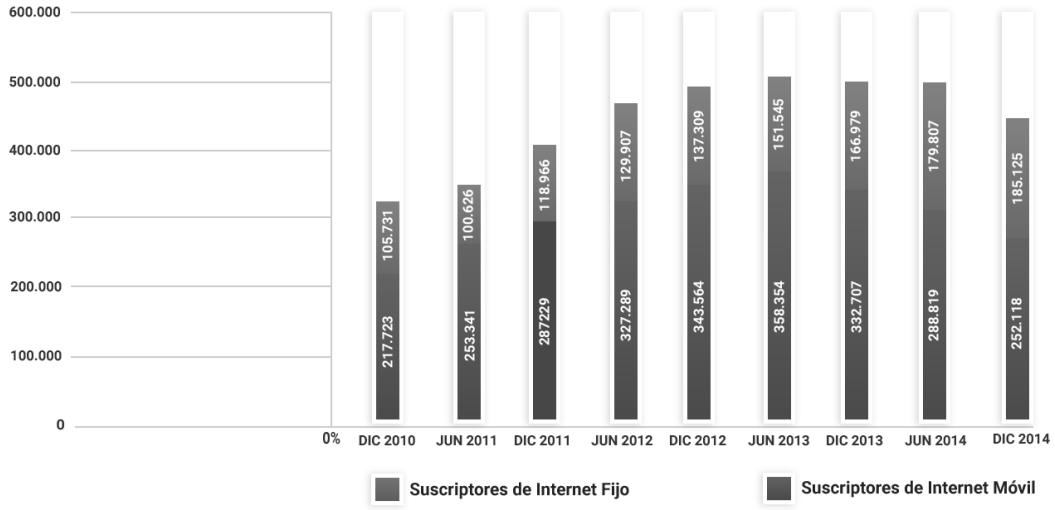
Gráfico 1: Población Total vs Usuarios de Internet (2009-2014)



Fuente: Indicadores del Desarrollo Mundial (IDM) – Banco Mundial. Recuperado el 30 de noviembre de 2015[12].

En Paraguay se encuentran registradas únicamente el 5 por ciento de las casas, con Internet fijo. Sin embargo, el número aumenta al 25 por ciento de acceso al Internet cuando nos referimos a la telefonía móvil[13]. De hecho, el Internet por telefonía móvil tiene una cobertura amplia con redes de 2G/3G/4G, aunque la red 4G es aún muy limitada. Según datos de la Comisión Nacional de Telecomunicaciones (CONATEL), al final de 2014 Paraguay tenía 252.118 suscriptores de Internet móvil y 185.125 suscriptores de Internet fijo, con un total de 437.243 suscripciones (Gráfico 2).

Gráfico 2: Suscriptores de Internet Móvil y Fijo (2010-2014)



Fuente: CONATEL – Matriz de Indicadores de Desarrollo de Telecomunicaciones. Recuperado el 24 de noviembre de 2015[14].

[12] Disponible en: http://databank.worldbank.org/data/home.aspx.
[13] Según datos obtenidos junto a la CONATEL en la mesa de discusión conducida el 6 de mayo de 2015.
[14] Disponible en: http://www.conatel.gov.py/index.php?option=com_content&view=article&id=30&Itemid=115.

Cabe señalar que los costos de las conexiones han ido disminuyendo con los años, haciéndose cada vez más accesible. Según datos del Observatorio Regional de Banda Ancha (ORBA) de la Comisión Económica para América Latina y el Caribe (CEPAL), la tarifa de banda ancha fija de 1 Mbps como porcentaje del Producto Interno Bruto (PIB) per cápita contó con disminuciones con un promedio de 15 por ciento entre 2010 y 2014, correspondiendo actualmente al 5 por ciento del PIB per cápita. El servicio de banda ancha fija de 10 Mbps de velocidad equivale al 3,77 por ciento del PIB per cápita. La conexión de 2 Mbps se traduce en el 4,84 por ciento del PIB per cápita, mientras que los planes de banda ancha móvil están en 6,03 por ciento del PIB per cápita. No obstante, Paraguay sigue siendo el segundo país más caro de la región al 2014[15], consecuencia de varios factores, entre ellos su mediterraneidad.

La velocidad de descarga promedio en banda ancha global en Paraguay es 3,54 Mbps y la de carga es 3,33 Mbps. Finalmente, el informe identificó una brecha relativamente alta entre los hogares con acceso a Internet por conexión fija según zona geográfica del hogar (urbana o rural) – cerca del 29,1 por ciento. Según datos de 2013, el porcentaje de hogares con acceso al Internet por conexión fija en zonas urbanas era de casi un 40 por ciento, mientras que en las zonas rurales era menos de un 10 por ciento[16].

Esta situación puede estar relacionada con los altos costos de transporte de tráfico de Internet. En este contexto, el desarrollo de la infraestructura de la banda ancha avanzó en Paraguay por medio del Plan Nacional de Telecomunicaciones (2011-2015), cuya meta para el 2015 era conectar a 200 municipios con fibra óptica y acceso al Internet con banda ancha – hasta el momento el país tiene 155 municipios conectados[17]. La CONATEL está trabajando, con el apoyo del Banco Interamericano de Desarrollo (BID) y otras instituciones gubernamentales paraguayas, en el desarrollo de un Plan Nacional de Banda Ancha, que conlleva el propósito de expandir el servicio de Internet en Paraguay y reducir la brecha digital[18]. El modelo de gobierno adaptado dentro del Plan Nacional incluye tres factores principales: el desarrollo de un marco normativo y el espectro, la inversión en infraestructura, así como el uso y adopción de la banda ancha, logrando la interconexión entre redes[19]. Vale recalcar que en septiembre de 2015 se conformó un Grupo de Trabajo interinstitucional[20] para la implementación del Plan Nacional de Banda Ancha.

---

[15] http://repositorio.cepal.org/bitstream/handle/11362/38605/S1500568_es.pdf

[16] CEPAL. "Estado de la banda ancha en América Latina y el Caribe 2015". Disponible en: http://repositorio.cepal.org/bitstream/handle/11362/38605/S1500568_es.pdf?sequence=1. Recuperado el 24 de noviembre de 2015.

[17] Información compartida por CONATEL en el 6 de mayo de 2015 durante la "Misión de Asistencia Técnica para el Desarrollo de una Estrategia Nacional de Seguridad Cibernética en Paraguay".

[18] "Paraguay avanza hacia Plan Nacional de Banda Ancha". Disponible en: http://www.conatel.gov.py/index.php?option=com_content&view=article&id=728:paraguay-avanza-hacia-plan-nacional-de-banda-ancha&catid=31&Itemid=101. Recuperado el 24 de noviembre de 2015.

[19] "Paraguay debe invertir US$ 1.000 millones para mejora de banda ancha". Disponible en: http://www.lanacion.com.py/2015/09/03/paraguay-debe-invertir-us-1-000-millones-para-mejora-de-banda-ancha/. Recuperado el 04 de diciembre de 2015.

[20] "Deciden conformar Grupo de Trabajo para el Plan Nacional de Banda Ancha". Disponible en: http://www.mre.gov.py/v2/Noticia/3143/deciden-conformar-grupo-de-trabajo-para-el-plan-nacional-de-banda-ancha. Recuperado el 24 de noviembre de 2015.

La CONATEL, creada por la Ley N˚642/95 de Telecomunicaciones, ha llevado varios proyectos a licitaciones, proporcionando subsidios a los prestadores de servicios de comunicaciones para que avancen con la infraestructura necesaria. Más concretamente, la expansión de la infraestructura de acceso al Internet se realiza mediante alianzas público-privadas (APP), por medio de recursos de las propias operadoras y por subsidios provenientes del "Fondo de Servicios Universales" (FSU), administrado por CONATEL. El FSU fue establecido por el artículo 97 de la Ley N˚642/95 con la finalidad de subsidiar a los prestadores de servicios públicos en la expansión de los servicios de telecomunicaciones, así como promover el acceso a los servicios de manera eficiente, maximizando su beneficio económico, según el artículo 3 del Reglamento del FSU. El financiamiento proviene del 20 por ciento de aportes abonados por operadores por el concepto de Tasas por Explotación Comercial. Dicho pago de explotación equivale a un 1 por ciento de los ingresos brutos del prestador que son recaudados por la CONATEL[21].

La CONATEL, en el marco del FSU y por medio de licitaciones públicas, está llevando a cabo un programa de expansión de la infraestructura de las redes que sirven de plataforma para los servicios de acceso a Internet, Telefonía Móvil y el servicio básico en las zonas de interés público o social (ZIPS) de los Departamentos de San Pedro, Concepción, Amambay y Canindeyú. La CONATEL ha llevado a cabo licitaciones con la finalidad de implementar un servicio de acceso a Internet en instituciones educativas y gobernaciones del país, beneficiando un total de 287 instituciones educativas. El FSU también está financiando desde agosto de 2014 la implementación de 50 plazas públicas para el acceso gratuito a Internet en 36 municipios del país.

Cabe mencionar la implementación del primer "Punto de Intercambio de Internet" (IXP, por sus siglas en inglés) en Paraguay, que se dio en mayo del 2016, gracias al trabajo conjunto entre el Centro Nacional de Computación de la Universidad Nacional de Asunción (CNC), las empresas Compañía Paraguaya de Comunicaciones (COPACO) y Tecnología en Electrónica e Informática Sociedad Anónima (TEISA), bajo la coordinación de la CONATEL. El IXP es un componente de infraestructura de Internet que puede mejorar la calidad de acceso a Internet a nivel local, ya que no sólo mantiene el tráfico local dentro de infraestructuras locales, sino que también reduce los costos asociados con el intercambio de tráfico entre proveedores de servicios de Internet (PSI). Es decir, los IXPs permiten que redes locales, intercambien información de manera eficiente en un punto común dentro del país, sin la necesidad de intercambiar el tráfico local de Internet en el extranjero. Cabe destacar que físicamente, éste punto de intercambio se montó en el DATACENTER del CNC, donde actualmente llegan las conexiones de los PSI locales, ya adscriptos a ésta red.

Por lo tanto, la CONATEL se encarga del fomento, control y reglamentación de las telecomunicaciones, teniendo a su cargo la regulación administrativa y técnica, la planificación, programación, control y fiscalización así como la verificación de las telecomunicaciones, con sus funciones específicas definidas en la Ley de Telecomunicaciones. Su rol se enfoca principalmente en la expansión de la infraestructura y en la calidad de los servicios de

[21] Las fuentes de recursos del FSU, según el artículo 6 del Reglamento del Fondo de Servicios Universales son: a) El 20 por ciento de los aportes abonados por las empresas operadoras por el concepto de Tasa por Explotación Comercial; b) aquellas asignaciones, donaciones, legados, transferencias u otros aportes, por cualquier tipo proveniente de personas físicas o jurídicas nacionales o extranjeras, que son destinadas al objeto del FSU o que la CONATEL determine. Disponible en: http://www.conatel.gov.py/index.php?option=com_content&view=article&id=24&Itemid=166. Recuperado el 24 de noviembre de 2015.

comunicaciones. En cuanto a la seguridad, existe una preocupación respecto a la integridad de la red de telecomunicaciones y la seguridad del usuario en general.

Además de la infraestructura física que permite la prestación de los servicios de comunicación e Internet ya mencionados (ej. IXPs, fibra óptica), hay que destacar la gestión de los recursos críticos de Internet en Paraguay, tal como el nombre del dominio nacional ".PY"[22]. El ".PY" es el dominio de nivel superior de país (ccTLD, por sus siglas en inglés) asignado a Paraguay, siendo responsabilidad del NIC su mantenimiento. El Network Information Center – Paraguay (NIC.PY), que se conformó en 1995 a través de un acuerdo firmado entre el CNC y el Laboratorio de Electrónica Digital (LED)[23], es la organización administradora y patrocinadora del dominio de primer nivel .PY, y tiene como funciones mantener y conservar los servidores de nombres para el dominio .PY, generar actualizaciones a la información de la zona .PY y difundirla a los servidores secundarios autorizados, así como asegurar la continua y estable interoperabilidad del sistema de nombres de dominio en Internet[24]. Actualmente, Paraguay cuenta con aproximadamente 20 mil dominios .PY activos[25].

