www.observatoriociberseguridad.com

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

Reporte Ciberseguridad 2020

BID Mejorando vidas

OEA Más derechos para más gente

www.observatoriociberseguridad.com

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

Reporte Ciberseguridad 2020

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

Banco Interamericano de Desarrollo (BID)

Presidente

Luis Alberto Moreno

Coordinación de Proyecto

Miguel Porrúa

Equipo Técnico

Ariel Nowersztern

Darío Kagelmacher

Santiago Paz

Pablo Libedinsky

Florencia Cabral

Benjamin Roseth

Organización de los Estados Americanos (OEA)

Secretario General

Luis Almagro

Coordinación de Proyecto

Belisario Contreras

Equipo Técnico

Kerry-Ann Barrett

Rolando Ramírez

Mariana Cardona Clavijo

Manuela Orozco Jaramillo

Nathalia Foditsch

Barbara Marchiori

Centro Global de Capacidad en Seguridad Cibernética, Universidad de Oxford

Profesor Sadie Creese

Profesor Michael Goldsmith

Carolin Weisser Harris

Jakob Bund

Andraz Kastelic

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

TABLA DE CONTENIDOS

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

Mensajes institucionales

Mensaje de

Moisés J. Schwartz

Gerente, Instituciones para el Desarrollo del BID

La crisis propiciada a principios de 2020 por la pandemia del COVID-19 ha puesto de relieve nuestra dependencia de una infraestructura vital que, para la gran mayoría de los ciudadanos, resulta invisible o su existencia pasa prácticamente desapercibida.

Nuestra vida diaria gira alrededor de actividades cada vez más digitalizadas y, por consiguiente, más sensibles a amenazas cibernéticas. Cadenas de suministro de alimentos, transporte, pagos y transacciones financieras, actividades educativas, trámites gubernamentales, servicios de emergencia, y el suministro de agua y energía, entre un sinnúmero de actividades, operan en la actualidad a través de tecnologías digitales.

Las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la propiedad, así como para aumentar la confianza de los ciudadanos en las tecnologías digitales, y que éstos puedan sentirse cómodos accediendo a dichas tecnologías. El crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo. A nivel agregado, las cifras adquieren aún mayor magnitud pues los daños económicos de los ataques cibernéticos podrían sobrepasar el 1% del producto interno bruto (PIB) en algunos países. En el caso de los ataques a la infraestructura crítica, esta cifra podría alcanzar hasta el 6% del PIB.

El presente estudio pone en evidencia que la región de América Latina y el Caribe aún no está suficientemente preparada para enfrentar los ataques que se producen en el ciberespacio. Únicamente 7 países de los 32 analizados en este reporte cuentan con un plan de protección de su infraestructura crítica, y 20 han establecido algún tipo de grupo de respuesta a incidentes, llamado CERT o CSIRT, según sus siglas en inglés. Esto limita la capacidad de identificar ataques y responder oportunamente a los mismos.

Identificar un peligro cibernético es tan sólo el primer paso. Tomar medidas contra las amenazas y crímenes del ciberespacio es un reto aún mayor para nuestros países. En 22 de los países analizados se considera que hay pocas capacidades para investigar los delitos que se cometen en el ciberespacio. Más aún, que dichos delitos

resulten en juicio es todavía un reto mayor. Parte del problema se inicia muchas veces en la propia ley: en un tercio de los países no existe un marco legal sobre los delitos informáticos y únicamente 5 países de la región se han adherido a la Convención de Budapest, que facilita la cooperación internacional en la lucha contra el crimen informático. Para un delito que no conoce fronteras, trabajar de la mano con otros países es un factor indispensable para el éxito.

Si bien los gobiernos de nuestra región son conscientes de la necesidad de proteger el espacio digital del que tanto depende el funcionamiento de nuestra sociedad, la ciberseguridad no ha ganado presencia en la agenda política de la región con la urgencia que se esperaría. Hasta principios de 2020, solamente 12 países habían aprobado una estrategia nacional de ciberseguridad (un aumento con respecto a los 5 que tenían este tipo de estrategias en 2016), y únicamente 10 países han establecido un organismo gubernamental central responsable de la gestión de la ciberseguridad.

¿A qué se debe un avance tan tímido? Uno de los factores que limita el progreso de nuestra región en materia de ciberseguridad es la ausencia de talento humano calificado. La brecha de profesionales en ciberseguridad se estima en 600,000 personas en la región. El problema se agrava cuando se analiza desde la perspectiva de género, ya que menos de un cuarto de los profesionales son mujeres. Frente a esta escasez, únicamente 20 de los países estudiados cuentan con alguna oferta académica en ciberseguridad.

Desde el Banco Interamericano de Desarrollo (BID) estamos trabajando muy estrechamente con los gobiernos de la región y organizaciones multilaterales como la Organización de los Estados Americanos (OEA) para enfrentar el reto de la ciberseguridad. Además, dado el crecimiento que la ciberseguridad está experimentando a nivel global, desde el BID creemos que el desarrollo de políticas en esta materia en los países de América Latina y el Caribe abre un horizonte de oportunidades en un momento en el que nuestra región requiere reactivar su economía para superar la crisis originada por la pandemia del COVID-19. La puesta en práctica de políticas integrales de ciberseguridad permitirá a los países de nuestra región disfrutar de los beneficios de la Cuarta Revolución Industrial, protegiendo a sus ciudadanos y potenciando su actividad económica.

Quiero aprovechar este mensaje para expresar la gratitud del BID con los gobiernos de Israel y España, por el apoyo técnico y financiero que nos brindan. Ambos países han sido muy generosos compartiendo conocimiento y experiencias con una región que necesita de ese apoyo para avanzar con mayor rapidez. El ciberdelito no conoce fronteras y requiere de una respuesta global. Invito a todos los países de nuestra región a que nos convirtamos en un ejemplo de colaboración y coordinación en un área tan relevante para nuestra vida diaria. El BID está comprometido con esta tarea, y seguirá brindando su respaldo a los gobiernos de la región en sus esfuerzos para proteger a los ciudadanos de las amenazas que acechan nuestro espacio digital.

Mensaje de

Farah Diva Urrutia

Secretaria de Seguridad Multidimensional de la OEA

Desde el 2004, la OEA ha continuamente enfatizado la ciberseguridad en el hemisferio. La Organización se esfuerza por garantizar un ciberespacio abierto y seguro en todos los Estados Miembros de la OEA.

Con la publicación de la edición 2020 del informe "Ciberseguridad: riesgos, avances, y el camino a seguir en América Latina y el Caribe", la OEA busca proporcionar una descripción detallada de las capacidades nacionales de los países de América Latina y el Caribe (ALC) para combatir el ciberterrorismo y garantizar un acceso más seguro a Internet en la región. Este año en particular, la pandemia global de COVID-19 ha destacado el papel vital y el uso de las tecnologías de la información y la comunicación (TIC) en la prestación de servicios esenciales y su profunda integración en nuestras sociedades.

La pandemia de COVID-19 nos brinda la oportunidad de reflexionar sobre el progreso en la expansión de las TIC, la conectividad a Internet y la ciberseguridad en el hemisferio. Nuestra mayor dependencia del ciberespacio durante la crisis subraya la necesidad de extraer lecciones para lo que nos espera en la transformación continua de nuestras sociedades y economías, y en garantizar la ciberseguridad a nivel mundial.

En un sentido más general, en la última década, los ataques cibernéticos han aumentado en frecuencia e ingenio. El bajo costo y el riesgo mínimo que conllevan estos delitos han sido factores clave en su crecimiento. Con el simple uso de una computadora y el acceso a Internet, los ciberdelincuentes pueden causar daños enormes mientras permanecen relativamente anónimos.

Tanto las personas como las instituciones están expuestas a la incertidumbre y la impredecible naturaleza del delito cibernético. Por lo tanto, es imprescindible abordar estas amenazas. Los esfuerzos para hacerlo deben ser de naturaleza multidimensional, porque se requiere una variedad de factores para construir una cibersociedad resistente. Las políticas y los marcos legales deben ajustarse y todas las partes interesadas de la sociedad civil, así como los sectores público y privado, deben trabajar para crear una cultura de ciberconciencia y capacitar a profesionales calificados para construir una estrategia de ciberseguridad; por lo tanto, es un esfuerzo continuo y complejo.

Este informe, preparado en colaboración con el Banco Interamericano de Desarrollo (BID) y el Centro de Capacidad de Seguridad Cibernética Global de la Universidad de Oxford, analiza la capacidad de seguridad cibernética de los Estados Miembros de la OEA y alienta a los países a implementar los estándares más actualizados en ciberseguridad, mientras se protegen los derechos fundamentales de sus personas.

Como en la edición anterior, el estudio analiza la madurez cibernética de cada país en las cinco dimensiones identificadas en el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM): (i) Política y estrategia de ciberseguridad; (ii) Cibercultura y sociedad; (iii) Habilidades de educación, capacitación y ciberseguridad; (iv) Marcos Legales y Regulatorios; y (v) Normas, organizaciones y tecnologías.

El progreso realizado en la región, en gran parte con el apoyo de la OEA, es evidente. El informe de 2016, por ejemplo, indicó que cuatro de cada cinco países carecían de estrategias de ciberseguridad o de un plan de protección de infraestructura crítica. A principios de 2020, 12 países habían aprobado estrategias nacionales de ciberseguridad, incluidos Colombia (2011 y 2016), Panamá (2013), Trinidad y Tobago (2013), Jamaica (2015), Paraguay (2017), Chile (2017), Costa Rica (2017), México (2017), Guatemala (2018), República Dominicana (2018), Argentina (2019) y Brasil (2020), entre varios otros en progreso.

Con respecto a la recopilación y validación de datos realizada por nuestros Estados Miembros, el informe representa una visión general del complejo y cambiante universo del ciberespacio. Esperamos que este estudio brinde una perspectiva que nos permita apreciar dónde estamos, que nos permita tomar decisiones basadas en evidencia y que mejore nuestra comprensión colectiva de los desafíos y oportunidades que implica la ciberseguridad en nuestra región. La información y el análisis de este informe ayudarán a todas las partes interesadas (gobiernos, sector privado, academia y sociedad civil) a trabajar para construir un ciberespacio más seguro, más resistente y productivo en nuestro hemisferio.

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

¿Qué ha cambiado desde el reporte de 2016?

Miguel Porrúa
Especialista Principal en Gobierno Digital, Coordinador del Grupo de Datos y Gobierno Digital, **BID**

Belisario Contreras
Gerente del Programa de Ciberseguridad, **OEA**

Cuando se lanzó la primera edición del informe "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?" en marzo de 2016, el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) tuvieron como objetivo ofrecer a los países de la región no sólo una imagen del estado de la ciberseguridad, sino también una orientación acerca de los próximos pasos que se deben seguir para fortalecer las capacidades nacionales en esta materia. Este fue el primer estudio de este tipo en presentar el estado de la ciberseguridad con una visión integral y abarcando todos los países de América Latina y el Caribe.

Hasta la publicación del estudio, la región no parecía darse cuenta de la magnitud del problema. Mientras tanto, los ciberataques en la región han ido en aumento, apuntando principalmente a las instituciones financieras de América Latina. La pandemia de la COVID-19 y el incremento de la actividad digital que ha generado en la región, ha dejado aún más en evidencia las vulnerabilidades del espacio digital de América Latina y el Caribe. El Informe de Cibercrimen ThreatMetrix identificó a América Latina como un foco para el fraude en la creación de cuentas, con alrededor del 20% del volumen total frente a un promedio de la industria del 12,2%.[1] Cada año, millones de nuevos usuarios en América Latina y el Caribe se conectan a Internet por primera vez. Esto, a su vez, crea un crisol de nuevos clientes que no son tan expertos en tecnología como los clientes digitales más maduros, lo cual propicia un ambiente de mayor riesgo. Para este tipo de ataques, la región de América Latina y el Caribe no solo es un objetivo, sino que también es una fuente importante de los mismos.

El crecimiento en el número de ataques cibernéticos ha suscitado un mayor interés por la seguridad cibernética en la región. Para presentar un ejemplo simple, la búsqueda de la palabra ciberseguridad en línea en uno de los motores de búsqueda más conocidos,[2] de marzo de 2016 a junio de 2019, aumentó de 20 a 100.[3] En otras palabras, el interés por saber más sobre ciberseguridad se ha vuelto popular entre los usuarios de Internet en América Latina y el Caribe. Casualmente, los usuarios que indagan sobre ciberseguridad en la región tienden a buscar cursos y oportunidades de capacitación en el campo. Es decir: más personas en América Latina y el Caribe son conscientes de la importancia de la ciberseguridad e investigan formas de mejorar sus conocimientos.

Dado el aumento de los ciberataques, la OEA y el BID han visto necesario implementar nuevamente el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM, por sus siglas en inglés) a fin de poder medir el crecimiento y el desarrollo de las capacidades de nuestros Estados Miembros para defenderse de las crecientes amenazas del espacio cibernético. Las dos instituciones se complacen de ver cómo la ciberseguridad ha cobrado importancia en la agenda política de la región en los últimos años y cómo gobiernos, ciudadanos y empresas muestran

un enorme interés por conocer más sobre el tema. Contar con profesionales más capacitados se ha vuelto fundamental para diseñar e implementar las políticas y medidas de seguridad cibernética que son necesarias para garantizar la resiliencia del país frente a ciberataques cada vez más sofisticados y complejos. Tanto el BID como la OEA están prestando especial atención a esta necesidad y ofreciendo diversas oportunidades para que los profesionales de América Latina y el Caribe actualicen sus habilidades.

Este nuevo estudio nos ha dado una visión renovada sobre dónde estamos y cuáles son las oportunidades que nuestra región puede capitalizar. Por ejemplo, aunque América Latina y el Caribe ha mejorado sus capacidades de ciberseguridad desde 2016, el nivel de madurez promedio de la región todavía está entre 1 y 2, de acuerdo con el CMM (en el que 1 significa etapa Inicial y 5 significa Dinámica o Avanzada). En otras palabras, la mayoría de los países de América Latina y el Caribe han comenzado a formular iniciativas de seguridad cibernética, incluidas las medidas de creación de capacidad. Mejor aún: algunas de ellas ya están siendo implementadas, pero de manera ad hoc y sin coordinación entre los actores clave. Sin embargo, el nivel de madurez promedio de los 32 países en materia de ciberseguridad no debe opacar la importancia de los avances logrados por la región en los últimos cuatro años (2016-2020).

A partir del análisis, se ha observado que el nivel de madurez en ciberseguridad de la subregión del Cono Sur es el más alto en las cinco dimensiones del CMM, con un promedio de entre 2 y 3. Aunque el "Marco legal y regulatorio" es la dimensión más desarrollada, la de "Estándares, organizaciones y tecnologías" tuvo la mejoría más significativa. Cabe señalar que todas las dimensiones presentan niveles similares de madurez en ciberseguridad, lo que sugiere que los países de esta región están abordando la ciberseguridad desde una perspectiva integral. Uruguay fue el país calificado con la madurez más alta de la región en cuatro de las cinco dimensiones.

El Grupo Andino tiene un nivel promedio de madurez de seguridad cibernética de 2. Esto revela la importancia de concentrar los esfuerzos de seguridad cibernética para fortalecer el despliegue de estándares y controles técnicos de seguridad cibernética en la región y alentar la divulgación responsable. Colombia fue el país con mayor desarrollo en seguridad cibernética en este grupo, particularmente en las dimensiones "Política y estrategia" y "Cultura y sociedad".

En el caso de la región de Centroamérica y México, ambos presentaron un nivel de madurez promedio de 2 en las dimensiones "Cultura y sociedad" y "Educación, capacitación y habilidades", mientras que en las dimensiones "Política y estrategia" y "Estándares, organizaciones y tecnologías" el puntaje ha sido inferior a 2. Al igual que en el Grupo Andino, Centroamérica y México deberían centrarse en mejorar el despliegue de estándares de seguridad cibernética y controles técnicos, así como fomentar el desarrollo de un mercado de ciberseguridad. Cabe destacar que la dimensión "Marcos legales y regulatorios" tiene un nivel de madurez de entre 2 y 3. México presenta la mejor posición de la región, con un nivel de madurez de entre 2 y 3 en casi todas las dimensiones.

Finalmente, la región del Caribe tiene un nivel de madurez de entre 1 y 2 en todas las dimensiones. No obstante, mientras que "Marcos legales y regulatorios" es la dimensión más madura, como lo fue en 2016, la de "Política y estrategia" es la que presenta menos avance. El desarrollo de una estrategia nacional de seguridad cibernética, dota a un país de un enfoque más integral que permite comprender y atender mejor los desafíos de la seguridad cibernética. Asimismo, esta planificación estratégica permite priorizar sus objetivos e inversiones en seguridad cibernética. Es de destacar que dos de los países con mayor desarrollo en seguridad cibernética de la región tienen una estrategia nacional de seguridad cibernética, a saber: Trinidad y Tobago y Jamaica.

Los grandes retos de la ciberseguridad, al igual que los de Internet, tienen naturaleza global. Por tanto, los países de América Latina y el Caribe deben continuar fomentando una mayor cooperación entre ellos, involucrando a todos los actores relevantes, así como estableciendo mecanismos de monitoreo, análisis

y evaluaciones de impacto relacionados con la ciberseguridad, tanto a nivel nacional como regional. Contar con más datos en relación con el mundo cibernético permitirá introducir la cultura de gestión del riesgo cibernético, que es preciso extender tanto en el sector público como en el privado. Los países deben estar preparados para adaptarse rápidamente al entorno dinámico que nos rodea y tomar decisiones basadas en un panorama de amenazas en constante cambio. Pasar al siguiente nivel de madurez requerirá una política de ciberseguridad integral y sostenible, apoyada por la agenda política del país, con asignación de recursos financieros y capital humano calificado para llevarla a cabo.

La pandemia de la COVID-19 pasará, pero seguirán sucediéndose acontecimientos que exigirán un uso intensivo de las tecnologías digitales para que el mundo pueda seguir operando. Por lo tanto, el reto de proteger nuestro espacio digital continuará creciendo. El BID y la OEA esperan que la edición de este informe contribuya a que los países de América Latina y el Caribe logren una mejor comprensión del estado de su capacidad actual en materia de seguridad cibernética y que sea de utilidad en el diseño de las políticas e iniciativas que lleven a incrementar su nivel de ciberesiliencia.

Una mirada especializada

Tendencias regionales en el estado de preparación en ciberseguridad, 2016-2020

Sadie Creese
Directora,
Centro Global de Capacidad en Seguridad Cibernética,
Universidad de Oxford

En 2015 la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) fueron las primeras organizaciones del mundo que se embarcaron en un estudio profundo y amplio de las capacidades cibernéticas en toda una región, evaluando el estado del desarrollo en América Latina y el Caribe.

En este contexto, la segunda ronda de evaluaciones de seguridad cibernética presentada en este informe ofrece una perspectiva longitudinal sobre el desarrollo detallado de la capacidad de seguridad cibernética en toda la región. Esta perspectiva en el tiempo ofrece una oportunidad para que los gobiernos de la región evalúen sistemáticamente su progreso a la luz de los avances en las naciones vecinas. Este conocimiento también puede ayudar a los gobiernos a racionalizar sus esfuerzos, alineados con los hitos que han identificado a nivel estratégico, en estrategias nacionales de seguridad cibernética, planes de acción relacionados u otros programas de creación de capacidad cibernética. Además, estos datos les proporcionarán información adicional a los actores, que entregan recursos para el desarrollo de capacidades, sobre el impacto que su inversión ha tenido hasta la fecha y que les permitirá, del mismo modo que a profesionales, investigadores, organizaciones internacionales y gobiernos, identificar éxitos y mejores prácticas en la creación de capacidad. No menos importante es el hecho de que estos datos longitudinales también facilitan una mejor comprensión del valor de las evaluaciones de capacidad para orientar las políticas y las prioridades de inversión.

El Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM, por sus siglas en inglés), que fue la base de los estudios regionales de la OEA y el BID en 2016 y 2020, sigue un enfoque integral que entiende la capacidad dentro de cinco dimensiones: (i) política y estrategia; (ii) cultura y sociedad; (iii) educación, capacitación y habilidades; (iv) marcos legales y regulatorios, y (v) estándares, organizaciones y tecnologías. Para medir de manera confiable la capacidad de seguridad cibernética, cada dimensión se desglosa en factores, aspectos e indicadores, y cada nivel evalúa la capacidad con granularidad progresiva.

El CMM fue diseñado en 2013 por el Centro Global de Capacidad en Seguridad Cibernética (GCSCC, por sus siglas en inglés) de la Universidad de Oxford. Para garantizar que el CMM permanezca actualizado y sea una herramienta poderosa que capture desarrollos importantes, el modelo se somete a revisiones periódicas. A medida que evolucionan los requisitos de capacidad, se hace necesario reflejar este progreso en el modelo para capturar adecuadamente los avances y ofrecer información sobre los próximos pasos posibles para una mejora adicional. En este sentido, el modelo en sí se actualizó en febrero de 2017, en consonancia con la evolución de los desafíos de seguridad y en base a la experiencia de implementar el modelo en el campo.

Esta versión revisada del CMM, utilizada en el estudio de 2020, le agrega una gama de aspectos nuevos para el análisis, como el "modo de operación" de la capacidad de respuesta a incidentes, la "comprensión del usuario de la protección de información personal en línea", los "mecanismos para la presentación de informes", informes de incidentes cibernéticos por "medios y redes sociales", "legislación de protección de datos", "protección infantil en línea", "legislación de protección del consumidor", "legislación de propiedad intelectual", "cooperación formal" y "cooperación informal" sobre asuntos de delitos informáticos, "calidad del software", "controles técnicos de seguridad" y "controles criptográficos".

El presente estudio no sólo le aporta datos significativos a la comunidad internacional de capacidad de seguridad cibernética, sino que también muestra el valor de las evaluaciones de capacidad para guiar la estrategia, la política y la asignación nacional de recursos, y para resolver los beneficios de inversión en áreas de desarrollo de capacidades. En toda América Latina y el Caribe, se ha logrado un progreso visible en todos los aspectos cubiertos por el modelo desde 2015 hasta 2019 (el período entre los dos estudios), como se refleja en el aumento de los puntajes de madurez de capacidad. Los datos longitudinales de los dos estudios muestran varias tendencias e indicaciones de sinergias entre los esfuerzos de creación de capacidad para diferentes aspectos, que se detallan a continuación.

Los aspectos dentro de la dimensión "política y estrategia" han progresado más que otras dimensiones, lo que indica que un enfoque estratégico sistemático para la capacidad de ciberseguridad vale la pena. Los países con mejoras en el contenido o en los procesos de desarrollo de su estrategia nacional de ciberseguridad (NCS, por sus siglas en inglés) tuvieron mayores avances en todos los ámbitos, lo que indica que invertir en un enfoque estratégico tiene resultados positivos para la ciberseguridad. Desde 2015, el número de países de la región que han adoptado una NCS se ha más que duplicado. Colombia, que encabezó los esfuerzos en esta área al desarrollar la primera NCS de la región en 2011, actualmente está implementando la segunda iteración de su NCS.

También se registraron mejoras significativas en el fomento de una mentalidad de ciberseguridad al interior de los gobiernos y entre los usuarios de Internet. Aunque no forman parte de una campaña de sensibilización dedicada, las consultas de múltiples partes interesadas realizadas para la puesta en marcha de estrategias nacionales de ciberseguridad amplían la conciencia entre las organizaciones participantes sobre sus respectivas actividades, responsabilidades y capacidades. Estas ganancias de conciencia pueden filtrarse a otros y ayudar a extender y mantener la capacidad en este espacio. Los avances en la organización y el contenido de las estrategias se reflejan en una mayor consideración de los problemas de seguridad de las TIC entre los representantes del gobierno. Sin embargo, los datos sugieren que ambos grupos, tanto funcionarios gubernamentales como usuarios de Internet en general, aún están rezagados con respecto al sector privado; y la sensibilización de los usuarios de Internet a la seguridad en general sigue siendo relativamente baja. En este sentido, vale la pena recordar que el desarrollo de capacidades de seguridad cibernética sigue siendo un esfuerzo continuo y de toda la nación que sólo podrá tener éxito si se basa en un enfoque inclusivo que incorpore a los grupos vulnerables en toda la sociedad.

Ciertamente, los usuarios de países con legislación más avanzada y específica también informaron niveles más altos de confianza en su uso de Internet. Esto quizá se deba a que, de acuerdo con su experiencia

en línea, los usuarios han percibido un aumento de la seguridad, producido gracias a leyes específicas en materia de TIC, legislación de datos, protección del consumidor y protección infantil en línea (introducidas como nuevas medidas por el modelo actualizado).

Entre 2016 y 2020 los puntajes de madurez para la "legislación sobre delitos cibernéticos sustantivos" no progresaron, posiblemente porque ese aspecto ya tiene el puntaje promedio más alto de toda la región. Este avance en la legislación sustantiva se ha complementado cada vez más con el progreso en la "legislación procesal del delito cibernético", que es el aspecto legal que ha registrado la mayor actividad en el período desde 2015. Sin embargo, la legislación sustantiva experimentará mayores aumentos de capacidad en "términos reales", ya que la exigibilidad depende crucialmente de las disposiciones procedimentales.

La única excepción a este marcado progreso en la capacidad tuvo lugar en las evaluaciones de la "Coordinación de Defensa" cibernética. Sin embargo, la "Coordinación de Defensa" es un tema delicado también fuera de las Américas; más que en otros aspectos, creemos que las evaluaciones de los esfuerzos de "Coordinación de Defensa" están limitadas por la sensibilidad de la información involucrada y la renuencia potencial a compartir detalles relevantes, factores que también pueden suponer un impedimento para la "Coordinación de Defensa" en sí misma.

La investigación comparativa adicional sobre los datos longitudinales podría proporcionar información extra sobre si los avances en áreas hasta ahora poco priorizadas podrían catalizar avances en otras áreas y, por lo tanto, convertirse en un foco en el futuro. Todos los aspectos de la educación y capacitación en ciberseguridad, por ejemplo, se ubican en la mitad inferior, en términos de progreso. La escasez en la fuerza laboral de profesionales calificados en ciberseguridad es un desafío casi universal. Sin embargo, sin el financiamiento adecuado para la capacitación y educación profesional, el desajuste entre la oferta y la demanda conlleva el riesgo de retrasar las ganancias de madurez a futuro; también la falta de una base de habilidades de seguridad cibernética de apoyo podría tener efectos negativos en cascada en los esfuerzos de creación de capacidad en otras áreas. Estas consideraciones resaltan la necesidad de equilibrar las inversiones en ganancias de madurez a corto plazo para abordar las amenazas de seguridad inmediatas con planes a largo plazo para fomentar habilidades y educación que contribuyan de manera sustancial y autosostenible a las posturas nacionales de ciberseguridad.

"Divulgación responsable" fue el aspecto con el puntaje de madurez más bajo de la región. La amplitud y el enfoque integrado del CMM permiten contextualizar aún más las puntuaciones de los aspectos individuales. En este sentido, los riesgos asociados con la falta de un mecanismo institucionalizado para compartir información sobre vulnerabilidades descubiertas y políticas sobre piratería ética podrían verse agravados por los puntajes igualmente bajos para las capacidades de respuesta interna, incluyendo "organización de protección de infraestructura crítica", "gestión de crisis", "gestión y respuesta a riesgos" y "seguro de delito informático", que se ubican en la parte inferior y han visto pocas mejoras desde 2015.

Un propósito clave de cualquier evaluación de CMM es descubrir medidas que funcionen bien, pero también identificar brechas. En este sentido, el BID, la OEA y todos los países participantes de la región merecen un reconocimiento por presentar esta línea de base actualizada y por trazar un camino que otras regiones podrían seguir para lograr una mayor conciencia fundamentada de sus niveles de capacidad.

Además de los compromisos con el desarrollo de capacidades de seguridad cibernética a nivel nacional, América Latina y el Caribe ha sido más que el fundamento de una serie de iniciativas regionales muy dinámicas. Por ejemplo, en 2016 se realizó el lanzamiento de CSIRT Américas, una plataforma que permite la cooperación regional y el intercambio de información entre los equipos de respuesta a incidentes gubernamentales y nacionales de los Estados Miembros de la OEA. A raíz del ataque del

ransomware WannaCry en 2017, CSIRT Américas, una ha facilitado la identificación y el aislamiento temprano de los puntos críticos de infección en las Américas para frenar la propagación de WannaCry dentro de la región. Para mitigar brotes futuros, la plataforma ha creado un depósito central de herramientas para sus componentes regionales de modo de prevenir y combatir las infecciones de ransomware. Desde 2015, la propia comunidad de respuesta a incidentes ha crecido a 20 CSIRT nacionales dentro de la región.

