GESI
GRUPO DE ESTUDIOS EN SEGURIDAD INTERNACIONAL
INTERNATIONAL SECURITY STUDIES GROUP

UNIVERSIDAD DE GRANADA

Publicado en *GESI* (http://www.seguridadinternacional.es)

Feb
27
2018

Estrategias Nacionales de Ciberseguridad en América Latina

por José Carlos Her...

Análisis GESI, 8/2018

Resumen: el presente trabajo tiene el objetivo de destacar los aspectos clave de las Estrategias de Ciberseguridad que se han aprobado en América Latina hasta la fecha (Colombia, Panamá, Paraguay, Costa Rica, Chile y México), haciendo énfasis en sus enfoques, principios rectores y objetivos. Así mismo, se hará referencia a las estructuras institucionales encargadas de implementar y hacer el seguimiento de las distintas Estrategias.

*****

Introducción

La expansión de Internet y del uso de las tecnologías de la información y la comunicación (TIC) durante los últimos años permite, como nunca antes, la circulación de ingentes volúmenes de información y el establecimiento de comunicaciones de manera fácil. Cada vez en mayor medida las actividades sociales, económicas y hasta militares de un Estado se hacen más dependientes del uso de las TIC, lo que irremediablemente implica a su vez una mayor vulnerabilidad y exposición a los ciberataques.

Tal y como señala Torres (2013), existe un precario equilibrio entre interoperabilidad y agilidad, por un lado, y seguridad, por otro. Con la pretensión de alcanzar un ciberespacio seguro se corre el riesgo de limitar la agilidad de los sistemas informáticos. Además, es prácticamente imposible imaginar un ciberespacio 100% seguro.

En las últimas décadas, casos como la explosión en el sistema de distribución de gas en la URSS (1982), el ciberataque contra empresas estadounidenses conocido como Titan Rain (2003 – 2005), el ciberataque contra Estonia (2007), el ciberataque contra Siria (2007), las acciones de ciberguerra durante la guerra en Osetia del Sur (2008) y el ciberataque contra el programa nuclear iraní (2010) han constituido episodios destacados de ciberguerra (Torres, 2013). Así mismo, en 2016, un informe conjunto de la Organización de los Estados Americanos (OEA) y del Banco Interamericano de Desarrollo (BID) señaló que el cibercrimen le cuesta anualmente al mundo unos 575.000 millones de dólares, es decir, un 0,5% del PIB global. En el caso concreto de América Latina y el Caribe, la cifra es de unos 90.000 millones anuales (BID y OEA, 2016).

Los ataques infligidos en el ciberespacio cuentan con una serie de características que han contribuido a su proliferación. Los ciberataques se pueden llevar a cabo con un bajo costo, son difícilmente rastreables y hay un problema en cuanto a la atribución de la autoría. Se sabe que hay Gobiernos que contratan a hackers para que realicen acciones en favor de sus intereses, pero puede que esos actores ni tan siquiera estén en el territorio de esos Estados (Leiva, 2015).

Ante esta realidad, aludiendo específicamente a América Latina, la mayor parte de los Estados dispone de capacidad de respuesta ante ciberataques, pero lo cierto es que sólo seis han diseñado una Estrategia de Ciberseguridad. El último en presentar su Estrategia fue México, el 13 de noviembre de 2017, uniéndose al pequeño grupo de países latinoamericanos que, según la OEA (2017), cuenta con este tipo de políticas. El resto son Colombia (2011 y 2016), Panamá (2013), Paraguay (abril de 2017), Chile (abril de 2017) y Costa Rica (abril de 2017)[1].

Según Leiva (2015), que sólo seis Estados hayan aprobado este tipo de Estrategia obedece a que en América Latina hay dos factores que bloquean su adopción: 1) la falta de recursos dedicados a este tema; y 2) la carencia de experiencia práctica y conocimientos especializados para diseñar e implementar este tipo de medidas. No obstante, la OEA viene jugando un papel relevante en lo que a apoyo técnico se refiere.

Además de los dos factores anteriores, cabría añadir un tercero que no es exclusivo de la región. La gestión del ciberespacio es responsabilidad tanto de actores públicos como privados, por lo que una Estrategia de Ciberseguridad tiene que contar con la cooperación del sector privado, los Gobiernos y las agencias de seguridad (Torres, 2013), lo que añade un grado de dificultad a la aprobación de este tipo de políticas.

Dicho esto, el presente trabajo tiene el objetivo de destacar los aspectos clave de las Estrategias de Ciberseguridad que se han aprobado en América Latina hasta la fecha, haciendo énfasis en sus enfoques, principios rectores y objetivos. Así mismo, se hará referencia a las estructuras institucionales encargadas de implementar y hacer el seguimiento de las distintas Estrategias.

El trabajo, excluyendo esta introducción, se estructura en dos partes. En una primera parte se destacarán los aspectos esenciales de las Estrategias de Ciberseguridad de los países latinoamericanos mencionados[2], mientras que en una segunda parte se realizarán unos comentarios finales.

Estrategias Nacionales de Ciberseguridad

Colombia: Política Nacional de Seguridad Digital

Colombia fue el primer país latinoamericano en aprobar una Estrategia Nacional de Ciberseguridad, en el año 2011. Cinco años más tarde, el 11 de abril de 2016, una nueva Estrategia vio la luz en el país andino, bajo el nombre de Política Nacional de Seguridad Digital[3]. Ésta cambió el enfoque de la anterior, incluyendo la gestión de riesgo. La Estrategia anterior ponía el foco sobre la protección en el ciberespacio para atender amenazas. La actual, a través del fortalecimiento de las capacidades de los potenciales afectados para identificar y gestionar el riesgo, intenta reducir la probabilidad de que las amenazas sean efectivas.