Otro recurso crítico de Internet son las direcciones de Protocolo de Internet (IP, por sus siglas en inglés) que consisten en números únicos con los cuales se identifica una computadora conectada a una red. A Paraguay se distribuyó 59 bloques de dirección IPv4 y 29 bloques de dirección IPv6, la nueva versión del IP y que está destinada a sustituir al estándar IPv4 que actualmente cuenta con un límite de direcciones en la red[26]. Cabe recalcar que la Compañía Paraguaya de Comunicaciones S.A. (COPACO) está apoyando la migración hacia el IPv6 en Paraguay[27]. En agosto de 2015, COPACO completó la implementación de IPv6 en su red, constituyéndose en la primera de su tipo en el país[28]. Durante la transición de IPv4 a IPV6 ambos protocolos deberán coexistir.

El fomento al uso de las TIC

Para el fomento al uso de las TIC, existen entidades gubernamentales involucradas directamente en proyectos de desarrollo de las TIC en Paraguay. El Ministerio de la Industria y Comercio (MIC), desde 2012[29] es la autoridad de aplicación de la Ley de la Firma Digital (Ley N˚4017/2010) que de acuerdo con el artículo 2º de la referida Ley es una "firma electrónica certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo a su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría". Es decir, al

[22] El dominio de primer nivel .PY fue asignado al Paraguay según la ISO 3166-1.
[23] El CNC (Contacto Técnico del ccTLD-PY) es responsable de la administración y operación de los servidores DNS y el LED (Contacto Administrativo del ccTLD-PY) es responsable de las aprobaciones de las solicitudes de delegación de dominios.
[24] "Acerca del NIC-PY". Disponible en: http://www.nic.py/about.php. Recuperado el 24 de noviembre de 2015.
[25] Información detallada disponible en la presentación "Deployment of second level domains ccTLD.PY" (ICANN53, Buenos Aires, Argentina, 24 de junio de 2015). Disponible en: https://buenosaires53.icann.org/en/schedule/wed-ccnso-members/presentation-sld-deployment-24jun15-en. Recuperado el 24 de noviembre de 2015.
[26] Disponible en: http://portalipv6.lacnic.net/reporte-de-terminacion-de-direcciones-ipv4/. Recuperado el 24 de noviembre de 2015.
[27] LACNIC, Portal IPv6, "¿Quiénes implementan?" Disponible en: http://portalipv6.lacnic.net/quienes-implementan/. Recuperado el 24 de noviembre de 2015.
[28] Disponible en: http://ipv6.copaco.com.py/portal/. Recuperado el 24 de noviembre de 2015.
[29] En el año de 2012 se promulga la Ley 4.610/2012, que introduce modificaciones importantes a la Ley 4017/2010, tal como el cambio de la autoridad de aplicación de referida norma, que de ser el Instituto de Tecnología y Normalización pasó a ser el Ministerio de Industria y Comercio.

sustituir la firma manual en documentos por la firma digital se puede garantizar la identidad de las partes, la confidencialidad y la integridad de la información, evitando falsificaciones y manipulaciones del contenido de los documentos.

El MIC también es la Autoridad de Aplicación de la Ley de Comercio Electrónico, Ley N°4.868/2013, que estableció el marco jurídico relativo al comercio y contratación realizados a través de medios electrónicos o tecnológicamente equivalentes, así como las responsabilidades y obligaciones de los proveedores de bienes y servicios por vía electrónica, de los proveedores de acceso al Internet, proveedores de servicios de intermediación, y los proveedores de enlace. Dicha Ley fue reglamentada por el Poder Ejecutivo, a través del Decreto N°1.165/2014, instituyendo el mecanismo para su aplicación y su alcance.

El comercio electrónico en Paraguay es aproximadamente un 2,6 por ciento del comercio electrónico de la América Latina, lo que corresponde a US$ 1.300 millones, según datos del Instituto Latinoamericano de Comercio Electrónico (eInstituto).

La Ley de Comercio Electrónico establece obligaciones relativas a la seguridad de la información a los proveedores de servicios de acceso al Internet, tales como "a) informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otras cosas, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados; b) informar sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios no deseados en Internet o que puedan resultar nocivos para la niñez y la adolescencia" (artículo 9). Tales obligaciones se consideran cumplidas por medio de medidas sencillas y de bajo costo, como la inclusión de referida información en la página de Internet del proveedor.

Cabe señalar que la Ley dispone el plazo de almacenamiento de los datos de conexión y tráfico generados –el cual es de seis meses– el tipo de datos a ser retenidos, y la utilización de los mismos. Los datos deben ser almacenados únicamente a los efectos de facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información. Los Proveedores de Servicios de Alojamiento de Datos deberán almacenar sólo aquellos datos imprescindibles para identificar su origen y el momento en que se inició la prestación del servicio. Cabe destacar que no se podrán utilizar los datos almacenados para fines distintos a los que están permitidos por la Ley, y se deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos. El Decreto prevé la obligación de los proveedores de bienes y servicios por vía electrónica y de los proveedores de Internet de comunicar al usuario el destino que se dará a sus datos personales y su deber de emplear mecanismos seguros en el tratamiento de los datos y respecto a los medios de pago.

Finalmente, es interesante observar que el Decreto N°1.165/2014 ha establecido en su artículo 29 que el MIC impulsará la elaboración de Códigos de Conducta voluntarios por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores en cuestiones relativas al comercio electrónico.

A partir de la Ley N˚4989 del año 2013 "Que crea el Marco de Aplicación de Tecnologías de la Información y Comunicación en el Sector Público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)", se crea la institución del Poder Ejecutivo encargada de implementar los principios y fines de las TIC en el sector público. Conforme lo dispone la referida Ley, la investigación, el fomento y el desarrollo de las TIC son una política de

Estado que involucra a todos los sectores y la sociedad. Las TIC deben servir al interés general y es deber del Estado promover su acceso de manera eficiente y en igualdad de oportunidad a todos los ciudadanos.

Siendo así, la SENATICs es la institución del Poder Ejecutivo que define, fiscaliza y apoya la implementación de políticas y estrategias transversales para garantizar el acceso y el uso de las TIC a la población paraguaya con el fin de mejorar su calidad de vida y apoyar el desarrollo sostenible del país. Para lograrlo, una de las líneas de acción en las que trabaja es el Gobierno Electrónico, ofreciendo servicios de hosting, ingeniería en TIC, asistencia técnica, implementación de portales, computación en la nube, automatización de trámites, aplicaciones ciudadanas, capacitaciones, trámites en línea, entre otros numerosos servicios.

En cuanto a la materia de ciberseguridad, el artículo 12, inciso h, de la Ley N°4.989/2013, atribuye expresamente a la SENATICs la tarea de "establecer y gestionar las políticas de protección de la información personal y gubernamental, y cultivar los conocimientos sobre la industria de seguridad de la información, para lo cual deberá establecer un sistema de organización de seguridad, proponer una política de seguridad a nivel nacional, y establecer un plan de integración de protección de información". Asimismo, el Artículo 14, inciso g) dispone la atribución de "establecer y gestionar políticas de protección de la información personal y gubernamental, y cultivar los conocimientos sobre la industria de seguridad de la información, para lo cual deberá establecer un sistema de organización de seguridad, proponer una política de seguridad a nivel nacional y establecer un plan de integración de protección de información", y el inciso h) "diseñar e implementar estándares, mecanismos y medidas tecnológicas de seguridad para el adecuado y correcto funcionamiento de los programas y servicios de acceso electrónico para el ciudadano".

La gestión de incidentes y vulnerabilidades cibernéticas es conducida por el Centro de Respuesta a Incidentes Cibernéticos del Paraguay (CERT-PY) que, a su vez, es la principal autoridad en materia de ciberseguridad en el país, establecida bajo la estructura funcional de la SENATICs por Decreto N˚11.624/13.

La respuesta a incidentes cibernéticos

El CERT-PY, bajo la Dirección General de Políticas y Desarrollo de TIC de la SENATICs (Decreto N°11.624/2013), se estableció con el objetivo de facilitar y fomentar la protección de los sistemas cibernéticos y de la información que respaldan la infraestructura nacional tanto gubernamental como del sector privado, así como garantizar una respuesta eficaz y oportuna a los incidentes cibernéticos. El CERT-PY ofrece servicios de difusión de boletines y noticias de ciberseguridad[30], auditorías de seguridad, respuesta a incidentes, análisis de malware, así como un canal de reporte de incidentes cibernéticos desde su portal así como también a través de correo electrónico y redes sociales[31].

Además del tratamiento de los incidentes, otro objetivo importante es la capacitación técnica orientada a profesionales de tecnologías de la información y funcionarios de las entidades gubernamentales, así como la promoción de la concientización sobre los problemas de ciberseguridad, del análisis de los niveles actuales, las tendencias y la relación entre los

[30] Disponible en: http://www.cert.gov.py/index.php/boletines. Recuperado el 24 de noviembre de 2015.

[31] Reporte de incidentes por medio del correo electrónico abuse@cert.gov.py.

diferentes incidentes que ocurren dentro del país. En esa línea de acción, el CERT-PY ha llevado adelante una importante campaña de sensibilización contra el *grooming* en Internet[32]. El *grooming* es una forma en que se manifiesta el acoso sexual en la Red hacia los menores, y se está haciendo cada vez más frecuente.

Asimismo, el CERT-PY ha tomado medidas para desarrollar sus lazos cooperativos con otros CERTs de la región, lo que le ha permitido mantenerse informado permanentemente acerca de la evolución de las técnicas y amenazas cibernéticas. El CERT-PY también mantiene una estrecha relación con las instituciones responsables de la investigación y persecución de delitos informáticos en Paraguay, como el Ministerio Público y la Policía Nacional.

En este punto, cabe hacer notar que para una efectiva respuesta ante incidentes cibernéticos y delitos informáticos o cometidos en el ámbito cibernético, se necesita fomentar la colaboración entre el sector privado, la sociedad civil y el sector público. En tal sentido, 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.

La investigación de delitos informáticos

Por Resolución N˚3459 de la Fiscalía General del Estado, se creó la Unidad Especializada de Delitos Informáticos en 2010, para hacer frente a aquellos delitos que derivan del uso malintencionado de las tecnologías de información y comunicación. La iniciativa surge como respuesta a la necesidad de combatir de manera frontal y eficiente estos delitos. La Unidad tiene jurisdicción sobre hechos cometidos en todo el territorio nacional y es la principal autoridad a cargo de la investigación y preparación de la acción judicial en casos de delitos informáticos, tales como alteración de datos en computadora, sabotaje de computadoras, operaciones fraudulentas por computadoras, alteración de datos relevantes para la prueba, entre otros previstos en la ley.

A la fecha, el Ministerio Público es la única autoridad gubernamental con atribución para solicitar información a los prestadores de servicio internacionales cuando dicha información sea necesaria para una investigación. No obstante, el Código Procesal Penal de Paraguay (Ley N°1286/98) establece que toda persona que tenga conocimiento de un hecho punible de acción penal pública, podrá denunciarlo ante el Ministerio Público o la Policía Nacional. Asimismo, dispone que tendrán obligación de denunciar, las personas que por disposición de la ley, de la autoridad, o por algún acto jurídico, tengan a su cargo el manejo, la administración, el cuidado o control de bienes o intereses de una institución, entidad o persona, respecto de los hechos punibles cometidos en perjuicio de éste o de la masa o patrimonio puesto bajo su cargo o control, siempre que conozcan del hecho por el ejercicio de sus funciones.

Debido a la cantidad significativa de casos de pornografía infantil, la Unidad Especializada de Delitos Informáticos actúa conjuntamente en equipos investigativos conformados con la Unidad Especializada en la Lucha contra la Trata de Personas y la Explotación Sexual de Niños, Niñas y Adolescentes. Asimismo, la Unidad Especializada de Delitos Informáticos firmó un importante

[32] Disponible en: http://www.conectateseguro.gov.py/index.php/noticias/grooming-en-internet. Recuperado el 24 de noviembre de 2015.

acuerdo en enero de 2014 con el Centro Nacional de Niños Desaparecidos y Explotados (NCMEC, por sus siglas en inglés). Según informó el Ministerio Público, hay un promedio de 400 casos de pornografía infantil por año en Paraguay, y un 10 por ciento de condenas, en razón de las evidencias recolectadas en el Internet [33].

En Paraguay, con el apoyo del Ministerio Público, bajo la coordinación del Ministerio de Relaciones Exteriores, se está trabajando para posibilitar la adhesión al Convenio de Budapest sobre Ciberdelincuencia. Entre los años 2010-2011 se realizaron cambios importantes en la legislación nacional penal, adecuándola a los estándares mínimos que dispone dicho convenio. La Ley N˚4.439/2011 modificó tres artículos del Código Penal e introdujo seis nuevos artículos. Más específicamente, dicha Ley modificó los artículos 140 (pornografía relativa a niños y adolescentes), 145 (sabotaje de sistemas informáticos), y 188 (estafa mediante sistemas informáticos). En la misma Ley se amplió el Código Penal, introduciéndose los artículos 146b, 146c, 146d, 174b, 175b, y 248b relativos al acceso indebido a datos, a la intercepción de datos, a la preparación de acceso indebido e interceptación de datos, al acceso indebido a sistemas informáticos, a la instancia, y a la falsificación de tarjetas de débito y otros medios electrónicos de pago, respectivamente.