Desde 2016, los equipos de las Américas se han entrenado junto con sus homólogos de Europa, África y Asia en ejercicios anuales regulares, organizados en colaboración entre la OEA, el Instituto Nacional de Seguridad Cibernética (INCIBE) y el Centro Nacional de Protección de Infraestructura Crítica. En 2018, la OEA, el BID y el INCIBE organizaron un primer desafío conjunto de ciberseguridad específicamente para apoyar y alentar a jóvenes talentos en España y las Américas a seguir una carrera en campos relacionados con la ciberseguridad.

En su compromiso por promover el cumplimiento de las líneas de base para el comportamiento responsable en el ciberespacio identificado por los informes de consenso del grupo de Expertos Gubernamentales sobre Seguridad de la Información de Naciones Unidas, en 2017 la OEA estableció un grupo de trabajo sobre medidas de cooperación y fomento de la confianza en el ciberespacio. A través del intercambio de mejores prácticas con la Organización para la Seguridad y la Cooperación en Europa (OSCE), el Grupo de trabajo ha desarrollado dos conjuntos de medidas de fomento de la confianza, las cuales ya han sido adoptadas por los Estados Miembros de la OEA.

Como parte de estas medidas, los Estados Miembros de la OEA han resuelto compartir información sobre políticas nacionales de seguridad cibernética, establecer un punto de contacto nacional para discutir las amenazas cibernéticas a nivel regional, identificar un punto de contacto separado dentro de sus ministerios de Asuntos Exteriores en apoyo de la cooperación internacional, y la cooperación y el diálogo, y apoyar estos canales, cuando corresponda, con plataformas y acuerdos para promover prácticas que fortalezcan la estabilidad en el ciberespacio. Entre otros compromisos se incluyen además la capacitación de diplomáticos y funcionarios gubernamentales en general en asuntos de seguridad cibernética y el fortalecimiento de iniciativas de creación de capacidad a través de campañas de sensibilización tanto en el sector público como en el privado.

La OEA y el GCSCC tienen una relación especial. Las dos organizaciones han estado colaborando desde el desarrollo del CMM, han implementado proyectos piloto conjuntos del modelo en Jamaica y Colombia en 2015 y una evaluación posterior en Brasil en 2018. Esta asociación estratégica se formalizó mediante un memorando de entendimiento en 2015 y, siendo un socio confiable, la OEA fue un contribuyente activo en el proceso de revisión de la CMM. La colaboración entre las dos organizaciones también se extiende más allá de la CMM, e incluye iniciativas conjuntas en eventos de partes interesadas como el Foro para la Gobernanza de Internet (IGF, por sus siglas en inglés). En el futuro, la OEA y el GCSCC trabajarán en estrecha colaboración para poner a prueba un Marco de daño cibernético, que se implementará junto con el CMM, así como para establecer un centro regional en América Latina como parte de una constelación global más grande de centros de capacidad regionales de ciberseguridad.

La perspectiva integral de la UE para afrontar las amenazas del ciberespacio

Pawel Herczynski
Director Gerente de PCSD y Respuesta a Crisis,
Servicio Europeo de Acción Exterior

La ciberseguridad es crítica para nuestra prosperidad y seguridad. Las actividades cibernéticas maliciosas no sólo amenazan las economías, sino también el funcionamiento mismo de nuestras democracias, libertades y valores. Nuestra seguridad futura depende de que sepamos transformar la capacidad para protegernos contra las amenazas cibernéticas: tanto la infraestructura civil como la capacidad militar dependen de sistemas digitales seguros.

Esto ha sido reconocido en la Estrategia Global para la Política Exterior y de Seguridad de la Unión Europea (UE).[4] La UE considera los enfoques del Mercado Único Digital, la Estrategia Global, la Comunicación Conjunta al Parlamento Europeo y al Consejo de Resiliencia, Disuasión y Defensa,[5] la Agenda Europea de Seguridad,[6] el Marco conjunto sobre la lucha contra las amenazas híbridas[7] y la Comunicación sobre el lanzamiento del Fondo Europeo de Defensa.[8] Sobre la base de todos ellos, la UE ha decidido ha decidido construir una mayor resiliencia y autonomía estratégica, aumentar las capacidades en términos de tecnología y habilidades, conformar un mercado único fuerte, y desarrollar e implementar un enfoque integral para la ciberdiplomacia a nivel mundial.

Resiliencia

Una resiliencia cibernética fuerte requiere un abordaje colectivo y amplio. Se necesitan estructuras eficaces para promover la ciberseguridad y responder a los ciberataques en los Estados Miembros de la UE, pero también en las propias instituciones, agencias y organismos de la UE. Asimismo, esto demanda un enfoque más integral y de políticas transversales para construir resiliencia cibernética y autonomía estratégica, con un mercado único fuerte, grandes avances en la capacidad tecnológica de la UE y un número mucho mayor de expertos calificados.

La Directiva NIS, sobre medidas para un alto nivel común de seguridad de redes y sistemas de información,[9] cumple un papel vital en el desarrollo de una nueva cultura de ciberseguridad en la UE. Gracias a la Directiva NIS, los Estados miembros de la UE intercambian información sobre incidentes de seguridad cibernética, comparten mejores prácticas de seguridad cibernética, cooperan y están mejor coordinados. El Grupo de Cooperación NIS, creado por la directiva mencionada, apoya y facilita la cooperación estratégica y el intercambio

de información entre los Estados Miembros de la UE. Según la Directiva NIS, los operadores de servicios esenciales (por ejemplo, bancos, empresas de telecomunicaciones, proveedores de energía, hospitales, etc.) están obligados a informar a las autoridades nacionales cuando se ven afectados por incidentes graves de seguridad cibernética y tienen planes de evaluación de riesgos para identificarlos. Las responsabilidades para garantizar la seguridad de la red y los sistemas de información recaen, en gran medida, en los operadores de servicios esenciales y proveedores de servicios digitales. Sin embargo, debe promoverse y desarrollarse una cultura de gestión de riesgos, que implique la evaluación de riesgos y la implementación de medidas de seguridad apropiadas a los riesgos enfrentados, a través de requisitos reglamentarios adecuados y prácticas voluntarias de la industria. Se necesita más que nunca la cooperación y el intercambio de información, así como la combinación de diferentes habilidades y expertos, ya que las amenazas cibernéticas y los incidentes de seguridad cibernética se están volviendo cada vez más sofisticados en nuestra economía y sociedad digital.

Ya se dio un paso hacia la mejora de la respuesta del derecho penal a los ciberataques con la adopción en 2013 de la Directiva relativa a los ataques contra los sistemas de información.[10] Esta establecía reglas mínimas sobre la definición de delitos y sanciones penales en el área de ataques contra los sistemas de información y preveía medidas operativas para mejorar la cooperación entre las autoridades. La Directiva ha producido avances sustanciales en la criminalización de los ciberataques a un nivel comparable en todos los Estados Miembros, lo que facilita la cooperación transfronteriza de las autoridades policiales que investigan este tipo de delitos. Dada la naturaleza sin fronteras de Internet, el marco de cooperación internacional provisto por el Convenio de Budapest sobre Ciberdelincuencia del Consejo de Europa[11] ofrece la oportunidad, entre un grupo diverso de países, de utilizar un estándar legal óptimo para las diferentes legislaciones nacionales que abordan el delito informático. Ahora se está explorando una posible incorporación de un protocolo al convenio, lo que también podría brindar una oportunidad útil para abordar la cuestión del acceso transfronterizo a la evidencia electrónica en un contexto internacional.

Investigación y desarrollo

Al cooperar, uniendo los conocimientos especializados de ciberseguridad de la UE y desarrollando una hoja de ruta común europea de investigación e innovación (I+I) en ciberseguridad y una estrategia industrial europea de ciberseguridad, Europa puede ayudar a que la industria de la ciberseguridad y el ecosistema crezcan, lo que también daría lugar a un aumento de la capacidad de ciberseguridad de la UE. Por ello, en 2016 la Comisión Europea firmó con la Organización Europea de Seguridad Cibernética (ECSO, por sus siglas en inglés) una asociación público-privada (APP) contractual. Esta es fundamental para estructurar y coordinar los recursos industriales de seguridad digital en Europa. La misma incluye una amplia gama de actores, desde pequeñas y medianas empresas (pyme) innovadoras hasta productores de componentes y equipos, operadores de servicios esenciales e institutos de investigación, reunidos bajo el paraguas de ECSO. La UE se ha comprometido a invertir hasta €450 millones en esta asociación bajo su programa de investigación e innovación Horizon 2020; a cambio, la industria tiene que invertir tres veces más en las mismas áreas. Como siguiente paso ambicioso, en septiembre de 2018 se propuso expedir un nuevo reglamento que establece una Red de Centros Nacionales de Coordinación de Ciberseguridad y el nuevo Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad. Esta propuesta está siendo discutida actualmente entre los colegisladores de la UE. El Centro se convierte así en una forma de abordar la fragmentación del ecosistema de ciberseguridad de Europa, afronta la falta de habilidades y experiencia en ciberseguridad, une los recursos europeos, coordina los esfuerzos para fortalecer las capacidades de ciberseguridad de la UE y permite que las industrias de la UE desarrollen productos y servicios competitivos a nivel mundial. Lo anterior allanará el camino para una Europa digital segura, abordando todos los próximos desafíos de ciberseguridad derivados de las tecnologías emergentes (por ejemplo, IoT,

inteligencia artificial, cuántica, computación de alto rendimiento, blockchain) y que son utilizados en sectores críticos, tales como transporte, energía, salud, finanzas, fabricación, defensa. También configurará e implementará las inversiones apropiadas en ciberseguridad para el próximo Marco Financiero Plurianual (MFP) de la UE.

Creación de capacidad

La estabilidad cibernética global se basa en la capacidad local y nacional de todos los países para prevenir y reaccionar ante incidentes cibernéticos e investigar y procesar casos de delitos cibernéticos. El apoyo a las gestiones para desarrollar resiliencia nacional en terceros países aumentará el grado de ciberseguridad a nivel mundial, con consecuencias positivas para la UE. Para contrarrestar las amenazas cibernéticas en rápida evolución, se debe contar con políticas, legislación y capacitación, así como con equipos de respuesta a emergencias informáticas y unidades de ciberdelincuencia en todos los países del mundo.

Desde 2013, la UE ha liderado la creación de capacidades internacionales de seguridad cibernética y ha vinculado sistemáticamente estos esfuerzos con su cooperación para el desarrollo. La UE continuará promoviendo un modelo de creación de capacidades basado en derechos, en línea con el enfoque Digital4Development.[12] Las prioridades en este sentido abarcan tanto la vecindad de la UE como países en desarrollo que experimentan una conectividad en rápido crecimiento y un veloz surgimiento de amenazas. Los esfuerzos de la UE serán complementarios a la luz de la Agenda 2030 para el Desarrollo Sostenible y los esfuerzos generales para la puesta en marcha de capacidades institucionales.

La UE también definió su enfoque sobre la creación de capacidad cibernética en junio de 2018, cuando el Consejo, al presentar sus conclusiones sobre las directrices externas de creación de capacidad cibernética de la UE, recordó que dicha creación se está convirtiendo en uno de los temas clave de la agenda internacional de política cibernética, y destacó el papel del desarrollo de capacidades cibernéticas en los países y regiones socias como un componente estratégico de la gestión de la diplomacia cibernética de la UE.

Diplomacia cibernética

Guiada por los valores y derechos fundamentales de la UE, como la libertad de expresión y el derecho a la privacidad y protección de datos personales, además de la promoción del ciberespacio abierto, libre y seguro, la política internacional de ciberseguridad de la UE está diseñada para abordar el desafío en constante evolución de promover la estabilidad cibernética global, así como contribuir a la autonomía estratégica de Europa en el ciberespacio. Dada la naturaleza global de la amenaza, la construcción y preservación de alianzas y asociaciones sólidas con terceros países es fundamental para la prevención y disuasión de los ataques cibernéticos, que son cada vez más trascendentales para la estabilidad y la seguridad internacional. La UE le dará prioridad al establecimiento de un marco estratégico para la prevención de conflictos y la estabilidad en el ciberespacio en sus compromisos bilaterales, regionales, de múltiples partes interesadas y multilaterales. La UE promueve firmemente la posición de que el derecho internacional, y en particular la Carta de las Naciones Unidas, se aplica al ciberespacio. Como complemento del derecho Internacional vinculante, la UE respalda las normas, reglas y principios de carácter voluntario y no vinculante de comportamiento responsable de los Estados que han sido articulados por el Grupo de Expertos Gubernamentales de Naciones Unidas. También alienta el desarrollo y la implementación de medidas regionales de fomento de la confianza, tanto en la Organización para la Seguridad y la Cooperación en Europa como en otras regiones. A nivel bilateral, los diálogos cibernéticos[13] se desenvuelven y complementan aún más con las gestiones para facilitar la cooperación con terceros países, y para reforzar los principios de debida diligencia y responsabilidad estatal en el ciberespacio. La UE también destaca que la ciberseguridad no es un pretexto para la protección del mercado y la limitación de los derechos y

libertades fundamentales, incluida la libertad de expresión y el acceso a la información. Un enfoque integral de la ciberseguridad requiere el respeto de los derechos humanos. A ese respecto, la UE destaca la importancia de la participación de todos los interesados en la gobernanza de Internet.

Adoptado en 2017, el marco de una respuesta diplomática conjunta de la UE a las actividades cibernéticas maliciosas (la "caja de herramientas de la diplomacia cibernética"[14]) establece las medidas de la Política Exterior y de Seguridad Común, incluidas las disposiciones restrictivas que pueden utilizarse para fortalecer la respuesta de la UE a las actividades que perjudican sus intereses políticos, de seguridad y económicos. El marco constituye un paso importante en el desarrollo de la señalización y las capacidades reactivas a nivel de la UE y de los Estados Miembros.

Conclusiones

La preparación cibernética de la UE es fundamental tanto para el Mercado Único Digital como para la Seguridad y Defensa de la Unión. Es imprescindible fortalecer la ciberseguridad europea y abordar las amenazas a objetivos civiles y militares. En este gran esfuerzo, contamos igualmente con el apoyo de nuestros socios globales. Solo juntos, siendo resistentes, capaces de proteger a nuestra población de manera efectiva al anticipar posibles ciberamenazas e incidentes de ciberseguridad, al construir una fuerte resiliencia en nuestras estructuras y defensa, al recuperarnos rápidamente de cualquier ciberataque y al disuadir a los responsables, podremos proporcionar un ciberespacio abierto, seguro y protegido para todos.

Amenazas emergentes en ciberseguridad: implicaciones para América Latina y el Caribe

Nayia Barmpaliou,
Jefa de Políticas e Iniciativas Públicas
Centro para la Ciberseguridad,
Foro Económico Mundial

La ciberseguridad en la era de la hiperconectividad y las pandemias

La pandemia mundial del COVID-19 ha marcado un punto de inflexión fundamental en nuestra senda mundial y ha acentuado como nunca antes nuestra dependencia de la infraestructura digital. Si bien esta crisis ha expuesto las deficiencias estructurales que nuestra sociedad ha venido acarreando en múltiples sistemas –tales como salud, economía, empleo y educación–, también ha resaltado el papel catalizador de la tecnología en la forma en que hemos enfrentado colectivamente la pandemia.

En un lapso de tres meses, experimentamos una aceleración de la transformación digital que se había anticipado que ocurriría en tres años.[15] Con el tiempo, nuestra transición a la era "digital de todo" ha reconfigurado profundamente nuestra vida profesional y personal. Incluso en el entorno más disruptivo de la pandemia, Internet y la infraestructura digital global han hecho posible la provisión de servicios esenciales, han permitido a las empresas continuar operando y han sostenido nuestros contactos sociales individuales. El resultado de esta transición ha sido un extraordinario aumento de la superficie de ataque cibernético, en el contexto de un ecosistema digital de vulnerabilidades ya amplificadas que incluye más de 20.000 millones de dispositivos de Internet de las cosas (IoT, por sus siglas en inglés) conectados en todo el mundo.[16]

Incluso antes de la pandemia, las brechas de ciberseguridad y las filtraciones de datos se estaban convirtiendo en los principales obstáculos de la economía digital. Los cibercriminales aprovechan rápidamente los nuevos vectores de ataque y se benefician de los vacíos en la cooperación de las fuerzas del orden público en las diferentes jurisdicciones, dada la naturaleza inherentemente transnacional de sus actividades maliciosas. A su vez, el riesgo de ataques cibernéticos en infraestructura crítica y fraude o robo de datos ha sido siempre una prioridad para los líderes empresariales a nivel mundial. Según el Informe de Riesgos Globales 2020 del Foro Económico Mundial,[17] el riesgo de ciberataques a la infraestructura crítica y el fraude o robo de datos se clasificaron entre los 10 principales riesgos con mayor probabilidad de ocurrir, mientras que la reciente Perspectiva de Riesgos del COVID-19 del Foro Económico Mundial,[18] identificó

los ciberataques como la tercera mayor preocupación debido a nuestra actual y sostenida transición hacia los patrones de trabajo digital.

Los datos disponibles respaldan estas preocupaciones; se estima que los daños por delitos cibernéticos alcanzarán los US$6 billones para 2021, lo que equivale al producto interno bruto (PIB) de la tercera economía más grande del mundo.[19] Además del costo financiero, el cibercrimen y los ciberataques socavan la confianza de los usuarios en la economía digital. Las encuestas indican que, de la población mundial con acceso a Internet, menos del 50% confía en que la tecnología mejorará sus vidas, lo que demuestra una creciente y profunda falta de confianza con respecto a la privacidad de los datos.[20]

Estas tendencias son particularmente pertinentes para la región de América Latina y el Caribe (ALC), que en los últimos cinco años ha sido testigo de una enorme expansión en el uso de las tecnologías de la información y la comunicación (TIC). A medida que la región avanza cada vez más hacia la economía digital, aumenta la necesidad de garantizar la confianza digital. Los protocolos de gestión de riesgos de seguridad digital y protección de la privacidad constituyen responsabilidades compartidas por los gobiernos, el sector privado y los usuarios individuales en una economía cada vez más impulsada por los datos.[21] Gracias a la priorización de la creación de capacidad de seguridad cibernética en la agenda de desarrollo de la región, producto de los esfuerzos coordinados e intensificados del Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) en los últimos años, la necesidad de integrar la ciberseguridad y la lucha contra el cibercrimen en las estrategias y políticas digitales de la región también se ha reflejado al más alto nivel como parte de la "Propuesta de Agenda Digital para América Latina y el Caribe".[22]

Un asunto transversal en la política Nacional

La intrusión del continuo digital en todas las áreas de actividad humana, así como los niveles sin precedentes de innovación e interdependencia tecnológicas, han hecho que sea imposible tratar la ciberseguridad de forma aislada, como un asunto técnico o un área de políticas independiente. En los últimos años, la ciberseguridad ha roto la barrera de los silos técnicos y se encuentra en la intersección de múltiples disciplinas y áreas de políticas: acceso digital y conectividad, resiliencia, justicia penal, diplomacia, seguridad y defensa internacional, y economía digital y comercio, así como las nuevas tecnologías. En tanto que las naciones intentan cosechar los beneficios de la Cuarta Revolución Industrial, la seguridad cibernética se ha ganado un lugar en el enfoque de la política global. Esto ha resultado en un incremento significativo de la adopción o revisión de estrategias nacionales de ciberseguridad que adquieren un enfoque de todo el gobierno o, incluso a veces, de toda la sociedad, así como de la puesta en marcha o la adaptación de legislación nacional sobre cibercrimen, especialmente en países en desarrollo que no contaban con tales leyes vigentes.

Este informe proporciona evidencia prometedora de que los gobiernos de la región de ALC han dado importantes pasos en el desarrollo y la eficacia de sus estrategias nacionales de seguridad cibernética, que también han servido como vehículos para mejorar la cultura y las prácticas nacionales de seguridad cibernética desde su última encuesta, realizada en 2016. Además, desde entonces, cuatro países de ALC se han unido al Convenio sobre Cibercrimen del Consejo de Europa (o "Convenio de Budapest"), cuyo objetivo es promover una política penal común contra el cibercrimen, ofreciendo un marco común de legislación nacional y cooperación internacional.

Fracaso y oportunidad del mercado para la ciberseguridad en la economía digital

El rápido avance de las tecnologías digitales pone de relieve las grandes innovaciones, pero también crea nuevas vulnerabilidades a un ritmo más rápido de lo que se las puede atender. Hasta la fecha, el desequilibrio entre el tiempo de comercialización y el "tiempo de seguridad" sigue siendo una cuestión predominante, debido a la presión de las fuerzas del mercado en favor de los productos de nuevas tecnologías, sin incentivos para priorizar los elementos de seguridad desde el inicio del ciclo de vida del producto[23].

Es llamativo que, a pesar los cambios perceptibles en el comportamiento de los consumidores con respecto a las crecientes preocupaciones sobre privacidad y seguridad, los objetivos del mercado no se estén adaptando con suficiente rapidez, lo cual conducirá inevitablemente a diferentes experimentos en términos de intervenciones y regímenes regulatorios. Por ahora, vemos que la habitual falta de un enfoque de "seguridad por diseño" en las innovaciones tecnológicas ha generado una tendencia hacia esquemas de certificación voluntaria en ciberseguridad para productos TIC, por ejemplo en la Unión Europea y Singapur, y hay más países que se centran específicamente en el IoT. En el otro extremo del espectro, esta falla del mercado ha dado lugar a la ciberseguridad como uno de los sectores más diversos y de rápida expansión en todo el mundo. Antes de la crisis del COVID-19, se esperaba que el gasto global en productos y servicios de seguridad cibernética aumentara en un 88% en los próximos ocho años.[24] La recesión económica causada por la pandemia podría conducir a la consolidación de este mercado. En el caso de ALC, a medida que la región avanza hacia una mayor madurez en su seguridad cibernética, es importante que las estrategias de implementación de ciberseguridad nacional consideren medidas orientadas a limitar el riesgo de una mayor superficie de ataque, y que se inspiren en los estándares existentes o en esquemas voluntarios.

El imperativo estratégico de ciberseguridad empresarial

En los últimos cinco años, la noción de que la estrategia de ciberseguridad forma parte integral de la estrategia comercial ha ganado más tracción e implementación real por parte de las empresas. Esto se debe en parte a la publicidad alusiva a ciertas grandes brechas en materia de seguridad, así como a mayores consideraciones legales y regulatorias, incluyendo la entrada en vigor en mayo de 2018 del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) de la Unión Europea, el cual tiene un impacto significativo a nivel global. En la práctica, este ha sido un factor clave para que los líderes empresariales y las juntas corporativas comprendan mejor los riesgos cibernéticos de su modelo operativo comercial y logren el equilibrio adecuado entre proteger la seguridad de sus activos, mitigar las pérdidas y mantener la rentabilidad en un ambiente competitivo. Esta mayor conciencia a nivel del liderazgo corporativo es un primer paso crucial para potenciar la toma de decisiones corporativas informadas para la planificación de la seguridad cibernética, los mecanismos de respuesta y las inversiones. El lanzamiento en 2019 del "Manual de Supervisión del Riesgo Cibernético para las Juntas Corporativas" por parte de la OEA y de la Alianza por la Seguridad en Internet[25] marcó un importante esfuerzo consultivo para crear tal conciencia en la región de ALC entre las partes interesadas de las juntas corporativas, la alta gerencia, los gobiernos y la academia, y adaptar el asesoramiento a las particularidades regionales.

Mientras tanto, a medida que las empresas más grandes han estado invirtiendo más en ciberseguridad y en innovación en materia de seguridad, los análisis recientes señalan un aumento significativo de los ataques dirigidos a pequeñas y medianas empresas (pyme). Esto crea un riesgo significativo en el ecosistema digital, especialmente teniendo en cuenta que las pyme no tienen los recursos financieros para invertir fuertemente en ciberseguridad, o simplemente la cultura de seguridad no constituye uno de los principales impulsores de sus agendas.

De hecho, los desafíos que enfrentan estas firmas para asegurar su entorno digital en términos de falta de recursos financieros o cultura de seguridad son bastante diferentes de los de las organizaciones más grandes. Al reflexionar sobre esta realidad en el contexto regional de ALC, cabe considerar que, según la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la estructura económica de ALC está compuesta en un 99,5% por micro, pequeñas y medianas empresas (mipyme).[26] Por lo tanto, aumentar la conciencia de seguridad cibernética y promover la higiene básica de seguridad cibernética en las pyme de la región debería ser una prioridad crítica en los próximos años.

Las nuevas tecnologías reestructuran el panorama de ciberseguridad y de políticas

Las tecnologías "antiguas" y "nuevas" no solo están reestructurando la industria y el panorama de la ciberseguridad, sino que desafían más ampliamente las formas tradicionales de operación de la sociedad. La convergencia de las tecnologías de la información con la tecnología operativa y los sistemas heredados ya plantea grandes desafíos en todo el ecosistema digital. La aparición de nuevas tecnologías y sus aplicaciones, tales como inteligencia artificial, big data, redes de quinta generación, computación en la nube, IoT y computación cuántica, cuestionan drásticamente nuestro pensamiento convencional sobre el futuro de la economía digital. Por un lado, ofrecen inmensas oportunidades de eficiencia e innovación, pero también amplifican la superficie de ataque y pueden crear riesgos de seguridad y privacidad de datos todavía desconocidos. Por esta razón, las empresas y los gobiernos deben trabajar juntos para desarrollar una comprensión sólida de los riesgos emergentes de ciberseguridad relacionados desde una perspectiva de políticas, de los riesgos y de las operaciones. Parte del desafío será fomentar la confianza entre las diferentes partes interesadas del ecosistema para reducir la fricción en los actuales modelos regulatorios y de aseguramiento. Vale destacar que, para los países de la región de ALC y otras economías emergentes, estos problemas de seguridad incipientes deberán abordarse de una manera que no exacerbe las barreras para acceder a los beneficios de las nuevas tecnologías.

La ciberseguridad en una arquitectura global fragmentada y polarizada

En la era de un orden global multipolar y multiconceptual, el contexto geopolítico y social influye en el desarrollo de la tecnología y a la vez también se ve afectado por la tecnología. Por un lado, la aparición de nuevas tecnologías tiene el potencial de reorganizar significativamente las dinámicas y alianzas geopolíticas, mientras que actualmente la convergencia de nuevas tecnologías con aplicaciones tradicionales desempeña un papel importante en la amplificación de las tensiones existentes alrededor de los valores de gobernanza de una Internet abierta y descentralizada, versus el enfoque en la "cibersoberanía", o el uso del ciberespacio como un entorno para la competencia estratégica. Tal polarización puede socavar tanto la seguridad en el ciberespacio como la confianza para la cooperación global contra los desafíos comunes de ciberseguridad. Los enfoques divergentes de las principales potencias cibernéticas en relación con la forma en que se aplica el derecho internacional en el ciberespacio, la cual se encuentra en discusión en los foros relevantes de Naciones Unidas,[27] reflejan un entorno internacional bastante conflictivo, exacerbado aún más por los llamados a la "autonomía estratégica" digital, lo que incluso sería problemático lograr en un contexto de rápido cambio tecnológico y cadenas de valor globales.

En este marco, las organizaciones regionales se han posicionado como actores clave en la promoción de la estabilidad regional, la seguridad y los esfuerzos para fomentar la confianza en el ciberespacio mediante medidas de generación de seguridad. La región de ALC también ha demostrado un progreso significativo en esta dirección, cuando en 2017 el Comité Interamericano contra el Terrorismo de la OEA instauró el Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio.[28]

La necesidad de un cambio de paradigma en la cooperación público-privada

La naturaleza intrínsecamente compleja y diseminada del ecosistema digital, junto con las múltiples dimensiones de la política cibernética pública y corporativa, ha creado con el tiempo una arquitectura complicada de partes interesadas. La digitalización ha transformado nuestra sociedad en un "sistema de sistemas", donde las funciones críticas se distribuyen entre los actores públicos y privados en ubicaciones dispersas y con interdependencias complejas. Por lo tanto, los últimos años nos han enseñado que la cooperación público-privada en materia de ciberseguridad requiere pensar fuera de los formatos tradicionales y rígidos para superar las barreras y ser verdaderamente efectivos. Para abordar esta elevada complejidad y responsabilidad compartida, necesitamos una nueva generación de alianzas público-privadas que invaliden el "pensamiento en silos" y adopten un enfoque sistémico para navegar la dinámica compuesta de los factores de políticas, tecnológicos, económicos, sociales y geopolíticos que dan forma al entorno de riesgo de ciberseguridad y sus interdependencias. A medida que los países de la región de ALC aceleran su transformación digital, tienen la oportunidad de entretejer tal pensamiento sistemático en su arquitectura de cooperación público-privada, pudiendo este ser un factor diferenciador para su resistencia cibernética.