La Estrategia incluye cuatro principios fundamentales y cinco dimensiones estratégicas que guían la consecución de los objetivos. En este sentido, se establece un objetivo general, cinco objetivos específicos y 18 estrategias que se implementarán para lograrlos. Además, y este es un punto a destacar, es de las pocas Estrategias examinadas que incluye un cronograma de implementación y un esquema para su financiamiento de forma tan detallada.

Los cuatro principios fundamentales por lo que se rige la Estrategia son: *1) Salvaguardar los derechos humanos y los valores fundamentales*, cuya limitación, en el caso de que sea necesaria, ha de hacerse con apego a la Constitución; 2) *Adoptar un enfoque incluyente y colaborativo* que, de forma activa, involucre a las partes interesadas; *3) Asegurar una responsabilidad compartida*, promoviendo la cooperación y colaboración entre las partes interesadas; y *4) Adoptar un enfoque basado en la gestión de riesgos*, que permita a los ciudadanos llevar a cabo sus actividades en el entorno digital de manera segura.

Por su parte, las cinco dimensiones estratégicas son; 1) *Gobernanza de la seguridad digital*, mediante la articulación de las partes interesadas, bajo el liderazgo del Gobierno de la Nación; *2) Marco legal y regulatorio de la seguridad digital*, que recoja los aspectos necesarios para adoptar la Estrategia; 3) *Gestión sistemática y cíclica del riesgo de seguridad digital*, a través de los procedimientos, metodologías e iniciativas necesarias; *4) Cultura ciudadana para la seguridad digital*, mediante la sensibilización de las partes interesadas; y 5) fortalecimiento de las *capacidades para la gestión del riesgo de seguridad digital* de todas las partes interesadas.

Como se puede observar, existe una constante alusión al término de “partes interesadas”. Esto se puede interpretar en el sentido de que las autoridades colombianas son conscientes de que la ciberseguridad no sólo es un asunto que atañe a los Gobiernos, sino que afecta muy especialmente a la ciudadanía. Una muestra de lo anterior la encontramos en la misma Política Nacional de Seguridad Digital, en cuyo diagnóstico aparecen los ciudadanos como los principales afectados por incidentes digitales durante el año 2015 (42,4%).

En otro orden de cosas, el objetivo general de la Estrategia es el de

> Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país. (CONPES, 2016: 47).

Para cumplir con este objetivo general se formulan, bajo los principios fundamentales señalados anteriormente, cinco objetivos específicos. A fin de cumplirlos, se prevé la ejecución de 18 estrategias, las cuales están determinadas por las cinco dimensiones estratégicas citadas anteriormente. Así mismo, se diseña un plan de acción en el que se detallan cada una de las estrategias, las acciones a llevar a cabo y la importancia de cada una de éstas para el cumplimiento del objetivo general, los periodos de ejecución de las mismas, las entidades responsables de cada acción, los recursos necesarios para llevarlas a cabo y una valoración del impacto económico de la Estrategia.

A continuación se exponen los cinco objetivos específicos.

1. *Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos*, involucrando a las partes interesadas.

Para alcanzar este objetivo, el Gobierno establecerá un marco institucional adecuado e implementará un modelo de gestión de riesgos. En este sentido, se crea la figura del Coordinador Nacional de Seguridad Digital, que habrá de estar ocupada por un funcionario dependiente del Departamento Nacional de Planeación. Entre sus funciones cabe destacar la dirección y seguimiento de la implementación de la Estrategia y la coordinación intersectorial e interinstitucional en asuntos de seguridad digital. Además, este Coordinador ha de definir un enlace sectorial en los temas de seguridad digital en cada ministerio y departamento administrativo de orden nacional. Así mismo, se armoniza la institucionalidad de la Comisión Nacional Digital y de Información Estatal, siendo ésta la instancia de máximo nivel intersectorial e interinstitucional en el Gobierno.

2. *Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de la seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital*.

El Gobierno nacional será el encargado de llevar a cabo las cinco estrategias para alcanzar este objetivo específico. Mediante éstas, se establecen mecanismos para gestionar el riesgo, se adecúa el marco legal relacionado con asuntos de seguridad digital, se identifican y afrontan los potenciales impactos negativos que otras políticas puedan tener sobre las actividades desempeñadas por las partes interesadas, se genera confianza entre dichas partes y se promueven comportamientos responsables en el entorno digital en los diferentes niveles de formación.

3. *Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos.*

A través de este objetivo, bajo el liderazgo del Gobierno nacional, se busca empoderar al Estado y a los ciudadanos en relación con los riesgos propios del entorno digital, así como consolidar las capacidades de Colombia para enfrentar la delincuencia, el crimen y otros fenómenos que, desde dicho entorno, afectan la seguridad nacional. Este empoderamiento se hará a través de ejercicios de sensibilización y concientización.

4. *Fortalecer la defensa y la soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.*

Se trata de desarrollar capacidades de prevención, detección, contención, respuesta, recuperación y defensa, así como de preservar la integridad y mejorar la protección y la resiliencia de las infraestructuras críticas. Hay que señalar que no existe un catálogo fijo de infraestructuras críticas, sino que se ha de construir de forma conjunta entre las partes interesadas y el Ministerio de Defensa.

Por otro lado, también se prevé la creación de Computer Security Incident Response Teams (en adelante, CSIRT) sectoriales con el fin de gestionar los incidentes digitales que se produzcan en los distintos ramos de la economía.