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. Se creó dicha División por medio de la Resolución N°1.078, de 7 de diciembre de 2010, con las siguientes funciones: a) planificar e implementar el curso de acción, conforme a la estrategia y política nacional de la lucha contra los delitos informáticos; b) programar conjuntamente a corto, mediano y largo plazo, cargar el banco de datos, con las informaciones obtenidas, para ser procesadas, evaluadas, integradas y analizadas para la elaboración de dossier y proceder conforme al Manual de Procedimientos de la Policía Nacional; c) recibir denuncias conforme lo establece la legislación paraguaya; d) investigar y procesar las denuncias conforme al debido trámite; e) coadyuvar con los demás organismos del Estado para prevenir, investigar y reprimir los delitos informáticos; f) proponer programas de perfeccionamiento profesional y técnico para el personal a su cargo, a través de seminarios, simposios, cursos, paneles y otros; g) responder a los requerimientos del Poder Judicial o del Ministerio Público; h) coordinar con el sector privado sean estas nacionales o extranjeras, para capacitación e intercambio oportuno y eficaz de informaciones; y I) elaborar plan anual de estrategia y políticas de prevención (Artículo 2 de la Resolución N°1.078/2010).

Se discute la posibilidad de modificar el rango de la "División Especializada" contra Delitos Informáticos de la Policía Nacional, al rango de "Departamento", lo que conferiría mayor autonomía a la unidad y reduciría la burocracia en el manejo de delitos informáticos. Sin embargo, el cambio de rango solamente sería posible por medio de enmiendas a la Ley Orgánica de la Policía Nacional (Ley N˚222/93).

[33] Información compartida por la Unidad Especializada en Delitos Informáticos del Ministerio Público en el 7 de mayo de 2015 durante la "Misión de Asistencia Técnica para el Desarrollo de una Estrategia Nacional de Seguridad Cibernética en Paraguay".

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.

La administración pública y empresas públicas

Con respecto a la Administración Pública Central, el Poder Ejecutivo se compone de la Presidencia de la República y sus 15 dependencias, 19 Secretarías, y 12 Ministerios. Asimismo, el país cuenta con 21 entidades descentralizadas, 5 empresas públicas[35] y entidades binacionales.

El Decreto N°6234/2016 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, así como también faltan estándares para la implementación de sistemas de protección de las TIC. 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.

Algunos servicios esenciales son prestados por empresas públicas, como la Administración Nacional de Electricidad (ANDE), la Compañía Paraguaya de Comunicaciones S.A. (COPACO), la Empresa de Servicios Sanitarios del Paraguay S.A. (ESSAP), Petróleos Paraguayos (PETROPAR), y el Banco Nacional de Fomento (BNF). La mayoría de estas empresas públicas cuentan con algún tipo de sistema de control industrial (Supervisión Control y Adquisición de Datos – SCADA, Sistema de Control Distribuido – DCS, por ejemplo) y ya empezaron la formulación de políticas de ciberseguridad con énfasis en la sensibilización de sus funcionarios. Sin embargo, 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.

Paraguay también cuenta con hidroeléctricas binacionales que son esenciales para la economía del país, como las entidades binacionales Yacyretá[36] e Itaipú[37].

---

[34] ENSC – Estrategia Nacional de Seguridad Ciudadana (Diciembre 2014). Disponible en: http://www.mdi.gov.py/images/pdf_mdi/ENSC%20estrategia%20ciudadanamail.pdf Recuperado el 24 de noviembre de 2015.
[35] Disponible en: http://www.paraguay.gov.py/poder-ejecutivo. Recuperado el 25 de noviembre de 2015.
[36] Disponible en: http://www.eby.gov.py/. Recuperado el 24 de noviembre de 2015.
[37] Disponible en: http://www.itaipu.gov.py/es. Recuperado el 24 de noviembre de 2015

El sector privado

En términos de ciberseguridad, no hay aún en el sector privado empresas certificadas por el ISO 27001[38], y se estima que un alto porcentaje de las empresas no cumplen con los registros de seguridad en TIC para manejos de documentos[39].

El Viceministerio de las micro, pequeñas y medianas empresas (MIPYMES) registra un total de 225 mil MIPYMES, lo que representa más del 90 por ciento de la infraestructura económica de Paraguay. En este sentido, la Ley N°4.457/2012, reglamentada por el Decreto N°11.453/2013, tiene por objeto proveer un marco regulatorio que permita promover y fomentar la creación, desarrollo y competitividad de las MIPYMES para incorporarlas a la estructura formal de productoras de bienes y servicios. Para asegurar el cumplimiento de una política nacional que posibilite un trabajo armonizado y en conjunto con otros órganos públicos y privados, se creó el Sistema Nacional de MIPYMES bajo la dirección y coordinación del Viceministerio de MIPYMES del MIC.

Dichas normativas también buscan impulsar la modernización tecnológica del tejido empresarial de las MIPYMES y el desarrollo del mercado de servicios tecnológicos como elementos de soporte a una innovación continua en el país. La promoción, articulación y operatividad de la investigación e innovación tecnológica es coordinada por el MIC, el Consejo Nacional de Ciencia y Tecnología (CONACYT), universidades y centros de investigación con las MIPYMES.

El sector financiero, por su parte, es uno de los principales blancos de ataques cibernéticos. En este contexto, la Asociación de Bancos de Paraguay (ASOBAN) y la Asociación de Entidades Financieras del Paraguay (ADEFI) cuentan con un Comité de Seguridad de la Información, y con un esquema de comunicación sobre incidentes cibernéticos con otras organizaciones financieras de Sudamérica. Sin embargo, este intercambio de información solamente ocurre cuando es considerado necesario y no es una práctica periódica. Cabe destacar que hubo una reducción de incidentes de *phishing* (suplantación de identidad) en el sector financiero. Las entidades financieras hacen campañas de sensibilización junto a sus clientes acerca del buen uso de las TIC, pero no existe una campaña de sensibilización conjunta y coordinada entre todas las entidades.

Sensibilización y educación

El Gobierno ha lanzado una campaña denominada "Conéctate Seguro PY", cuyo principal objetivo es concientizar a las personas sobre los riesgos de publicar información personal sensible en las redes. En 2013, SENATICs adoptó una iniciativa complementaria, PARAPIENSACONECTATE., que se encuentra en su fase de implementación. El Ministerio Público por su parte también organiza campañas de sensibilización. En el 2014 se realizó un concurso contra *ciberbullying* en todas las escuelas, donde los alumnos dibujaron caricaturas contra la práctica. Sin embargo, falta coordinación entre los diferentes actores.

[38] ISO 27001 es un estándar para la seguridad de la información aprobado y publicado como estándar internacional por la Organización Internacional de Normalización (ISO, por sus siglas en inglés).
[39] Información compartida en la mesa de discusión con el Sector Académico, Centros de Investigación y Sociedad Civil en el 7 de mayo de 2015 durante la "Misión de Asistencia Técnica para el Desarrollo de una Estrategia Nacional de Ciberseguridad en Paraguay".

Con respecto a niños, niñas y adolescentes, Paraguay también cuenta con las acciones de la sociedad civil, como la organización Protección Online que realiza proyectos junto a las escuelas a fin de presentar buenas prácticas para el uso de la tecnología. En vista de que estos programas no son suficientes, el Programa también desarrolla campañas en la Web, trabaja con programas de televisión, y permite que los ciudadanos hagan denuncias de forma anónima en línea. Cabe destacar que el Fondo para la Infancia de las Naciones Unidas (UNICEF) y algunas empresas del sector privado también promueven acciones similares, pero son *ad hoc*. En términos de educación, en el país existen instituciones de enseñanza superior y organizaciones no gubernamentales (ONGs) que ofrecen especializaciones en seguridad informática y derecho informático. Sin embargo, la oferta académica en programas especializados en estas áreas es muy reducida. En consecuencia, existe un número significativo de personas que acceden a algún tipo de formación en el área de seguridad de la información mediante programas ofrecidos por instituciones extranjeras, en convenio con centros de entrenamiento y universidades debidamente acreditadas.

Aunque no exista una carrera de nivel superior específica en ciberseguridad, algunas universidades en Paraguay abordan el tema de la ciberseguridad dentro de otras carreras de manera más general por medio de mallas extra-curriculares. Las mallas curriculares de las TIC y ciberseguridad son cubiertas de manera general a través de materias optativas. Algunos programas de postgrado requieren la preparación de una tesis por los alumnos, con la oportunidad de profundizar más en el tema.

Los alumnos tienen la posibilidad de estudiar en el exterior por medio de becas gubernamentales y de las propias universidades. Con respecto a las becas gubernamentales, el Consejo Nacional de Ciencia y Tecnología (CONACYT) ofrece financiamiento a través de becas de maestría e investigación. CONACYT lanzó en mayo de 2015, en el marco del "Programa Paraguayo para el Desarrollo de la Ciencia y Tecnología" (ProCiencia), el Programa de Incentivos para la Formación de Docentes-Investigadores (becas nacionales para maestrías y doctorados). El Programa de Incentivos está dirigido a estudiantes que se dediquen de forma exclusiva al programa de postgrado. Este programa es financiado a través del Fondo para la Excelencia de la Educación y la Investigación (FEEI) asignado por el Fondo Nacional de Inversión Pública y Desarrollo (FONACIDE), según la Ley N°4.758/2012. El Programa incluye financiamiento para la Maestría en Ciencia de la Computación y al Doctorado en la Ciencia de la Computación de la Facultad Politécnica-UNA. Existe también el Programa Nacional de Incentivo a los Investigadores (PRONII), para estudiantes de postgrado en algunas áreas, incluso los temas de Ingenierías y Tecnologías, Matemática, Informática, y Física.

Otra iniciativa relevante fue la creación de la Maestría y Especialización en Tecnologías de la Información y la Comunicación[40], con énfasis en Ingeniería de Software, Redes y Comunicación de Datos, Auditoría y Seguridad de la Información, impartida en la Facultad Politécnica de la Universidad Nacional de Asunción (UNA). La maestría tiene una duración de 24 meses y cuenta con profesores nacionales y extranjeros especialistas en diversas áreas, incluyendo TIC. Sin embargo, la misma no abarca todas las áreas de conocimiento del campo de la Ciberseguridad.

Es importante señalar que Paraguay se ha conectado a inicios del año 2016, a la Cooperación Latinoamericana de Redes Avanzadas (Red CLARA), que consiste en una organización de derecho internacional sin fines de lucro que desarrolla, administra y dirige una red regional de

[40] http://www.pol.una.py/mtic/

Internet avanzada[41], mediante la conformación de un Grupo Impulsor de la Red Nacional de Educación e Investigación, bajo el liderazgo de la SENATICs y con el apoyo y financiamiento de la Entidad Binacional Itaipú, acompañando también la Universidad Nacional de Asunción y el Consejo Nacional de Ciencia y Tecnología (CONACYT). Actualmente, se está impulsando la conformación de la Red Nacional, la cual ya tuvo como antecedente en el año 2011 una constitución que no llegó a perfeccionarse. En ese escenario, luego de conectar al Paraguay a la Red CLARA, se convocó nuevamente a las instituciones que integraron ese proceso inicial, para dar impulso y finiquitar todas las exigencias para la constitución de la Asociación y su reconocimiento y existencia como persona jurídica. En ese escenario, se está tramitando la constitución formal de la RED NACIONAL PARA LA CIENCIA, LA INVESTIGACIÓN Y LA TECNOLOGÍA "ARANDU", y se están realizando las operaciones técnicas de conexión de más de 13 universidades que ya lo han solicitado.

Conclusión

Se puede concluir que en los últimos años hubo una serie de iniciativas con el propósito de fomentar el uso de las TIC en los distintos sectores del país. Actualmente, hay proyectos para el desarrollo del gobierno electrónico e inclusión digital, el despliegue de fibra óptica, la implementación de IXP para la mejora de la calidad del Internet, así como la implementación de acceso gratuito a Internet en plazas públicas de diversos municipios del país. Asimismo, hubo proyectos para fomentar el uso de las TIC en los negocios, como los proyectos relativos a la firma digital y al comercio electrónico. El CERT-PY también ha desarrollado trabajos de tratamiento de incidentes cibernéticos y de concientización. La Unidad Especializada de Delitos Informáticos del Ministerio Público y la División Especializada contra Delitos informáticos de la Policía Nacional también han desarrollado importantes proyectos en la lucha contra delitos informáticos. Teniendo estos proyectos en cuenta, este Plan Nacional busca no sólo complementar las iniciativas existentes con componentes relativos a la ciberseguridad, sino que también implementar otras medidas para disponer de un ciberespacio resiliente y seguro.