Conclusión

El carácter complejo de la ciberseguridad es un claro ejemplo de cómo nuestra actual arquitectura global fragmentada no es idónea para enfrentar los retos del siglo XXI. El efecto catalizador de la pandemia del COVID-19 en la economía ha ejercido una enorme presión sobre nuestro entorno digital para que permanezca seguro, resiliente y efectivo. La ciberseguridad es un componente integral y una herramienta clave para esta conectividad sin precedentes, y esta "nueva normalidad" ha reafirmado su valor como un bien público global.

Más allá de la protección operativa de los sistemas y redes, la ciberseguridad es, y seguirá siendo, fundamental para garantizar la integridad y la capacidad de recuperación de los procesos interconectados socioeconómicos, de gobierno y de negocios que operan en el marco de nuestro siempre complejo ecosistema tecnológico. Abordar el riesgo cibernético en todos los ámbitos requiere continuos esfuerzos y adaptación. El presente informe ofrece inestimables observaciones sobre los esfuerzos realizados a nivel nacional dentro de la región de ALC, al capturar y cuantificar el progreso de los países en diferentes dimensiones de seguridad cibernética, en comparación con el análisis de 2016, lo cual permite demostrar la mejora de la postura de seguridad cibernética de la región a lo largo del tiempo. Este trabajo puede constituir una herramienta invaluable para los encargados de la toma de decisiones de los sectores público y privado a la hora de identificar intervenciones prioritarias, mientras avanzan con el fin de mejorar aún más el estado de la ciberseguridad en la región de ALC a través de medidas concertadas y escalables de colaboración nacional, regional e internacional.

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

La necesidad de una respuesta armonizada a las amenazas de ciberseguridad: El camino a seguir

Sven Mikser,
Ministro de Relaciones Exteriores,
República de Estonia

Durante la última década, han surgido una serie de amenazas en el ciberespacio que requieren la atención de los gobiernos de todo el mundo. Tres de los problemas internacionales de seguridad cibernética más apremiantes tienen que ver con la creciente inestabilidad causada por el delito informático, las intrusiones en redes críticas y las operaciones motivadas políticamente. Todos estos elementos han estado o están en proceso de implementación en las agendas políticas de los Estados de todo el mundo. Sin embargo, el nivel en el que los temas descritos se han convertido en una prioridad difiere mucho entre los Estados. Esto señala una mayor necesidad de armonizar los esfuerzos de los Estados para aumentar su ciberseguridad. Entonces, la cuestión es cómo incentivar a los Estados para que cooperen en un campo que convencionalmente se consideraría un área relacionada con sus asuntos internos.

Una de las formas posibles de abordar los desafíos emergentes de ciberseguridad entre los Estados sería implementar un enfoque internacional que se centre en la armonización de las capacidades de ciberseguridad. Debido al alto nivel de interconexión de los Estados en el ciberespacio, la estabilidad de uno afecta el bienestar de todos los que lo rodean. Por lo tanto, un enfoque regional podría estimular a muchos Estados para que participen en el desarrollo de capacidades de seguridad cibernética. Hay muchas organizaciones regionales que han tomado iniciativas para resolver el problema. Por ejemplo, la Organización de los Estados Americanos (OEA) ha estado activa en el dictado de talleres de creación de capacidad cibernética durante varios años. Estos eventos son particularmente importantes para sentar las bases para construir capacidades sólidas a nivel de los Estados, al aumentar la conciencia sobre las amenazas cibernéticas emergentes y el desarrollo de posibles mecanismos para afrontarlas. Teniendo en cuenta las primeras gestiones que determinados actores han adelantado en la sensibilización sobre la seguridad en este campo en América Latina y el Caribe, se podrían dar nuevos pasos para lograr un ciberespacio más estable y próspero basado en una cooperación regional de seguridad cibernética más fuerte.

A continuación, se detalla cómo la cooperación regional y los valores comúnmente compartidos sobre ciberseguridad podrían ayudar a los Estados a superar las tres amenazas clave destacadas anteriormente y se ofrecen algunas sugerencias sobre cómo avanzar a partir de la situación actual.

¿Cómo pueden las capacidades de ciberseguridad internacionales armonizadas garantizar un espacio más seguro?

Si se considera la naturaleza sin fronteras de los delitos que se perpetran en el ciberespacio, la cooperación regional en el desarrollo de capacidades es vital para poder reaccionar ante el crimen informático organizado y detener los ataques cibernéticos antes de que lleguen a niveles incontrolables. Los incidentes de ciberseguridad más recientes de 2017 y 2018 han demostrado el riesgo de un mayor daño financiero, y en términos de la cantidad de personas y Estados a los que afectan. Hemos sido testigos de operaciones de cibercrimen de enorme magnitud, que han detenido el desarrollo normal de las economías nacionales, teniendo como objetivo específico algunos de los pilares centrales de las economías de los Estados, como los sectores industrial y bancario.

La creación de conciencia entre los expertos técnicos, políticos y las fuerzas del orden podría ayudar a que los países sean menos vulnerables al delito cibernético. La naturaleza de los actos criminales que tienen lugar en el ciberespacio está cambiando rápidamente, por lo que los países deben invertir más en educar a su personal en la aplicación de la ley, los sistemas judiciales y otras instituciones gubernamentales relevantes. Adaptarse a las nuevas circunstancias es clave también para la puesta en marcha de asociaciones público-privadas (APP) confiables. El intercambio de información entre los actores del sector privado, así como entre el sector privado y las instituciones gubernamentales, ya se puede documentar en algunos países, pero es menos notorio en otros. La armonización regional de marcos legales para abordar el delito cibernético y las mejores prácticas de aplicación de la ley podrían contribuir a obtener seguridad y estabilidad regional en el ciberespacio.

Además del aumento del número de incidentes de delitos cibernéticos, el robo intelectual habilitado cibernéticamente se ha generalizado en muchas partes del mundo. El nivel de sofisticación utilizado para robar propiedad intelectual hace que sea imposible evitar su atribución a un actor estatal. Algunos de los programas maliciosos que se han utilizado muestran signos de tener un origen regional y están diseñados específicamente para atacar ciertas zonas del mundo. Esta es una de las razones por las cuales la cooperación regional en la lucha contra el robo intelectual cibernético debería considerarse parte de un enfoque internacional y armonizado, dirigido por los Estados.

En el contexto de las actividades antes mencionadas, las operaciones de influencia política llevadas a cabo en el ciberespacio podrían convertirse en una seria preocupación para países democráticos. En el año 2018 hubo elecciones presidenciales en las tres democracias más grandes de América Latina: Brasil, Colombia y México. Si bien la cobertura de las noticias públicas solo refleja pequeños márgenes de desinformación durante las campañas electorales y los períodos de votación, es muy probable que el tema de la interferencia electoral continúe en la agenda de la mayoría de los países democráticos en años venideros. La intromisión electoral, las campañas de desinformación y la seguridad de la infraestructura de votación se consideran áreas de preocupación cuando se trata de propagar influencia política en países extranjeros. Mediante la explotación de la difusión de los medios cibernéticos, algunos países extranjeros pueden continuar intentando socavar las instituciones democráticas y la formulación de políticas en la región. El cambio de opiniones públicas a través de los medios en línea se ha convertido en una parte persistente de la política contemporánea que se acentúa más durante la temporada electoral y las estructuras para abordarlo deberían estar operando antes de las elecciones.

Un enfoque regional para armonizar el nivel de las capacidades de ciberseguridad

El avance de las políticas de ciberseguridad a nivel regional debería comenzar por el desarrollo de elementos básicos nacionales. Una estrategia nacional de ciberseguridad podría funcionar como el principal instrumento de sensibilización y planificación en los diferentes Estados. Las estrategias de ciberseguridad existentes podrían ofrecer una variedad de ejemplos y lecciones que se pueden aprender.

Algunos de los países que lanzaron sus estrategias de ciberseguridad en la década del 2000 han sido testigos de primera mano de los avances que se han producido con el tiempo, con una visión estratégica sobre ciberseguridad. En Estonia la ciberseguridad se ha convertido en parte del trabajo diario y constante de diferentes ministerios e instituciones estatales. Su efecto principal ha sido lograr la coordinación de políticas intraestatales profundamente arraigadas dentro de los marcos de la formulación de políticas estratégicas del Estado. Mientras que el énfasis en la primera estrategia de ciberseguridad de Estonia surgió de un caso de campaña híbrida debido a los eventos de 2007 ocurridos en Tallin y se convirtió en parte de la respuesta a la crisis, las dos estrategias posteriores se han centrado más en fortalecer la capacidad y la resiliencia cibernética.

El desarrollo de una política de ciberseguridad es un trabajo incesante. Entre otros objetivos estratégicos, la tercera estrategia de seguridad cibernética de Estonia (2019-2021) ha abordado la educación cibernética como parte de las áreas futuras donde se deberán realizar más inversiones. La dimensión cibernética también se incluyó en la regulación nacional de respuesta a crisis del país. Algunas de las mejores prácticas que tenemos para continuar el trabajo a nivel nacional involucran contar con una mejor coordinación nacional y mecanismos de intercambio de información; superar las brechas entre el nivel de expertos y los principales encargados de la toma de decisiones nacionales en los sectores público y privado; y crear instituciones y estructuras de coordinación de seguridad cibernética. Estas prácticas siguen siendo parte de nuestro trabajo continuo hoy.

Como las actividades maliciosas habilitadas por el ciberespacio pueden propagarse fácilmente de un país a otro, las investigaciones no pueden ser efectivas sin cooperación internacional. Como sabemos, un número cada vez mayor de nuestros sistemas nacionales de información e infraestructura crítica dependen de la seguridad de nuestras redes. Una estrategia de seguridad cibernética a nivel de todo el gobierno, que incluya posibles medidas preventivas, legislación nacional para abordar el delito cibernético y la cooperación operativa internacional entre los Estados, debería ser uno de los requisitos más importantes para evitar actividades que exploten las vulnerabilidades críticas de la infraestructura.

Formas de cooperación regional en América Latina y el Caribe

Una mayor cooperación regional para desarrollar una visión compartida y aprender de las mejores prácticas de otros Estados es clave para armonizar las capacidades de ciberseguridad nacionales. Varios Estados Miembros de la OEA han adoptado con éxito una legislación penal nacional, que significa contar con disposiciones para delitos relacionados con la informática, así como estrategias de ciberseguridad. Además de las disposiciones legales, muchos Estados ya se han adherido al Convenio de Budapest sobre Ciberdelincuencia. Desde la perspectiva nacional e internacional, el Convenio de Budapest ofrece un marco legal internacional integral y confiable para combatir el delito cibernético, y durante las casi dos décadas de su existencia, se ha convertido en un instrumento de referencia global. Por lo tanto, el Convenio de Budapest se ha transformado en un modelo preferido para muchos países, en términos de la promoción de su propia legislación nacional, en la construcción de la cooperación internacional y en cuanto al intercambio de pruebas electrónicas.

Dado que las amenazas cibernéticas son cada vez más sofisticadas, es responsabilidad de los Estados garantizar que las actividades de los perpetradores

no pasen desapercibidas. Por lo tanto, las iniciativas políticas y legislativas, junto con las medidas de creación de capacidad, son algunos de los elementos clave para combatir las amenazas derivadas del ciberespacio, incluida la conducta de los delincuentes. Por ello, la implementación de legislación relevante y la adopción de métodos estratégicos respaldarán la efectividad del trabajo realizado para la obtención de justicia penal a nivel nacional y la cooperación internacional entre los Estados de la OEA bajo el auspicio de las disposiciones del derecho internacional.

La creación de conciencia sobre las amenazas cibernéticas a nivel político es sólo el primer paso para desarrollar capacidades de seguridad cibernética más armonizadas en una región. La adopción e implementación de políticas nacionales de ciberseguridad conduciría a un desarrollo económico y político más seguro y estable en la región y aportaría a la estabilidad local y global del ciberespacio. Los actores regionales de América Latina y el Caribe, como la OEA, ya han contribuido a este proceso. Ahora es el momento de acometer una implementación más práctica.

Construyendo capacidades de ciberseguridad: El reto de la educación terciaria en América Latina y el Caribe

Prof. Pablo Ruiz Tagle-Vial
Decano, Facultad de Derecho, **Universidad de Chile**
Prof. Daniel Álvarez Valenzuela
Coordinador Académico, Centro de Estudios en Derecho Informático, Facultad de Derecho, **Universidad de Chile**

En los últimos años, diversos países de América Latina y el Caribe han sido testigos y también víctimas del incremento de las amenazas a la ciberseguridad, las cuales han afectado no sólo a instituciones públicas y del sector privado, sino también a ciudadanos de estos países. Este incremento se contabiliza tanto en el número de ataques registrados, como en la intensidad y sofisticación que han tenido.

El diagnóstico sobre las causales de este incremento es por todos conocido. Ya en la versión previa de este informe –publicado en 2016–[29] se daba cuenta del crecimiento de los niveles de penetración de las tecnologías digitales en la región y de los incipientes procesos de transformación digital que diversos países están llevando a cabo; los cuales, junto con la dependencia que la tecnología genera, son factores que han incidido decisivamente en el incremento de los riesgos y amenazas a la seguridad digital que los países de la región enfrentan.

Sumado a lo anterior, la versión previa de este informe también nos dio luces sobre lo escasamente preparados que se encontraban nuestros países para enfrentar estos nuevos escenarios de riesgos para resguardar la seguridad de sus habitantes y, en consecuencia, para resguardar y proteger efectivamente sus derechos, cuestión que se manifestaba en todas las dimensiones analizadas con el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM) desarrollado por el Centro Global de Capacidad en Seguridad Cibernética (GCSCC, por sus siglas en inglés) de la Universidad de Oxford.[30]

En la presente versión del informe, el nivel de madurez de los países en materia de educación, formación y desarrollo de capacidades sigue siendo extremadamente dispar, un hecho que está ligado a las importantes desigualdades económicas, sociales y culturales que subsisten entre los diversos países de América Latina y el Caribe, tal como veremos a continuación.

Por una parte, tenemos un grupo de países –que representa un tercio del total de países analizados– que en los últimos dos años han incrementado considerablemente sus índices en áreas como educación y capacitación, alcanzando niveles de madurez de nivel medio. Se destacan los casos de

Uruguay, que logró un nivel de madurez estratégico en capacitación profesional, y de Guyana, que incrementó sus índices en casi todos los ámbitos evaluados.

En este grupo de países se encuentran además Argentina, Chile, Colombia, Costa Rica, México, Paraguay, República Dominicana y Trinidad y Tobago, que son, coincidentemente, los países que casi en su totalidad cuentan con una política o estrategia nacional de ciberseguridad y que han desarrollado una oferta educativa, tanto pública como privada, que considera la formación especializada en ciberseguridad tanto desde el punto de vista técnico como jurídico.

Por otra parte, el presente reporte da cuenta de un escaso o nulo avance en el nivel de madurez de dos tercios de los países de América Latina y el Caribe en materia de educación, capacitación y desarrollo de habilidades en ciberseguridad. En estos países, la oferta de formación especializada en seguridad digital es inexistente o tiene carácter de incipiente, y usualmente considera sólo la dimensión técnica de la ciberseguridad.

Estos resultados nos invitan a repensar las estrategias que deberían adoptar cada uno de estos países y sus organizaciones públicas y privadas para mejorar sus actuales niveles de madurez, junto con la promoción de mecanismos de cooperación internacional, tanto a nivel regional como subregional. De esta forma, aquellos países que han logrado avanzar en densificar y mejorar su oferta educacional podrían, por ejemplo, apoyar a aquellos que están en una situación de desventaja.

Como tantas veces se ha dicho, el factor humano es y seguirá siendo un elemento fundamental en cualquier estrategia que pretenda ser exitosa, y las instituciones de educación superior desempeñan un rol esencial en este aspecto. Desde nuestro punto de vista, los desafíos que enfrentamos son múltiples y requieren soluciones complejas y diferenciadas según la realidad política, económica y social de los diversos países que forman parte de América Latina y el Caribe.

Para los países que se encuentran en los primeros niveles de madurez de este reporte, parecería ineludible avanzar en el desarrollo de una oferta especializada de estudios de grado y posgrado en Tecnologías de la Información (TI) y Ciberseguridad, con énfasis en el desarrollo de las capacidades necesarias para una formación técnica de calidad. Como se ha realizado en el pasado, la cooperación internacional aquí puede cumplir un rol clave, al igual que las alianzas público-privadas (APP) que permitan identificar y priorizar las necesidades más importantes para cada país.

Por su parte, aquellos países que están en la fase formativa o han transitado hacia la fase consolidada, además de fortalecer y ampliar la oferta especializada de estudios de grado y posgrado, deberían iniciar procesos de innovación curricular para la tranversalización de los contenidos mínimos que cualquier profesional tendría que adquirir en materia de TI y seguridad digital, incluyendo, por cierto, la perspectiva de género que permita además superar otras brechas que se han identificado en los últimos años. Entre los contenidos mínimos podemos mencionar la gestión de riesgos, y la regulación de tecnologías como la que atañe a la protección de datos personales, a los delitos informáticos, etc.

Asimismo, se requiere avanzar en el desarrollo de programas multidisciplinarios que permitan la formación de profesionales integrales que comprendan el quehacer de su propia disciplina desde una perspectiva más amplia. Esto resulta imprescindible en este tránsito hacia una sociedad digital que varios de nuestros países están experimentando, lo que requiere no sólo profesionales y técnicos especialistas del área de las TI y la ciberseguridad sino también profesionales de las ciencias sociales, como el derecho, la ciencia política, la economía, la comunicación social, por mencionar algunos. En este ámbito no podemos dejar de citar los programas de postítulo que la Universidad de Chile ofrece desde hace décadas en su Escuela de Ingeniería[31] y más recientemente desde nuestra Facultad de Derecho,[32] iniciativas que desde su diseño han considerado la multidisciplinariedad como un factor imprescindible en la formación especializada de posgrado.

El grupo de países que está en el nivel consolidado requiere un compromiso mayor de sus universidades e institutos superiores con la investigación y el desarrollo, el cual –a través de esfuerzos públicos y privados– debe orientarse hacia diversos aspectos relacionados con la ciberseguridad, como, por ejemplo, la criptografía y sus diversas aplicaciones, el estudio de modelos y técnicas de análisis de incidentes, la utilización de inteligencia artificial y redes neuronales en la solución de problemas complejos, las posibilidades de utilización de la seguridad, entre otros. Esta investigación se podría nutrir de la información recolectada por las autoridades nacionales de ciberseguridad, por el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, según sus siglas en inglés) de las Américas que gestiona la Organización de los Estados Americanos (OEA) y por las empresas especializadas que operan en cada país.

El círculo virtuoso que es posible generar a partir de este intercambio continuo de información, adoptando las medidas de confidencialidad y seguridad técnicas y jurídicas necesarias, permitirá que alguno de estos países pueda transitar hacia niveles de madurez estratégicos y dinámicos. De esta forma, la oferta de educación, capacitación e investigación podrá orientarse a las necesidades reales y los objetivos estratégicos de cada país, según las definiciones adoptadas en sus respectivas políticas o estrategias nacionales de ciberseguridad, manteniendo un sistema de identificación y gestión de riesgos actualizado según los tipos de amenazas y vulnerabilidades que los afecten.

Finalmente, el desafío que enfrentamos como instituciones de educación superior debería ser asumido, al menos por las instituciones públicas o estatales, como un desafío-país cuya superación nos permitirá contar con un ciberespacio libre, abierto, seguro y resiliente, en directo beneficio de las personas y del pleno ejercicio de sus derechos fundamentales en el ciberespacio.

El Modelo de Madurez de la Capacidad de Ciberseguridad

El Centro Global de Capacidad en Seguridad Cibernética *(GCSCC, por sus siglas en inglés)*[33] de la Universidad de Oxford, en consulta con más de 200 expertos internacionales provenientes de gobiernos, la sociedad civil y la academia, desarrolló el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones *(CMM, por sus siglas en inglés)*. Se trata de un modelo que busca ofrecer una evaluación del nivel de madurez de las capacidades de ciberseguridad de un país, asignándole una etapa específica que corresponde a su grado de logro en materia de ciberseguridad. Las cinco etapas de madurez, que se fijan por medio de una evaluación, van desde la más básica *(inicial)* hasta la más avanzada *(dinámica)*.

Las cinco etapas se definen[34] como sigue (véase el gráfico 1):

- ***Inicial:*** En esta etapa no existe madurez en ciberseguridad o bien se encuentra en un estadio muy embrionario. Puede haber discusiones iniciales sobre el desarrollo de capacidades de ciberseguridad, pero no se han tomado medidas concretas. Falta evidencia observable de la capacidad de seguridad cibernética.

- ***Formativa:*** Algunos aspectos han comenzado a crecer y formularse, pero pueden ser ad hoc, desorganizados, mal definidos, o simplemente nuevos. Sin embargo, se puede demostrar claramente evidencia de este aspecto.

- ***Consolidada:*** Los indicadores están instalados y funcionando. Sin embargo, no se le ha dado mucha consideración a la asignación de recursos. Se han tomado pocas decisiones acerca de los beneficios con respecto a la inversión relativa en este aspecto. Pero la etapa es funcional y está definida.

- ***Estratégica:*** En esta etapa se han tomado decisiones sobre qué indicadores de este aspecto son importantes y cuáles lo son menos para la organización o el Estado en particular. La etapa estratégica refleja el hecho de que estas elecciones se han realizado condicionadas por las circunstancias particulares del Estado o de las organizaciones.

- ***Dinámica:*** En esta etapa existen mecanismos claros para alterar la estrategia en función de las circunstancias prevalentes, como la sofisticación tecnológica del entorno de amenaza, el conflicto global o un cambio significativo en un área de preocupación (por ejemplo, delito informático o privacidad). Las organizaciones dinámicas han desarrollado métodos para cambiar las estrategias con calma. Sin embargo, la rápida toma de decisiones, la reasignación de recursos y la atención constante al entorno cambiante son características de esta etapa.

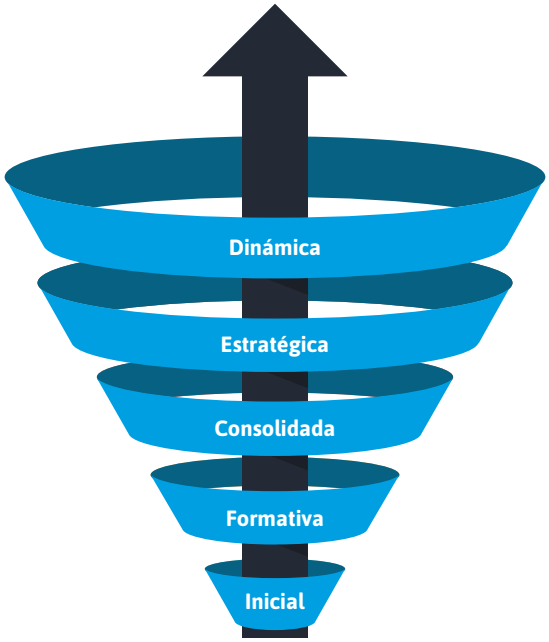


Gráfico 1: Las cinco etapas de madurez de la capacidad de ciberseguridad

La evaluación de los niveles de madurez se divide en cinco dimensiones (véase el gráfico 2) que corresponden a aspectos esenciales y específicos de la ciberseguridad, entre ellos: (i) política y estrategia de ciberseguridad; (ii) cultura cibernética y sociedad; (iii) educación, capacitación y habilidades en ciberseguridad; (iv) marcos legales y regulatorios; y (v) estándares, organizaciones y tecnologías. Estos se subdividen en un conjunto de factores que describen y definen lo que significa poseer capacidad de seguridad cibernética en cada factor, e indican cómo mejorar la madurez.

La siguiente tabla detalla cada uno de los factores que comprenden las dimensiones:

Dimensión 1 Política y Estrategia de Ciberseguridad (Diseño de estrategia y resiliencia de ciberseguridad)	**D1.1** Estrategia Nacional de Ciberseguridad **D1.2** Respuesta a Incidentes **D1.3** Protección de Infraestructura Crítica (IC) **D1.4** Gestión de Crisis **D1.5** Defensa Cibernética **D1.6** Redundancia de Comunicaciones
Dimensión 2 Cultura Cibernética y Sociedad (Fomentar una cultura de ciberseguridad responsable en la sociedad)	**D2.1** Mentalidad de Ciberseguridad **D2.2** Confianza y Seguridad en Internet **D2.3** Comprensión del Usuario de la Protección de Información Personal en Línea **D2.4** Mecanismos de Presentación de Informes **D2.5** Medios y Redes Sociales
Dimensión 3 Educación, Capacitación y Habilidades en Ciberseguridad (Desarrollo del conocimiento de ciberseguridad)	**D3.1** Sensibilización **D3.2** Marco para la Educación **D3.3** Marco para la Formación Profesional

Dimensión 4 Marcos Legales y Regulatorios (Creación de marcos legales y regulatorios efectivos)	**D4.1** Marcos Legales **D4.2** Sistema de Justicia Penal **D4.3** Marcos de Cooperación Formal e Informal para Combatir el Delito Cibernético
Dimensión 5 Estándares, Organizaciones y Tecnologías (Control de riesgos a través de estándares, organizaciones y tecnologías)	**D5.1** Adhesión a los Estándares **D5.2** Resiliencia de Infraestructura de Internet **D5.3** Calidad del Software **D5.4** Controles Técnicos de Seguridad **D5.5** Controles Criptográficos **D5.6** Mercado de Ciberseguridad **D5.7** Divulgación Responsable

Gráfico 2: Las cinco dimensiones del CMM

Los datos primarios utilizados en este reporte se recopilaron mediante un instrumento en línea que se distribuyó a todos los Estados Miembros de la OEA. Tras la recopilación de datos del instrumento en línea, se hizo una referencia cruzada con la investigación documental y la consulta con Estados Miembros para la validación de los resultados declarados. Utilizando el CMM como línea de base, este reporte presenta los resultados de la revisión de la capacidad de seguridad cibernética de la región de América Latina y el Caribe en base a los datos validados a diciembre de 2019. La sección de cada país concluye con una tabla resumen que presenta las cinco dimensiones y su respectivo nivel de madurez en función de los reportes de los años 2016 y 2020.

Los valores de 2016 utilizados se actualizaron para reflejar el Modelo de madurez de la capacidad de ciberseguridad para la edición revisada de las naciones (CMM). Todas las evaluaciones realizadas en la publicación de 2016 siguen siendo las mismas, excepto la inclusión de nuevos indicadores.

Perfiles de países

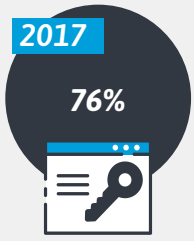
Antigua y Barbuda

Habitantes
*Ref: Banco Mundial**

Abonos a teléfonos celulares
*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet
*Ref: ITU***



Si bien Antigua y Barbuda no ha adoptado formalmente una estrategia nacional de ciberseguridad ni ha establecido un CSIRT nacional, se han tomado medidas importantes para abordar la ciberseguridad a nivel nacional. En 2017, el gobierno creó la posición de "Director de Ciberseguridad" en el Ministerio de Información, Radiodifusión, Telecomunicaciones y Tecnología de la Información y nombró un director en noviembre de ese mismo año.

En cuanto a la participación en actividades de ciberseguridad, Antigua y Barbuda participó en la "II Reunión de partes interesadas del Caribe sobre ciberseguridad y ciberdelincuencia" en marzo de 2016, organizada por la Unión de Telecomunicaciones del Caribe (UTC), en conjunto con la Secretaría de la Mancomunidad, en la que se presentó un plan de acción regional de ciberseguridad.[35] El plan de acción incluye áreas como capacitación, legislación, capacidad técnica y cumplimiento de la ley.[36] Además, en mayo de 2017, Antigua y Barbuda organizó la Semana y el Simposio de las TIC y, entre los temas tratados, se consideraron la ciberseguridad y el delito cibernético.[37] Antigua y Barbuda igualmente colabora con organizaciones tanto regionales como internacionales, tales como INTERPOL y CARICOM IMPACS para la investigación del cibercrimen. Además, el Ministerio de Información, Radiodifusión, Telecomunicaciones y Tecnología de la Información tenía en su presupuesto para el año fiscal 2017 una referencia a la contratación de especialistas para abordar cuestiones de ciberseguridad y la creación de un equipo de respuesta a incidentes de ciberseguridad.[38]

Aunque escasa, Antigua y Barbuda tiene una prestación de servicios de seguridad cibernética por parte del sector privado. Sin embargo, la participación de este sector y también de la sociedad civil en temas de seguridad cibernética es limitada, aunque algunas empresas han comenzado a darle prioridad a la ciberseguridad al identificar prácticas de alto riesgo y recibir capacitación en ciberseguridad.[39]

Antigua y Barbuda forma parte de la campaña internacional STOP.THINK.CONNECT que promueve prácticas seguras en Internet.[40] En cuanto a la disponibilidad de capacitación formal para la ciberseguridad, aunque no existen títulos especializados en ciberseguridad, el Instituto Internacional de Tecnología de Antigua y Barbuda sí ofrece títulos en informática y ciencias de la computación.[41] Asimismo, en junio de 2013 el gobierno lanzó una política nacional de TIC en educación para el país.