5. *Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional.*

Este quinto y último objetivo específico pretende dinamizar la cooperación nacional e internacional en materia de seguridad digital. A tal fin, Colombia buscará adherirse a convenios internacionales relativos a seguridad digital. Así mismo, el Ministerio de Tecnologías de la Información y las Comunicaciones (MTIC) será el encargado de profundizar la cooperación nacional entre las múltiples partes interesadas.

Las entidades encargadas de ejecutar la Estrategia son el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Departamento Nacional de Planeación y la Dirección Nacional de Inteligencia.

Panamá: Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas

Esta es la Estrategia que con menor nivel de detalle alude al estado de la ciberseguridad en los ámbitos nacional e internacional y a los principios y objetivos marcados. Esta falta de profundidad se puede percibir en su propia extensión, ya que apenas ocupa diez cuartillas. Quizá se puede deber a que es la más antigua de las que se tratan en este trabajo, o puede que el motivo sea la existencia de una normativa amplia en

ciberseguridad que haga innecesaria la adopción de una Estrategia más detallada. Sea como fuere, a continuación se expondrán sus aspectos principales.

El objetivo del Estado panameño, mediante el desarrollo de la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas, es el de

> aunar los esfuerzos de sus ciudadanos, empresas e instituciones públicas para redundar en un incremento de la seguridad cibernética que permita el uso confiable de las tecnologías de la información en todos los ámbitos nacionales, todo esto salvaguardando los derechos y libertades fundamentales de los ciudadanos y un entorno económico regulatorio favorable al crecimiento y desarrollo de las empresas y permitiendo el buen funcionamiento del Estado. (Consejo Nacional para la Innovación Gubernamental, 2013: 3).

Para alcanzar este objetivo se desarrollarán una serie de acciones al objeto de minimizar los factores que facilitan la materialización de las amenazas cibernéticas. Dichos factores se concentran en los ejes organizativo, legal, tecnológico y cultural. Así mismo, se busca proteger los sistemas y redes informáticas y sensibilizar a las partes implicadas en el uso de las TIC de los potenciales riesgos que se derivan de su uso.

Aunque, como se ha apuntado anteriormente, esta Estrategia no contempla específicamente un catálogo de principios rectores, objetivos generales y objetivos específicos, sí que se detectan una serie de principios y, bajo el nombre de “pilares”, lo que en otras Estrategia se conoce como objetivos generales.

Los principios contenidos en la Estrategia se pueden resumir en protección de los derechos humanos y las libertades fundamentales, no discriminación, corresponsabilidad en el uso de las TIC y colaboración entre múltiples partes interesadas. Por otro lado, la Estrategia panameña contiene los seis pilares que se exponen a continuación.

1. *Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio.*

El Estado panameño se compromete a establecer un marco regulatorio que garantice la privacidad e intimidad de los ciudadanos en el ciberespacio, haciendo un énfasis especial en la protección de los menores.

2. *Prevenir y detener las conductas delictivas en el ciberespacio o el uso de éste para cualquier tipo de delitos o actos ilícitos.*

Se trata de reforzar las capacidades de los organismos encargados de la investigación e impartición de justicia, así como de establecer una más estrecha colaboración con otros Estados para abordar los ciberdelitos y de impulsar la adopción de normas internacionales en la materia.

3. *Fortalecer la seguridad cibernética de las infraestructuras críticas nacionales.*

Este objetivo se pretende lograr a través de una mayor colaboración entre el sector público y el sector privado, incluyendo la realización de simulacros de emergencia para garantizar que los canales de comunicación funcionan. Para este objetivo se toma como referencia el modelo del Canal de Panamá.

4. *Fomentar el desarrollo de un tejido empresarial nacional fuerte en seguridad cibernética, como referencia para la región.*

El Estado panameño articulará acciones para alinear sus prioridades en seguridad cibernética con las capacidades de las empresas nacionales, a las cuales se hará partícipes de la definición y desarrollo de las acciones que se lleven a cabo en el marco de la Estrategia.

5. *Desarrollar una cultura de seguridad cibernética a través de la formación, innovación y la adopción de estándares.*

Se reconoce la necesidad de incorporar los conceptos asociados a la ciberseguridad en los planes educativos, así como la de llevar a cabo acciones de formación, sensibilización y difusión en todos los sectores implicados en la seguridad cibernética.

6. *Mejorar la seguridad cibernética y capacidad de respuesta ante incidentes de los organismos públicos.*

El Estado panameño, para la consecución de éste objetivo, fomentará el desarrollo de programas tendentes a clasificar la información del sector público atendiendo al grado de criticidad de la misma, a adoptar estándares de seguridad para la gestión de la información y a incrementar las capacidades de respuesta ante incidentes de ciberseguridad.

Además de lo señalado anteriormente, la Estrategia identifica los riesgos que afronta el país en el uso de las TIC y los clasifica atendiendo a su origen y a los objetivos a los que los ciberataques pueden dirigirse. Además, como órganos encargados de la ciberseguridad se contemplan la Autoridad de Innovación Gubernamental, el Consejo Nacional para la Innovación Gubernamental y el CSIRT Panamá.

Paraguay: Plan Nacional de Ciberseguridad

En el Plan Nacional de Ciberseguridad de Paraguay se afirma que el país cuenta con la población de usuarios que más rápido ha crecido en la región durante el periodo 2010 – 2014. Por este motivo, las autoridades paraguayas creyeron prioritario el fortalecimiento de la ciberseguridad en el país mediante la aprobación de una Estrategia.