En este contexto, basándose en el marco normativo actual y en las políticas existentes, se buscó en las próximas secciones establecer principios orientadores para la ciberseguridad en el país, a fin de que las políticas para un ciberespacio seguro fomenten un entorno económico innovador y respeten los derechos fundamentales. Este diagnóstico también permitió la definición de los siete Ejes de Acción de este Plan Nacional, así como sus objetivos y líneas de acción.

[41] "RedCLARA es +Red +Ciencia, y su conectividad y servicios que sobre su infraestructura de Internet Avanzada operan en línea están destinados a fomentar el desarrollo de iniciativas de colaboración científico-académicas latinoamericanas; a través de RedCLARA investigadores, científicos y académicos de la región pueden colaborar con sus pares en el mundo, desarrollar investigaciones y proyectos, realizar pruebas de sus desarrollos y más". Disponible en: http://www.redclara.net/index.php/somos/faq-s. Recuperado el 24 de noviembre de 2015.

3. PRINCIPIOS ORIENTADORES PARA LA CIBERSEGURIDAD EN PARAGUAY

Este Plan Nacional busca avanzar con la ciberseguridad en Paraguay de modo a fomentar el uso confiable de las TIC en el país, impulsando un cambio cultural en la sociedad para el uso seguro del ciberespacio, así como el progreso y la innovación en el país, fomentando un entorno económico favorable al crecimiento, desarrollo y competitividad de nuevas tecnologías. Este Plan será implementado a través de la cooperación y coordinación del sector público con el sector privado, la academia y la sociedad civil, con el máximo respeto a la Constitución Nacional y a los derechos y libertades fundamentales de los ciudadanos.

Los principios orientadores para la formulación e implementación de cualquier política pública de ciberseguridad en Paraguay son:

Proporcionalidad: Las medidas a ser aplicadas deben ser adecuadas, necesarias y proporcionales, respetando los derechos fundamentales, en especial los derechos a la intimidad, privacidad, libertad de expresión y libre asociación, que son la prioridad máxima del Estado. Además, es necesario sopesar las oportunidades y amenazas, asegurando la proporcionalidad de las medidas de protección adoptadas, a fin de que no perjudiquen la promoción de la innovación y el desarrollo de nuevas tecnologías.

Coordinación de esfuerzos y uso eficiente de recursos escasos: Todos los sistemas conectados a Internet son potencialmente vulnerables, así que es importante tener en cuenta que es imposible asegurar un ciberespacio totalmente seguro y confiable. Por ello, se debe adoptar la gestión de riesgo en la implementación de políticas de ciberseguridad, a fin de priorizar y justificar las acciones elegidas. Se reconoce la limitación de recursos, así que se promoverá el máximo aprovechamiento de los recursos disponibles y el adecuado análisis y gestión de riesgo, a fin de priorizar y justificar las acciones elegidas.

Responsabilidad compartida: Todos los integrantes de la sociedad comparten responsabilidades en esta materia, incluyendo al Estado, el sector privado empresarial, la academia, las organizaciones de la sociedad civil y los ciudadanos en general. Todos ellos han de sentirse involucrados en la implementación de este Plan Nacional. Para ello, es necesario la implementación de mecanismos de coordinación, diálogo, trabajo conjunto y fomentando y propiciando la cooperación, participación e integración de las múltiples partes interesadas, capaces de compatibilizar iniciativas y propiciar el intercambio de información y conocimiento.

Desarrollo e innovación: Se reconoce la importancia de la innovación para el desarrollo de una economía digital, lo que demanda un ambiente cibernético seguro y capital humano capacitado en el área de TIC y ciberseguridad.

Cooperación internacional: El carácter transnacional de las amenazas hace que sea esencial promover la cooperación regional y global, ya que muchas de las posibles medidas sólo resultarán eficaces si se adoptan internacionalmente con la adecuada cooperación y coordinación entre los gobiernos de los países y organismos internacionales. Así también, para generar espacios de discusión sobre ciberseguridad y gobernanza en Internet en ámbitos supranacionales.

Monitoreo y evaluación: La calidad de las políticas públicas de ciberseguridad requiere un proceso continuo de monitoreo y evaluaciones periódicas. Se incorporará el monitoreo en las políticas públicas de ciberseguridad, con el fin de retroalimentar la gestión de las mismas y corregirlas eventualmente.

4. EJES Y OBJETIVOS

El avance de las TIC debe ser acompañado por una política de ciberseguridad, de forma a dotar de las capacidades y habilidades necesarias a los usuarios, para la utilización confiable y provechosa de estas herramientas, considerando también que con el mayor uso de la tecnología también aumenta el volumen y sofisticación de las amenazas. Para lograr la adopción de medidas de ciberseguridad que garanticen y promuevan el uso seguro y confiable de las TIC, así como el progreso y la innovación en el país, este Plan Nacional se concentra en siete ejes de acción: (i) Sensibilización y Cultura; (ii) Investigación, Desarrollo e Innovación; (iii) Protección de Infraestructuras Críticas; (iv) Capacidad de Respuesta antes Incidentes Cibernéticos; (v) Capacidad de Investigación y Persecución de la Ciberdelincuencia; (vi) Administración Pública; y (vii) Sistema Nacional de Ciberseguridad. Esta sección también ilustra los objetivos en cada eje temático, que son los efectos fundamentales a largo plazo a los que se aspira para la ciberseguridad del país.

4.1 Sensibilización y Cultura

Para que la implementación del Plan Nacional de Ciberseguridad sea sostenible a largo plazo, es de gran importancia que se sensibilice y capacite a los ciudadanos sobre la importancia del uso seguro y responsable de la Internet. Por medio de la concientización ciudadana, se puede empezar a afectar positivamente el comportamiento, desarrollando una comprensión amplia sobre la ciberseguridad en toda la sociedad. El cambio se logrará a través de la incorporación progresiva de buenas prácticas de ciberseguridad, hasta que la misma se vuelva una práctica diaria de los individuos, de las empresas y del gobierno.

La Sociedad de la Información y el uso de las TIC pueden traer muchos beneficios, pero para maximizarlos es esencial promover una sólida cultura de ciberseguridad basada en la adopción de legislación y medidas que garanticen la protección de los datos, así como la conexión segura de los equipos. La cultura cibernética existe cuando el conocimiento de técnicas y de conceptos de ciberseguridad sirve de orientación para las prácticas de los usuarios finales de la red. Por lo tanto, es necesario tomar las acciones de sensibilización para que todos conozcan los riesgos y tengan el acceso a las herramientas de protección. Esto es particularmente importante si se tienen en cuenta las inversiones que se están llevando a cabo en Paraguay para la expansión de los servicios de acceso a Internet como, por ejemplo, la implementación de acceso gratuito a Internet en plazas públicas de los municipios del país. La ciberseguridad debe ser considerada igual de importante que el acceso a Internet (uno no puede existir sin el otro).

Es esencial que los ciudadanos y ciudadanas, al conectarse a sus dispositivos, tengan aplicaciones de protección actualizadas en sus equipos y que no compartan información confidencial en redes abiertas al público en general. Es decir, es fundamental que prácticas como las descritas sean algo permanente en la vida de los ciudadanos conectados a la red. Avisos con recomendaciones de buenas prácticas de ciberseguridad son medidas de bajo costo y pueden ser implementadas en las páginas web de operadoras y proveedores de servicios de Internet, o antes de que los usuarios se conecten a Internet por sitios públicos. De hecho, la Ley de Comercio

Electrónico (Ley N° 4.868/2013) ya establece esta obligación a los proveedores de servicio de acceso al Internet[42], de tal manera que esta medida se puede reproducir en otros frentes.

Además de campañas para el usuario final en general, es importante elaborar proyectos de sensibilización enfocados en grupos específicos, a fin de que los mensajes sean más efectivos. El primer paso para el cambio cultural debe empezar desde la base, promoviendo la incorporación de conceptos de ciberseguridad en los primeros niveles educativos, teniendo en cuenta que los menores de edad muchas veces son los más vulnerables. De hecho, el número de casos de pornografía infantil detectados en Paraguay entre febrero del 2014 y abril del 2015, refleja la importancia de los proyectos de sensibilización enfocados a este grupo vulnerable. Así mismo, estas campañas deben incluir también a los padres y educadores, quienes tienen a su cargo velar por el desarrollo integral de los niños.

En Paraguay, se han identificado programas de sensibilización dirigidos a niños y niñas y a sus padres, como los promovidos por el Ministerio Público (ej. contra el ciberbullying), el CERT-PY (ej. contra el acoso sexual de menores), y por organizaciones no gubernamentales. Sin embargo, es fundamental que estas entidades trabajen de manera más coordinada, a fin de que las campañas de sensibilización tengan mayor impacto. Asimismo, es necesaria la inclusión de educación TIC en la currícula educativa, ya que acciones puntuales ayudan pero no generan el impacto deseado. De igual manera, es esencial la implementación de mecanismos que faciliten el reporte de crímenes cibernéticos relativos a la pornografía de infantil, como líneas directas para reporte (hotline) que cuenten con el apoyo y participación de los proveedores de servicios de acceso a Internet, del Ministerio Público, y de las organizaciones no gubernamentales que actúan en esta área.

Es importante contar con el apoyo de los más altos niveles dentro de las entidades gubernamentales y del sector privado para la adopción de prácticas de ciberseguridad. Si no se toman en serio las mejores prácticas de ciberseguridad y no se cuenta con el apoyo de los ministros, autoridades, directores y funcionarios de alto nivel, el compromiso en los funcionarios públicos y empleados será más difícil de lograr. La oportunidad de liderar el cambio cultural comenzando desde arriba para mostrar un ejemplo a los demás. Es muy importante establecer medidas destinadas a la construcción de la formación de la conciencia de los funcionarios y empleados acerca de la ciberseguridad y del uso responsable de las tecnologías, dado que muchas veces los ataques se dirigen a estos, para tener acceso a los sistemas de información de las organizaciones.

Las empresas deben ser conscientes de la responsabilidad en la seguridad de sus sistemas, la protección de la información de sus clientes y proveedores, y la seguridad de los servicios que prestan. Mantener la confianza del consumidor es fundamental para el desarrollo de una economía digital. Lo mismo aplica para el Gobierno en la prestación de sus servicios a los ciudadanos. En este sentido, se buscan concretizar los siguientes objetivos para un verdadero cambio cultural:

[42] "Artículo 9 – Los Proveedores de Servicios de Intermediación consistentes en la prestación de servicios de acceso a Internet, estarán obligados, sin perjuicio de las disposiciones vigentes sobre los Servicios de Acceso a Internet y Transmisión de Datos establecidas por la Autoridad Competente a: a) informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otras cosas, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados; b) informar sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios no deseados en Internet o que puedan resultar nocivos para la niñez y la adolescencia;

a. Las campañas de sensibilización pública son reconocidas y promovidas por el público general, y se aumenta el conocimiento sobre mejores prácticas de ciberseguridad y comportamiento seguro en el ciberespacio.
b. Los programas enfocados en la sensibilización sobre ciberseguridad dirigidos a menores, son coordinados entre las distintas entidades gubernamentales, academia, sector privado y sociedad civil, concientizando a los niños y a las niñas, así como a sus padres o encargados y profesores, sobre buenas prácticas y/o las medidas que se deben tomar en caso de un incidente cibernético.
c. Los profesionales, las empresas y las entidades gubernamentales son conscientes de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías para la adecuada prestación de los servicios y para el fomento de una economía digital segura.

4.2 Investigación, Desarrollo e Innovación

El primer paso hacia la instauración de buenas prácticas de seguridad digital, es garantizar que el país cuente con personal capacitado en ciberseguridad, en todos sus distintos sectores. Para ello, el aprendizaje sobre la ciberseguridad desde los primeros niveles de la enseñanza es importante para fomentar el interés profesional de los jóvenes. Hay muchos jóvenes talentosos en esta área, y por eso es esencial captar su interés en el tema desde muy temprano para que participen de manera positiva en la construcción de un país más conectado, con un ciberespacio seguro y confiable.