Antigua y Barbuda ha contado con legislación sobre delitos electrónicos y protección de datos desde 2013. Más específicamente, la Ley de delitos electrónicos establece la "prevención y el castigo de delitos electrónicos y asuntos relacionados".[42] Además, la Ley de Protección de Datos también se promulgó en 2013 y prevé la protección de la información privada almacenada en bases de datos públicas y privadas. Esta ley cubre tanto la protección de datos personales como la transparencia en el procesamiento de los mismos.[43]

También ha habido un progreso significativo en ofrecer a los ciudadanos un número limitado de servicios gubernamentales en línea, como la renovación de la licencia de conducir.[44] Además, en enero de 2018 Antigua y Barbuda organizó la Cumbre y el Simposio de Gobierno del siglo XXI, sobre las formas más eficaces de utilizar las TIC para proporcionar y prestar servicios a sus ciudadanos.[45] Esto demuestra la voluntad de seguir avanzando en el desarrollo del gobierno electrónico.

Indicadores: Antigua y Barbuda

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3

2016 | 2020

Formación, Capacitación y Habilidades de Seguridad Cibernética

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4

2016 | 2020

Marcos Legales y Regulatorios

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5

2016 | 2020

Estándares, Organizaciones y Tecnologías

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

Argentina

Habitantes

*Ref: Banco Mundial**

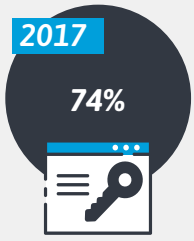
Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***



En los últimos años se han tomado numerosas medidas para implementar políticas y realizar cambios administrativos y regulatorios para los sectores de telecomunicaciones, Internet y tecnología en Argentina. En 2017, el Decreto 577/2017 creó el "Comité de Ciberseguridad" dependiente de la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros y con representantes del Ministerio de Defensa y el Ministerio de Seguridad con el objetivo de desarrollar una estrategia nacional de seguridad cibernética.[46] Asimismo, se encuentra en trámite un proyecto de Acto Administrativo para ampliar la composición del Comité de modo de incluir la Secretaría de Asuntos Estratégicos de la Jefatura de Ministros, el Ministerio de Justicia y Derechos Humanos y el de Relaciones Exteriores y Culto.[47] Otros cambios administrativos incluyen la creación de la Subsecretaría de Ciberdefensa en el Ministerio de Defensa y de la Dirección de Cibercrimen en el Ministerio de Seguridad, así como el establecimiento de unidades fiscales especializadas en cibercrimen a nivel nacional y en la jurisdicción de la Ciudad Autónoma de Buenos Aires.[48] La Estrategia Nacional de Ciberseguridad se aprobó mediante la resolución publicada en el Boletín Oficial (829/2019) y se creó la Unidad Ejecutora, en el marco del Comité de Ciberseguridad y bajo la autoridad de la Secretaría de Modernización de la Nación e invitó a las Provincias y Ciudad Autónoma de Buenos Aires para adherirse a la Estrategia.

A través de un préstamo basado en políticas (policy-based loan o PBL, por sus siglas en inglés) aprobado en 2019, el BID brinda su apoyo al gobierno argentino en la implementación de políticas relacionadas con infraestructura crítica, seguridad de los datos personales y buenas prácticas en el uso de las TIC, con acciones puntuales hacia el fortalecimiento de las capacidades nacionales en ciberseguridad.[49] Además, para fortalecer los lazos internacionales y sus políticas de seguridad cibernética, Argentina se asoció con Estados Unidos para establecer un grupo de trabajo que mejorará la cooperación en materia de seguridad cibernética.[50] Asimismo, se han firmado acuerdos con España y Chile, y se encuentran bajo análisis memorandos de entendimiento con China, República de Corea y Rusia.[51]

Argentina también ha establecido un Programa Nacional de Infraestructura de Información Crítica y Ciberseguridad (ICIC), bajo la Resolución JGM N° 580/2011, para crear y adoptar un marco regulatorio orientado a definir y proteger la infraestructura estratégica y crítica de los sectores público y privado, así como organizaciones interjurisdiccionales.[52] ICIC es, entre otras cosas, el hogar del CSIRT nacional. Aunque el ICIC-CERT no es miembro de CSIRT Américas, que nuclea los esfuerzos liderados por la OEA, BA-CSIRT (CSIRT de la ciudad de Buenos Aires) es miembro y puede beneficiarse de la red.

Aunque ICIC colabora con el sector privado, un informe de PwC encontró que el 53% de las empresas encuestadas en Argentina no tiene una estrategia general de seguridad de la información, el 61% no tiene un plan de contingencia sobre cómo responder frente a un incidente y solo el 46% cuenta con un programa de seguridad para los empleados.[53]

Hay varias oportunidades para que los argentinos continúen su educación en seguridad cibernética, en universidades públicas y privadas, y también ofrecidos por la sociedad civil. Además, BA-CSIRT brinda capacitaciones y charlas de sensibilización para enseñar a los interesados sobre seguridad cibernética y el uso de las TIC. En cuanto a la legislación, Argentina promulgó la Ley N° 26.388 en 2008, que modificó el código penal para incluir el delito cibernético.[54] Además, la Ley N° 26.904 incorpora la figura del grooming en el Código Penal. La afectación de infraestructura crítica y otros delitos están tipificados en un proyecto de ley próximo a ser enviado al Congreso Nacional.[55] Por otra parte, la adhesión de Argentina al Convenio de Budapest sobre Ciberdelincuencia del Consejo de Europa fue ratificada en junio de 2018.[56]

Argentina también tiene la Ley N° 25.326 de 2000 que cubre la protección de datos personales.[57] De hecho, Argentina ha sido uno de los primeros países de las Américas en tener un marco regulatorio para la protección de datos personales, y lo ha fortalecido y actualizado desde entonces. Es uno de los pocos países de las Américas que participa en el "Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" del Consejo de Europa (CdE).[58] En 2018 se remitió un proyecto de Ley modificatorio de la Ley N° 25.326 del año 2000 enfocado en actualizar el marco normativo vigente.

Argentina tiene dos decretos sobre gobierno electrónico. El Decreto N° 378/2005 describe la estrategia de gobierno electrónico para aumentar las TIC a fin de mejorar la entrega y prestación de servicios gubernamentales.[59] El segundo y más reciente es el Decreto N° 87/2017 para la creación de una plataforma digital orientada a facilitar la interacción entre las personas y el Estado.[60] El Decreto N° 996/2018 ha creado la "Agenda Digital Argentina", la cual tiene entre sus objetivos "desarrollar capacidades en ciberseguridad para generar confianza en los entornos digitales".[61]

Indicadores: Argentina

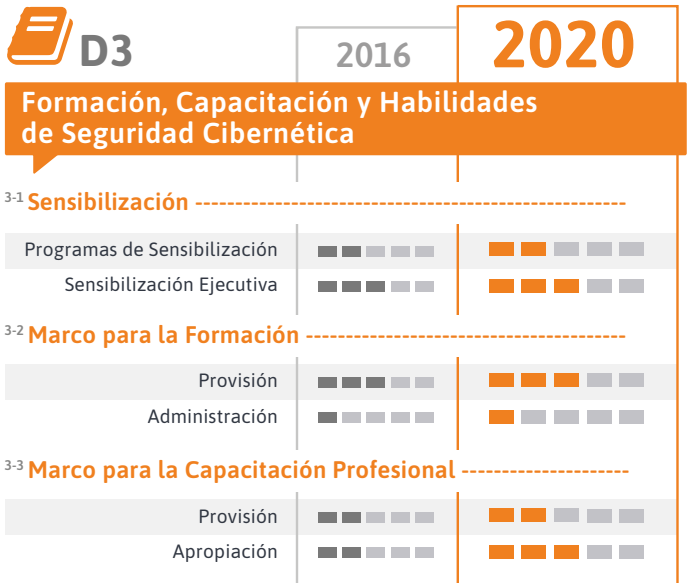
D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética



D4 Marcos Legales y Regulatorios

D5 Estándares, Organizaciones y Tecnologías

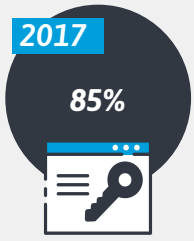
Bahamas
(Mancomunidad de las)

Habitantes
*Ref: Banco Mundial**

Abonos a teléfonos celulares
*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet
*Ref: ITU***



El Gobierno de la Mancomunidad de las Bahamas inició las gestiones para desarrollar en 2014 una estrategia nacional de seguridad cibernética que contemplaba la creación del equipo nacional de respuesta a incidentes de seguridad informática (CSIRT).[62] La puesta en marcha de la estrategia de ciberseguridad y el establecimiento de un CSIRT nacional son acciones críticas, dado que la ciberdelincuencia ha aumentado en los últimos dos años, a pesar de que el país ha visto una disminución general de los delitos graves.[63] Aunque la estrategia aún no se ha adoptado, en 2017 la Policía de Bahamas combinó la Sección de Rastreo y Decomiso de la Unidad de Control de Drogas y la Sección de Delitos Comerciales bajo la Unidad Central de Detectives para crear la nueva Unidad de Ciberseguridad.[64] Esta unidad ahora le entrega a Bahamas un actor centralizado encargado de proteger el ciberespacio del país.

Después de que Bahamas ocupase el puesto 129 en el Índice de Ciberseguridad Global (CGI, por sus siglas en inglés), los líderes del sector privado manifestaron la necesidad de mejorar la preparación cibernética en el país.[65] Existen algunos proveedores de servicios de ciberseguridad del sector privado y también se cuenta con capacitación, pero persiste la necesidad general de que el sector privado tenga una mayor participación para que se proteja activamente de los ataques cibernéticos.

En 2003 Bahamas aprobó legislación tanto para la ciberdelincuencia como para la protección de datos, a saber, la Ley de uso indebido de computadoras y la Ley de protección de datos. La primera proporciona una descripción general de los actos delictivos, así como los aspectos procesales de enjuiciar el delito cibernético,[66] mientras que la segunda abarca las definiciones y los trámites que deben cumplir los controladores de datos privados y públicos.[67] Además, el gobierno también ha implementado la Ley de Transacciones y Comunicaciones Electrónicas (2006).

El BID ha promovido y alentando el fortalecimiento de las políticas y acciones de seguridad cibernética en Bahamas. Así, como resultado de la operación de préstamo "Transformación digital del gobierno para fortalecer la competitividad", aprobada en 2018, el Banco está brindando apoyo técnico y financiero a la agenda digital del país, que incluye un componente específico sobre ciberseguridad.[68]

El gobierno electrónico forma parte de la Declaración de Política de las Bahamas sobre Comercio Electrónico y la Agenda Digital Bahameña de 2003 del Ministerio de Finanzas con el objetivo de facilitar el intercambio de información entre todos los ministerios y agencias relacionadas.[69] Además, el borrador de 2016 del Plan Nacional de Desarrollo 2040 va un paso más allá y describe la necesidad de contar con una "estrategia de ventanilla única de servicio al ciudadano".[70] Actualmente, el gobierno ofrece algunos servicios en línea a través del portal de servicios electrónicos para empresas, ciudadanos/residentes y no residentes.[71]

Los programas educativos centrados en la ciberseguridad no son comunes en Bahamas. Si bien el Institute of Business and Technology ofrece un título en Tecnología de la Información, no existen títulos específicos para ciberseguridad.[72] El Institute of Financial Services de Bahamas también brinda un Certificado Avanzado en Ciberseguridad. Sin embargo, este programa solamente dura tres meses.[73] Finalmente, en términos de gestiones relacionadas con la sensibilización nacional, en mayo de 2018 la Cámara de Comercio y la Confederación de Empleadores de las Bahamas (BCCEC, por sus siglas en inglés) organizó un Foro de Ciberseguridad y en junio de 2018 el Banco Central de las Bahamas llevó adelante un seminario sobre seguridad de la información para aumentar la concienciación en ciberseguridad y delito informático, entre otros objetivos.[74] En diciembre de 2019, el gobierno de las Bahamas y el BID realizaron una conferencia para compartir experiencias internacionales en ciberseguridad.

Indicadores: Bahamas (Mancomunidad de las)

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

D4 Marcos Legales y Regulatorios

D5 Estándares, Organizaciones y Tecnologías

Barbados

Habitantes

*Ref: Banco Mundial**

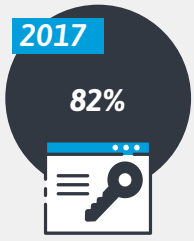
Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***



El Gobierno de Barbados se encuentra en las primeras etapas de la discusión con partes interesadas para lograr el desarrollo de una estrategia nacional de ciberseguridad.[75] Este proceso recibe aportes de diferentes partes interesadas, lo que permite avanzar para delinear una estrategia que satisfaga las necesidades de un gran número de partes. Además, a pesar de no tener una estrategia de ciberseguridad, Barbados cuenta con un CSIRT nacional bajo la Unidad de Telecomunicaciones del Ministerio de Innovación, Ciencia y Tecnología Inteligente. El CSIRT también es miembro de CSIRT Américas y se beneficia de la naturaleza colaborativa de la plataforma. El BID está cooperando con el gobierno de Barbados para apoyar sus iniciativas y políticas de seguridad cibernética, que fortalecerán la capacidad del país para gestionar las amenazas en este campo. A su vez, como resultado de la operación de préstamo "Programa de Modernización del Sector Público", aprobada en noviembre de 2019, el BID está brindando apoyo técnico y financiero a la agenda digital del país, que incluye apoyo específico sobre ciberseguridad.[76]

Durante el Foro de Gobernanza de Internet realizado en Barbados en junio de 2017, se evidenció que se necesitaban más campañas de concientización para los ciudadanos, ya que hubo un consenso general en cuanto a que los ciudadanos pueden no ser conscientes de las amenazas a las que están expuestos cuando utilizan Internet,[77] a pesar de los esfuerzos de las empresas del sector privado para hacer de la ciberseguridad una prioridad. Resulta interesante el hecho de que el Departamento de Procesamiento de Datos de Barbados, la Unidad de Telecomunicaciones, la Fuerza de Defensa y la Corporación de Inversión y Desarrollo de Barbados (BIDC, por sus siglas en inglés) unieron sus fuerzas con el Centro de Defensa Cibernética de Israel del Caribe (CICCD, por sus siglas en inglés) para crear conciencia sobre los riesgos en materia de ciberseguridad y la importancia que esto entraña para Barbados, debido al nuevo Reglamento Europeo de Protección de Datos (GDPR, por sus siglas en inglés) que podría resultar en grandes multas en casos de violaciones de ciberseguridad de cualquier institución que maneje información de ciudadanos de la UE.[78] Además, aunque hay algunos proveedores de servicios de ciberseguridad del sector privado, estos son limitados.[79]

Barbados cuenta con una ley de uso indebido de computadoras, que abarca el derecho sustantivo y procesal del delito cibernético.[80] Además, tiene actualmente el Proyecto de Ley para Protección de Datos que se aplicará a cualquier controlador de datos establecido en Barbados o que utilice equipos para procesar datos en dicho país.[81]

Desde 2006 Barbados lleva adelante una estrategia de gobierno electrónico con la visión de "empoderar a los ciudadanos al mejorar la conveniencia, la velocidad, la eficiencia, la calidad y la variedad de servicios e información entregados por el gobierno".[82] El gobierno electrónico también se menciona en parte del Plan Estratégico Nacional de las TIC 2010-2015 como una herramienta a través de la cual el gobierno puede convertirse en un modelo para el uso de las TIC en la prestación de servicios. El Plan de TIC también ordena la conformación de un comité directivo para supervisar la implementación de una política de gobierno electrónico.[83] En 2017 el Primer Ministro anunció que se estaba lanzando una estrategia de gobierno digital para proporcionar una hoja de ruta para el trabajo que aún debía realizarse para la digitalización de los servicios brindados por el gobierno.[84] Por lo tanto, Barbados está en camino de tener una ruta clara hacia la gobernabilidad electrónica. Además, ha realizado grandes avances en tecnologías líderes, como la tecnología de cadena de bloques (blockchain) y ha emprendido proyectos para la implementación de una red de pago digital.[85]

Por último, en 2017, uno de los siguientes pasos propuestos en el Foro de Gobernanza de Internet fue que la Internet Society, la Unidad de Telecomunicaciones y la Universidad de las Indias Occidentales se asociaran con el Ministerio de Educación, Ciencia y Tecnología para promover el conocimiento, desde una edad temprana, sobre cómo funciona Internet.[86] Con respecto a la educación superior, no hay títulos en ciberseguridad, aunque la Universidad de las Indias Occidentales sí ofrece títulos en ciencias de la computación.[87]

Indicadores: Barbados

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

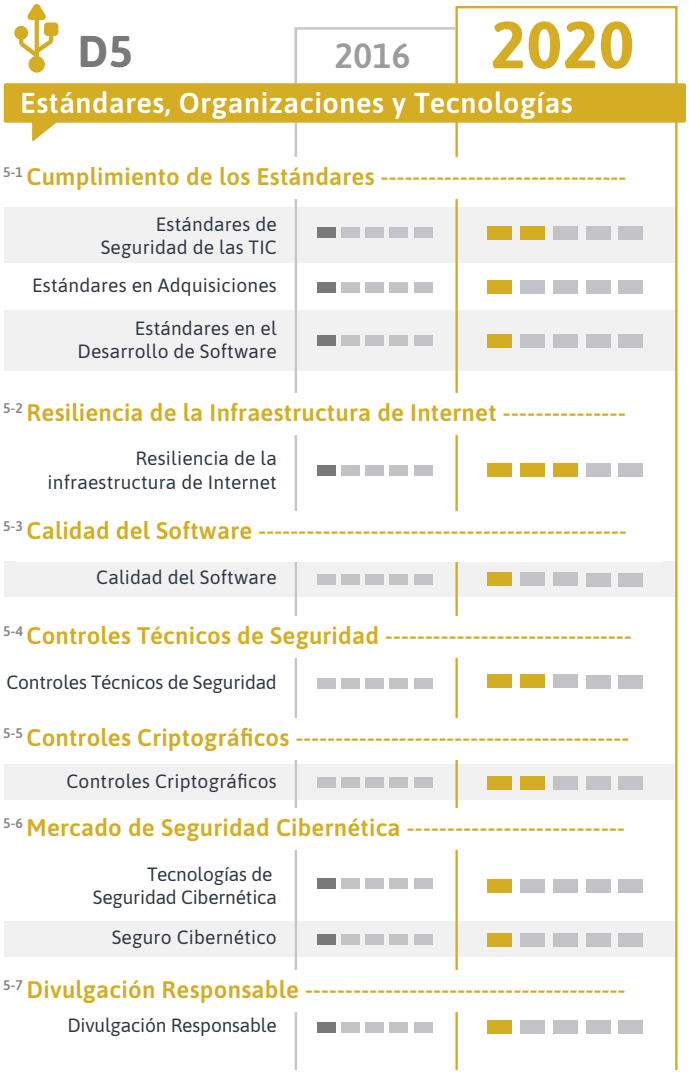
D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

D4 Marcos Legales y Regulatorios

D5 Estándares, Organizaciones y Tecnologías



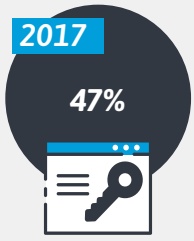
Belize

Habitantes
*Ref: Banco Mundial**

Abonos a teléfonos celulares
*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet
*Ref: ITU***



El gobierno de Belize está desarrollando actualmente una estrategia nacional de ciberseguridad mediante un proceso de múltiples partes interesadas llamado Grupo de Trabajo Nacional de Ciberseguridad (CSTF, por sus siglas en inglés). El CSTF se encarga de redactar la estrategia nacional de ciberseguridad mediante un proceso de consulta con las partes interesadas nacionales. Belice también ha desarrollado iniciativas nuevas relacionadas con las TI, incluida una política nacional que pretende aumentar los servicios de gobierno electrónico en el país. Con el propósito de crear conciencia sobre los riesgos y oportunidades relacionados con la ciberseguridad, la Comisión de Servicios Públicos de Belice (PUC, por sus siglas en inglés) organizó el Primer Simposio Nacional de Ciberseguridad en la Ciudad de Belice en abril de 2017. Uno de los objetivos del simposio fue identificar los pasos a seguir para poner en marcha una agenda de ciberseguridad y delito informático, con el objeto de garantizar que el país esté encaminado para comenzar el proceso.

Si bien existe una falta general de conciencia y participación del sector privado con respecto a la ciberseguridad en Belice, el simposio sobre ciberseguridad impulsó la toma de conciencia sobre su importancia. La participación, tanto de los agentes de la ley, de la comunidad judicial y jurídica, y del gobierno, como el sector privado, muestra la creciente relevancia que ha cobrado el tema para todas las partes.[88] Con respecto a la educación y capacitación en ciberseguridad, la oferta sigue en manos de las empresas del sector privado que brindan capacitación. No hay títulos de ciberseguridad en las universidades de Belize, aunque la Facultad de Ciencia y Tecnología sí ofrece una licenciatura en Tecnología de la Información.[89]

Con el fin de desarrollar una mentalidad de seguridad cibernética más fuerte, la Oficina Central de Tecnología de la Información (CITO) promueve la concientización sobre ciberseguridad entre las diferentes instituciones gubernamentales mediante el envío de encuestas mensuales con consejos sobre ciberseguridad y mejores prácticas. CITO también ha desarrollado una encuesta orientada a mejorar la notificación de incidentes cibernéticos entre las instituciones públicas. La Unidad de TI del Departamento de Policía de Belice también ha realizado importantes gestiones para mejorar sus capacidades de respuesta a incidentes mediante el establecimiento de un laboratorio forense. Actualmente, Belice ha promulgado cuatro leyes relacionadas con la ciberseguridad: (i) la Ley de telecomunicaciones; (ii) la Ley de prueba electrónica; (iii) la ley de propiedad intelectual; y (iv) la Ley de interceptación de comunicaciones, pero no tiene una legislación de privacidad y protección de datos.[90] Por otro lado, el Departamento de Policía de Belice está asociado a la Internet Watch Foundation para reportar casos de pornografía infantil. Sin embargo, la falta de una ley integral sobre delitos informáticos dificulta el enjuiciamiento de la ciberdelincuencia.[91] Es necesario actualizar la legislación del país y el marco de aplicación de la ley para poder tipificar como delito tales infracciones y procesarlas. En consecuencia, el gobierno ha estado analizando las leyes de delitos cibernéticos de países similares con la intención de desarrollar su propia legislación nacional, de modo que permita un enjuiciamiento más exhaustivo de los delitos informáticos.

Existe un plan integral de gobierno electrónico que detalla la hoja de ruta para el diseño y la implementación de la visión del gobierno electrónico del país en términos de “un gobierno integrado y colaborativo que brinde servicios públicos seguros y de calidad que conecten y empoderen a las personas”.[92] Sin embargo, hasta el momento no se ha implementado un portal de gobierno electrónico.

Indicadores: Belize

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

Bolivia

Habitantes

*Ref: Banco Mundial**

2017

11.192.854

Abonos a teléfonos celulares

*Ref: ITU***

2017

10.963.224

Personas con acceso a Internet

2017

4.906.083

Porcentaje de penetración de Internet

*Ref: ITU***

2017

44%

En los últimos años, Bolivia ha dado los primeros pasos para mejorar su seguridad cibernética desde que el Senado aprobó, en 2017, una ley que declara la puesta en marcha de una estrategia nacional de seguridad cibernética como una prioridad para el país.[93] Además, el Decreto Supremo N° 2.514 de septiembre de 2015 ya había establecido la creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), con el objetivo de liderar el proceso de desarrollo e implementación de e-gobierno y TIC para la transformación de la gestión pública y la construcción de la soberanía científica y tecnológica del Estado Plurinacional de Bolivia.[94]

Por su parte, a través del Decreto Supremo N° 2.514 se creó el Centro de Gestión de Incidentes Informáticos (CGII), cuya misión es proteger la información crítica del Estado y promover la conciencia de la seguridad para prevenir y responder a los incidentes de seguridad.[95] Además, el CGII forma parte de la plataforma CSIRT Américas desarrollada por la plataforma de la OEA cuyo objetivo es promover la colaboración, el intercambio, el estímulo y la participación en proyectos técnicos entre los CSIRT nacionales, de defensa, policiales y gubernamentales de los países miembros.[96]

Bolivia cuenta con la participación del sector privado en el ámbito de la seguridad cibernética. Hay varias compañías que ofrecen servicios de seguridad cibernética y, en general, existe consciencia acerca este ámbito por parte del sector privado.[97]

No hay legislación específica sobre los delitos informáticos o la protección de datos personales, pero sí existe una legislación vigente que se puede aplicar para hacer frente a los delitos informáticos,[98] el acceso a la información[99] y otros temas relacionados. Del mismo modo, en la Constitución de 2009 se incluyó un apartado sobre la protección de la privacidad.

En el ámbito del gobierno electrónico, Bolivia ha dado importantes pasos al desarrollar un plan para la implementación del gobierno electrónico entre 2017 y 2025. El objetivo de este plan es modernizar y hacer más transparente la gestión pública del país, generar y establecer un mecanismo tecnológico que aumente la participación y conciencia social a través del uso de las TIC por parte de la población.[100] Además, en 2018, una ley con el objeto de "establecer condiciones y responsabilidades para el acceso pleno y ejercicio de la ciudadanía digital" ha sido aprobada.[101]

Existen cursos de titulación en temas relacionados a la ciberseguridad. Además, hay algunas oportunidades en el sector público y privado para capacitación en gobierno digital y seguridad cibernética.

Indicadores: Bolivia

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia	1	2
Organización	1	2
Contenido	1	2
1-2 Respuesta a Incidentes		
Identificación de Incidentes	1	3
Organización	2	3
Coordinación	2	2
Modo de Operación	0	2
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación	1	2
Organización	1	1
Gestión de Riesgos y Respuesta	1	1
1-4 Manejo de Crisis		
Manejo de Crisis	1	1
1-5 Defensa Cibernética		
Estrategia	1	2
Organización	2	2
Coordinación	1	1
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones	1	1

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno	2	2
Sector Privado	2	2
Usuarios	1	1
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario	2	2
Confianza del Usuario en los Servicios de Gobierno Electrónico	2	2
Confianza del Usuario en los Servicios de Comercio Electrónico	2	2
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea	0	2
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia	0	2
2-5 Medios y Redes Sociales		
Medios y Redes Sociales	0	2

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

Brasil

Habitantes

*Ref: Banco Mundial**

Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***

El 5 de febrero de 2020, Brasil publicó el Decreto Federal N° 10.222[102] aprobando la Estrategia Nacional de Ciberseguridad (el Decreto). Más específicamente, este busca guiar a Brasil en la seguridad cibernética e incluye acciones para aumentar su resistencia frente a amenazas cibernéticas y fortalecer su desempeño a nivel internacional. Además, el Decreto crea un modelo de gobernanza centralizado para promover la coordinación entre los diferentes actores relacionados con la ciberseguridad, y establece un consejo nacional de ciberseguridad.

La madurez de la capacidad de Brasil para proteger la infraestructura crítica difiere entre los operadores públicos y privados en este ámbito. Todas las instituciones federales deben realizar evaluaciones de riesgo cibernético, que se actualizan anualmente en función de las lecciones aprendidas de los principales eventos. Las partes interesadas de infraestructura crítica públicas incluyen compañías de telecomunicaciones, transporte, energía e instituciones financieras, las que cooperan y coordinan a través de canales formales de comunicación con el Ministerio de Defensa. Existen políticas y procedimientos claramente definidos que todas las instituciones públicas deben seguir en función de la información proporcionada por la herramienta de conciencia situacional que posee el CERT nacional. El CERT nacional (CERT.br) continúa siendo la principal entidad responsable de manejar los informes de incidentes a nivel nacional y las actividades en las redes brasileñas.

Aún no se ha establecido un programa nacional de sensibilización sobre seguridad cibernética, dirigido por una organización designada (de cualquier sector) que aborde una amplia gama de datos demográficos. Sin embargo, el gobierno ha reconocido la necesidad de priorizar la ciberseguridad en todas sus instituciones y se percibe que son cada vez más los usuarios y las partes interesadas dentro de los sectores público y privado que tienen un conocimiento general sobre cómo se maneja la información personal en línea y emplean buenas prácticas (proactivas) de ciberseguridad para proteger su información personal en línea.