En el apartado de principios se explicita que el Plan Nacional se implementará mediante la cooperación y coordinación del sector público con la sociedad civil, el sector privado y la academia. En total, son seis los principios que han de orientar el diseño y la implementación de las políticas públicas de ciberseguridad: *1) Proporcionalidad* de las medidas aplicadas; *2) Coordinación de esfuerzos y uso eficiente de recursos escasos*; *3) Responsabilidad compartida* entre todos los miembros de la sociedad; *4) Desarrollo e innovación* para desarrollar una economía digital; *5) Cooperación internacional*, necesaria por la propia naturaleza de las amenazas; y *6) Monitoreo y evaluación* de las políticas públicas de ciberseguridad.

La Política Nacional presenta, respecto al resto, una diferencia en cuanto a los objetivos. En las otras Estrategias Nacionales de Ciberseguridad aparece un objetivo general y varios objetivos específicos (con excepción de la de Panamá). En cambio, en el caso de Paraguay aparece una serie de objetivos generales bajo el nombre de ejes, dentro de los cuales se detallan 20 objetivos específicos para su consecución y 60 líneas de acción[4]. Concretamente, son siete los ejes que se recogen.

1. *Sensibilización y Cultura.*

Se reconoce la importancia de promover una cultura de la ciberseguridad a fin de maximizar los beneficios del uso de las TIC y se busca sensibilizar y capacitar a los ciudadanos sobre la importancia de usar Internet de una forma responsable y segura. Para ello se prevé la puesta en marcha de campañas de sensibilización, así como la elaboración de proyectos educativos que incorporen conceptos de ciberseguridad en todos los niveles.

2. *Investigación, Desarrollo e Innovación.*

Se pretende que el país cuente con personal capacitado en ciberseguridad, para lo que es vital introducir planes educativos que incluyan dicha temática. Se reconoce la necesidad de que exista una buena coordinación entre sector público, sector privado, sociedad civil y academia a fin de

impulsar proyectos de I+D+i.

3. *Protección de Infraestructuras Críticas.*

No existe un listado único de infraestructuras críticas de las TIC, pero se explicita que su protección atañe tanto al ámbito físico (siendo un ejemplo las redes o los equipos) como al inmaterial (como pueden ser los nombres de dominios o los sistemas de control industrial), y que la responsabilidad de dicha protección es compartida entre los operadores privados y el Estado. Además, se busca promover un análisis de riesgo de dichas infraestructuras, verificando su vulnerabilidad y probabilidad de sufrir un ataque.

4. *Capacidad de Respuesta ante Incidentes Cibernéticos.*

Se afirma que el Centro de Respuesta ante Incidentes Cibernéticos de Paraguay (CERT – PY) ha sido capaz de promover campañas de sensibilización sobre ciberseguridad y de responder a incidentes cibernéticos, entre otras actividades. No obstante, se reconoce la necesidad de destinar más recursos para garantizar su adecuada operación. Por este motivo se plantea como propósito que el CERT – PY tenga una asignación presupuestaria explícita y un plan operativo.

5. *Capacidad de Investigación y Persecución de la Ciberdelincuencia.*

Se establece la necesidad de dotar de recursos y herramientas adecuadas a las entidades encargadas de la investigación de los delitos informáticos, así como de implementar programas de capacitación para los órganos encargados de la administración de justicia. Además, se busca fortalecer la cooperación policial y judicial internacional.

6. *Administración Pública.*

Se pretende que la Administración Pública cuente con unas infraestructuras que le permitan garantizar un entorno digital seguro y que cada agente sea consciente de su función referente a la ciberseguridad.

7. *Sistema Nacional de Ciberseguridad.*

Se prevé la designación de un Coordinador Nacional de Ciberseguridad encargado de la evaluación y el monitoreo del Estrategia, que deberá trabajar cooperando con todos los sectores implicados en el Sistema Nacional de Ciberseguridad.

El Sistema Nacional de Ciberseguridad es la estructura institucional que se crea para aplicar la Estrategia, cuyos componentes son el Coordinador Nacional de Ciberseguridad y la Comisión Nacional de Ciberseguridad. Del primero ya se señalaron anteriormente sus funciones, mientras que las de la Comisión se pueden resumir en reforzar la colaboración, coordinación y cooperación entre las partes interesadas en la ciberseguridad. A su vez, la Comisión Nacional de Ciberseguridad se encuentra dividida en siete Subcomités Especializados, cuyos nombres responden a cada uno de los siete ejes expuestos anteriormente.

Por último, hay que señalar que tanto la Política Nacional de Ciberseguridad como su Plan de Acción serán revisados cada tres años.

Estrategia Nacional de Ciberseguridad de Costa Rica

La Estrategia Nacional de Ciberseguridad costarricense cuenta con cuatro principios rectores: 1) *Las personas son prioridad*, por ello se busca promover el uso de las TIC para mejorar su calidad de vida de forma segura; 2) *Respeto a los Derechos Humanos y la Privacidad*, principio que debe regir todas las acciones y medidas que se deriven de la Estrategia; 3) *Coordinación y corresponsabilidad de múltiples partes interesadas*, en el proceso de implementación de las acciones que se deriven de la Estrategia y, cuando sea pertinente, en el diseño de las mismas; y 4) *Cooperación Internacional*, con entidades públicas y privadas.