Asimismo, en la educación superior se deben crear líneas de investigación e incluir en las mallas curriculares cursos de ciberseguridad, que posibiliten al estudiante obtener su grado con una concentración en seguridad, por ejemplo. Es fundamental también estimular la investigación a nivel de postgrado con maestrías y doctorados que, a su vez, deben ser acompañados de becas para investigación y programas de intercambio. Fomentar la investigación es esencial para que se desarrollen soluciones innovadoras adaptadas a las necesidades y a la idiosincrasia de la sociedad paraguaya. Se debe promocionar la inclusión de cursos de ciberseguridad en las mallas curriculares de otras áreas, como en Derecho y Gestión Pública. Finalmente, es importante tener en cuenta que el desarrollo de la investigación, y de otros programas de postgrado con enfoque más profesional, solamente será posible con una inversión mínima orientada a la formación de docentes por medio de becas, por ejemplo.

Además, es necesaria una coordinación entre la sociedad civil, academia, empresas y gobierno, de modo a que haya una colaboración enfocada a impulsar proyectos en estas áreas para mejorar no sólo la calidad de los servicios y de los productos, sino también la calidad de vida de los ciudadanos en general. El intercambio de conocimiento es importante, así como una colaboración entre estos sectores posibilitará un mejor uso de recursos en proyectos de interés para el desarrollo de la economía y la sociedad paraguaya. De hecho, existen en el país programas que buscan impulsar la modernización tecnológica y fomentar el desarrollo de un tejido empresarial fuerte, particularmente dirigidos al comercio electrónico y a las MIPYMES. Tales programas son ejecutados de manera coordinada entre el MIC, la CONACYT, y entidades académicas. En este contexto, sería importante incluir en tales programas componentes de ciberseguridad, de manera que los servicios y productos tecnológicos desarrollados, estén de acuerdo con las mejores prácticas de seguridad internacional.

Asimismo, sería importante no sólo el fomento al desarrollo de servicios y productos tecnológicos -como ya se hace en Paraguay-[43], sino también la implementación de programas orientados a incentivar al sector privado, particularmente las MIPYMES, a que adopten reglas de seguridad. Otra medida interesante sería el fomento del comercio electrónico, especialmente en el lado de la oferta, por medio de la implementación de sellos de confianza en línea con los comercios nacionales. Esto contribuiría al fortalecimiento del comercio electrónico confiable y al desarrollo de la economía digital en el país. Para el desarrollo de una economía digital en Paraguay, se requiere fomentar y mantener actividades de investigación, enfocadas en el desarrollo e innovación en materia de TIC y ciberseguridad. Se buscan concretizar los siguientes objetivos con este Plan Nacional:

a. El interés por las TIC y la ciberseguridad es incentivado en todos los niveles de la enseñanza– desde la básica a la superior – por medio de programas y cursos específicos en estas áreas.
b. Los institutos de enseñanza superior y centros de investigación trabajan en conjunto con el sector privado, las ONGs y el sector público para impulsar proyectos de ciberseguridad.
c. Hay capacitación continua en ciberseguridad, promoviendo el fortalecimiento de la seguridad en las organizaciones e incentivando la profesionalización en el sector de la seguridad de la información.
d. Se fomenta la innovación y el desarrollo de una economía digital por medio de un tejido empresarial fuerte y un ciberespacio seguro.

4.3 Protección de Infraestructuras Críticas

Se puede decir que las sociedades son dependientes de un sistema complejo de servicios esenciales denominados infraestructuras críticas. Este sistema está compuesto por operadores y activos involucrados en la prestación de tales servicios, que garantizan no sólo la seguridad de los ciudadanos, sino que también su bienestar económico y social.

Cabe recalcar que no existe una definición única o un listado de infraestructuras críticas; cada país define las infraestructuras críticas según su realidad. De manera general, las infraestructuras críticas consisten en sistemas y activos, físicos o virtuales, esenciales para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población, y cuya perturbación o destrucción tendría un impacto debilitante en la seguridad nacional, generando una cascada de efectos negativos que afectarían gravemente al país. Dicho de otro modo, estas infraestructuras sostienen el funcionamiento de actividades cotidianas de los ciudadanos, como servicios públicos esenciales y las principales actividades económicas del país.

Con el propósito de desarrollar este Plan Nacional de Ciberseguridad, se busca proteger las infraestructuras de las TIC, tanto su infraestructura física (ej. redes, puntos de intercambio de tráfico, equipos) como en su vertiente inmaterial (ej. sistemas de informáticos, sistemas de control industrial, nombres de dominios), que soportan las infraestructuras críticas mencionadas anteriormente.

[43] Por ejemplo, la Ley de Firma Digital (Ley no 4017/2010) y la Ley de Comercio Electrónico (Ley no 4.868/2013).

Vale recalcar que las infraestructuras críticas están incorporando cada vez más estas tecnologías de información y comunicación, lo que permite mejorar y optimizar los servicios prestados, gestionando las instalaciones de manera más eficiente. Sin embargo, el uso de forma creciente de las TIC y de los sistemas integrados al Internet en los servicios esenciales, puede representar un aumento de riesgo de ataques cibernéticos. En especial, si la implementación de las TIC en las infraestructuras no está acompañada de medidas de seguridad. El reto de la optimización en la prestación de los servicios esenciales y la conquista de mayor eficiencia y efectividad, se acompaña del desafío del avance en la protección y seguridad de las infraestructuras TIC.

En este contexto, es esencial que Paraguay defina cuáles son sus infraestructuras críticas en términos de ciberseguridad, es decir, las infraestructuras críticas que utilizan TIC y sistemas integrados al Internet para su operación. Así, se debe realizar un estudio sobre las condiciones de seguridad de estas infraestructuras, tanto del sector público como del sector privado; establecer normas claras, protocolos y un plan de comunicación nacional para proteger la infraestructura crítica en el caso de un ataque cibernético.

Operadores de infraestructuras críticas deben llevar a cabo periódicamente las mejores prácticas en ciberseguridad, tales como evaluaciones para identificar las vulnerabilidades de seguridad en las computadoras, las redes y la infraestructura de comunicación, así como los mecanismos para hacer frente a estas vulnerabilidades. Es de gran importancia que los operadores de infraestructuras críticas adopten medidas de ciberseguridad específicas para gestionar la evolución de los riesgos y su capacidad de resiliencia. En otras palabras, es esencial promover un análisis de riesgo de las infraestructuras, verificando su nivel de vulnerabilidad y probabilidad de ataque, así como la magnitud del impacto y la capacidad de recuperación ante un incidente cibernético. Debe ser evitada cualquier violación de la seguridad que tenga un impacto significativo en las operaciones del proveedor de servicios.

En Paraguay, algunos servicios esenciales son prestados por empresas públicas (p.ej. ANDE, COPACO, ESSAP, PETROPAR, BNF). A pesar de su carácter crítico, no hay obligación por parte de los operadores de infraestructuras de adoptar reglas y normas específicas de ciberseguridad. De hecho, la regulación de las empresas públicas encargadas por la prestación de servicios esenciales no es centralizada. 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.

Finalmente, es esencial que haya cooperación entre los sectores públicos y privado para la protección de infraestructuras críticas. Los servicios esenciales, así como sus sistemas y activos, también se encuentran en manos del sector privado, por lo tanto, la colaboración entre el sector público y el sector privado es necesaria para garantizar la seguridad y resistencia de las infraestructuras críticas y garantizar un entorno cibernético seguro para el desarrollo del país. El intercambio permanente de información entre el sector público y privado acerca de los incidentes cibernéticos que ocurren, permitirá identificar las tendencias de los incidentes de ciberseguridad en el país, su frecuencia y tipo. Con esta información, se pueden hacer inversiones más eficaces para la protección y seguridad, así como capacitación, sensibilización y concienciación que promuevan un uso eficiente de la tecnología.

En este contexto, se buscan concretizar los siguientes objetivos generales para el fortalecimiento de la protección de infraestructuras críticas en Paraguay:

a. Las infraestructuras críticas paraguayas son resilientes ante las amenazas cibernéticas y garantizan la estabilidad de los servicios esenciales.
b. La responsabilidad por la ciberseguridad de las infraestructuras críticas es compartida entre el Estado y operadores privados, fomentando la cooperación público-privada.

4.4 Capacidad de Respuesta ante Incidentes Cibernéticos

Los países deben estar preparados para responder de manera eficaz a los incidentes de ciberseguridad. Para lograr este objetivo, es esencial formar un equipo nacional de respuesta ante emergencias informáticas. De hecho, los CERTs (Centros de Respuesta ante Incidentes Cibernéticos, CERT por sus siglas en inglés), hacen mucho más: no sólo son los principales proveedores de servicios de seguridad informática a los gobiernos y ciudadanos, sino que también promueven la sensibilización en ciberseguridad en toda la sociedad. Como se mencionó, el CERT-PY, como el equipo nacional de respuesta a incidentes del Paraguay, ha venido realizando estas actividades: responder ante incidentes cibernéticos, ofrecer capacitación en materia de ciberseguridad, promover campañas de sensibilización sobre ciberseguridad, testing de infraestructuras, entre otras.

Sin embargo, para seguir trabajando en este sentido, es fundamental que el CERT-PY cuente con las herramientas necesarias. Por lo tanto, el CERT-PY debe contar con recursos humanos suficientes, infraestructura adecuada, y una asignación presupuestaria específica que garantice su adecuada operación. En este contexto, es importante que se implementen programas de capacitación orientados al personal del CERT-PY, de modo que se desarrolle un grupo de expertos y se garantice la actualización del conocimiento y habilidades de los profesionales, en un área tan dinámica como lo es la ciberseguridad. Se buscará también implementar medidas que posibiliten que el CERT-PY opere de manera eficiente y esté equipado para determinar rápidamente las amenazas y aplicar medidas para disuadir futuras amenazas y para recuperarse de las amenazas existentes.

Además de la adecuada infraestructura, el CERT-PY necesita de información sobre incidentes cibernéticos que ocurren en el país para que su trabajo sea más efectivo. En el ámbito de ciberseguridad, el intercambio de información se ha vuelto fundamental para evaluar y garantizar la respuesta y la recuperación ante intrusiones cibernéticas o ataques a diversos sistemas de información. Para garantizar el intercambio de información eficaz, es de suma importancia la confidencialidad y la protección de los datos que se comparten. Se buscará promover un ambiente de confianza para el intercambio rutinario de información de comunicaciones críticas sobre amenazas, vulnerabilidades, intrusiones y anomalías relacionadas con la ciberseguridad, así como las contramedidas y mecanismos de recuperación.

El CERT-PY desarrollará un repositorio de información sobre las amenazas, mejores prácticas y planes de recuperación. Para la consolidación de este repositorio, el CERT-PY necesita de la colaboración y cooperación de otras entidades gubernamentales, así como del sector privado, academia y sociedad civil. Esta alianza será establecida por medio de convenios para el intercambio de información sobre incidentes cibernéticos.

En particular, los operadores y prestadores de servicios de conexión a Internet cuentan con información esencial para que el CERT-PY tenga un mejor entendimiento sobre las tendencias de los incidentes cibernéticos. Es importante considerar el establecimiento de un “Código de Conducta” voluntario (a ejemplo de lo que hace MIC y las asociaciones comerciales en cuestiones relativas al comercio electrónico) para los operadores de infraestructura de

telecomunicaciones que incluya el compromiso de compartir información sobre incidentes con el CERT-PY y entre los demás operadores, así como una definición clara sobre incidentes cibernéticos.

El CERT-PY continuará operando bajo SENATICs, pero se apuntará a que tenga una asignación presupuestal explícita y un plan operativo. Se buscan concretizar los siguientes objetivos:

a. El intercambio de información sobre incidentes cibernéticos se convierte en una práctica común entre las entidades gubernamentales, el CERT-PY, el sector privado, la sociedad civil y los ciudadanos.
b. Los agentes responsables de las respuestas ante incidentes cibernéticos están capacitados y poseen el conocimiento necesario para conducir su trabajo.
c. La unidad encargada de la respuesta a incidentes cuenta con una infraestructura y herramientas adecuadas para conducir sus respectivas tareas de manera oportuna y eficaz.