El Marco de Derechos Civiles de Brasil para Internet (Ley N° 12.965) (en portugués: Marco Civil da Internet) se desarrolló a través de un proceso de consulta de múltiples partes interesadas para regular el uso de Internet en Brasil mediante el establecimiento de principios, garantías, derechos y deberes para los usuarios de Internet. Sin embargo, Brasil no tiene una ley específica de protección de datos o privacidad, sino que se basa en varias disposiciones establecidas en la Constitución Federal,[103] el Código Penal de Brasil,[104] el Código de Protección al Consumidor[105] y el Marco de Derechos Civiles de Brasil para proteger la privacidad en Internet.

En particular, algunos aspectos de los procesos gubernamentales y las estructuras institucionales se han diseñado en respuesta a los riesgos para la seguridad cibernética, pero las iniciativas se basan principalmente en agencias líderes particulares. En general, la cultura de ciberseguridad en Brasil varía según las diferentes partes del país y los distintos sectores del gobierno y de la economía. El sector financiero y el de las TIC están más avanzados en ciberseguridad, debido a que son objetivos frecuentes y, por lo tanto, están invirtiendo más en ciberseguridad. Sin embargo, la sociedad en su conjunto aún carece de una mentalidad de ciberseguridad. Los usuarios pueden ser conscientes de los riesgos de seguridad cibernética, pero a menudo no actúan en consecuencia en sus prácticas cotidianas.

Los principales interesados en el gobierno y la industria han identificado la necesidad de mejorar la educación en ciberseguridad en escuelas y universidades. Las cualificaciones y la oferta de educadores están fácilmente disponibles en ciberseguridad.

Se ofrecen cursos especializados en informática a nivel universitario. Los profesionales del sector público asisten a las cualificaciones profesionales de las TI en el extranjero y reciben certificados de TIC registrados por instituciones internacionales como el Certificado de Seguridad de Sistemas de Información Profesional (CISSP) o el de Gerente de Seguridad de Información Certificado (CISM).

Por último, el gobierno federal cuenta con un marco de divulgación de vulnerabilidades. Las organizaciones han establecido procesos formales para difundir información automáticamente y el CERT nacional recibe esta información y proporciona informes completos sobre cómo abordar los incidentes.

Indicadores: Brasil

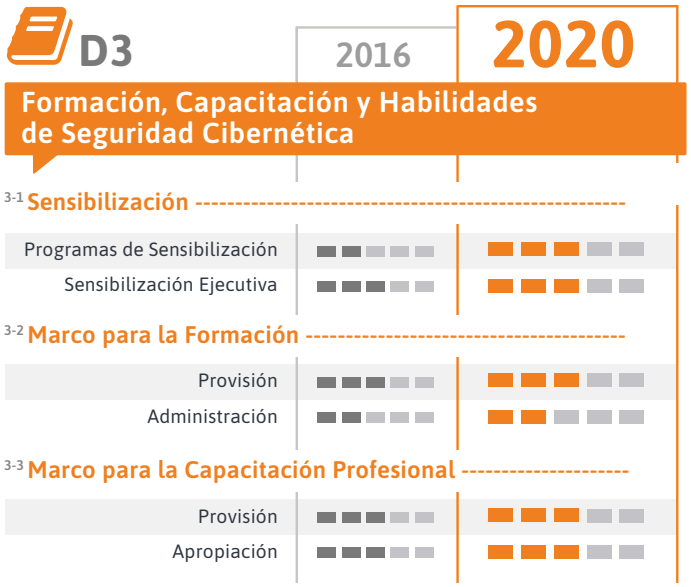
D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética



D4 Marcos Legales y Regulatorios

D5 Estándares, Organizaciones y Tecnologías

Chile

Habitantes

*Ref: Banco Mundial**

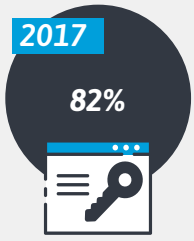
Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***



Chile presentó su estrategia nacional de seguridad cibernética en abril de 2017 con la idea de alcanzar los siguientes objetivos para el año 2022: (i) tener una infraestructura de información sólida y resiliente; (ii) garantizar los derechos de las personas en el ciberespacio por parte del Estado; (iii) desarrollar una estrategia de seguridad cibernética basada en educación, buenas prácticas y responsabilidad en la gestión de tecnologías digitales, estableciendo relaciones de cooperación en seguridad cibernética con otros actores; y (iv) promover el desarrollo de una industria de seguridad cibernética para cumplir sus objetivos estratégicos.[106] Además, de conformidad con la Política Nacional de Ciberseguridad, en 2018 el Presidente de la República nombró un asesor presidencial que le informa directamente sobre asuntos de ciberseguridad y se realizó una reestructuración en la Subsecretaría del Interior para llevar a cabo las medidas descritas en la mencionada política, a través de la Unidad de Coordinación de Ciberseguridad (Resolución Exenta N° 5.006).

Durante ese año, el asesor promovió una serie de medidas relacionadas con los objetivos estratégicos. Una de ellas consistió en fortalecer el CSIRT de Gobierno, el cual depende del Ministerio del Interior y Seguridad Pública,[107] de conformidad con la Política Nacional de Ciberseguridad. Sumado a lo anterior, en marzo de 2018, se aprobó una Política Nacional de Ciberdefensa y se creó una unidad específica para coordinación de la Defensa Nacional,[108] dependiente del Ministerio de Defensa, y una para la industria y los sectores estratégicos, a través del Ministerio de Hacienda. Mediante el recientemente aprobado "Programa de Fortalecimiento de la Gestión Estratégica de la Seguridad Pública en Chile", el BID y el gobierno de Chile acordaron incluir un componente específico para fortalecer la política nacional de ciberseguridad a fin de garantizar "un ciberespacio libre, abierto, seguro y resiliente".[109] En paralelo, el BID apoya al gobierno de Chile con asesoría técnica en la evaluación de los niveles de preparación y respuesta en materia de ciberseguridad en el país con el objetivo de identificar, planificar y diseñar mejoras. El CSIRT de Gobierno es miembro de CSIRT Américas, lo que le da acceso a toda la información que la plataforma tiene para ofrecer, incluyendo el intercambio dinámico de información a través del Malware Information Sharing Platform and Threat Sharing (MISP) desplegado en la red hemisférica.

Asimismo, el gobierno coordina a los reguladores financieros en materia de ciberseguridad y riesgo operacional en general a través del Grupo de Trabajo de Continuidad Operacional del Consejo de Estabilidad Financiera. El mandato del Grupo es: analizar los riesgos operacionales de la infraestructura del mercado financiero y sus participantes y principales usuarios, entre los que se incluyen bancos, corredoras de valores, fondos de pensiones y compañías de seguros, y proponer los cambios legales y regulatorios necesarios para mitigar estos riesgos y sus efectos sobre el sistema financiero. Los miembros de este Grupo de Trabajo pertenecen al Ministerio de Hacienda, al Banco Central de Chile, a la Comisión para el Mercado Financiero y a la Superintendencia de Pensiones, y sesionan generalmente una vez por mes.

Uno de los pasos para alcanzar el primer objetivo de la estrategia es identificar y priorizar la infraestructura crítica de información del país. De acuerdo con la estrategia, "la infraestructura de la información de los siguientes sectores será considerada como crítica: energía, telecomunicaciones, servicios sanitarios, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa, entre otras".[110]

La estrategia también le da al Ministerio del Interior y Seguridad Pública la tarea de crear un grupo de trabajo permanente para establecer un marco normativo para infraestructura crítica en Chile.[111] Además, de acuerdo con la estrategia, "deberá evaluarse la pertinencia de crear un CSIRT de infraestructura crítica". El sector privado, la academia y la sociedad civil también han sido actores activos, apoyando la redacción de la estrategia nacional de seguridad cibernética, lo cual se llevó a cabo a través de una consulta pública.[112]

La Alianza Chilena de Ciberseguridad, recién creada, reúne a organizaciones públicas y privadas, así como a instituciones académicas, con el fin de promover la educación y el uso responsable de la tecnología, y generar canales de comunicación entre el sector

privado y el gobierno, entre otras cosas.[113] Sin embargo, después de los ataques cibernéticos ocurridos en 2018, existe una mayor preocupación por parte de las empresas y organizaciones del sector privado en cuanto al fortalecimiento de sus redes y sistemas.[114] De todos modos, en Chile hay varios proveedores de servicios de seguridad cibernética.

Chile tiene un marco legal que se encuentra en proceso de modificación en materia de delitos informáticos y de la protección de datos personales. Con todo, en materia de delitos informáticos existe la Ley N° 19.223 del año 1993, que sanciona a aquellos que realicen ilícitos sobre sistemas de información.[115] Para proteger los datos personales, Chile cuenta con la Ley N° 19.628. [116] Además, en 2018 se aprobó una reforma al numeral 4 del artículo 19 de la Constitución Política de la República de Chile, el cual reconocía el derecho a la honra y vida privada, y se introdujo la protección de datos personales.[117] Actualmente se encuentran en tramitación en el Congreso dos proyectos de ley, uno que modifica la normativa en materia de protección de datos personales (Boletín N° 11.144-07[118]) y otro que adecúa la normativa chilena al Convenio de Budapest sobre Ciberdelincuencia, además de hacer otras modificaciones en otros cuerpos legales (Boletín N° 12.192-25[119]). Finalmente, existen iniciativas legales en materia financiera (modificaciones a la Ley General de Bancos en materia de riesgo operacional e incorporación de normas específicas de Información de Incidentes Operacionales (RAN 20-8) y Gestión de Continuidad del Negocio (RAN 20-9) de la Comisión para el Mercado Financiero (CMF).

Cabe agregar que el gobierno se comprometió a ingresar el proyecto de Ley Marco de Ciberseguridad para fines de 2019; además de los esfuerzos legales realizados en esta materia, se ha trabajado en modificaciones de cuerpos reglamentarios con el propósito de mejorar los estándares de ciberseguridad al interior de la administración del Estado y articular de manera efectiva las funciones del Comité Interministerial de Ciberseguridad.

En 2018, Naciones Unidas clasificó a Chile como el segundo país más desarrollado en términos de gobierno electrónico entre los países de América Latina y Caribe.[120] Además, el gobierno digital forma parte de la "Agenda Digital 2020", que consiste en "una hoja de ruta que define los próximos pasos para concretar una política de desarrollo inclusivo y sostenible a través de las Tecnologías de la Información y la Comunicación (TIC)".[121] El "Gobierno Digital" es uno de los ejes de la "Agenda Digital 2020", junto con los "Derechos para el Desarrollo Digital", la "Conectividad Digital", la "Economía Digital" y las "Competencias Digitales".[122] Con fecha 24 de enero 2019, se dictó un instructivo presidencial en materia de transformación digital en el que se detallan cuatro medidas: Identidad Digital, Cero Filas, Cero Papel y Coordinación y Seguimiento.[123] El 11 de noviembre de 2019, se publicó la Ley N° 21.180 sobre "Transformación Digital"[124] que viene a realizar una reforma integral en materia de procedimientos administrativos al interior del Estado. Esta establece el formato electrónico para los actos administrativos, además de fomentar el uso de plataformas de interoperabilidad entre los órganos de la administración del Estado, la creación de un repositorio digital y la trazabilidad de toda comunicación entre los distintos órganos de la administración del Estado.

En las universidades tanto públicas como privadas hay carreras de grado, así como posgrados y diplomados de especialización relacionados con la ciberseguridad. Se han desarrollado también otras iniciativas, como la del Ministerio de Educación, que tiene el proyecto "Internet Segura" con el objetivo de "entregar herramientas a los adultos para que puedan acompañar a niños, niñas y jóvenes en su travesía digital" y proporcionar "orientaciones a las escuelas y liceos, desde una mirada más pedagógica, para que puedan formar ciudadanos digitales conscientes de sus deberes y derechos"[125] Desde la entrada en vigor de la Política Nacional de Ciberseguridad, se han impulsado varios programas de educación continua y posgrado en materia de ciberseguridad, tanto desde la perspectiva técnica como legal, con el fin de formar recursos humanos capacitados en estas áreas.

Indicadores: Chile

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia	■■□□□	■■■■□
Organización	■■□□□	■■■□□
Contenido	■■□□□	■■■□□
1-2 Respuesta a Incidentes		
Identificación de Incidentes	■■□□□	■■■□□
Organización	■■□□□	■■■□□
Coordinación	■■□□□	■■□□□
Modo de Operación	□□□□□	■■■□□
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación	■■□□□	■■□□□
Organización	■■□□□	■■□□□
Gestión de Riesgos y Respuesta	■■□□□	■■□□□
1-4 Manejo de Crisis		
Manejo de Crisis	■■□□□	■■□□□
1-5 Defensa Cibernética		
Estrategia	■■□□□	■■■□□
Organización	■■□□□	■■■□□
Coordinación	■■□□□	■■□□□
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones	■■□□□	■■□□□

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno	■■□□□	■■■□□
Sector Privado	■■■□□	■■■□□
Usuarios	■■□□□	■■■□□
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario	■■□□□	■■■□□
Confianza del Usuario en los Servicios de Gobierno Electrónico	■■□□□	■■■□□
Confianza del Usuario en los Servicios de Comercio Electrónico	■■■□□	■■■□□
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea	□□□□□	■■■□□
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia	□□□□□	■■■□□
2-5 Medios y Redes Sociales		
Medios y Redes Sociales	□□□□□	■■■□□

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

Colombia

Habitantes

*Ref: Banco Mundial**

Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***

Colombia adoptó en 2016 una segunda política nacional en materia de seguridad cibernética, después de cinco años de presentada la primera,[126] cuyo objetivo general es el de fortalecer las capacidades del Estado para responder a las amenazas en materia de seguridad cibernética y defensa en este campo del país. La nueva política de seguridad digital apunta a fortalecer aún más las capacidades de todas las partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.[127] Dentro de los principales aportes de la nueva política, se encuentra la figura de un coordinador nacional de seguridad digital, rol que es ejercido por la Presidencia de la República de Colombia.

Asimismo, como ente máximo para tratar temas intersectoriales de seguridad digital, se creó el Comité de Seguridad Digital, liderado por el Coordinador Nacional de Seguridad Digital.[128] Por otra parte, dentro de sus políticas de gestión y desempeño,[129] el gobierno nacional por primera vez incluyó la política de seguridad digital como parte integral de la operación estratégica de las entidades públicas y privadas.

Al mismo tiempo, el Ministerio de Tecnología y las Comunicaciones (MinTIC) tiene desplegado a nivel nacional y territorial el modelo de seguridad y privacidad para apoyar la gestión e implementación de buenas prácticas y estándares para proteger los activos críticos de información, infraestructura tecnológica, y sistemas de información y comunicaciones, fomentando la mejora continua.

Colombia además cuenta con el ColCERT, un equipo nacional de respuestas a incidentes de seguridad digital, que actualmente depende del Ministerio de Defensa Nacional, y es el encargado de atender en primer término los incidentes cibernéticos y proteger la infraestructura crítica cibernética nacional (ICCN).[130] De igual forma, se ha venido desarrollando un plan para fortalecer la protección de la infraestructura crítica cibernética mediante una guía para la identificación de la ICCN y programas de protección sectorial de la misma.[131] En apoyo a la transformación digital de Colombia, a finales de 2018 el BID aprobó el "Programa para la mejora de la conectividad y digitalización de la economía" a través de un "Préstamo Basado en Políticas" (Policy-Based Loan o PBL, por sus siglas en inglés).[132] Este programa concreta iniciativas de fortalecimiento de las capacidades nacionales en ciberseguridad. Si bien el gobierno ha tomado medidas significativas para asegurar el ciberespacio del país con las dos políticas de seguridad cibernética, el sector privado (en particular las pyme) aún tiene un largo camino por recorrer para estar preparado para las actuales amenazas en este campo.

Los colombianos tienen amplias oportunidades de continuar con estudios en seguridad cibernética tanto a nivel de grado como de posgrado. Además, el MinTIC ha otorgado becas a funcionarios públicos de las áreas de seguridad digital y ciberdefensa,[133] y también patrocina cursos de seguridad digital y capacitaciones para las diferentes ramas del servicio público relacionadas con las TIC.[134] De igual forma, se han realizado varios programas de capacitación en colaboración con otras instituciones como MinTIC, la OEA y la Fundación Citi, y se han beneficiado 40 estudiantes de ingeniería de bajos ingresos.[135] Finalmente, MinTIC tiene una campaña llamada "En TIC Confío" que busca promover y crear conciencia sobre el uso responsable de Internet y las TIC.[136]

El delito cibernético está cubierto en la Ley N° 1.273 de 2009 que modifica el Código Penal de forma de incluir esta modalidad de delito.[137] Para la protección de datos y privacidad, Colombia cuenta con la Ley N° 1.581 de 2012.[138] Asimismo, el país también tiene una Delegatura de protección de datos personales,[139] que se encarga, entre otros temas, de velar por que se cumpla toda la normativa relacionada con la protección de datos y por divulgar a los usuarios sus derechos con respecto a la protección de datos personales. Esta ley se aplica a las bases de datos públicas y privadas.

Colombia es miembro tanto de Interpol como de Europol[140] y ha priorizado su participación en escenarios internacionales.[141] Además, mediante la Ley N° 1.928 del 24 de julio de 2018, se aprobó el Convenio sobre la Ciberdelincuencia (Convenio de Budapest, 2001)[142] y depositó su instrumento de adhesión el 16 de marzo de 2020.

La política de gobierno digital[143] está establecida en el Decreto N° 1.008 de 2018, donde se la describe como "el uso y aprovechamiento de las TIC para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital".

Indicadores: Colombia

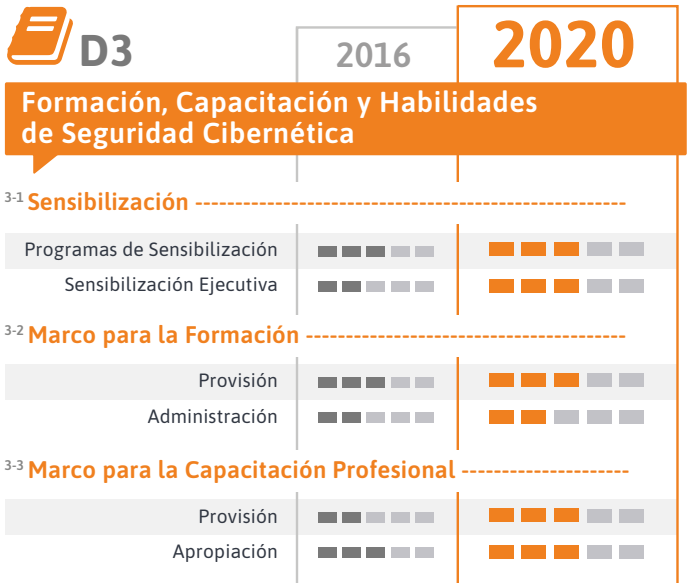
D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

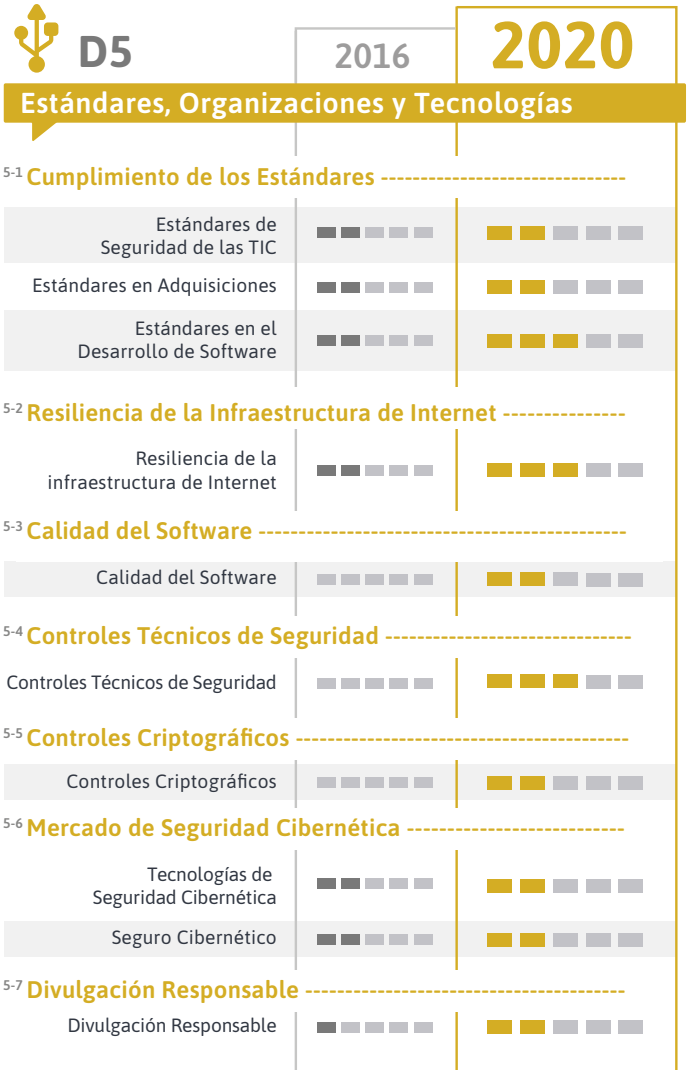
	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética



D4 Marcos Legales y Regulatorios

D5 Estándares, Organizaciones y Tecnologías



Costa Rica

Habitantes

*Ref: Banco Mundial**

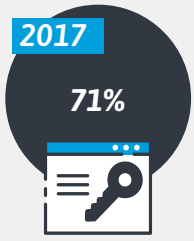
Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***



En 2017 el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) de Costa Rica presentó la Estrategia Nacional de Ciberseguridad con el objetivo de diseñar un marco para orientar las acciones que el país puede tomar con respecto al uso seguro de las TIC, desarrollar la coordinación y cooperación entre las partes interesadas, y promover medidas de educación, prevención y mitigación del riesgo de utilizar las TIC.[144] Sin embargo, si bien las normas de seguridad cibernética a nivel nacional se publicaron hace poco, Costa Rica ya había dado pasos significativos para asegurar su ciberespacio. En 2012 se creó un CSIRT nacional bajo el MICITT por medio del Decreto N° 37.052 para coordinar entre los diferentes interesados todo lo relacionado con información y seguridad cibernética, y para formar un equipo de expertos en seguridad TIC destinado a prevenir y responder a los incidentes cibernéticos contra las instituciones gubernamentales.[145] Además, CSIRT-CR es miembro de la red CSIRT Américas.

La Estrategia Nacional define la infraestructura crítica en términos de "sistemas de información y redes, que en caso de falla podrían tener un impacto serio en la salud, la seguridad física y operativa, la economía y el bienestar de los ciudadanos, o el funcionamiento efectivo del gobierno y economía del país". La Estrategia también describe la necesidad de determinar la infraestructura crítica del país y crear un comité para generar políticas conformadas por miembros de entidades públicas y privadas clasificadas como infraestructura crítica.

El conocimiento sobre cuestiones de seguridad cibernética por parte del sector privado es limitado, pero desde 2017 proliferan las empresas enfocadas en brindar soluciones y servicios de ciberseguridad.[146]

Los costarricenses tienen muchas oportunidades de seguir estudiando sobre seguridad cibernética, y algunas universidades ofrecen programas más cortos de capacitación y diplomados.[147] También se han realizado varios eventos de creación de capacidad en colaboración con instituciones internacionales, como la capacitación brindada por el Centro Criptológico Nacional de España para funcionarios públicos y la capacitación profesional en colaboración con la OEA y la Fundación Citi.[148]

En 2012, Costa Rica aprobó el Decreto Legislativo N° 9.048, mediante el cual se reformó el Código Penal para introducir formalmente disposiciones para el delito cibernético.[149] Algunos argumentan que esto no es suficiente, ya que hay problemas con la aplicación del marco y el decreto no es exhaustivo, lo que deja sin regulación los delitos como *skimming* (robo de información de la tarjeta de crédito), *grooming* (generar la confianza de alguien para aprovecharse de este), o el ciberacecho.[150] Costa Rica ha adherido al Convenio de Budapest en 2017, así como también a otros convenios, y está desarrollando una estrategia nacional contra el ciberdelito.

Para la privacidad y protección de datos, Costa Rica cuenta con la Ley N° 8.968 de Protección de la Persona frente al tratamiento de sus datos personales.[151] Esta ley se aplica a las bases de datos de los sectores público y privado.

Desde 2010 Costa Rica tiene un borrador de estrategia para el gobierno electrónico con la visión de ser un país de referencia en América Latina en lo que concierne al gobierno digital mediante servicios centrados en el ciudadano, transparencia en los servicios e interconexión de instituciones gubernamentales basadas en un entorno favorable para las TIC y el establecimiento de una sociedad igualitaria y segura.[152]

Indicadores: Costa Rica

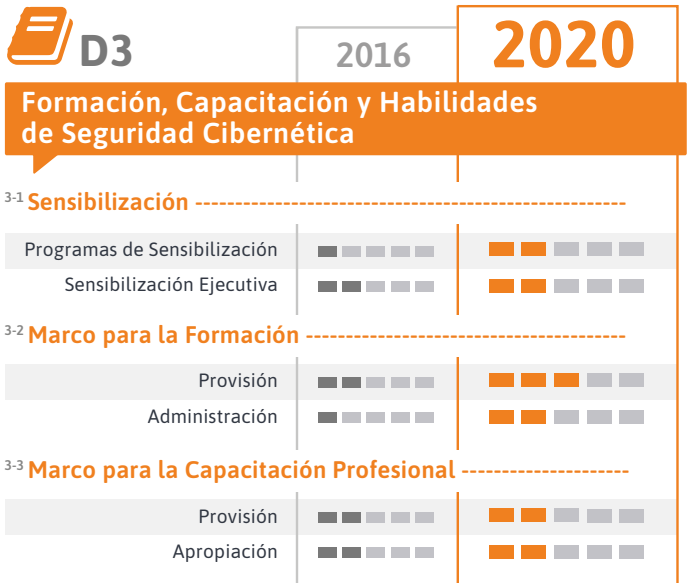
D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

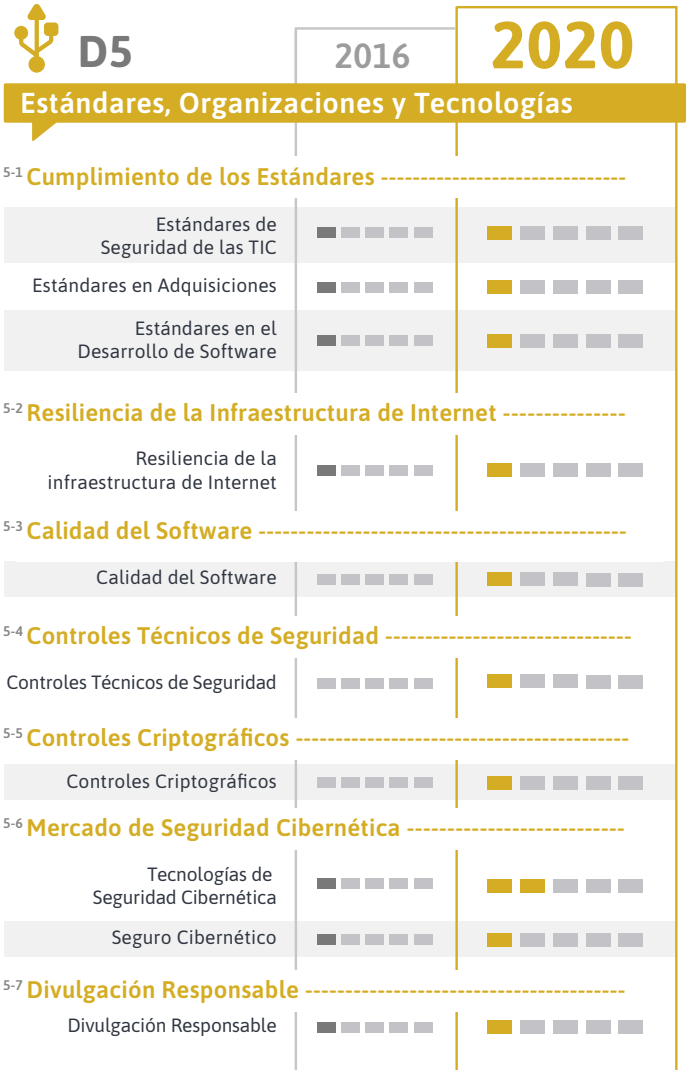
	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética



D4 Marcos Legales y Regulatorios

D5 Estándares, Organizaciones y Tecnologías



Dominica

Habitantes

*Ref: Banco Mundial**

2017

71.458

Abonos a teléfonos celulares

*Ref: ITU***

2017

75.230

Personas con acceso a Internet

2017

49.749

Porcentaje de penetración de Internet

*Ref: ITU***

2017

70%

Dominica aún no ha establecido una estrategia nacional de ciberseguridad, pero ya ha redactado un borrador en colaboración con la OEA: la Iniciativa contra el Delito Informático de la Mancomunidad y el Consejo de Europa. Este borrador de estrategia describe cuatro pilares: (i) el gobierno y la ley para fortalecer la capacidad de gobernar, mediante mecanismos de ciberseguridad, y enjuiciar los delitos cibernéticos; (ii) la cooperación de las partes interesadas en la distribución de las responsabilidades de ciberseguridad entre todas las partes afectadas; (iii) la creación de capacidad y sensibilización para garantizar que haya suficientes profesionales técnicamente capacitados para trabajar en el campo de la ciberseguridad; y (iv) las consideraciones técnicas que exigen la creación de un CSIRT nacional. Además, el borrador de la estrategia, que define qué es la infraestructura crítica, incluye la red eléctrica, las comunicaciones, los métodos de suministro financiero, agua y alcantarillado, transporte, aduanas y autoridades portuarias, y el dominio de nivel superior de código de país (CCTLD, por sus siglas en inglés).