Además de los principios anteriores, se establece un objetivo general y ocho específicos, cada uno de los cuales comprende una serie de líneas estratégicas, sumando éstas un total de 20. En cuanto al objetivo general, se pretende

> Desarrollar un marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentando la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente a los riesgos en cuanto al uso de las TIC para lograr un entorno más seguro y confiable para todos los habitantes del país. (MICITT, 2017: 38).

Para la consecución del anterior objetivo se establecen ocho objetivos específicos.

1. *Coordinación Nacional.*

Se busca establecer una coordinación entre el sector público, el sector privado, la comunidad técnica, la sociedad civil, las ONGs y la academia con el fin de establecer el papel de cada una de ellas y sus correspondientes líneas de acción en caso de incidente de seguridad cibernética. Dicha coordinación, en el caso de las entidades gubernamentales y el sector privado, incluirá un intercambio de información.

2. *Conciencia pública.*

Llevar a cabo campañas de concienciación y educación sobre seguridad cibernética, dirigidas a empresas, funcionarios públicos y ciudadanos, que fomenten la corresponsabilidad en relación con la protección digital.

3. *Desarrollo de la Capacidad Nacional de Seguridad Cibernética.*

Se pretenden desarrollar campañas de formación y concienciación dirigidas exclusivamente a los miembros del sector público a fin de que estos adquieran conocimientos en técnicas de seguridad cibernética. Este objetivo incluye la necesidad de tejer alianzas con universidades para llevar a cabo investigaciones sobre amenazas emergentes y desarrollar soluciones.

4. *Fortalecimiento del marco jurídico en Ciberseguridad y TIC.*

Modificar el marco jurídico existente a fin de conseguir una mejora en la investigación y enjuiciamiento de la ciberdelincuencia. Así mismo, se trata la necesidad de capacitar en materia de ciberseguridad a los responsables de administrar justicia.

5. *Protección de Infraestructuras Críticas.*

Se pretenden identificar las infraestructuras críticas y elaborar políticas públicas tendentes a prevenir los incidentes de ciberseguridad que se dirijan a dañar dichas infraestructuras. Al igual que en las Estrategias anteriores, tampoco en la elaborada por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) costarricense se detalla una lista con las infraestructuras críticas.

6. *Gestión del Riesgo.*

Mediante el fortalecimiento de las capacidades de los potenciales afectados para identificar y gestionar el riesgo, se intenta reducir la probabilidad de que las amenazas sean efectivas. En este sentido, se intenta mejorar la seguridad de los productos y servicios, utilizados por las organizaciones públicas y privadas, vinculados a la seguridad de la información. Ello implica, entre otros, al sector financiero y a las entidades gubernamentales.

7. *Cooperación y Compromiso Internacional.*

A través de la participación en espacios especializados a nivel nacional e internacional se busca implicar a la comunidad internacional en el apoyo a los objetivos contenidos en la Estrategia.

8. *Implementación, Seguimiento y Evaluación.*

El fin de este objetivo es el de proponer los ajustes necesarios tras la evaluación del cumplimiento de las líneas de acción. El MICITT es el encargado de supervisar la implementación y hacer el seguimiento de las tareas que se le hayan asignado a cada uno de los actores implicados en la Estrategia. Además, en su papel de Coordinador Nacional, llevará a cabo la evaluación del grado de cumplimiento de los objetivos e informará con una periodicidad de un año al Consejo de Gobierno y al Presidente de la República sobre el avance de la implementación de la Estrategia, cuya revisión habrá de hacerse cada dos años.

En cuanto a la estructura institucional, la principal entidad responsable es el MICITT, y para hacer frente a los incidentes se cuenta con el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT – CR). El CSIRT – CR fue creado en 2012, y es la entidad encargada de coordinar los asuntos relacionados con la seguridad cibernética e informática y de prevenir y responder ante los incidentes de seguridad informática. Además, se conforma un Comité Consultivo compuesto por representantes del MICITT, del Poder Judicial, de la Superintendencia de Comunicaciones (SUTEL), de la sociedad civil, de la academia y del sector privado. Así mismo, recae en el MICITT la figura del Coordinador Nacional en Ciberseguridad, cuyas funciones esenciales son supervisar la implementación de la Estrategia y coordinar a las distintas partes implicadas en el cumplimiento de las líneas de acción.

Por último, la Estrategia de Ciberseguridad de Costa Rica no cuenta con un cronograma ni con un apartado donde se detallen los recursos destinados a cada una de las acciones.

Chile: Política Nacional de Ciberseguridad

La Política Nacional de Ciberseguridad de Chile (PNC) recoge de forma detallada el desarrollo de tareas a corto y medio plazo, así como las instituciones que intervienen en asuntos de ciberseguridad[5]. De hecho, el cumplimiento de los objetivos recogidos en la PNC chilena tiene como horizonte el año 2022. Además, incluye un apartado con 41 medidas de política pública a llevar a cabo en el periodo 2017 – 2018, así como el órgano responsable de la implementación de cada una de ellas.

Los objetivos para el año 2022 son seis, cada uno de los cuales contiene una serie de objetivos específicos[6], sumando estos un total de 22. A continuación se exponen sucintamente los objetivos generales y sus respectivos objetivos específicos.

1. Desarrollar una infraestructura de las TIC que, bajo una óptica de gestión de riesgos, sea capaz de resistir y recuperarse de incidentes de ciberseguridad.