4.5 Capacidad de Investigación y Persecución de la Ciberdelincuencia

La Unidad Especializada de Delitos Informáticos del Ministerio Público y la División Especializada contra Delitos Informáticos, dependiente del Departamento contra Delitos Económicos y Financieros de la Policía Nacional, trabajan conjuntamente en la investigación de delitos informáticos. Las dos entidades han avanzado significativamente en los últimos años para mejorar la ejecución de su trabajo en casos que involucren sistemas informáticos. Sin embargo, particularmente en el caso de la Policía Nacional, existe una falta de recursos y herramientas adecuadas para los trabajos de peritaje y manejo de la evidencia digital. Además, es esencial implementar programas de capacitación nacional e internacional para los órganos de denuncias, investigación y administración de la justicia, no sólo cursos técnicos como manejo de evidencia digital, sino también cursos sobre la temática de delitos informáticos y en el ámbito cibernético. Es importante que agentes fiscales, de policía y jueces entiendan mejor los aspectos técnicos de Internet y cómo se llevan a cabo ataques cibernéticos u operaciones criminales, para saber enfrentarlas.

Aunque hubo cambios importantes en la legislación a fin de posibilitar la investigación y persecución de delitos informáticos, todavía faltan modificaciones esenciales. El objetivo es reforzar a los organismos participantes en la cadena judicial, con un marco regulatorio actualizado y capacidades operativas que aumenten la posibilidad de identificar a los responsables. El Plan Nacional de Ciberseguridad tratará de complementar la legislación de Paraguay en materia de ciberseguridad a través de recomendaciones legales, convenciones internacionales y otros documentos legales propuestos por autoridades internacionales, para modernizar y adecuar la aplicación del marco regulatorio de Paraguay.

Para afrontar adecuadamente las amenazas cibernéticas, es imprescindible el fortalecimiento de la cooperación judicial y policial internacional, articulando los instrumentos adecuados de colaboración e intercambio de información y la armonización de las legislaciones nacionales, con el desarrollo y mantenimiento de una regulación sólida y eficaz. En concreto, este Plan Nacional promoverá la ratificación del Convenio de Budapest y la creación de leyes adicionales para la ejecución de sus compromisos en virtud de dicho Convenio. Se buscan concretizar los siguientes objetivos:

a. Los agentes responsables de la investigación de delitos informáticos están capacitados y poseen el conocimiento necesario para conducir su trabajo.
b. Las unidades encargadas de la investigación de delitos informáticos cuentan con infraestructura y herramientas adecuadas para conducir sus tareas de manera oportuna y eficaz.
c. Paraguay cuenta con una legislación en materia de ciberseguridad que permite la investigación adecuada y persecución de casos de delitos informáticos.

4.6 Administración Pública

Con el fin de garantizar un entorno digital seguro, la Administración Pública elaborará 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.

Se fomentará en las distintas instituciones de la Administración Pública la creación de unidades especializadas en TIC, que trabajarán de forma conjunta en la implementación del Plan Nacional de Ciberseguridad y con el Coordinador Nacional; en un sistema de trabajo coordinado, para facilitar la difusión rápida y eficaz. En ese contexto se pretende lograr que:

a. La administración pública, tanto la central como las entidades y organismos descentralizados, cuentan con infraestructura adecuada para garantizar un entorno digital seguro.
b. Las gestiones gubernamentales de ciberseguridad se coordinan con cada agente responsable consciente de su función y papel referente a la ciberseguridad.

4.7 Sistema Nacional de Ciberseguridad

Por Resolución de la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs), será designado un Coordinador Nacional de Ciberseguridad, con la responsabilidad de monitorear y evaluar la implementación del Plan Nacional de Ciberseguridad. El Coordinador Nacional deberá trabajar de cerca y coordinar con todas las demás entidades gubernamentales y de los demás sectores que tienen responsabilidades en virtud del Plan Nacional de Ciberseguridad.

El intercambio de información entre los distintos actores es esencial para la efectividad de la ciberseguridad. Hay algunos factores que afectan la distribución oportuna y el intercambio de esta información, como son las clasificaciones de la información y el temor a la divulgación. Se gestionará para proporcionar un ambiente de confianza y fortalecer las líneas de comunicación existentes. El diálogo y la cooperación entre el sector privado y el Estado son requisitos esenciales para este fin. Por lo que se encuadran como objetivos que:

a. El Coordinador Nacional de Ciberseguridad es designado y se pone en funcionamiento el Sistema Nacional de Ciberseguridad, promoviendo la participación, representatividad y cooperación de todos los sectores.
b. Se elabora el Plan de Ejecución del Plan Nacional de Ciberseguridad, para cada eje estratégico y sus respectivas líneas de acción.
c. Se realiza el acompañamiento, seguimiento y control del grado de cumplimiento del Plan Nacional de Ciberseguridad.

5. SISTEMA NACIONAL DE CIBERSEGURIDAD

Con el propósito de garantizar una visión integral de la ciberseguridad en el país, así como políticas coordinadas y adecuadas para implementar las líneas de acción de este Plan Nacional, es necesaria una estructura que posibilite la acción conjunta entre los distintos actores. Para asegurar la implementación efectiva de este Plan Nacional de Ciberseguridad, es crítico el establecimiento y la definición de roles para la adecuada coordinación. Será aprobado por Decreto del Poder Ejecutivo el Plan Nacional de Ciberseguridad, bajo el liderazgo de un Coordinador Nacional y la ejecución de una Comisión Nacional de Ciberseguridad, con la responsabilidad de aplicación de este Plan Nacional. El Sistema Nacional de Ciberseguridad tendrá los siguientes componentes: (i) el Coordinador Nacional de Ciberseguridad y (ii) la Comisión Nacional de Ciberseguridad.

5.1 Coordinador Nacional de Ciberseguridad

El Coordinador Nacional de Ciberseguridad será nombrado por la Resolución de la Máxima Autoridad de la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs), y responderá directamente a la Comisión Nacional de Ciberseguridad. El Coordinador tendrá la autoridad para monitorear y evaluar la implementación de los objetivos y de las líneas de acción de este Plan Nacional por parte de los distintos actores gubernamentales. Sus funciones específicas serán determinadas en el respectivo Decreto que apruebe el Plan.

5.2 Comisión Nacional de Ciberseguridad

La Comisión Nacional de Ciberseguridad, presidida por el Coordinador Nacional de Ciberseguridad, reforzará relaciones de coordinación, colaboración y cooperación entre los distintos sectores y partes interesadas en la ciberseguridad, incluyendo al Estado, el sector privado, la academia y la sociedad civil. Desde este espacio se promoverán análisis, estudios y propuestas de iniciativas tanto en el ámbito nacional como internacional, que favorezcan el ecosistema de la ciberseguridad. La Comisión Nacional deberá reportarse e informar el progreso en la implementación de este Plan Nacional al Coordinador Nacional. Para tal fin, la Comisión Nacional deberá trabajar de cerca y coordinar con todas las demás entidades que tienen responsabilidades en virtud del Plan Nacional, así como buscará promover el intercambio de información y el desarrollo e implementación de soluciones de ciberseguridad conjuntas. Se buscará desde allí reafirmar los principios de coordinación de esfuerzos y responsabilidades compartidas entre las múltiples partes interesadas.

La composición de la Comisión Nacional de Ciberseguridad refleja la importancia de coordinar aquellas acciones que se deban abordar de forma conjunta con el fin de optimizar los recursos y evitar la duplicación de esfuerzos. La Comisión Nacional de Ciberseguridad será compuesta por representantes de las instituciones designadas en el respectivo Decreto de aprobación del Plan, pudiendo no obstante modificarse su composición a fin de incluir a otros órganos gubernamentales con actuación pertinente en esta materia. Asimismo, se garantizará la participación y representatividad en la Comisión Nacional de todos los demás sectores involucrados en la realización del Plan Nacional, como ser la academia, el sector privado, la sociedad civil organizada.

Para constatar el carácter multidimensional que el presente Plan Nacional propone para la implementación de políticas de ciberseguridad, conviene advertir que sus siete ejes se definen en los 20 objetivos y 60 líneas de acción delineadas (Anexo 1). La Comisión Nacional de

Ciberseguridad será dividida en siete Subcomités Especializados, según los ejes definidos en este Plan Nacional: (i) Subcomité de Sensibilización y Cultura; (ii) Subcomité de Investigación, Desarrollo e Innovación; (iii) Subcomité de Protección de Infraestructuras Críticas; (iv) Subcomité de Respuesta ante Incidentes Cibernéticos; (v) Subcomité de Investigación y Persecución de la Ciberdelincuencia; (vi) Subcomité de la Administración Pública; y (vii) Subcomité del Sistema Nacional de Ciberseguridad.

La composición de los Subcomités Especializados será determinada por los miembros de la Comisión Nacional de Ciberseguridad. Cabe recalcar que otras entidades que no se encuentran representadas en la Comisión Nacional de Ciberseguridad, podrán formar parte de los Subcomités Especializados de acuerdo con la decisión de los miembros de la Comisión. Los Subcomités tendrán la tarea de formular la estrategia de implementación de los ejes de este Plan Nacional, definiendo las entidades que serán responsables de la implementación concreta de las líneas de acción.

Además de los Subcomités Especializados, se conformarán, cuando sea necesario, Grupos de Trabajo Temáticos donde se invitarán a actores relevantes del sector privado, gremios profesionales, academia, sociedad civil y especialistas. La Comisión Nacional establecerá los criterios de selección de las instituciones y de los individuos que conformarán los grupos de trabajo según las áreas establecidas, así como el producto final deseado con cada Grupo de Trabajo Temático. Los Grupos de Trabajo Temáticos serán conformados para apoyar a la Comisión Nacional y a los Subcomités Especializados cuando haya la necesidad de analizar un tema y realizar investigaciones de manera más detallada.

6. MONITOREO Y EVALUACIÓN

Esta sección tiene como propósito asegurar la eficiencia y la eficacia del Plan Nacional de Ciberseguridad, tanto en el uso de los recursos como en la orientación de las iniciativas definidas. El monitoreo de las acciones constituye uno de los principios orientadores del Plan Nacional junto con la idea de evaluación que, a su vez, requiere el diseño de indicadores. Los indicadores tienen como propósito analizar la implementación de las políticas de ciberseguridad y permitir la retroalimentación para una eventual corrección de las políticas por medio de decisiones basadas en evidencia. Es decir, un enfoque basado en evidencias facilita la priorización de los objetivos en la toma de decisiones, garantizando la legitimidad y la credibilidad de las políticas de ciberseguridad en Paraguay.

Los indicadores constituyen una expresión cuantitativa o cualitativa que permite comparar el desempeño de una política con respecto a los objetivos pre-establecidos, buscando determinar si la implementación de la política ha avanzado y si los procesos de trabajo que se realizan permitirán alcanzar los efectos deseados. Los indicadores deben seguir un conjunto de parámetros técnicos. Es decir, los indicadores deben ser específicos, cuantificables, alcanzables, relevantes, y susceptibles de monitorear, según el conjunto de características propuestas por el modelo SMART[44].

[44] Acrónimo en inglés para Specific, Measurable, Achievable, Relevant y Trackable.

El Plan Nacional de Ciberseguridad cuenta con un Plan de Acción (Anexo 1) que define las líneas de acción para el cumplimiento de los objetivos de largo plazo. Se buscará definir, para la adecuada implementación de este Plan Nacional, los productos inmediatos que se buscan y los resultados intermedios[45], así como los respectivos indicadores[46]. Es fundamental que los productos inmediatos estén vinculados a los resultados intermedios que, por su parte, deben estar vinculados a los objetivos de largo plazos definidos en el Plan. Los indicadores son esenciales no sólo para seguir el progreso de la implementación de este Plan Nacional de Ciberseguridad, sino también para apoyar en la revisión general, asegurándose que alcance sus objetivos de manera eficiente y eficaz.

Para la implementación de mecanismos de monitoreo y evaluación que permitirán una mayor transparencia de las políticas de ciberseguridad, se pondrán a disposición de la ciudadanía, sociedad civil y demás órganos extra poder, todos los procesos e iniciativas realizados en el marco del Plan Nacional de Ciberseguridad (resguardando la privacidad y seguridad de la información en cuanto así se requiera), constituyendo todo lo actuado en el marco de este Plan, información pública a disposición de la ciudadanía e interesados. De esta manera, todos los actores de los distintos sectores, estarán facultados a dar seguimiento a estas acciones, evaluarlas y presentar las observaciones que consideren pertinentes, como así también a solicitar mayor información respecto a las acciones realizadas.

Una rendición de cuenta periódica se gestionará una vez que se ejecute la colecta de datos de implementación y de cumplimiento del plan de acción establecido, mediante la preparación de informes periódicos acerca de los avances en la implementación del Plan Nacional de Ciberseguridad.

7. REVISIÓN

Se prevé que este Plan Nacional de Ciberseguridad y su Plan de Acción sea actualizado y revisado cada 3 años o cuando sea necesario, de acuerdo con la propuesta de revisión del Coordinador Nacional de Ciberseguridad y anuencia de la Comisión Nacional de Ciberseguridad.