La oportunidad para que los dominiqueses reciban capacitación en ciberseguridad es muy limitada. De todos modos, si bien no se ofrecen títulos cibernéticos específicos a nivel nacional, el Dominica State College sí ofrece títulos de Licenciatura en Informática y Tecnología de la Información.[153]

El gobierno, en asociación con India, también ha abierto el Centro de Excelencia de las TIC para brindarles a los ciudadanos la oportunidad de aprender sobre estas tecnologías. Como siguiente paso, el Director de Telecomunicaciones explorará el establecimiento de un Centro para la Excelencia en Ciberseguridad.[154]

En años recientes, Dominica ha promulgado legislación relacionada con el ciberespacio, dentro de la cual cabe citar la Ley de evidencia electrónica de 2010,[155] la Ley de archivo electrónico de 2013,[156] la Ley de transferencia electrónica de fondos de 2013[157] y Ley de transacciones electrónicas de 2013.[158] En relación con la criminalización de los delitos cibernéticos, Dominica cuenta con un proyecto de ley sobre delitos electrónicos de 2013 que dispone la "prevención y el castigo de los delitos electrónicos y asuntos relacionados". Sin embargo, aún no se ha convertido en ley. Del mismo modo, también existe el Proyecto de Ley de Protección de Datos para legislar sobre la protección de la información privada procesada por organismos públicos y privados. No obstante, al igual que en el caso del proyecto de ley de delitos electrónicos, este todavía se está revisando y está siendo considerado para su aprobación como ley.

Indicadores: Dominica

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia	2	2
Organización	1	1
Contenido	1	1
1-2 Respuesta a Incidentes		
Identificación de Incidentes	1	1
Organización	1	1
Coordinación	1	1
Modo de Operación	0	1
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación	1	1
Organización	1	1
Gestión de Riesgos y Respuesta	1	1
1-4 Manejo de Crisis		
Manejo de Crisis	1	1
1-5 Defensa Cibernética		
Estrategia	1	1
Organización	1	1
Coordinación	1	1
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones	1	1

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno	2	2
Sector Privado	2	2
Usuarios	1	1
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario	2	2
Confianza del Usuario en los Servicios de Gobierno Electrónico	2	2
Confianza del Usuario en los Servicios de Comercio Electrónico	2	2
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea	0	1
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia	0	1
2-5 Medios y Redes Sociales		
Medios y Redes Sociales	0	2

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

	2016	2020
3-1 Sensibilización		
Programas de Sensibilización		
Sensibilización Ejecutiva		
3-2 Marco para la Formación		
Provisión		
Administración		
3-3 Marco para la Capacitación Profesional		
Provisión		
Apropiación		

D4 Marcos Legales y Regulatorios

	2016	2020
4-1 Marcos Legales		
Marcos Legislativos para la Seguridad de las TIC		
Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea		
Legislación Sobre Protección de Datos		
Protección Infantil en Línea		
Legislación de Protección al Consumidor		
Legislación de Propiedad Intelectual		
Legislación Sustantiva Contra el Delito Cibernético		
Legislación Procesal Contra el Delito Cibernético		
4-2 Sistema de Justicia Penal		
Fuerzas del Orden		
Enjuiciamiento		
Tribunales		
4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético		
Cooperación Formal		
Cooperación Informal		

D5 Estándares, Organizaciones y Tecnologías

	2016	2020
5-1 Cumplimiento de los Estándares		
Estándares de Seguridad de las TIC		
Estándares en Adquisiciones		
Estándares en el Desarrollo de Software		
5-2 Resiliencia de la Infraestructura de Internet		
Resiliencia de la infraestructura de Internet		
5-3 Calidad del Software		
Calidad del Software		
5-4 Controles Técnicos de Seguridad		
Controles Técnicos de Seguridad		
5-5 Controles Criptográficos		
Controles Criptográficos		
5-6 Mercado de Seguridad Cibernética		
Tecnologías de Seguridad Cibernética		
Seguro Cibernético		
5-7 Divulgación Responsable		
Divulgación Responsable		

Ecuador

Habitantes

*Ref: Banco Mundial**

2017

16.785.361

Abonos a teléfonos celulares

*Ref: ITU***

2017

14.651.404

Personas con acceso a Internet

2017

9.613.353

Porcentaje de penetración de Internet

*Ref: ITU***

2017

57%

Si bien Ecuador aún no cuenta con una estrategia de seguridad cibernética, sí ha logrado hacer avances significativos en la mejora de sus capacidades cibernéticas y en el enfrentamiento de amenazas, apoyado por el establecimiento de un grupo de trabajo para el desarrollo de la estrategia nacional de ciberseguridad. Esto se debe en gran parte al establecimiento de EcuCERT, el equipo de respuesta ante incidentes cibernéticos del país que depende de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).[159] Además, desde 2018 el BID está aportando asesoramiento técnico al país para que se puedan identificar, evaluar y planificar los niveles de preparación en seguridad cibernética nacional, de modo de contar con elementos técnicos, estratégicos, normativos y de gobernanza que el gobierno pueda utilizar en su formulación de la Estrategia Nacional de Ciberseguridad.

Cabe destacar que EcuCERT es miembro de CSIRT Américas, por lo que se beneficia de la red de colaboración, intercambio, estímulo y participación en proyectos técnicos entre los CSIRT nacionales, de defensa, policiales y gubernamentales de los países miembros que proporciona la organización. Además, la Dirección de Arquitectura Tecnológica y Seguridad de la Información es responsable de la coordinación de la seguridad cibernética del país y tiene, como una de sus tareas, la formulación, evaluación, coordinación y gestión de los programas gubernamentales de seguridad cibernética.[160]

Si bien existe cierta provisión de servicios de seguridad cibernética por parte del sector privado, parece haber una necesidad de mejora en cuanto a la conciencia y la preparación para enfrentar amenazas en este campo. Un estudio realizado por Deloitte en 2018 encontró que el 50% de las empresas "ha implementado un programa de concientización en ciberseguridad de los empleados". Sin embargo, "el 70% de las organizaciones afirma no tener certeza de la efectividad de su proceso de respuesta ante incidentes de ciberseguridad" y el presupuesto para la ciberseguridad es la barrera más importante con que se enfrentan las organizaciones.[161]

Las universidades públicas y privadas ofrecen algunos cursos, y también hay cursos de capacitación enfocados en seguridad cibernética y en otros importantes temas TIC. Sin embargo, Ecuador enfrenta actualmente un déficit en profesionales de seguridad cibernética.[162]

La Ley N° 2002-67 sobre comercio electrónico, firma electrónica y mensajes de datos describe las normas que rigen sobre delito cibernético y señala las reformas pertinentes del Código Penal.[163] Además, los artículos 229 a 234 del Código Penal establecen el marco para el tratamiento de los delitos contra los activos de los sistemas de información y comunicación.[164] Con respecto a la protección de datos y la privacidad, estos ámbitos cuentan con protección constitucional.[165] En efecto, la Constitución estipula que los ciudadanos tienen derecho a la protección de sus datos personales. Hay leyes y reglamentos relacionados con la protección de datos personales, pero no hay una ley específica acerca del tema.[166] Sin embargo, existe un proyecto de ley sobre la Protección de la Privacidad de los Datos Personales.[167] Además, el Sistema Nacional de Registro de Datos Públicos (SINARDAP) está realizando mesas de trabajo para la revisión del anteproyecto que será presentado a la Asamblea Nacional.[168]

Respecto del gobierno electrónico, Ecuador estableció el Plan de Gobierno Electrónico 2014-2017, cuyo objetivo es ejecutar un modelo de gobierno electrónico sostenible e inclusivo que tenga en cuenta los aspectos políticos, sociales y ambientales, con el objetivo de consolidar un gobierno cercano, abierto, eficiente y efectivo.[169] Este plan fue actualizado con el Plan Nacional de Gobierno Electrónico 2018-2021, que toma los diferentes aspectos del primero y determina qué mejoras necesita.[170]

Por último, la Ley del Sistema Nacional de Contratación Pública, reformada en 2018, requiere seguridad de la información durante todo el proceso de adquisiciones, y ha creado el Servicio Nacional de Contratación Pública (SERCOP), organismo autónomo responsable, entre otras cosas, de establecer las políticas y condiciones de uso de la información y herramientas electrónicas, y de modernizar herramientas conexas al sistema electrónico de contratación pública y subastas electrónicas.[171]

Indicadores: Ecuador

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

El Salvador

Habitantes

*Ref: Banco Mundial**

2017

6.388.122

Abonos a teléfonos celulares

*Ref: ITU***

2017

9.478.044

Personas con acceso a Internet

2017

2.160.509

Porcentaje de penetración de Internet

*Ref: ITU***

2017

34%

Si bien El Salvador actualmente no cuenta con una estrategia nacional de seguridad cibernética, tener una Política Nacional de Ciberseguridad es uno de los objetivos de la Estrategia de Gobierno Digital 2018-2022,[172] "resultado de un proceso de consulta, donde participaron expertos internacionales, la academia, instituciones del gobierno, el sector privado y organizaciones de sociedad civil".[173] El país tiene un CSIRT reconocido a nivel nacional, SalCERT, que debe responder a incidentes de seguridad cibernética y coordinarse con otros equipos de respuesta.

En los últimos años, El Salvador ha intercambiado conocimientos sobre temas como la protección de la infraestructura crítica y la mejora de la seguridad cibernética, con Ecuador, España, Israel y República de Corea, entre otros países.[174]

El Salvador cuenta con la participación del sector privado en la provisión de servicios de seguridad cibernética, lo cual abarca desde análisis hasta capacitación. Con respecto a la educación en seguridad cibernética, se han abierto oportunidades de estudio en algunas universidades.[175] Asimismo, hay algunas empresas privadas que ofrecen cursos de capacitación en seguridad cibernética, y han descubierto que existe una brecha en este campo en las instituciones de educación superior.

Donde El Salvador ha logrado un avance significativo es en materia de legislación relativa al delito cibernético. En 2016 se aprobó la Ley Especial contra los Delitos Informáticos y Conexos con el objetivo de proteger los derechos legales de las conductas delictivas cometidas utilizando TIC, así como de prevenir delitos cometidos contra datos almacenados, procesados y/o transferidos.[176]

Los artículos 24 a 26 del Decreto N° 260 de la Ley Especial contra los Delitos Informáticos y Conexos se refieren a la protección contra el uso, la contratación y la transferencia, y la revelación indebida de datos personales. Además, el Decreto N° 133[177] de la Ley de Firma Electrónica protege los datos personales que necesitan los proveedores de servicios. Sin embargo, no existe una legislación integral sobre el tema, por lo que la protección de datos y la privacidad no se abordan adecuadamente.

Además del desarrollo de la Estrategia de Gobierno Digital 2018-2022,[178] El Salvador ha tomado algunas medidas concretas para establecer el gobierno electrónico, como el lanzamiento del proyecto para el Sistema Integrado de Gestión Administrativa y la Política Nacional de Datos Abiertos que se agregó al nuevo portal datos.gob.sv, un sitio que contiene más de 20 bases de datos de información pública.[179] Asimismo, en 2016 se creó la Dirección de Gobierno Electrónico, que es la encargada de coordinar iniciativas con las instituciones públicas, y hay una plataforma que está en funcionamiento desde inicios del 2017[180] para facilitar el intercambio de información del gobierno aplicando los lineamientos de seguridad.[181]

Indicadores: El Salvador

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

Grenada

Habitantes

*Ref: Banco Mundial**

Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***

En 2014 la Comisión Nacional de Regulación de las Telecomunicaciones de Grenada informó que estaba trabajando con el gobierno para establecer una estrategia de ciberseguridad que también permitiría el establecimiento de un CSIRT nacional.[182] Sin embargo, hasta la fecha no ha habido más anuncios al respecto. En este sentido, el gobierno ha estado invirtiendo en varios proyectos relacionados con las TIC, como el programa Una tablet por niño(a) (*One Tablet One Child*) del Ministerio de Educación y una base de datos centralizada para facilitar la oferta de servicios gubernamentales a los ciudadanos en línea. Por otro lado, hay poca evidencia de coordinación entre el gobierno y los propietarios de activos de infraestructura crítica.[183]

En general, la sociedad civil y el sector privado tienen un conocimiento y una conciencia limitados sobre ciberseguridad. Al no contar con mecanismos de notificación, se hace muy difícil sacar a la luz la ciberdelincuencia. En lo que respecta a educación y capacitación, la educación en TI forma parte de la estrategia TIC. Sin embargo, aún existen oportunidades muy restringidas en capacitación a nivel local sobre seguridad cibernética.

En 2013, Granada adoptó la Ley de delitos electrónicos, cuyo objetivo es incluir ese tipo de delitos en el Código Penal. La Ley define los delitos específicos, así como el procedimiento para investigarlos.[184] Si bien Granada no tiene legislación para la protección de datos y de la privacidad, forma parte de la Organización de Estados del Caribe Oriental, que cuenta con una ley de protección de datos que se aplica a la manera en que se procesan los datos en los Estados Miembros.[185]

El país tiene una estrategia de gobierno electrónico, como parte de la Estrategia TIC 2006-2010, cuyo objetivo es estar "centrada en el ciudadano, en la prestación de mejores niveles de servicio al cliente y en una mayor satisfacción ciudadana". [186] Además, Granada integra la estrategia de gobierno electrónico de la Comunidad del Caribe (CARICOM) de 2014, que apunta a proporcionar mejoras sostenibles para la prestación de servicios públicos mediante el uso de TIC.[187] Sin embargo, hay poca evidencia que sugiera que se ha avanzado mucho en la provisión electrónica de servicios públicos.[188]

Indicadores: Grenada

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

Guatemala

Habitantes

*Ref: Banco Mundial**

Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***

Junto con República Dominicana, Guatemala es el país de la región que más recientemente se unió al grupo de aquellos que cuentan con estrategias nacionales de seguridad cibernética. En efecto, en junio de 2018, el gobierno lanzó su estrategia nacional de seguridad cibernética con el objetivo de fortalecer las capacidades de la nación, creando el entorno y las condiciones necesarias para garantizar la participación, el desarrollo y el ejercicio de los derechos humanos en el ciberespacio.[189] Además, Guatemala tiene el CSIRT-gt como un equipo de respuesta a incidentes, bajo la supervisión del Ministerio de Gobernación[190] y el cual es miembro de la red CSIRT Américas.

Aunque aún no hay una definición formal de infraestructura crítica en el país, uno de los pasos establecidos en el eje legislativo de la estrategia de seguridad consiste en crear, aprobar e implementar una ley de infraestructura crítica para identificar y analizar las características principales de los sectores que proveen servicios esenciales, y establecer medidas de prevención, protección y recuperación contra amenazas.

Guatemala tiene varios proveedores de servicios de seguridad cibernética, además de un CERT para el sector privado.[191] Asimismo, algunas empresas buscan sensibilizar a la población sobre la seguridad cibernética.[192] Del mismo modo, el Capítulo de Guatemala de Internet Society cuenta con un grupo de trabajo que, entre otras cosas, tiene el objetivo crear conciencia sobre la seguridad cibernética y ofrece talleres sobre cómo gestionar los incidentes.[193]

Si bien no existen muchas oportunidades para continuar la educación terciaria en ciberseguridad, hay algunas opciones de formación adicional disponibles. Además, la estrategia nacional de seguridad cibernética tiene un eje educativo con el objetivo de aumentar la oferta en educación y capacitación en seguridad cibernética en Guatemala para poder satisfacer la demanda técnica y profesional en todos los sectores. También se han desarrollado varios eventos de capacitación de parte del gobierno, en colaboración con otras entidades, como el taller sobre amenazas cibernéticas[194] o la capacitación para el primer CSIRT en colaboración con la OEA.[195]

Guatemala no tiene una legislación específica para el delito cibernético. Sin embargo, existe la Iniciativa legislativa N° 5.254 de 2017, que "dispone aprobar una ley contra la ciberdelincuencia".[196] El proyecto de ley "tiene por objeto dictar medidas de prevención y sanción de los actos ilícitos de naturaleza informática, cometidos a través de artificios tecnológicos, mensajes de datos, sistemas o datos informáticos, así como medidas de protección contra la explotación, la pornografía y demás formas de abuso sexual con menores de edad y que se realicen por medio de sistemas informáticos".[197] Del mismo modo, existe una iniciativa legislativa para la protección de datos y de la privacidad, que se aplicará a las bases de datos del sector público y privado.[198]

Por último, el país tampoco cuenta con una estrategia de gobierno electrónico. Sin embargo, el gobierno electrónico es uno de los ejes de acción de la Comisión Presidencial de Gestión Pública Abierta y Transparencia, cuya misión es apoyar las acciones de los ministerios e instituciones del Poder Ejecutivo para continuar la aplicación de las medidas que provienen de convenciones internacionales sobre transparencia, gobierno electrónico, lucha contra la corrupción y gobierno abierto.[199]

Indicadores: Guatemala

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia	■□□□□	■■■□□
Organización	■□□□□	■■□□□
Contenido	■□□□□	■■■□□
1-2 Respuesta a Incidentes		
Identificación de Incidentes	■■□□□	■■□□□
Organización	■□□□□	■■□□□
Coordinación	■□□□□	■■□□□
Modo de Operación	□□□□□	■□□□□
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación	■□□□□	■□□□□
Organización	■□□□□	■□□□□
Gestión de Riesgos y Respuesta	■□□□□	■□□□□
1-4 Manejo de Crisis		
Manejo de Crisis	■□□□□	■□□□□
1-5 Defensa Cibernética		
Estrategia	■□□□□	■□□□□
Organización	■□□□□	■□□□□
Coordinación	■□□□□	■□□□□
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones	■□□□□	■■□□□

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno	■□□□□	■■□□□
Sector Privado	■■□□□	■■□□□
Usuarios	■□□□□	■■□□□
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario	■■□□□	■■□□□
Confianza del Usuario en los Servicios de Gobierno Electrónico	■□□□□	■■□□□
Confianza del Usuario en los Servicios de Comercio Electrónico	■■□□□	■■□□□
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea	□□□□□	■■□□□
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia	□□□□□	■□□□□
2-5 Medios y Redes Sociales		
Medios y Redes Sociales	□□□□□	■■□□□

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

D4 Marcos Legales y Regulatorios

D5 Estándares, Organizaciones y Tecnologías

Guyana

Habitantes

*Ref: Banco Mundial**

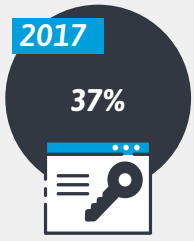
Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***



En marzo de 2019 se estableció en Guyana un Grupo de Trabajo de Estrategia Nacional de Ciberseguridad para desarrollar una estrategia nacional bajo la guía de la OEA. Como parte de esta iniciativa, y en asociación con la OEA, en julio de 2019 se realizó una consulta nacional con las partes interesadas. Actualmente se está revisando un borrador preliminar de la estrategia. El país estableció su CSIRT nacional, el CIRT.GY, en 2013,[200] con la misión de "mejorar la preparación y respuesta de ciberseguridad nacional a través de medidas de seguridad proactivas y mecanismos de intercambio de información". Los servicios se ofrecen a los sectores público y privado, así como a los miembros de la sociedad civil afiliados a Guyana. El CIRT.GY se enmarca en el ámbito del Ministerio de Telecomunicaciones Públicas.[201] Además, es miembro de CSIRT Américas, aprovechando la naturaleza colaborativa de la red, y se ha asociado con otros equipos de respuesta de emergencia (CERT) como los de Colombia, Estonia y los Países Bajos.

En Guyana siguen sin existir muchos proveedores de servicios de ciberseguridad del sector privado disponibles, y el enfoque de ciberseguridad para los ejecutivos se encuentra en fase reactiva. Sin embargo, la ciberseguridad está comenzando a ser discutida con mayor frecuencia en los altos niveles directivos. Por otro lado, las instituciones de la sociedad civil aún desconocen la importancia de las buenas prácticas en ciberseguridad.[202]

En cuanto a la capacitación en ciberseguridad, hay algunas oportunidades disponibles. Al nivel profesional o superior existen algunas ofertas de Licenciatura en Informática y TI. Si bien no se cuenta con un programa dedicado a la seguridad cibernética, ahora se ofrece un curso certificado de posgrado en Seguridad de la Red en el Centro para la Excelencia en Tecnología de la Información recientemente lanzado (se trata de un acuerdo bilateral entre el gobierno de India y el de Guyana). Este programa inicialmente se dirigió al sector público, pero existen planes para ampliar su audiencia de modo de incluir también al sector privado.

El gobierno ha tomado varias medidas para crear conciencia sobre ciberseguridad. En abril de 2019 Guyana se benefició de una campaña de sensibilización del público de un año de duración, diseñada por el Programa de Seguridad Cibernética del Reino Unido. La clave para su divulgación fue el lanzamiento del sitio web www.getsafeonline.gy.[203] Además, en septiembre de 2019 el Ministerio de Telecomunicaciones Públicas colaboró con Get Safe Online para organizar un taller de capacitación sobre sensibilización en ciberseguridad. Entre los participantes hubo 124 funcionarios públicos pertenecientes a 50 instituciones públicas. Asimismo, en octubre de 2019, para celebrar el mes de la concientización sobre ciberseguridad, se implementó una campaña nacional de concientización pública que incluyó charlas de radio, anuncios en redes sociales y sesiones de concientización en instituciones educativas secundarias y terciarias, así como en el sector público.

Con respecto al cibercrimen, en 2017 la Fuerza de Policía de Guyana, en colaboración con el sector privado, abrió un Centro de Ciberseguridad con el objetivo de enseñar a la policía, a la comunidad empresarial y al público en general cómo responder a este problema.[204] Más tarde, en enero de 2019, la Fuerza de Policía de Guyana estableció formalmente una Unidad de Delitos Cibernéticos orientado a investigar y enjuiciar delitos cometidos con tecnología informática. La legislación sobre delitos cibernéticos se promulgó en 2018, después de haber sido tratada durante dos años. [205,206] Esta abarca una serie de delitos de ciberdelincuencia y métodos de ejecución.[207] Guyana aún no ha aprobado legislación sobre privacidad y protección de datos.[208]

La estrategia de administración electrónica del país está anclada en la Estrategia de Desarrollo del Estado Verde: Visión 2040. Esta es la política nacional de desarrollo de 20 años de Guyana que refleja la visión y los principios rectores de la "agenda verde". El objetivo central es lograr un nivel de desarrollo que proporcione una mejor calidad de vida para todos los guyaneses, en función de la riqueza natural del país: su diversidad de gentes y sus abundantes recursos naturales (tierra, agua, bosques, minerales y agregados, biodiversidad). La utilización adecuada de las TIC puede mejorar la vida de todos los guyaneses y, por lo tanto, es un componente transversal de la Estrategia de Desarrollo del Estado Verde: Visión 2040. Las TIC tienen el potencial de hacer que los servicios gubernamentales sean más amplios, efectivos y receptivos, y la capacidad para impulsar la nueva actividad empresarial con sentido ecológico.[209]

Indicadores: Guyana

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

D4 Marcos Legales y Regulatorios

D5 Estándares, Organizaciones y Tecnologías

Haití

Habitantes

*Ref: Banco Mundial**

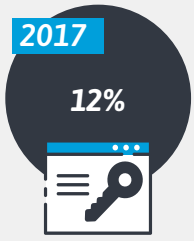
Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***



Haití aún no tiene una estrategia nacional de ciberseguridad ni un CSIRT nacional. Sin embargo, el gobierno es consciente de que la ciberseguridad cada vez cobra más importancia y en consecuencia ha tomado algunas medidas. En 2015 el Ministerio de Obras Públicas, Transporte y Comunicaciones (MPTC, por sus siglas en francés) creó un grupo de trabajo para la ciberseguridad y el delito informático (GTCSC, por sus siglas en francés) con la misión de desarrollar e implementar una estrategia nacional de ciberseguridad. En 2016 este grupo dirigió un taller sobre proyectos de ley para la ciberseguridad, la ciberdelincuencia, las interceptaciones de comunicación, las transacciones y las pruebas electrónicas con participantes del sector bancario, operadores de telefonía celular, proveedores de servicios de Internet, la Policía Nacional, el Ministerio de Seguridad Pública y otras instituciones estatales, diversas entidades de la Universidad Estatal de Haití, y los presidentes de las comisiones permanentes de telecomunicaciones, información y comunicación de ambas cámaras del Parlamento.[210] Además, en mayo de 2018 una delegación del Centro de Información de la Red de América Latina y el Caribe se reunió con el director general del Consejo Nacional de Telecomunicaciones (CONATEL) para estudiar, entre otras cosas, la colaboración para establecer un CSIRT nacional.[211]

Al sector privado le preocupa que las instituciones del sector público y las del propio sector privado no conozcan los riesgos para sus sistemas, y quienes forman parte de él consideran que se debería realizar periódicamente una "auditoría tecnológica" para ver dónde hay vulnerabilidades.[212] A medida que aumenta el uso de redes para asuntos personales o profesionales en Haití, el riesgo en ciberseguridad se eleva. Esto lleva a la necesidad de contar con políticas y legislación para regular el ciberespacio, elementos que aún son inexistentes en el país.[213] En general, el sector privado parece tener una conciencia general sobre la importancia de la ciberseguridad. Por otro lado, hay entidades involucradas en la organización de eventos para crear conciencia, y la realización de talleres y capacitaciones sobre ciberseguridad, como el "Haití Cybercon" que tuvo lugar en octubre de 2018.[214]

En cuanto a la formación específica, se ofrecen algunos cursos en ciberseguridad, aunque no hay títulos específicos en esta materia. Sin embargo, Haití envió a algunos participantes a capacitaciones organizadas por la OEA en 2017 y 2018, como el Summer Bootcamp organizado por la OEA y el INCIBE, o el Taller Subregional sobre Protección de Infraestructuras Críticas que tuvo lugar en Panamá.[215]

En la actualidad, Haití aún no cuenta con una legislación sobre delito informático, ni para la protección de datos y privacidad.[216] Sin embargo, se encuentra encaminada la legislación sobre delitos cibernéticos, como lo demuestra el taller de 2016 para la presentación de proyectos de ley sobre el tema. Con respecto a la protección de datos y privacidad, hay poca evidencia que demuestre que se esté haciendo algo en ese campo.

Por último, aunque Haití no tiene una estrategia de gobierno electrónico dedicada, parte de su Plan de Desarrollo Estratégico 2030 abarca la modernización digital de la administración pública.[217] El país cuenta con una plataforma de gobierno integrada,[218] pero todavía no les ofrece servicios de gobierno electrónico a sus ciudadanos.[219]

Indicadores: Haití

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

Honduras

Habitantes

*Ref: Banco Mundial**

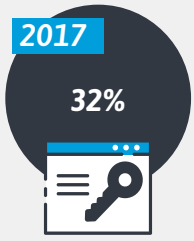
Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***



Honduras ha puesto en marcha el proyecto de Ley Nacional de Ciberseguridad y Medidas de Protección ante los Actos de Odio y Discriminación en Internet y Redes Sociales, que refleja la necesidad de crear una estrategia nacional de seguridad cibernética, así como un comité interinstitucional de seguridad cibernética que se encargue del desarrollo y de la implementación de la estrategia.[220] Asimismo, en 2016 el país llegó a un acuerdo de cooperación con Israel enfocado en "fortalecer las capacidades de prevención, defensa y reacción ante eventuales ciberataques a instituciones gubernamentales, administradores de infraestructura y servicios críticos".[221] Por otro lado, mediante el programa "Transformación Digital para una Mayor Competitividad", el BID y el gobierno de Honduras están por modernizar aspectos de la ciberseguridad del país.[222]

Honduras todavía no tiene un CSIRT nacional, pero existen entidades privadas que prestan servicios de respuesta a incidentes. Aunque hay mucho que avanzar en materia de proveedores de servicios de ciberseguridad, las principales firmas del sector privado han comenzado a priorizar la seguridad cibernética y tomar precauciones al respecto.[223]

El gobierno hondureño ha tomado varias medidas para fortalecer las oportunidades de capacitación en seguridad cibernética para sus funcionarios públicos y las fuerzas armadas. Para empezar, estas últimas firmaron un acuerdo con México para "mejorar las áreas de cooperación en educación naval y militar, adiestramiento y capacitación, seguridad y defensa nacional, ciberseguridad y ciberdefensa".[224] Además, la Comisión Nacional de Telecomunicaciones (CONATEL) organizó un taller de dos días sobre ciberseguridad como parte de una estrategia nacional[225] y, aunque limitada, existe una oferta de cursos de seguridad informática y de cursos introductorios virtuales gratuitos sobre el mismo tema.