Este objetivo contiene los siguientes seis objetivos específicos: *1) Identificación y gestión de riesgos*, llevando a cabo medidas de monitoreo a fin de generar un ciberespacio resiliente; *2) Protección de la infraestructura de la información*; *3) Identificación y jerarquización de las infraestructuras crítica de la información*, que se considerarán en los sectores del agua, la salud, la seguridad pública, la energía, las telecomunicaciones, los servicios financieros, la Administración Pública, el transporte, la defensa y la protección civil; *4) Contar con equipos de respuesta a incidentes de ciberseguridad*. Son los denominados CSIRT, de los cuales Chile contará con uno nacional, encargado de recopilar y sistematizar toda la información proveniente de otros CSIRT, y varios sectoriales, de cuya coordinación se encargará aquél. Además, se creará uno específico para la defensa; *5) Implementación de mecanismos estandarizados de reporte, gestión y recuperación de incidentes*, que se dedicarán a requerir la información necesaria para gestionar las amenazas; y *6) Exigencia de estándares diferenciados en materia de ciberseguridad*, en las infraestructuras de la información dependientes del Gobierno o que provean productos a éste o servicios a los ciudadanos.

2. Garantizar los derechos de los ciudadanos en el ciberespacio.

Este objetivo se alcanza mediante el cumplimiento de los siguientes cuatro objetivos específicos: *1) Prevención de ilícitos y generación de confianza en el ciberespacio*, a través de la minimización de riesgos y amenazas; *2) Establecimiento de prioridades en la implementación de medidas sancionatorias*, mediante la actualización y fortalecimiento de la legislación y de la creación de medidas transversales; *3) Prevención multisectorial*, ya que los ciberataques pueden ser realizados por múltiples actores; y *4) Respeto y promoción de derechos fundamentales*, de modo que las acciones llevadas a cabo en el marco de esta Política no permiten privar a los usuarios de acceder a la red por motivos de orden público, honor, seguridad nacional, etc. Además, se aboga por el principio de neutralidad de la red.

3. Desarrollar una cultura de ciberseguridad en torno a la responsabilidad en el uso de las TIC, a las buenas prácticas y a la educación.

Para cumplir con este objetivo, las autoridades chilenas pretenden implementar los siguientes objetivos específicos: *1) Una cultura de ciberseguridad*; *2) Sensibilización e información a la comunidad*; y *3) Formación para la ciberseguridad*. En síntesis, se trata de que los usuarios de las TIC sean conscientes de los riesgos y amenazas a las que se enfrentan y hagan un uso responsable de dichas tecnologías.

4. Establecer relaciones de cooperación con otros actores en materia de ciberseguridad y participar de forma activa en foros internacionales.

Son cuatro los objetivos específicos con los que se intenta alcanzar este cuarto objetivo general: *1) Principios de política exterior chilena*, lo que se traduce en la construcción de capacidades de cooperación con otros países y en el desarrollo de una diplomacia multilateral para disminuir los riesgos de conflicto en el ciberespacio; *2) Cooperación y asistencia*, de forma bilateral con otros actores internacionales; *3) Reforzar la participación en instancias multilaterales y en instancias de múltiples partes interesadas*, mediante el incremento de la participación de Chile en instancias globales y multilaterales, así como apoyando procesos de consulta en todos los niveles geográficos; y *4) Fomentar normas internacionales que promuevan la confianza y seguridad en el ciberespacio*, y ello a través de la promoción del debate multilateral y bilateral.

5. Desarrollar una industria de la ciberseguridad chilena, que sea útil a los objetivos estratégicos del país.

Este quinto y último objetivo general se desglosa en cinco objetivos específicos: *1) Importancia de la innovación y desarrollo en materia de ciberseguridad*, tanto para las actividades de seguridad como para las de defensa; *2) Ciberseguridad como medio para contribuir al desarrollo digital de Chile*. Se trata de generar una mayor demanda de las TIC y potenciar el desarrollo de la industria en la materia; *3) Desarrollo de la industria de ciberseguridad en Chile*; *4) Contribuir a la generación de oferta por parte de la industria local*, a través de programas de producción de nuevos bienes y servicios en materia de ciberseguridad; y *5) Generación de demanda de parte del sector público basado en los intereses estratégicos del Estado*, a fin de fortalecer la industria nacional de ciberseguridad.

Pasando ahora a la estructura institucional, la PNC prevé que una ley contemple tanto dicha estructura como un modelo de gobernanza de ciberseguridad. Además, también se plantea evaluar la creación de un consejo consultivo asesor. De forma transitoria, a nivel técnico, el CSIRT

del Gobierno es la instancia encargada de gestionar los incidentes generados en la Red de Conectividad del Estado, mientras que a nivel político se prorroga el mandato del Comité Interministerial sobre Ciberseguridad, cuyas funciones se circunscriben a los ámbitos de la comunicación, coordinación y seguimiento de las medidas contenidas en la PNC.

México: Estrategia Nacional de Ciberseguridad

México fue el último país de los aquí tratados en aprobar su Estrategia Nacional de Ciberseguridad (ENC). El Gobierno mexicano reconoce que el coste de los delitos informáticos a nivel global está ascendiendo y señala que, para el caso de México, dicho coste fue de 3.000 millones de dólares en el año 2014. Además, indica que en los últimos años se ha producido un aumento exponencial de fraude cibernético. Es en este contexto en el que surge la necesidad de adoptar dicha Estrategia.

La ENC de México plasma tres principios rectores, establece un objetivo general y cinco estratégicos, define ocho ejes trasversales e identifica a los actores involucrados.