[45] Los productos son las consecuencias directas de las acciones, y suelen ser tangibles y más fácilmente mensurables cuantitativa y cualitativamente. Los resultados intermedios, por su parte, reflejan los efectos de corto y mediano plazo de las políticas.

[46] Los indicadores de productos miden los entregables más inmediatos de un proyecto como, por ejemplo, el número de beneficiarios de un proyecto o la cantidad de servicios prestados o productos producidos. Por otro lado, los indicadores de resultados intermedios miden los resultados de corto y mediano plazo, lo que incluye cambios graduales de comportamiento, fortalecimiento de las capacidades y habilidades en ciberseguridad.

ANEXO 1 - PLAN DE ACCIÓN

Ejes	Objetivos	Líneas de Acción
1. Sensibilización y Cultura	1.a. Las campañas de sensibilización públicas son reconocidas y promovidas por el público general y se aumenta el conocimiento sobre mejores prácticas de ciberseguridad y comportamiento seguro en el ciberespacio.	1.a.1 Llevar a cabo estudios/encuestas de referencia nacional sobre la sensibilización de la ciberseguridad entre los ciudadanos, considerando los aspectos demográficos y geográficos, con el propósito de identificar necesidades específicas de cada grupo.
		1.a.2 Desarrollar campañas temáticas de sensibilización pública entre diversos grupos demográficos en Paraguay, en alianza con el sector privado, sociedad civil y academia.
		1.a.3 Desarrollar campañas de sensibilización de manera coordinada entre las distintas entidades gubernamentales, evitando la duplicación de esfuerzos y garantizando un mensaje más amplio y de mayor impacto; así como la concienciación necesaria en los actores gubernamentales y del estado.
		1.a.4 Promover la inclusión de avisos con recomendaciones de buenas prácticas de ciberseguridad (ej. uso de antivirus, firewall) dirigidos a los usuarios, antes de que se conecten cualquier red abierta disponible al público general.
	1.b. Los programas enfocados en la sensibilización sobre ciberseguridad, dirigidos a menores, son coordinados entre las distintas entidades gubernamentales, academia, sector privado y sociedad civil, concientizando a los niños y las niñas, así como a sus padres o encargados y profesores, sobre buenas prácticas y/o las medidas que se deben tomar en caso de un incidente cibernético.	1.b.1 Contar con el apoyo de las operadoras y proveedores de servicios de Internet en la implementación de avisos con recomendaciones de prácticas de ciberseguridad cuando el usuario utiliza alguno de sus servicios.
		1.b.2 Asegurar que los programas de incentivo al uso de las TIC por niños y niñas en las escuelas sean acompañados por material educativo en materia de seguridad digital, así como para padres o encargados y profesores, sobre el buen uso del equipo y buenas prácticas de seguridad en el uso de internet (ej. hoja de consejos de seguridad

1. Sensibilización y Cultura	1.b. Los programas enfocados en la sensibilización sobre ciberseguridad, dirigidos a menores, son coordinados entre las distintas entidades gubernamentales, academia, sector privado y sociedad civil, concientizando a los niños y las niñas, así como a sus padres o encargados y profesores, sobre buenas prácticas y/o las medidas que se deben tomar en caso de un incidente cibernético.	estudiantil, contrato de "código de conducta" del estudiante).
		1.b.3 Implantar módulos educativos de sensibilización en ciberseguridad orientados a los niños y niñas, adolescentes y padres, en escuelas de enseñanza inicial, básica y media.
		1.b.4 Fomentar la implementación de consejos de ciberseguridad juveniles, en los que tanto padres, estudiantes y personal de la escuela tengan la oportunidad de debatir sobre ciberseguridad y buenas prácticas para la mitigación de problemas. Implementar charlas de orientación y capacitación enfocadas a niños, jóvenes, adultos y educadores divididas en grupos, a ser llevadas a cabos en las instituciones educativas.
		1.b.5 Desarrollar y distribuir materiales en formato textual e ilustrativo para el fomento del debate y para trabajos pedagógicos dentro de las instituciones educativas, involucrando a los alumnos, padres y docentes sobre las principales problemáticas actuales (ej. *grooming*, *ciberbullying*, *sexting*).
		1.b.6 Implantar mecanismos que faciliten el reporte de incidentes cibernéticos, delitos informáticos o delitos cometidos en el ámbito cibernético, que afectan a los niños, niñas y adolescentes, fomentando procedimientos que puedan ser aplicados por las escuelas, colegios, padres, encargados y docentes ante tales casos.
	1.c. Los profesionales, las empresas y las entidades gubernamentales son conscientes de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías para la adecuada prestación de los servicios y para el fomento de una economía digital segura.	1.c.1 Desarrollar programas de sensibilización para el nivel ejecutivo y los responsables de toma de decisiones en las organizaciones (privadas y públicas), con un enfoque en la incorporación de la ciberseguridad en el ambiente organizacional, que incluya la dotación de recursos suficientes para los departamentos de TI para resolver los problemas de ciberseguridad.

		1.c.2 Fortalecer las capacidades de todos los funcionarios públicos de entidades gubernamentales y empleados del sector privado para adoptar ciertas prácticas básicas de ciberseguridad a través de su tarea diaria que implica el uso de tecnología y manejo de información sensible (por ejemplo, las mejores prácticas en la creación de contraseñas y salvaguarda de los datos sensibles, entre otros).
2. Investigación, Desarrollo e Innovación	2.a. El interés por las TIC y la ciberseguridad es incentivado en todos los niveles de la enseñanza – desde la básica a la superior – por medio de programas y cursos específicos en estas áreas.	2.a.1 Crear programas de fomento al uso de las TIC, con enfoque en la ciberseguridad, a estudiantes de la enseñanza básica.
		2.a.2 Establecer en las mallas curriculares de la enseñanza superior, cursos en ciberseguridad que posibiliten la capacitación sobre el tema de jóvenes profesionales (hombres y mujeres) de distintas áreas, tales como Ciencias Informáticas, Ingeniería, Derecho, Gestión Pública, entre otras.
		2.a.3 Incentivar la investigación y el estudio en campos afines a la ciberseguridad en los cursos de postgrados, con perspectiva de Derechos Humanos.
		2.a.4 Crear programas de formación de docentes en esta área.
	2.b. Los institutos de enseñanza superior y centros de investigación trabajan en conjunto con el sector privado, las ONGs y el sector público para impulsar proyectos de ciberseguridad.	2.b.1 Extender y ampliar los programas de investigación avanzada y proyectos en ciberseguridad en cooperación con universidades, centros especializados, el sector público y el sector privado, con el objetivo de buscar soluciones para las necesidades específicas de la economía y de la sociedad paraguaya.
		2.b.2 Buscar líneas de financiamiento junto a los sectores privado y público para becas y otras oportunidades de capacitación para la academia y profesionales del área.
		2.c.1 Promover programas de capacitación en ciberseguridad orientados a los profesionales de tecnología de la información.

2. Investigación, Desarrollo e Innovación	2.c. Hay capacitación continua en ciberseguridad, promoviendo el fortalecimiento de la seguridad en las organizaciones e incentivando la profesionalización en el sector de la seguridad de la información.	2.c.2 Promover programas de entrenamiento en conceptos básicos de buenas prácticas de ciberseguridad en el momento de la contratación de profesionales y de manera regular en las organizaciones.
		2.c.3 Promover eventos y talleres profesionales periódicos en ciberseguridad mediante alianzas entre los distintos sectores.
		2.c.4 Fomentar la participación de los actores del Sistema Nacional de Ciberseguridad en espacios de diálogo y discusión del ámbito internacional y de Organismos Supranacionales, sobre ciberseguridad y gobernanza de internet.
	2.d. Se fomenta la innovación y el desarrollo de una economía digital por medio de un tejido empresarial fuerte y un ciberespacio seguro.	2.d.1 Crear programas gubernamentales específicos para el fomento de productos y servicios en materia de TICs y ciberseguridad.
		2.d.2 Impulsar el desarrollo y adopción de códigos de conducta y buenas prácticas en ciberseguridad, para la prestación de servicios, con el fin de mejorar conjuntamente las capacidades de ciberseguridad en los sectores de la industria y servicios de Paraguay.
		2.d.3 Desarrollar programas de incentivo a las MIPYMES para la adopción de buenas prácticas en ciberseguridad, así como la generación de *startups* de tecnología que apliquen, fomenten o presten servicios basados en estándares de seguridad.
		2.d.4 Impulsar sellos de confianza en línea para los comercios nacionales con el propósito de fomentar el comercio electrónico confiable y seguro.
		2.d.5 Impulsar el desarrollo de estándares de ciberseguridad y promover su adopción en el sector privado (ej. ISO 27001).

3. Protección de Infraestructuras Críticas	3.a. Las infraestructuras críticas paraguayas son resilientes ante las amenazas cibernéticas y garantizan la estabilidad de los servicios esenciales.	3.a.1 Crear una base de datos de toda la infraestructura crítica (público y privada) con los sistemas de información asociados.
		3.a.2 Impulsar la implementación de una normativa en ciberseguridad para la protección de infraestructuras críticas que abarque tanto el ámbito físico como el tecnológico. Este marco normativo debe identificar las infraestructuras críticas del país y el desarrollo de planes de protección, siendo obligatoria su aplicación por los operadores de estas infraestructuras. Deberá asimismo prever mecanismos de control, auditoría y verificación del cumplimiento de la normativa.
		3.a.3 Realizar análisis de riesgo de las deficiencias sistemáticas, organizacionales y técnicas, de forma anual, en todas las infraestructuras críticas y activos críticos. Se podrán promover ejercicios y simulacros de emergencias para validar los planes de protección y asegurar que los canales de comunicación, la activación de emergencias y las propias medidas de contingencia funcionan apropiadamente.
		3.a.4 Elaborar directrices técnicas para la gestión de sistemas de control industrial de las empresas públicas.
		3.a.5 Llevar a cabo, en coordinación con los países con los que Paraguay comparte infraestructuras críticas, proyectos específicos de control industrial y ciberseguridad.
	3.b. La responsabilidad por la ciberseguridad de las infraestructuras críticas es compartida entre el Estado y los operadores privados, fomentando la cooperación público-privada.	3.b.1 Hacer reuniones periódicas con los representantes del Ministerio Público y del CERT-PY para relevar información acerca de incidentes y delitos informáticos con el objetivo de desarrollar procedimientos que mejoren la cooperación para la pronta y efectiva atención a los mismos.
		3.b.2 Desarrollar en forma conjunta y colaborativa, un procedimiento de cooperación entre operadores de infraestructuras críticas, el Ministerio

		Público, y el CERT-PY, que permita la comunicación directa y la reacción efectiva ante incidentes de ciberseguridad.
		3.b.3 Fomentar la participación del sector privado en ejercicios de simulación de incidentes cibernéticos, que permitan la comprensión del rol que compete a cada sector, ante incidentes de ciberseguridad.
4. Capacidad de Respuesta ante Incidentes Cibernéticos.	4.a. El intercambio de información sobre incidentes cibernéticos se convierte en una práctica común entre las entidades gubernamentales, el CERT-PY, el sector privado, la sociedad civil y los ciudadanos.	4.a.1 Establecer una base de datos nacional actualizada de los incidentes cibernéticos detectados, incluyendo la alerta temprana sobre amenazas.
		4.a.2 Establecer convenios de colaboración y cooperación entre el sector privado y las entidades gubernamentales, por medio del CERT-PY, para el intercambio fluido de información sobre incidentes cibernéticos y amenazas.
		4.a.3 Desarrollar un Código de Conducta voluntario para los operadores de la infraestructura de telecomunicaciones que incluya el compromiso de compartir información sobre incidentes con el CERT-PY y entre los demás.
		4.a.4 Establecer mecanismos de cooperación entre el CERT-PY y el NIC.PY para el intercambio de información y colaboración.
		4.a.5 Incentivar la creación de más equipos de respuesta a incidentes en otros sectores de la sociedad paraguaya, y crear una base de datos de todos los CERTs privados, públicos, académicos, entre otros.
		4.a.6 Establecer mecanismos para compartir información de manera segura con otros CERTs nacionales, regionales e internacionales sobre incidentes cibernéticos y buenas prácticas.