Con respecto a la legislación, Honduras ha progresado este año. El Congreso está revisando la Ley de Seguridad Cibernética, nombre con el que se conoce a la mencionada Ley Nacional de Ciberseguridad y Medidas de Protección Ante los Actos de Odio y Discriminación en Internet y Redes Sociales. Asimismo, para proteger los datos y la privacidad, el Congreso aprobó el proyecto de legislación sobre la protección de la información personal después del tercer y último debate en abril de 2018.[226] Esta nueva ley se aplica a las bases de datos del sector público y privado.[227]

En lo que respecta a los avances en tecnología, el gobierno digital es uno de los cuatro ejes estratégicos de la Agenda Digital de Honduras 2014-2018. El objetivo es promover las TIC para crear un nuevo modelo de administración pública que mejore la provisión de servicios e información, así como aumentar la eficiencia, efectividad y transparencia del sector público. Las principales iniciativas que se pondrán en marcha abarcan la creación de una red gubernamental, que incluye un portal gubernamental, un centro de contacto, un sistema electrónico para contratación pública, una página web de negocios, una ventana para el sistema electrónico de aduanas, una base de datos gubernamental y un sistema nacional para la certificación digital.[228]

Indicadores: Honduras

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

Jamaica

Habitantes

*Ref: Banco Mundial**

Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***

Jamaica lanzó su estrategia nacional de ciberseguridad en enero de 2015 con cuatro objetivos principales, a saber: establecer medidas técnicas para proteger y responder eficazmente a los ciberataques; aumentar los recursos humanos y el desarrollo de capacidades en el área de seguridad de la información; mejorar el marco regulatorio; e incrementar la educación y la conciencia pública sobre ciberseguridad.[229] Como parte de las medidas técnicas y de desarrollo de capacidades, Jamaica estableció un CSIRT nacional (JA-CIRT) bajo el Ministerio de Ciencia, Energía y Tecnología (MSTEM, por sus siglas en inglés) para monitorear el ciberespacio del país y coordinar las respuestas a incidentes cibernéticos.[230] JA-CIRT es miembro de CSIRT Américas y, por lo tanto, tiene acceso a toda la red de CSIRT. Jamaica también desarrolló el Plan Sectorial TIC 2009-2030 y una Política TIC que se aprobó en 2011. A su vez, con el apoyo del BID, en el presupuesto 2018-2019 Jamaica ha asignado fondos específicos para diferentes iniciativas de ciberseguridad en el Ministerio de Seguridad Nacional y el Ministerio de Ciencia, Energía y Tecnología.[231]

La estrategia nacional de ciberseguridad de Jamaica también dio el paso en la definición de la infraestructura crítica nacional, a la que detalló como: "los sistemas y activos, ya sean físicos o virtuales, tan críticos que la incapacitación o destrucción de tales sistemas y activos tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la seguridad o salud pública nacional, o cualquier combinación de las mismas".[232] Estas pueden incluir "redes de agua y alcantarillado, agricultura, sistemas de salud, servicios de emergencia, TI y telecomunicaciones, banca y finanzas, energía (eléctrica y eólica), transporte (aire, carretera, puerto), entidades postales y navieras".[233] En consecuencia, la estrategia le otorgó el papel principal de proteger la infraestructura crítica nacional al MSTEM, a eGov Jamaica y a los operadores de infraestructura crítica.

El gobierno ha tomado medidas importantes para mejorar la ciberseguridad del país; sin embargo, muchas empresas aún carecen de planes de respuesta a incidentes de ciberseguridad.[234] Además, con el objetivo de educar a la sociedad civil como parte de la estrategia nacional de ciberseguridad, el gobierno ha lanzado un programa de concientización pública sobre ciberseguridad en colaboración con el sector privado.[235] De hecho, la propia estrategia de ciberseguridad resalta la importancia de la participación del sector privado en actividades de ciberseguridad y en proteger los recursos privados y públicos.

En cuanto a la educación superior en ciberseguridad, existen algunos proveedores privados de servicios de ciberseguridad que realizan capacitaciones. Mientras tanto, el gobierno ha llevado a cabo varias sesiones y talleres (algunos en colaboración con JA-CIRT) para impartir formación, tanto a los funcionarios públicos como al sector privado, en habilidades y conocimientos sobre ciberseguridad.[236]

Jamaica tiene un marco regulatorio fuerte para enfrentar el delito cibernético. La Ley de Delitos Cibernéticos de 2010[237] dispone "una sanción penal por el uso indebido de sistemas informáticos o datos y el abuso de los medios electrónicos cuando se realizan transacciones y la facilitación de la investigación y el enjuiciamiento de los delitos cibernéticos".[238]

Esta Ley fue enmendada en 2015, después de una revisión exhaustiva que involucró no solo a las partes interesadas locales sino también a actores internacionales.[239] Además, actualmente se está discutiendo en el Parlamento la Ley de protección de datos que apunta a proteger "la privacidad de ciertos datos y asuntos relacionados". La Ley de protección de datos se aplicará tanto a los controladores de datos privados como a los públicos, proporcionando así una legislación integral sobre la protección de datos y privacidad. [240]

Jamaica también desarrolló el Plan Sectorial de TIC 2030[241] y una Política de TIC que se aprobó en 2011.[242] A su vez, ya está en ejecución la Ley de identificación y registro nacional,[243] aprobada en 2017; esta ley ha sido diseñada para albergar información biográfica, biométrica y demográfica en entornos independientes y altamente seguros.[244]

Indicadores: Jamaica

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia	3	3
Organización	2	2
Contenido	2	3
1-2 Respuesta a Incidentes		
Identificación de Incidentes	2	2
Organización	1	2
Coordinación	1	2
Modo de Operación	0	2
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación	2	2
Organización	1	1
Gestión de Riesgos y Respuesta	1	1
1-4 Manejo de Crisis		
Manejo de Crisis	1	1
1-5 Defensa Cibernética		
Estrategia	1	1
Organización	1	1
Coordinación	1	1
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones	1	2

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno	2	2
Sector Privado	2	2
Usuarios	1	2
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario	2	2
Confianza del Usuario en los Servicios de Gobierno Electrónico	2	2
Confianza del Usuario en los Servicios de Comercio Electrónico	2	2
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea	0	2
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia	0	2
2-5 Medios y Redes Sociales		
Medios y Redes Sociales	0	2

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

México

Habitantes

*Ref: Banco Mundial**

2017

124.777.324

Abonos a teléfonos celulares

*Ref: ITU***

2017

114.329.353

Personas con acceso a Internet

2017

79.673.128

Porcentaje de penetración de Internet

*Ref: ITU***

2017

64%

México presentó su estrategia nacional de seguridad cibernética en 2017 con el objetivo principal de identificar y establecer las acciones de seguridad cibernética aplicables a las áreas social, económica y política para permitirles a la población y las organizaciones públicas y privadas el uso de las TIC de manera responsable para el desarrollo sostenible del Estado mexicano.[245] La infraestructura de información crítica se define en la estrategia nacional de seguridad cibernética como la infraestructura de información que se considera estratégica por estar vinculada a la provisión de servicios públicos esenciales y cuyo deterioro podría comprometer la seguridad nacional. Desde hace años, México tiene un CSIRT nacional, el CERT-MX, para prevenir y mitigar las amenazas cibernéticas.[246] El CERT-MX se encuentra bajo la órbita de la Policía Federal y forma parte de la red CSIRT Américas.

Con el cibercrimen como una preocupación creciente, las organizaciones mexicanas que conducen proyectos de transformación digital han observado que grupos de interés con responsabilidades en la toma de decisiones (tales como ejecutivos) han incluido personal de seguridad y privacidad en el 96% de los casos (91% a nivel mundial) y el 44% de los casos (53% a nivel mundial), respectivamente. También, por diseño, contempla la gestión proactiva de los riesgos cibernéticos y de la privacidad en su planificación y presupuesto de proyectos como una consideración clave.[247]

En cuanto a la educación superior, hay suficientes oportunidades para que los mexicanos realicen estudios tanto de grado como de posgrado centrados en la seguridad cibernética. Asimismo, el gobierno ha promovido varios eventos en este campo, como el foro sobre ciberseguridad, con énfasis en el sector financiero,[248] o el curso básico de ciberseguridad para funcionarios públicos ofrecido por la Policía Federal.[249]

México no cuenta con una ley dedicada de delito cibernético, pero el artículo N° 211 del Código Penal prevé el delito informático.[250] Sin embargo, estas disposiciones son limitadas y dejan varias lagunas, lo que dificulta la lucha contra el cibercrimen. En términos de protección de datos y privacidad, existen dos leyes por separado: una para las bases de datos públicas y la otra para bases de datos privadas.[251]

México ha tenido una estrategia digital nacional, parte del Plan Nacional de Desarrollo 2013-2018, cuyo primer objetivo es “aumentar la digitalización de México”.[252] Esta estrategia se basaba en fomentar “tanto el despliegue y la ampliación de infraestructura de telecomunicaciones, como la adopción y la utilización de las TIC por parte de la población para aprovechar sus beneficios”.[253] Esta transformación busca construir una nueva relación entre la sociedad y el gobierno, centrada en la experiencia del ciudadano como usuario de los servicios públicos mediante la adopción de las TIC en el gobierno. Actualmente, México ofrece a sus ciudadanos el portal gob.mx, que proporciona varios servicios que incluyen identificación, salud y servicios de visado, entre otros.[254]

Indicadores: México

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

Nicaragua

Habitantes

*Ref: Banco Mundial**

2017

6.384.855

Abonos a teléfonos celulares

*Ref: ITU***

2017

8.179.876

Personas con acceso a Internet

2017

1.779.015

Porcentaje de penetración de Internet

*Ref: ITU***

2017

28%

Nicaragua se encuentra en proceso de formular una estrategia nacional de ciberseguridad, que dentro de sus ejes contendrá, entre otros puntos, la conformación de un centro de respuesta a ciberincidentes y la actualización de los marcos jurídicos, administrativos, penales y procesales que permitirán de manera amplia prevenir, investigar, juzgar y sancionar el ciberdelito.

Actualmente los incidentes de ciberseguridad son atendidos desde la Unidad de Ciberdelitos de la Policía Nacional y la Unidad Especializada de Delitos contra el Crimen Organizado del Ministerio Público, en conjunto con instituciones especializadas en la materia.

Con respecto a la legislación en el ámbito de la ciberseguridad, el país cuenta con el siguiente marco jurídico:

1) Constitución Política de la República: protege los sistemas de comunicación nacional y la administración y gestión del espectro radioeléctrico y satelital.

2) Ley N° 983 (Ley de Justicia Constitucional): regula el recurso de habeas data.

3) Ley N° 919: (Ley de Seguridad Soberana): identifica las amenazas a la seguridad soberana, entre ellas el ataque externo a la seguridad cibernética.

4) Ley N° 787 (Ley de Protección de Datos Personales):[255] protege el tratamiento automatizado de datos personales de la sociedad nicaragüense, a fin de garantizar la autodeterminación informativa.

5) Ley N° 641 (Código Penal):[256] tipifica algunas conductas relacionadas con delitos cibernéticos.

Las instituciones públicas han fortalecido sus capacidades orientadas a la seguridad cibernética, mediante el equipamiento y la capacitación especializada. El sector privado ha ampliado su oferta de servicios de ciberseguridad, los que incluyen servicios de protección en la nube pública y privada.

Con respecto al acceso a las TI, a partir de la implementación de los ejes del Programa Nacional de Desarrollo Humano 2018-2021, que contempla la promoción de la ciencia, tecnología e innovación, se continuó ejecutando el Programa Nacional de Banda Ancha con el apoyo del BID. Mediante este programa, se facilita el acceso de los municipios más alejados del país a los servicios de telecomunicaciones, fortaleciendo la conectividad del sistema nacional de salud y agropecuario.

La ampliación del acceso a las TI ha permitido extender las carreras y cursos técnicos en modalidades no presenciales, mediante el uso de la educación virtual. También se han implementado servicios y trámites públicos en línea.

De acuerdo con las estadísticas del Instituto Nicaragüense de Telecomunicaciones y Correos (TELCOR), en 2018 se registró un total de 8.179.876 abonados de telefonía móvil, con una cobertura de banda ancha fija del 92% y de banda ancha móvil del 98%, y una cobertura móvil 3G que abarca el 100% del territorio nacional.

Indicadores: Nicaragua

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia	■	■
Organización	■	■
Contenido	■	■
1-2 Respuesta a Incidentes		
Identificación de Incidentes	■	■
Organización	■	■
Coordinación	■	■
Modo de Operación		■
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación	■	■
Organización	■	■
Gestión de Riesgos y Respuesta	■	■
1-4 Manejo de Crisis		
Manejo de Crisis	■	■
1-5 Defensa Cibernética		
Estrategia	■	■
Organización	■	■
Coordinación	■	■
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones	■	■■

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno	■	■■
Sector Privado	■	■■
Usuarios	■	■
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario	■	■
Confianza del Usuario en los Servicios de Gobierno Electrónico	■	■
Confianza del Usuario en los Servicios de Comercio Electrónico	■	■
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		■
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		■
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		■■

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

Panamá

Habitantes

*Ref: Banco Mundial**

Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***

Panamá comenzó a implementar su estrategia de ciberseguridad en marzo de 2013 con la aprobación de la Resolución N° 21;[257] se trata de la Estrategia Nacional de Ciberseguridad y Protección de Infraestructuras Criticas, puesta en marcha con el lema "Panamá confiable en el ciberespacio, una labor de todos".[258] Los pilares de la misma son: proteger la privacidad; prevenir e interrumpir los delitos en el ciberespacio; fortalecer la infraestructura crítica; fomentar el desarrollo del sector privado; impulsar una cultura en materia de ciberseguridad, y en cuanto a la formación, innovación y adopción de estándares; y mejorar la capacidad de los organismos públicos para dar respuesta a incidentes.

Uno de los aspectos de la ciberseguridad que se destaca en la estrategia es la protección de la infraestructura crítica, ya que esta es "vital para el bienestar de la población, los servicios básicos, el funcionamiento del gobierno y las organizaciones privadas, el bienestar económico y la calidad de vida de las personas",[259] y de la que requiere "una protección integral".

CSIRT Panamá se estableció como el equipo nacional de respuesta a incidentes de seguridad informática en 2011 a través del Decreto Ejecutivo N° 709 en el marco de la Autoridad Nacional para la Innovación Gubernamental.[260] Además de prevenir, tratar, identificar y resolver incidentes de seguridad cibernética, CSIRT Panamá también tiene como tarea aumentar el conocimiento general del país sobre seguridad cibernética.[261] Para fortalecer esas capacidades, el gobierno de Panamá y el BID acordaron apoyar iniciativas especificas en materia de ciberseguridad a través de la operación de préstamo "Programa Panamá en Línea" aprobada en 2016.[262] Además, CSIRT Panamá es miembro de CSIRT Américas y, por lo tanto, se beneficia de todo lo que la red tiene para ofrecer.

Los proveedores del sector privado del país ofrecen su apoyo en una variedad de servicios de seguridad cibernética, desde la provisión de seguridad para las bases de datos hasta distintos tipos de capacitaciones. Además, los ciudadanos panameños tienen la gran oportunidad de continuar con su formación terciaria en seguridad cibernética y TI, lo cual incluye no sólo carreras de grado sino también maestrías. Para alentar el estudio de la seguridad cibernética, la Autoridad Nacional para la Innovación Gubernamental, en colaboración con Citi y la OEA, ha ofrecido becas para capacitaciones en seguridad cibernética con el objetivo de disminuir la deficiencia de profesionales de esta especialidad en la región.[263] Además, CSIRT Panamá ofrece formación continua en seguridad cibernética para profesionales en los departamentos de tecnología de las instituciones gubernamentales.[264]

En cuanto a la legislación, el Código Penal de Panamá contempla algunas disposiciones relacionadas con el delito cibernético.[265] Además, el Proyecto de Ley N° 558 de 2017[266] busca modificar el Código Penal, de manera de "cumplir con los estándares internacionales de seguridad informática", incluyendo el Convenio de Budapest, aprobado por Panamá en 2013.[267]

Por último, existe un proyecto de legislación para la protección de datos personales que será aplicable tanto al sector público como al privado una vez que esté aprobado.[268] Asimismo, cabe destacar que Panamá cuenta con una estrategia de gobierno electrónico y otros importantes lineamientos y reglas relacionados con la ciberseguridad y la gobernanza de las TIC, que se encuentran en su Plan Estratégico de Gobierno 2015-2019 y en la Agenda Digital 2014-2019.[269]

Indicadores: Panamá

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia	3	3
Organización	3	3
Contenido	2	2
1-2 Respuesta a Incidentes		
Identificación de Incidentes	3	3
Organización	3	3
Coordinación	2	2
Modo de Operación	0	3
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación	1	2
Organización	1	2
Gestión de Riesgos y Respuesta	1	2
1-4 Manejo de Crisis		
Manejo de Crisis	1	2
1-5 Defensa Cibernética		
Estrategia	1	2
Organización	1	1
Coordinación	1	2
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones	2	2

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno	2	2
Sector Privado	2	2
Usuarios	1	2
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario	1	2
Confianza del Usuario en los Servicios de Gobierno Electrónico	2	2
Confianza del Usuario en los Servicios de Comercio Electrónico	2	2
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea	0	2
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia	0	2
2-5 Medios y Redes Sociales		
Medios y Redes Sociales	0	2


D3
2016
2020
Formación, Capacitación y Habilidades de Seguridad Cibernética
3-1 Sensibilización
Programas de Sensibilización
Sensibilización Ejecutiva
3-2 Marco para la Formación
Provisión
Administración
3-3 Marco para la Capacitación Profesional
Provisión
Apropiación
D4
2016
2020
Marcos Legales y Regulatorios
4-1 Marcos Legales
Marcos Legislativos para la Seguridad de las TIC
Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
Legislación Sobre Protección de Datos
Protección Infantil en Línea
Legislación de Protección al Consumidor
Legislación de Propiedad Intelectual
Legislación Sustantiva Contra el Delito Cibernético
Legislación Procesal Contra el Delito Cibernético
4-2 Sistema de Justicia Penal
Fuerzas del Orden
Enjuiciamiento
Tribunales
4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético
Cooperación Formal
Cooperación Informal


D5
2016
2020
Estándares, Organizaciones y Tecnologías
5-1 Cumplimiento de los Estándares
Estándares de Seguridad de las TIC
Estándares en Adquisiciones
Estándares en el Desarrollo de Software
5-2 Resiliencia de la Infraestructura de Internet
Resiliencia de la infraestructura de Internet
5-3 Calidad del Software
Calidad del Software
5-4 Controles Técnicos de Seguridad
Controles Técnicos de Seguridad
5-5 Controles Criptográficos
Controles Criptográficos
5-6 Mercado de Seguridad Cibernética
Tecnologías de Seguridad Cibernética
Seguro Cibernético
5-7 Divulgación Responsable
Divulgación Responsable

Paraguay

Habitantes
*Ref: Banco Mundial**

Abonos a teléfonos celulares
*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet
*Ref: ITU***

En abril de 2017 Paraguay aprobó su plan nacional de ciberseguridad e integró su Comisión Nacional de Ciberseguridad con representantes de distintas instituciones públicas, con el objetivo de adoptar medidas de seguridad cibernética que garanticen y promuevan el uso seguro y confiable de las TIC, así como el progreso y la innovación en el país.[270] Además, el plan define claramente siete ejes de acción (sensibilización y cultura, investigación, desarrollo e innovación, protección de infraestructura crítica, capacidad de respuesta a incidentes cibernéticos, investigación y capacidad de enjuiciamiento cibernético, administración pública, y sistema nacional de seguridad cibernética), y en todos ellos se detallan unos "pasos a seguir" muy claros. El plan fue desarrollado como complemento para establecer iniciativas en el campo de la seguridad cibernética. Asimismo, cabe destacar que el CSIRT nacional de Paraguay (CERT-PY) es miembro de la red CSIRT Américas.[271]

Con el objetivo de incrementar las capacidades de Paraguay, en 2018 el BID aprobó el Programa de Apoyo a la Agenda Digital, operación de préstamo que comprende acciones y componentes específicos para asegurar el fortalecimiento del marco nacional de ciberseguridad.[272]

El plan nacional de ciberseguridad define la infraestructura crítica en términos de "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".[273] Esto subraya la necesidad de cooperación entre el sector público y el privado en la protección de la infraestructura crítica del país. Si bien en el sector privado ya hay algunos proveedores de servicios de seguridad cibernética, la estrategia busca aumentar la conciencia de la importancia de contar con buenas prácticas de seguridad en dicho sector. En 2017 aún no se contaba con empresas del sector privado certificadas por ISO 27001, una norma internacional de seguridad de la información, la cual fue adoptada en forma idéntica como Norma Paraguaya en noviembre de 2014 por el Instituto Nacional de Tecnología y Normalización, a través de un comité integrado por representantes de instituciones públicas, empresas privadas, asociaciones de consumidores y universidades[274] No obstante, el sector privado participó en la elaboración del plan nacional de ciberseguridad y en el establecimiento de la Norma Paraguaya ISO 27001, lo que indica su voluntad de participar cada vez más y de crear conciencia acerca de la importancia de la seguridad cibernética.

En octubre de 2018 se creó el Ministerio de Tecnologías de la Información y Comunicaciones (MITIC), uno de cuyos ejes estratégicos es la Ciberseguridad y Protección de la Información. A través de la Dirección General de Ciberseguridad y Protección de la Información, el MITIC cuenta hoy en día con los siguientes roles y atribuciones, establecidos en la Ley N° 6207/2018, que instituyó su creación:

- Construir un ecosistema digital seguro, confiable y resiliente, que incluya a los sectores público y privado, así como a la academia y la ciudadanía.
- Establecer políticas de protección de la información personal y gubernamental.
- Velar por la protección de sistemas, redes, procesos e información de los organismos y entidades del Estado.
- Idear planes y estrategias de ciberseguridad a nivel nacional.
- Ejercer la autoridad en ciberseguridad, prevención, gestión y control de incidentes cibernéticos.
- Definir y proteger la infraestructura tecnológica crítica.

El MITIC ofrece varios cursos de TI en línea de forma gratuita, los cuales se encuentran a disposición de cualquier persona que cuente con una computadora y acceso a Internet, incluidos algunos sobre seguridad de la información. Además, hay varios programas de capacitación ofrecidos por universidades y compañías de seguridad, aunque las oportunidades de realizar estudios de grado en seguridad cibernética son limitadas. Por su parte, el gobierno ha llevado a cabo campañas de educación destinadas a concientizar a la población en esta materia.[275]

Asimismo, desde la Dirección General de Ciberseguridad y Protección de la Información, perteneciente al MITIC, se cuenta con diversas iniciativas y se ofrecen diversos servicios, entre ellos alertas y boletines de seguridad, gestión de incidentes cibernéticos, auditorías de vulnerabilidades

de los sistemas gubernamentales, diagnósticos de seguridad a instituciones gubernamentales, y actividades de concienciación y capacitación para ciudadanos, empresas, el gobierno, la academia y otros sectores.

En 2011, a través de la Ley N° 4.439/11, Paraguay modificó y amplió el catálogo de hechos punibles existentes en la Ley N° 1.160/97 del Código Penal, que hace referencia a ciertos artículos que describen conductas ilícitas realizadas a través del uso de la tecnología, cuya esencia radica en su naturaleza informática, y son conocidas con el nombre de delitos informáticos.[276]

Paraguay también cuenta dentro de su legislación nacional con la Ley N° 1.682, que reglamenta la información de carácter privado y cuyo objetivo es normar "la recolección, el almacenamiento, el procesamiento y la publicación de datos o características personales". [277]

En 2017, por medio de la Ley N° 5.994/17, Paraguay se adhirió a la Convención de Budapest sobre ciberseguridad y su protocolo adicional, cuyo principal objetivo es "perseguir una política penal común dirigida a la protección de la sociedad contra el delito cibernético, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional".[278] Actualmente, como Estado parte de esta Convención, el país es beneficiario del Programa GLACY+ (Acción Global contra la Ciberdelincuencia Extendida), llevado adelante por el Consejo de Europa juntamente con la UE, con el objeto de respaldar a los países miembros a fin de lograr la implementación y armonización efectiva de la Convención a la legislación positiva nacional, a través de la promoción de estrategias legislativas contra el ciberdelito, el fortalecimiento de capacidades de los operadores de justicia y la cooperación jurídica internacional. En diciembre de 2019 Paraguay recibió a la Comitiva del Consejo de Europa a los efectos de realizar la misión inicial, compuesta por consultores expertos en el área de ciberdelincuencia, a fin de evaluar el estado en que se encuentra el país en el ámbito de la lucha contra la ciberdelincuencia, para fijar los lineamientos a seguir a través de un plan de trabajo con los diversos actores intervinientes en el área de la delincuencia informática.

El Ministerio Público posee una Unidad Especializada en Delitos Informáticos, compuesta por una Fiscalía Adjunta, una Fiscalía Delegada y tres unidades penales en la capital; también cuenta con agentes fiscales especializados en ciberdelincuencia en las principales cabeceras departamentales, para intervenir en denuncias de hechos punibles de naturaleza informática. A su vez, se destaca la existencia de una oficina de apoyo técnico para la gestión fiscal, que se encarga de dar asistencia técnica y respaldo, a los efectos de realizar diligencias de investigación que importen el uso de tecnología informática o electrónica. Por su parte, la Policía Nacional también cuenta con una división especializada de lucha contra el cibercrimen, que trabaja juntamente con el Ministerio Público.

En un proceso de innovación y adaptación a los nuevos tiempos que requieren profesionales especializados en un área que ha ido creciendo vertiginosamente en los últimos tiempos, el Ministerio de Defensa, a través del Instituto de Altos Estudios Estratégicos, viene implementando desde 2019 el Programa de Especialización en Ciberdefensa y Ciberseguridad Estratégica. Este programa representa una táctica para formar individuos capacitados para crear estrategias de lucha contra las nuevas amenazas que tienen lugar en el ciberespacio, una señal de que la modernidad ha llegado a la institución, de la cual saldrá la primera promoción de egresados.