Los principios rectores son los siguientes: 1) *Perspectiva de derechos humanos*, que ha de estar presente en cada una de las acciones en materia de ciberseguridad que se lleven a cabo en el marco de la Estrategia; 2) *Enfoque basado en gestión de riesgos*, es decir, un enfoque de prevención basado en la capacitación de los usuarios a fin de minimizar los riesgos y las amenazas del ciberespacio; y 3) *Colaboración multidisciplinaria y de múltiples actores*, para así conseguir que la Estrategia se desarrolle de forma integral y transversal.

Por otro lado, la ENC de México tiene por objetivo general

> Fortalecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano. (Gobierno de México, 2017: 16).

Así mismo, la ENC contiene ocho ejes transversales, los cuales pretenden alcanzar los cinco objetivos estratégicos que se detallan a continuación.

1. *Sociedad y derechos.*

El Estado mexicano pretende generar las condiciones para que los ciudadanos lleven a cabo sus actividades en el ciberespacio de manera confiable, libre y responsable.

2. *Economía e innovación.*

El fin de este objetivo es el de proteger la economía de los distintos sectores productivos, impulsar la industria nacional de ciberseguridad y el desarrollo y la innovación tecnológica.

3. *Instituciones públicas.*

Se trata de proteger los sistemas informáticos de las instituciones públicas, así como su información, a fin de que éstas desempeñen sus labores de forma óptima y presten los servicios a los ciudadanos con continuidad.

4. *Seguridad pública.*

Incrementar las capacidades de prevención e investigación de ciberdelitos que afectan a los ciudadanos y su patrimonio.

5. *Seguridad Nacional.*

Con este objetivo se busca salvaguardar la integridad, independencia y soberanía nacional mediante el desarrollo de capacidades para prevenir riesgos y amenazas en el ciberespacio.

La ENC contiene, además, ocho ejes transversales cuyo desarrollo facilitará el cumplimiento de los objetivos estratégicos. Dichos ejes son: *1) Cultura de ciberseguridad*, entendida como el conjunto de principios, valores y acciones en materia de educación, formación y concientización; *2) Desarrollo de capacidades*, es decir, el conjunto de acciones tendentes a generar y fortalecer las capacidades de capital humano, recursos tecnológicos y organizaciones en materia de ciberseguridad; *3) Coordinación y colaboración*, entendidas como el conjunto de acciones dirigidas a establecer y coordinar la colaboración entre instituciones públicas, sociedad civil, academia y organizaciones privadas, mediante un modelo de gobernanza de ciberseguridad; *4) Investigación, desarrollo e innovación en TIC*. Se trata de las acciones dirigidas a fomentar la I+D+i en el uso de las TIC en materia de ciberseguridad; *5) Estándares y criterios técnicos*, entendidos como el conjunto de acciones orientadas a desarrollar, adoptar y fortalecer los criterios técnicos y de normalización, así como los estándares, en materia de ciberseguridad, que permitan aplicar las mejores prácticas en un entorno de ciberseguridad; *6) Infraestructuras críticas*. Se trata de llevar a cabo las acciones y medidas necesarias para proteger las infraestructuras críticas, minimizando la probabilidad de riesgos y vulnerabilidades en el uso de las TIC. Dichas acciones se llevarán a cabo en el marco de la Ley de Seguridad Nacional; *7) Marco jurídico y autorregulación*. Se traduce en llevar a cabo una serie de acciones tendentes a adecuar el marco jurídico nacional vinculado a la ciberseguridad; y *8) Medición y seguimiento*, generando indicadores y estadísticas que permitan medir y dar seguimiento a los resultados obtenidos con la implementación de la ENC, así como su impacto en el desarrollo socioeconómico de México.

En cuanto a la estructura institucional, en octubre de 2017 se creó, en el marco de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE), la Subcomisión de Ciberseguridad, entre cuyos integrantes se encuentran varias entidades y dependencias de la Administración Pública Federal[7]. En la etapa inicial, la Subcomisión de Ciberseguridad será la encargada de coordinar al Gobierno y articular los esfuerzos de los distintos actores a fin de implementar y hacer un seguimiento de la Estrategia. Además, entre sus funciones cabe destacar la de aprobar la ENC.

Comentarios finales

Como se ha podido observar, son pocos los países de América Latina que cuentan con una Estrategia Nacional de Ciberseguridad. De estos, un número aún menor ha elaborado una Estrategia que recoja un conjunto de acciones concretas para alcanzar cada uno de sus objetivos, que detalle cuál es el presupuesto para cada una de esas acciones y que especifique qué órgano habrá de encargarse de implementarlas. En este sentido, tal y como se ha podido comprobar, son las Estrategia de Colombia, Paraguay y Chile las que presentan un mayor grado de detalle.

La Política Nacional de Ciberseguridad de Chile incluso se marca como fecha límite 2022 para llevar a cabo una serie de políticas públicas en materia de ciberseguridad. Es cierto que esto no es garantía de que se cumplan tales plazos, pero al menos es un primer paso en la adopción de un mayor compromiso con la consecución de los objetivos marcados. En esta misma línea, incluyendo un cronograma de implementación de medidas, la Estrategia de Colombia figura entre las más avanzadas. Quizás se deba a que el país ya cuenta con experiencia en la materia, pues aprobó su primera Estrategia en 2011.

En contraposición a unas Estrategias con grados aceptables de detalle, se encuentra la de Panamá, que parece ser más la plasmación de un compromiso que una Estrategia de Ciberseguridad que merezca tal nombre. No obstante, al Estado panameño hay que atribuirle el mérito de haberla adoptado hace ya varios años (2013), cuando sólo Colombia figuraba entre los países latinoamericanos que habían aprobado una Estrategia de Ciberseguridad.