	4.b. Los agentes responsables de las respuestas ante incidentes cibernéticos están capacitados y poseen el conocimiento necesario para conducir su trabajo.	4.b.1 Fomentar la participación en cursos de capacitación y actualización del personal del CERT-PY, de modo a generarse un grupo de expertos en áreas consideradas prioritarias para la adecuada respuesta a incidentes cibernéticos.
	4.c. La unidad encargada de la respuesta a incidentes cuenta con infraestructura y herramientas adecuadas para conducir sus respectivas tareas de manera oportuna y eficaz.	4.c.1 Fortalecer los recursos técnicos y la infraestructura del CERT-PY para mejor coordinación a nivel nacional con todos los actores.
5. Capacidad de Investigación y Persecución de la Ciberdelincuencia	5.a. Los agentes responsables de la investigación de delitos informáticos están capacitados y poseen el conocimiento necesario para conducir su trabajo.	5.a.1 Desarrollar e implementar un programa de capacitación para las instituciones encargadas de la denuncia, investigación y persecución de delitos informáticos, incluyendo pruebas y análisis forense digital
		5.a.2 Desarrollar e implementar un programa de capacitación a las instituciones encargadas de impartir la justicia y jueces, sobre los aspectos técnicos del Internet, el cibercrimen y delitos informáticos contemplados en la legislación vigente, respetando la privacidad y con la perspectiva de Derechos Humanos, entre otros.
	5.b. Las unidades encargadas de la investigación de delitos informáticos cuentan con infraestructura y herramientas adecuadas para conducir sus tareas de manera oportuna y eficaz.	5.b.1 Invertir en recursos técnicos y en herramientas adecuadas para la División especializada contra delitos informáticos de la Policía Nacional y la Unidad Especializada en Delitos Informáticos del Ministerio Público (licencia de softwares para informática forense, recuperación de archivos, peritaje informático, equipos, etc.)
		5.b.2 Establecer requisitos mínimos y control de calidad que serán implementados en las Unidades, a fin de asegurar que las herramientas adquiridas y sus proveedores tengan documentación y un nivel mínimo de calidad.
		5.c.1 Elaborar propuestas de modificación, mejoramiento y elaboración de reglamentaciones, que sean necesarias y efectivas para la persecución de delitos que utilizan para su comisión tecnologías de la

5. Capacidad de Investigación y Persecución de la Ciberdelincuencia	5.c. Paraguay cuenta con una legislación en materia de ciberseguridad que permite la investigación adecuada y persecución de casos de delitos informáticos.	información y comunicación, tanto en lo que respecta a la parte sustantiva como la procesal, y que son adecuados, necesarios y proporcionales conforme al enfoque de Derechos Humanos vigente..
		5.c.2 Llevar a cabo sesiones de consulta con redactores legislativos y otras partes interesadas para garantizar que la legislación contra delitos informáticos esté de acuerdo con las demás normativas nacionales y con los principios fundamentales de los derechos a la intimidad, privacidad, libertad de expresión y libre asociación.
		5.c.3 Fomentar la adecuación y actualización permanente del marco legal, conforme a Convenios internacionales que sean ratificados por el Paraguay, recomendaciones de organismos especializados, directrices, entre otros.
6. Administración Pública	6.a. La administración pública, tanto la central como las entidades y organismos descentralizados, cuentan con infraestructura adecuada para garantizar un entorno digital seguro.	6.a.1 Elaborar directrices para la adquisición, desarrollo y gestión de productos y servicios TIC ofrecidos a/por la Administración Pública, que garanticen un entorno digital seguro que permitan la prevención de incidentes.
		6.a.2 Llevar a cabo un ejercicio de precalificación de productos y servicios TIC y proveedores de servicios en base a las especificaciones mínimas de seguridad para la estandarización e integración en redes y sistemas de información de la Administración Pública, facilitando la adquisición de softwares y hardware para el sector público.
		6.a.3 Fomentar la creación y funcionamiento de Unidades Especializadas de TIC y ciberseguridad adecuando el marco legal necesario a tal efecto.
		6.b.1 Poner en funcionamiento el Sistema Nacional de Ciberseguridad, bajo la figura de Coordinador Nacional designado por el Poder Ejecutivo y la Comisión Nacional de Ciberseguridad de múltiples partes interesadas.

6. Administración Pública	6.b. Las gestiones gubernamentales de ciberseguridad se coordinan con cada agente responsable consciente de su función y papel referente a la ciberseguridad.	6.b.2 Establecer una asociación y esquema de trabajo coordinado entre profesionales de las TIC de la Administración Pública, para facilitar la difusión rápida y eficaz de alertas tempranas sensibles al tiempo e información y para la implementación de políticas y estrategias comunes de seguridad para los sistemas y la infraestructura de gobierno.
		6.b.3 Potenciar la creación, difusión y aplicación de mejores prácticas en materia de ciberseguridad en el ámbito de la Administración Pública, por medio del desarrollo de una Guía de Buenas Prácticas de TIC y de Ciberseguridad.
		6.b.4 Crear procedimientos y líneas de acción específicas para el sector público, con canales de comunicación directo entre los Ministerios y Secretarías del Poder Ejecutivo.
7. Sistema Nacional de Ciberseguridad	7.a. El Coordinador Nacional de Ciberseguridad es designado y se pone en funcionamiento el Sistema Nacional de Ciberseguridad, promoviendo la participación, representatividad y cooperación de todos los sectores.	7.a.1 Convocar a través del Coordinador Nacional de Ciberseguridad, a las entidades gubernamentales que integran la Comisión Nacional de Ciberseguridad, así como a las demás partes interesadas de los distintos sectores.
		7.a.2 Garantizar la participación activa y mayor representatividad de todos los sectores, así como el equilibrio en las estructuras de la Comisión: Subcomités Especializados, Grupos de Trabajo, Revisión.
		7.a.3 Elaborar los documentos, Convenios, reglamentos u otros, necesarios para el funcionamiento del Sistema Nacional de Ciberseguridad, la determinación de responsabilidades para el trabajo coordinado y prestación efectiva de acciones de cooperación por parte de los integrantes de la Comisión.

7. Sistema Nacional de Ciberseguridad	7.b. Se elabora el Plan de Ejecución del Plan Nacional de Ciberseguridad, para cada eje estratégico y sus respectivas líneas de acción.	7.b.1. Realizar un proceso colaborativo, en cada Subcomité Especializado, para la elaboración del Plan de Ejecución de las líneas de acción correspondientes. Conjugar en un documento final, en el que se delimitarán las tareas específicas relacionadas con los objetivos y las líneas de acción.
		7.b.2. Definir los responsables para cada actividad del Plan de Ejecución, asegurando un modelo de gestión descentralizada, en el que las responsabilidades son compartidas por todos los sectores.
		7.b.3 Promover la generación de propuestas, iniciativas y acciones de parte de los integrantes de la Comisión, para el cumplimiento del Plan Nacional, generando un espacio de análisis, estudio y debates entre las múltiples partes interesadas.
	7.c. Se realiza el acompañamiento, seguimiento y control del grado de cumplimiento del Plan Nacional de Ciberseguridad.	7.c.1 Implementar en forma periódica, procedimientos para la revisión de cada uno de los compromisos asumidos en el Plan Nacional de Ciberseguridad.
		7.c.2. Elaborar informes periódicos, cuanto menos anuales, que reporten el cumplimiento de las acciones planificadas.

ANEXO 2 - GLOSARIO

Ataques de denegación de servicios (Dos): Es un ataque a un sistema de computadoras o red que causa que un servicio o un recurso de red no esté disponible para los usuarios legítimos, por lo general mediante la interrupción o la suspensión temporal de los servicios de un host conectado a Internet, generalmente por la sobrecarga de los recursos computacionales del sistema de la víctima.

CERT: Equipo de Respuesta ante Emergencias Tecnológicas (CERT, por sus siglas en inglés). Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidentes de seguridad en los sistemas de información. Un CERT también ofrece servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades, y ofrece información con el propósito de ayudar a mejorar la seguridad de estos sistemas.

Delito informático: Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, ya sea bien porque se utiliza el ordenador como herramienta del delito, o bien porque sea el sistema informático (o sus datos) el objetivo del delito.

Incidente Cibernético: Cualquier evento adverso real o sospechado en relación con la seguridad de sistemas de computación o redes de computación.

Infraestructura Crítica: Las infraestructuras críticas consisten en sistemas y activos, físicos o virtuales, esenciales para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población, y cuya perturbación o destrucción tendría un impacto debilitante en la seguridad nacional, afectando gravemente al país.

Buenas prácticas de ciberseguridad: Se refiere a las medidas que los usuarios finales de Internet pueden tomar con el propósito de protegerse a sí mismos y a la confidencialidad, integridad y disponibilidad de su información en línea. En general, las buenas prácticas de ciberseguridad incluyen el mantenimiento habitual de las actualizaciones y parches, realización de copias de seguridad de sus datos, uso de antivirus, y contraseñas más difíciles.

Phishing: O suplantación de identidad, es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta. El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico.

Seguridad Cibernética, Ciberseguridad o Seguridad Informática: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información en el medio informático, buscando asegurar la confidencialidad, la disponibilidad e integridad de la misma.

ANEXO 3 – MARCO LEGAL

Los siguientes instrumentos legales, en el orden cronológico en el que se exponen, demuestran el esfuerzo creciente en materia legislativa que fue dando forma y existencia al marco normativo nacional relativo a las TICs y por tanto relativo en menor o mayor grado a la ciberseguridad:

Normativas	Tema
642/1995	De telecomunicaciones y crea la Comisión Nacional de Telecomunicaciones (CONATEL)
Ley N° 1.337/1999	De Defensa Nacional y Seguridad Interna
Ley N° 4.017/2010	De validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico
Ley N° 4.439/2011	Que modifica y amplía varios artículos de la Ley N° 1.160/97 (Código Penal) referentes a los delitos informáticos
Decreto N° 7.706/2011	Por el cual se aprueba el Plan Director de Tecnologías de la Información y Comunicación (TICs) del Poder Ejecutivo
Decreto N° 8.716/2012	Por la cual se crea y reglamenta la Secretaría de Tecnologías de la Información y Comunicación (SETICs)
Ley N˚ 4.868/2013	De Comercio Electrónico
Decreto N˚ 10.517/13	Por el cual se autoriza a la Secretaría de Tecnologías de la Información y Comunicación (SETICs) a desarrollar, implementar y monitorear el Sistema de Intercambio de Información entre instituciones públicas
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)
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
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"
Decreto N˚ 6234/16	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 y se ordena la implementación de las unidades especializadas TICs en las instituciones dependientes del Poder Ejecutivo
Decreto N˚ 5323/2016	Por el cual se reglamentan los artículos 20 y 21 de la Ley N˚ 4989/13 "que crea el marco de aplicación de las TICs 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.
Ley N˚ 5653/16	De protección de Niños, Niñas y Adolescentes contra contenidos nocivos en internet

ANEXO 4 – INSTITUCIONES PARTICIPANTES DE LA ELABORACIÓN DEL PLAN

ANDE
ASOBAN
Avanza S.A.
Banco Central del Paraguay
CAPACE
Centro Nacional de Computación
CISOFT
CLARO
Code100
CONACYT
CONATEL
Confederación Paraguaya de Cooperativas
COPACO S.A.
Departamento de Identificaciones
Dirección del Registro Automotor
Dirección General de los Registros Públicos
Dirección Nacional de Aeronáutica Civil
Dirección Nacional de Contrataciones Públicas
eFirma
Escribanía Mayor de Gobierno
ESSAP S.A
Financiera El Comercio
FIUNA
FP-UNA
Fuerzas Militares
Hola PY
Honorable Cámara de Diputados
Honorable Cámara de Senadores
Instituto de Previsión Social
INTEC S.R.L
INTERFISA
Itau
Jurado de Enjuiciamiento de Magistrados
Metil S.A
Ministerio de Defensa Nacional
Ministerio de Hacienda
Ministerio de Industria y Comercio
Ministerio de Salud Pública y Bienestar Social
Ministerio del Interior
Ministerio Público
Municipalidad de Asunción
NETEL S.A
PERSONAL
PETROPAR
Poder Judicial
Policía Nacional
PRONET S.A
Protección Online
Registro del Estado Civil
Secretaría Técnica de Planificación
Secretaría Nacional de Tecnologías de la Información y Comunicación
Subsecretaría de Estado de Tributación
TEDIC
TIGO
Universidad Americana
Universidad Autónoma de Asunción
Universidad Católica Nuestra Señora de la Asunción
Universidad Columbia
Universidad de la Integración de las Américas
Universidad del Cono Sur de las Américas
Universidad Iberoamericana
Universidad Nacional de Asunción
VIT SA- eFirma
Yacyreta

SECRETARÍA
NACIONAL DE TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

TETÃ REKUÁI
GOBIERNO NACIONAL
Jajapo ñande raperã ko'ãga guive
Construyendo el futuro hoy