Actualmente, un buen número de países de la región se encuentran en proceso de elaboración de sus respectivas Estrategias de Ciberseguridad, y todo parece indicar que en fechas próximas saldrán a la luz algunas de ellas. De hecho, se podría decir que la situación lo requiere, pues la compañía Kaspersky Lab señala que, en el año 2018, en América Latina aumentarán los ataques a las pequeñas y medianas empresas, continuará la tendencia al alza del secuestro de datos y del robo de información personal, los procesos electorales serán el blanco de ciberataques y se producirán robos de grandes sumas de dinero a través del ciberespacio (Observatorio CISDE, 2017).

Una Estrategia de Ciberseguridad no garantizará que se puedan repeler todos estos ataques, pero una ausencia de la misma lo hará aún menos.

José Carlos Hernández *es politólogo y miembro del Grupo de Estudios en Seguridad Internacional (GESI) de la UGR.*

Referencias

Banco Interamericanos de Desarrollo (BID) y Organización de los Estados Americanos (OEA) (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Recuperado de: https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/ [1]

Consejo Nacional para la Innovación Gubernamental (2013). Gaceta Oficial Digital. Nº 21. Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas. Recuperado de: https://www.unodc.org/res/cld/lessons-learned/pan/estrategia_nacional_de_seguridad_cibernetica_y_proteccion_de_infraestructuras_criticas_html/Estrategia_Nacional_de_Seguridad_Cibe [2]

Documento CONPES 3854 (Consejo Nacional de Política Social y Económica) (2016). Política Nacional de Seguridad Digital. Recuperado de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf [3]

Gobierno de Chile (2017). Política Nacional de Ciberseguridad. Recuperado de: http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf [4]

Gobierno de México (2017). Estrategia de Ciberseguridad. Recuperado de: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf [5]

Leiva E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en Enfoque Top-Down desde una visión global a una visión local. *Revista Latinoamericana de Ingeniería de Software*, *3*(4). pp. 161-176, ISSN 2314-2642. Recuperado de: http://sistemas.unla.edu.ar/sistemas/gisi/papers/relais-v3-n4-161-176.pdf [6]

MICITT (2017). Estrategia Nacional de Ciberseguridad de Costa Rica. Recuperado de: https://micit.go.cr/images/imagenes_noticias/10-11-2017__Ciberseguridad/Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-11-10-17.pdf [7]

Observatorio CISDE (2017). Pronóstico de ciberseguridad para América Latina en 2018. Recuperado de https://observatorio.cisde.es/sin-categoria/pronostico-ciberseguridad-america-latina-2018/ [8]

OEA (2017). México presentó Estrategia Nacional de Ciberseguridad desarrollada con apoyo de la OEA. Recuperado de: http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-082/17 [9]

Secretaría Nacional de Tecnologías de la Información y la Comunicación (2017). Plan Nacional de Ciberseguridad. Retos, roles y compromisos. Recuperado de: http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg [10]

Torres, M. (2013). Ciberguerra. En Jordán, J. (coord.), *Manual de Estudios Estratégicos y Seguridad Internacional*. pp. 329-348. Madrid: Plaza & Valdés.

---

[1] Para el presente trabajo no se han tenido en cuenta los países caribeños, pero hay que tener presente que tanto Trinidad y Tobago (2013) como Jamaica (2015) cuentan con una Estrategia Nacional de Ciberseguridad.

[2]Por orden de aprobación.

[3] En este trabajo se contempla la Estrategia de 2016, pues es ésta la que se encuentra actualmente en vigor.

[4] La especificación de los objetivos y de las líneas de acción se encuentra en el Anexo 1 de la Política Nacional de Ciberseguridad.

[5] Son el Ministerio del Interior y Seguridad Pública, el Ministerio de Defensa Nacional, el Ministerio de Transportes y Telecomunicaciones, el Ministerio de Economía, Fomento y Turismo, el Ministerio de Justicia y Derechos Humanos, el Ministerio de Relaciones Exteriores, el Ministerio Secretaría General de la Presidencia, la Universidad de Chile, el Instituto Nacional de Normalización, el Ministerio Público y el Poder Judicial.

[6] Realmente, en la Política Nacional de Ciberseguridad, no se le otorga una definición a los puntos que incluye cada uno de los objetivos. En este trabajo se conocerá a dichos puntos como objetivos específicos.

[7] La Subcomisión de Ciberseguridad se encuentra presidida por la División Científica de la Policía Federal.

Editado por: Grupo de Estudios en Seguridad Internacional (GESI). Lugar de edición: Granada (España). ISSN: 2340-8421.

Ciberseguridad [12]

URL de origen: http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina

Enlaces:
[1] https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/
[2] https://www.unodc.org/res/cld/lessons-learned/pan/estrategia_nacional_de_seguridad_cibernetica_y_proteccion_de_infraestructuras_criticas_html/Estrategia_Nacional_de_Seguridad_Cibernetica_y_Proteccion_de_Infraestr
[3] https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
[4] http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf
[5] https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
[6] http://sistemas.unla.edu.ar/sistemas/gisi/papers/relais-v3-n4-161-176.pdf
[7] https://micit.go.cr/images/imagenes_noticias/10-11-2017__Ciberseguridad/Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-11-10-17.pdf
[8] https://observatorio.cisde.es/sin-categoria/pronostico-ciberseguridad-america-latina-2018/
[9] http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-082/17
[10] http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg
[11] http://creativecommons.org/licenses/by-nc-nd/3.0/deed.es_CO
[12] http://www.seguridadinternacional.es/?q=es/tags/ciberseguridad