Paraguay también tiene un borrador de Estrategia Nacional de TIC/Agenda Digital, que "se enmarca en los objetivos del Plan Nacional de Desarrollo Paraguay 2030".[279] Los ejes de la Agenda Digital son: (i) gobierno electrónico; (ii) inclusión, apropiación y uso; (iii) innovación y competitividad. La Ley N° 4.989/13 es otro importante instrumento acerca de la formulación de políticas TIC.[280] Del mismo modo, se adoptaron diversos estándares y directrices de ciberseguridad para el sector gubernamental, entre ellos:

- Controles críticos de ciberseguridad, basados en los CIS Controls, aprobados por la Resolución SENATIC 115/2018.[281]

- Criterios mínimos de seguridad para el desarrollo y adquisición de software, aprobados por resolución SENATIC 118/2018.[282]

- Directivas de ciberseguridad para canales de comunicación oficiales del estado, aprobadas por Resolución MITIC 432/2019.[283]

Indicadores: Paraguay

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

Perú

Habitantes

*Ref: Banco Mundial**

Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***

Si bien Perú aún no cuenta con una estrategia nacional de seguridad cibernética, sí ha puesto en marcha una política nacional de ciberseguridad que, entre otras cosas, destaca la necesidad de crear una estrategia nacional de ciberseguridad y un comité nacional de ciberseguridad.[284]

La Ley N° 30.618 de 2017 define la seguridad digital como la "situación de confianza en el entorno digital, frente a las amenazas que afectan las capacidades nacionales, a través de la gestión de riesgos y la aplicación de medidas de ciberseguridad y las capacidades de ciberdefensa, alineada al logro de los objetivos del Estado".[285] La Ley también define que la "Dirección Nacional de Inteligencia" es responsable por "realizar actividades y establecer los procedimientos destinados a alcanzar la seguridad digital en el ámbito de su competencia".[286]

El Decreto Supremo N° 106-2017-PCM "aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales", que son "recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales o que están destinados a cumplir dicho fin".[287]

Perú tiene un CSIRT nacional, PeCERT, cuya misión es coordinar la prevención, el tratamiento y la respuesta a incidentes de seguridad cibernética de instituciones del sector público, así como elaborar estrategias, prácticas y mecanismos necesarios para satisfacer las necesidades de seguridad de la información del Estado.[288] PeCERT se encuentra bajo la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y es miembro de la red CSIRT Américas. Además, según el Centro de Ciberseguridad Industrial, Perú está desarrollando una ley para la protección de la infraestructura crítica.[289] El gobierno de Perú y el BID, a través de la operación de préstamo "Proyecto de mejoramiento y ampliación de los servicios de soporte para la provisión de los servicios a los ciudadanos y las empresas a nivel nacional", acordaron impulsar proyectos específicos para fortalecer la ciberseguridad nacional.[290]

Perú tiene varios proveedores privados de servicios de seguridad cibernética, algunos de los cuales también ofrecen capacitación en la materia. Algunas universidades brindan la oportunidad de que los peruanos continúen su educación en seguridad cibernética, y además se han realizado eventos para tratar las temáticas organizadas por asociaciones independientes. El gobierno peruano también tomó la iniciativa en lo referente a la organización de eventos de seguridad cibernética, y así, en junio de 2018 llevó adelante la Conferencia Internacional Desafíos y Gestión en Seguridad Digital, organizada por la Dirección Nacional de Inteligencia y la Secretaría de Gobierno Digital.[291]

El tema del gobierno digital es importante para Perú, por ello se dictó la Ley de Gobierno Digital, la cual "tiene por objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno"[292] Además, se ha declarado de "interés nacional las estrategias, acciones, actividades e iniciativas para el desarrollo del gobierno digital, la innovación y la economía digital en el Perú con enfoque territorial"[293] en 2018,[294] y también se aprobaron los "lineamientos para la formulación del Plan de Gobierno Digital".[295]

Con respecto a la legislación, Perú cuenta con la Ley N° 30.096 sobre delitos informáticos, que brinda disposiciones sustantivas sobre dicho tipo de delito,[296] y la Ley N° 27.309, que incorporó el delito informático al Código Penal del país.[297] Por último, cabe mencionar la Ley N° 29.733 sobre protección de datos personales, que se aplica tanto a bases de datos públicas como privadas.[298]

Indicadores: Perú

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización
- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación
- Provisión
- Administración

3-3 Marco para la Capacitación Profesional
- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales
- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal
- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético
- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares
- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet
- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software
- Calidad del Software

5-4 Controles Técnicos de Seguridad
- Controles Técnicos de Seguridad

5-5 Controles Criptográficos
- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética
- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable
- Divulgación Responsable

República Dominicana

Habitantes

*Ref: Banco Mundial**

Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***

En junio de 2018, República Dominicana anunció su estrategia de seguridad cibernética en el marco del Decreto 230-18, que establece y regula la Estrategia Nacional de Ciberseguridad 2018-2021[299] La misión es implantar los mecanismos adecuados de seguridad cibernética para la protección del Estado, sus habitantes y, en términos más generales, la seguridad nacional.

La Estrategia Nacional se enmarca dentro del Programa República Digital creado a través del Decreto 258-16,[300] y cuenta con cuatro objetivos generales, 13 objetivos específicos, y 37 líneas de acción contenidos en los cuatro pilares que la conforman: 1) Marco legal y fortalecimiento institucional; 2) Protección de infraestructuras críticas nacionales e infraestructuras TI del gobierno; 3) Educación y cultura nacional de ciberseguridad; y 4) Alianzas nacionales e internacionales. Estos pilares, desarrollados con la participación del sector privado, tienen por finalidad establecer un mecanismo de diálogo y cooperación entre todos los sectores de la sociedad para promover las mejores prácticas, identificar problemas comunes y llevar adelante soluciones adecuadas para hacer frente a las amenazas cibernéticas.

En el marco de la Estrategia Nacional, la Protección de Infraestructuras Críticas Nacionales e Infraestructuras TI del Estado tiene como objetivo general: "Asegurar el continuo funcionamiento y la protección de la información almacenada en las infraestructuras críticas nacionales e infraestructuras TI relevantes del Estado". Para lograr este objetivo, se ha contemplado dentro de sus líneas de acción el establecimiento del Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD), que contribuye a mejorar la coordinación intersectorial e institucional para la protección de los sistemas de información y la infraestructura crítica y de TI nacionales relevantes del Estado y el sector privado.

La Estrategia Nacional contempla el establecimiento de alianzas estratégicas entre lo privado y lo público, tanto a nivel local como internacional, con el propósito de fortalecer la cooperación y sincronizar los esfuerzos para dar respuesta a los incidentes que se produzcan en materia de seguridad cibernética; por lo tanto, busca aumentar la participación del sector privado y la sociedad civil en cuestiones de seguridad cibernética. El objetivo fundamental de este pilar se centra en desarrollar la cooperación intersectorial a nivel local e internacional, con miras a compartir información sobre incidentes, amenazas, mejores prácticas, directivas y eventos e iniciativas para mejorar la resiliencia cibernética del país.

República Dominicana cuenta con una legislación específica que abarca el delito cibernético en la Ley N° 53-07[301] sobre Crímenes y Delitos de Alta Tecnología. En el mismo orden, existe la Ley N° 172-13,[302] cuyo objetivo es "la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados". Además, la Constitución de 2010 otorga[303] a todas las personas el derecho de acceder a cualquier dato que haya sobre su persona y el derecho a solicitarle a la autoridad judicial correspondiente que actualice, rectifique o destruya cualquier dato que pueda afectar ilegítimamente los derechos de una persona.[304]

República Dominicana ofrece oportunidades para que sus ciudadanos reciban capacitación en materia de seguridad cibernética y se planifican acciones para desarrollar una cultura nacional de ciberseguridad en toda la población, así como para fortalecer en la materia todos los niveles educativos, desde el nivel básico hasta los estudios terciarios y universitarios de grado y posgrado.

Indicadores: República Dominicana

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia	1	3
Organización	1	3
Contenido	1	3
1-2 Respuesta a Incidentes		
Identificación de Incidentes	2	2
Organización	2	3
Coordinación	1	2
Modo de Operación	0	2
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación	1	1
Organización	2	2
Gestión de Riesgos y Respuesta	1	1
1-4 Manejo de Crisis		
Manejo de Crisis	1	1
1-5 Defensa Cibernética		
Estrategia	1	1
Organización	1	1
Coordinación	1	1
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones	1	1

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno	2	2
Sector Privado	3	2
Usuarios	1	2
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario	2	2
Confianza del Usuario en los Servicios de Gobierno Electrónico	2	2
Confianza del Usuario en los Servicios de Comercio Electrónico	2	2
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea	0	2
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia	0	2
2-5 Medios y Redes Sociales		
Medios y Redes Sociales	0	3

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

D4 Marcos Legales y Regulatorios

D5 Estándares, Organizaciones y Tecnologías

Saint Kitts and Nevis

Habitantes

*Ref: Banco Mundial**

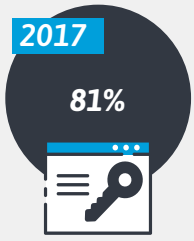
Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***



Saint Kitts and Nevis aún no ha desarrollado una estrategia nacional de ciberseguridad ni ha establecido un CSIRT nacional. Sin embargo, el gobierno es consciente de la creciente importancia de la ciberseguridad para la seguridad nacional general de un país y está trabajando para establecer un CSIRT. Además, se están realizando avances para desarrollar una estrategia nacional de ciberseguridad y un plan de implementación, establecer un Comité Nacional de Ciberseguridad, realizar entrevistas con las partes interesadas y revisar las encuestas que evalúan las necesidades actuales.

En una reunión de 2017 del Consejo de Ministros del Sistema de Seguridad Regional, presidida por el Primer Ministro de Saint Kitts and Nevis, la ciberseguridad fue uno de los puntos principales de la agenda.[305] Además, en la reapertura del Centro de TIC, las declaraciones públicas del Primer Ministro dejaron en claro que la defensa cibernética debe ser una prioridad para el país.[306] Por último, el presupuesto de 2018 menciona el Centro de TIC ahora renovado, un proyecto de infraestructura de red de gobierno electrónico y un proyecto de ciberseguridad.[307]

En el sector privado de Saint Kitts and Nevis hay algunos proveedores de servicios de ciberseguridad, aunque su alcance es limitado. Algunos prestan servicios técnicos y otros prestan servicios de sensibilización y capacitación. En ese contexto, el sector privado está comenzando a priorizar la ciberseguridad y está tomando medidas consecuentes. A nivel nacional, el gobierno ha facilitado algunos programas de capacitación en seguridad cibernética para funcionarios públicos, como la capacitación de riesgos ISO 31000.[308] Sin embargo, todavía no hay oportunidades para realizar cursos de educación superior sobre ciberseguridad.

Saint Kitts and Nevis ya contaba con una legislación para la ciberdelincuencia como la Ley de Delitos Electrónicos de 2009, que contiene delitos relacionados con el ámbito electrónico y los procedimientos para enjuiciarlos.[309] El nuevo proyecto de ley de protección de datos, promulgado en 2018, es muy similar al de la Organización de Estados del Caribe Oriental y se aplica a la información en poder del sector público y privado.[310]

El gobierno electrónico forma parte del Plan Estratégico Nacional de 2006 y tiene como objetivo aprovechar las TIC con el propósito de proporcionar información y servicios por parte del gobierno.[311] En 2016, a través de una asociación público-privada (APP), se lanzó un nuevo portal electrónico del gobierno, con la finalidad de aumentar la eficiencia en las transacciones con el gobierno. Además, el portal también conectaría diferentes ministerios y agencias gubernamentales para facilitar el intercambio de información.[312] Para 2019 se espera que se formule una estrategia digital nacional y que se incremente el despliegue de sistemas de información interconectados. Además, se espera que se implemente una nueva arquitectura empresarial gubernamental, con un diseño orientado a la seguridad, la interoperabilidad y el servicio.[313]

Indicadores: Saint Kitts and Nevis

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia	1	1
Organización	1	1
Contenido	1	1
1-2 Respuesta a Incidentes		
Identificación de Incidentes	1	1
Organización	1	1
Coordinación	1	1
Modo de Operación	0	1
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación	2	2
Organización	1	1
Gestión de Riesgos y Respuesta	1	1
1-4 Manejo de Crisis		
Manejo de Crisis	1	1
1-5 Defensa Cibernética		
Estrategia	1	1
Organización	1	1
Coordinación	1	1
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones	1	2

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno	1	2
Sector Privado	2	2
Usuarios	1	1
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario	1	1
Confianza del Usuario en los Servicios de Gobierno Electrónico	2	2
Confianza del Usuario en los Servicios de Comercio Electrónico	2	2
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea	0	2
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia	0	1
2-5 Medios y Redes Sociales		
Medios y Redes Sociales	0	2

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

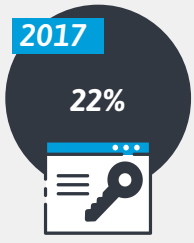
San Vicente y las Granadinas

Habitantes
*Ref: Banco Mundial**

Abonos a teléfonos celulares
*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet
*Ref: ITU***



San Vicente y las Granadinas recientemente ha tomado medidas para fortalecer su ciberseguridad, a pesar del hecho de que no se ha desarrollado una estrategia nacional en esta materia. Un ejemplo de la creciente atención a la ciberseguridad es que en diciembre de 2017 se celebró un simposio nacional sobre el tema.[314] El simposio, que atrajo a participantes de los Estados del Caribe Oriental, fue visto como un paso clave hacia un enfoque más coordinado de la ciberseguridad. Las discusiones abarcaron desde iniciativas educativas y de capacidad técnica para aumentar la concientización hasta los esfuerzos destinados a establecer un CSIRT, entidad que aún no existe en el país.[315]

El sector privado ofrece servicios de ciberseguridad, aunque limitados, y las oportunidades de estudio en este campo son escasas, pero el gobierno es consciente de la importancia del papel de la educación en ciberseguridad, en especial a nivel escolar y comunitario.[316] Finalmente, el gobierno no parece haber brindado oportunidades de capacitación en seguridad cibernética, aunque el país ha enviado representantes a varios eventos de capacitación organizados por la OEA. Cabe citar como ejemplos de esto último la capacitación internacional de cibercrimen sobre la preservación de pruebas digitales e investigaciones basadas en Internet, en colaboración con el Departamento de Estado de EE.UU. en 2016, y el Taller Subregional sobre Protección de Infraestructuras Críticas: Ciberseguridad y Protección de Fronteras, realizado en 2017. Además, en mayo de 2017 la Internet Society estableció un capítulo en San Vicente y las Granadinas con el objetivo de promover una Internet abierta y confiable.[317]

Si bien el país ya contaba con alguna legislación relacionada con la ciberseguridad, incluida la Ley de prueba electrónica de 2004 y la Ley de transacciones electrónicas de 2015,[318] no existía una ley específica para la ciberdelincuencia. Por eso, en agosto de 2016 los legisladores promulgaron el proyecto de ley de ciberdelincuencia,[319] lo que le otorgó al país un marco jurídico sustantivo y procesal para poder enfrentar de manera más efectiva el delito informático.[320]

Finalmente, en el país se puso en marcha un Plan de Estrategia de Desarrollo de Gobierno Electrónico de 2012 a 2015, con los pasos necesarios para que el programa "proporcione una infraestructura tecnológica compartida que sea estable, segura y que incluya un conjunto de políticas y estándares para la conexión a, y el uso de, esta infraestructura compartida".[321] Cabe destacar que el gobierno electrónico forma parte de la Estrategia y Plan de Acción Nacional de Tecnologías de la Información y la Comunicación de San Vicente y las Granadinas.[322]

Indicadores: San Vicente y las Granadinas

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia	2	2
Organización	1	1
Contenido	1	1
1-2 Respuesta a Incidentes		
Identificación de Incidentes	1	1
Organización	1	1
Coordinación	1	1
Modo de Operación	0	1
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación	1	1
Organización	1	1
Gestión de Riesgos y Respuesta	1	1
1-4 Manejo de Crisis		
Manejo de Crisis	1	1
1-5 Defensa Cibernética		
Estrategia	1	1
Organización	1	1
Coordinación	1	1
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones	1	2

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno	1	2
Sector Privado	2	2
Usuarios	1	1
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario	1	1
Confianza del Usuario en los Servicios de Gobierno Electrónico	1	2
Confianza del Usuario en los Servicios de Comercio Electrónico	2	2
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea	0	1
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia	0	1
2-5 Medios y Redes Sociales		
Medios y Redes Sociales	0	2

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

Santa Lucía

Habitantes

*Ref: Banco Mundial**

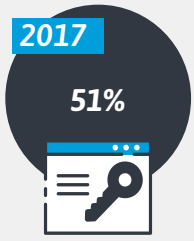
Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***



A través del Departamento de Servicio Público, el gobierno de Santa Lucía está tomando medidas para aumentar la resistencia a los ciberataques, creando así un entorno más seguro para sus operaciones e intercambio de datos.[323] En 2015 el Centro de Datos del Gobierno, administrado por los Servicios de Tecnología de la Información del Gobierno (GITS, por sus siglas en inglés), adquirió la certificación ISO 27001:2013. En abril de 2018 esta certificación debió haberse renovado debido a ciertas restricciones, pero esa formalidad no se cumplió. Actualmente, la División de Modernización del Sector Público (DPSM, por sus siglas en inglés), ubicada dentro del Departamento de Servicio Público, ha contratado los servicios de un consultor de apoyo para GITS en preparación para la recertificación de su Centro de Datos como ISO 27001:2013.

A través de la División de Modernización del Sector Público, el Departamento de Servicio Público se ha embarcado en un ejercicio para actualizar la Política Nacional de TIC y la Estrategia Sectorial. Esta estrategia busca trazar el camino a seguir para la implementación de las TIC en todos los sectores para modernizar el sector, crear nuevas oportunidades de negocios y fomentar la innovación. Con dicha finalidad, se realizó una consulta semanal con una muestra representativa de partes interesadas del gobierno, el sector privado y la sociedad civil. Así, se establecieron grupos de trabajo para revisar cada sector y hacer recomendaciones. Un sector de enfoque clave es el de seguridad nacional, que tendrá la seguridad cibernética como un punto de enfoque principal.

También ha habido apoyo del gobierno francés a la Real Policía de Santa Lucía para contribuir a construir la capacidad de recursos humanos en seguridad cibernética a través de diversas iniciativas de capacitación. La ley de uso indebido de computadoras de 2011 entró en vigor el 6 de julio de 2018 y la ley de transacciones electrónicas[324] y datos y privacidad[325] fue aprobada por el Parlamento de Santa Lucía en 2011.[326]

Además de esto, el DPSM ha establecido equipos de trabajo con el grupo de tareas de gobierno electrónico para desarrollar una hoja de ruta para el CSIRT, y una política y estrategia de seguridad cibernética. Una vez completada esta labor, sus resultados serán revisados y enviados para su aprobación y financiamiento.

A medida que Santa Lucía evoluciona hacia un gobierno más centrado en los ciudadanos a través de la implementación de iniciativas clave de TIC, las amenazas cibernéticas se convierten cada vez más en una realidad. Con este fin, el DPSM también participa en la respuesta a incidentes de ciberseguridad, cifrada en la creación de capacidad del programa de la Mancomunidad. Este es un esfuerzo para garantizar que la capacidad, el apoyo y los sistemas adecuados para desarrollar, mantener y hacer crecer un CSIRT estén dentro del gobierno. También se debe tener en cuenta que cada proyecto que emprende el DPMS se centra principalmente en la seguridad para garantizar que los recursos de datos y TIC estén protegidos. El DPSM también ha contratado los servicios de un consultor legal para revisar la legislación actual, identificar las brechas, hacer recomendaciones y, en algunos casos, redactar legislación relevante para su revisión e implementación a través de la Fiscalía General.

Indicadores: Santa Lucía

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

	2016	2020
3-1 Sensibilización		
Programas de Sensibilización		
Sensibilización Ejecutiva		
3-2 Marco para la Formación		
Provisión		
Administración		
3-3 Marco para la Capacitación Profesional		
Provisión		
Apropiación		

D4 Marcos Legales y Regulatorios

	2016	2020
4-1 Marcos Legales		
Marcos Legislativos para la Seguridad de las TIC		
Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea		
Legislación Sobre Protección de Datos		
Protección Infantil en Línea		
Legislación de Protección al Consumidor		
Legislación de Propiedad Intelectual		
Legislación Sustantiva Contra el Delito Cibernético		
Legislación Procesal Contra el Delito Cibernético		
4-2 Sistema de Justicia Penal		
Fuerzas del Orden		
Enjuiciamiento		
Tribunales		
4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético		
Cooperación Formal		
Cooperación Informal		

D5 Estándares, Organizaciones y Tecnologías

	2016	2020
5-1 Cumplimiento de los Estándares		
Estándares de Seguridad de las TIC		
Estándares en Adquisiciones		
Estándares en el Desarrollo de Software		
5-2 Resiliencia de la Infraestructura de Internet		
Resiliencia de la infraestructura de Internet		
5-3 Calidad del Software		
Calidad del Software		
5-4 Controles Técnicos de Seguridad		
Controles Técnicos de Seguridad		
5-5 Controles Criptográficos		
Controles Criptográficos		
5-6 Mercado de Seguridad Cibernética		
Tecnologías de Seguridad Cibernética		
Seguro Cibernético		
5-7 Divulgación Responsable		
Divulgación Responsable		

Suriname

Habitantes

*Ref: Banco Mundial**

Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***

Suriname aún no ha aprobado una estrategia nacional de ciberseguridad, pero a fines de 2014 el gobierno inició el proceso de desarrollar una en colaboración con la OEA.[327] Además, la "Visión 2020 de las TIC de Suriname" exige la mejora de la ciberseguridad y una mayor conciencia de las amenazas cibernéticas. Respecto de un CSIRT nacional, aún no se ha establecido, pero la Dirección de Seguridad Nacional está trabajando en uno.

En relación con los servicios de ciberseguridad, hay algunas empresas que los brindan, aunque en forma limitada. En cuanto a formación, existen algunas oportunidades para continuar la educación superior en ciberseguridad; el gobierno está comenzando a brindar capacitación sobre el tema, y el país ha recibido apoyo de organizaciones internacionales en capacitación técnica y análisis sobre ciberseguridad.[328]

Desde julio de 2019, el gobierno de Suriname ha instalado oficialmente el Comité Nacional de Ciberseguridad. Debido al aumento de los ciberataques y el cibercrimen en el país, se considera necesario mejorar la infraestructura de TI, en línea con la continua digitalización del mundo. En este sentido, la Dirección de Seguridad Nacional ha establecido el mencionado comité con las siguientes tareas:

• Actualizar el plan estratégico de ciberseguridad.

• Implementar el plan estratégico de ciberseguridad.

• Establecer el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT).

Suriname comenzó con sus sesiones de concientización sobre seguridad cibernética a través de infomerciales, redes sociales, programas de radio y televisión y sitios web oficiales.

Recientemente, el país incluyó el delito cibernético en su legislación, y también avanzó en la redacción de un proyecto de ley sobre privacidad y protección de datos, que actualmente está en curso en el Parlamento. En diciembre de 2018, el Parlamento aprobó una legislación de identificación electrónica (E-ID, por sus siglas en inglés).

Suriname tiene una estrategia de gobierno electrónico que apunta a mejorar el servicio a la ciudadanía mediante un funcionamiento gubernamental más eficiente, con el despliegue de nuevos recursos digitales. Para implementarlo, el gobierno estableció la Comisión de Gobierno Electrónico y priorizó la mejora de gobierno a gobierno, de gobierno a empresa y de gobierno a servicios ciudadanos.[329]

Indicadores: Suriname

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

	2016	2020
3-1 Sensibilización		
Programas de Sensibilización		
Sensibilización Ejecutiva		
3-2 Marco para la Formación		
Provisión		
Administración		
3-3 Marco para la Capacitación Profesional		
Provisión		
Apropiación		

D4 Marcos Legales y Regulatorios

	2016	2020
4-1 Marcos Legales		
Marcos Legislativos para la Seguridad de las TIC		
Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea		
Legislación Sobre Protección de Datos		
Protección Infantil en Línea		
Legislación de Protección al Consumidor		
Legislación de Propiedad Intelectual		
Legislación Sustantiva Contra el Delito Cibernético		
Legislación Procesal Contra el Delito Cibernético		
4-2 Sistema de Justicia Penal		
Fuerzas del Orden		
Enjuiciamiento		
Tribunales		
4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético		
Cooperación Formal		
Cooperación Informal		

D5 Estándares, Organizaciones y Tecnologías

	2016	2020
5-1 Cumplimiento de los Estándares		
Estándares de Seguridad de las TIC		
Estándares en Adquisiciones		
Estándares en el Desarrollo de Software		
5-2 Resiliencia de la Infraestructura de Internet		
Resiliencia de la infraestructura de Internet		
5-3 Calidad del Software		
Calidad del Software		
5-4 Controles Técnicos de Seguridad		
Controles Técnicos de Seguridad		
5-5 Controles Criptográficos		
Controles Criptográficos		
5-6 Mercado de Seguridad Cibernética		
Tecnologías de Seguridad Cibernética		
Seguro Cibernético		
5-7 Divulgación Responsable		
Divulgación Responsable		

Trinidad y Tobago

Habitantes

*Ref: Banco Mundial**

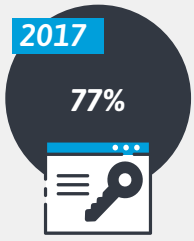
Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***



Trinidad y Tobago lanzó su estrategia de ciberseguridad en 2012 con el objetivo general de crear un entorno digital seguro para sus ciudadanos al desplegar las capacidades para proteger y gestionar incidentes de ciberseguridad y educar a la población sobre las mejores prácticas para que, en la mayor medida posible, puedan mitigar el riesgo. Además, la estrategia presenta cinco áreas clave que se deben abordar: gobernanza, gestión de incidentes, colaboración, cultura y legislación.[330] Como parte del área de gestión de incidentes, Trinidad y Tobago estableció el CSIRT nacional (TT-CSIRT) a través del Ministerio de Seguridad Nacional.[331] TT-CSIRT también es miembro de CSIRT Américas, lo que a su vez permite la colaboración internacional. La estrategia también describe la necesidad de que una agencia de ciberseguridad se haga cargo de la ciberseguridad del país. Para la creación de esta agencia, se propuso un proyecto de ley a fin de que "una ley estipule el establecimiento de la Agencia de Ciberseguridad de Trinidad y Tobago y para asuntos relacionados con la misma". Sin embargo, hasta el momento, este proyecto de ley no ha sido aprobado.

La estrategia de ciberseguridad define la infraestructura crítica en términos de "sistemas informáticos, dispositivos, redes, programas informáticos y datos informáticos, tan vitales para el país que la incapacidad, la destrucción o la interferencia con dichos sistemas y activos tendría un impacto debilitante en la seguridad, defensa o relaciones internacionales del Estado".[332] Sin embargo, no se ha establecido quién sería el responsable de la protección de la infraestructura crítica. Simplemente se menciona que es necesaria la colaboración entre el gobierno, el sector privado y la academia para proteger la infraestructura crítica de los incidentes cibernéticos.

El sector privado cuenta con algunos proveedores de servicios de ciberseguridad, pero la falta de participación de este sector es generalizada. El proyecto de ley de la Agencia de Ciberseguridad de Trinidad y Tobago exige la mejora de la cooperación entre el público y el sector relacionado con la ciberseguridad, pero recién ahora está empezando a percibirse la seguridad cibernética como una prioridad.[333]

Si bien no existe una amplia oferta de títulos terciarios o universitarios en ciberseguridad, las instituciones de educación superior de Trinidad y Tobago están comenzando a introducir algunos. Además, el gobierno ofrece ciertas oportunidades, como el taller de creación de capacidad en seguridad cibernética que realiza el Ministerio de Planificación y Desarrollo, donde los estudiantes de nivel secundario y terciario, así como los profesionales de TI, pueden aprender los aspectos básicos de la ciberseguridad.[334]

Con respecto a la legislación sobre delitos cibernéticos, Trinidad y Tobago tiene un proyecto de ley denominado "Una ley que prevé la creación de infracciones relacionadas con el delito informático y asuntos relacionados", que está pendiente de aprobación. Este proyecto de ley proporciona una definición completa de varias infracciones en materia de delitos informáticos, así como el enjuiciamiento de este tipo de delitos. Por otra parte, el país sí cuenta con una ley de protección de datos (Ley N° 13 de 2011), que cubre la protección de datos, la privacidad y la información personal.[335] Esta ley es aplicable a todos los "que manejan, almacenan o procesan información personal que pertenece a otra persona".

Aunque Trinidad y Tobago no tiene una estrategia de gobierno electrónico dedicada, sí forma parte del II Plan Nacional de las TIC de avance rápido, que se encuentra actualmente en su etapa preliminar. Uno de los objetivos estratégicos de este plan es mejorar la prestación de servicios públicos, y una de las estrategias es aumentar la eficiencia del gobierno. Trinidad y Tobago ha creado un portal gubernamental, ttconnect, que suministra una serie de servicios, pero apunta a ampliar la cantidad de servicios electrónicos disponibles para los consumidores.[336]

Indicadores: Trinidad y Tobago

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

	2016	2020
3-1 Sensibilización		
Programas de Sensibilización		
Sensibilización Ejecutiva		
3-2 Marco para la Formación		
Provisión		
Administración		
3-3 Marco para la Capacitación Profesional		
Provisión		
Apropiación		

D4 Marcos Legales y Regulatorios

	2016	2020
4-1 Marcos Legales		
Marcos Legislativos para la Seguridad de las TIC		
Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea		
Legislación Sobre Protección de Datos		
Protección Infantil en Línea		
Legislación de Protección al Consumidor		
Legislación de Propiedad Intelectual		
Legislación Sustantiva Contra el Delito Cibernético		
Legislación Procesal Contra el Delito Cibernético		
4-2 Sistema de Justicia Penal		
Fuerzas del Orden		
Enjuiciamiento		
Tribunales		
4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético		
Cooperación Formal		
Cooperación Informal		

D5 Estándares, Organizaciones y Tecnologías

	2016	2020
5-1 Cumplimiento de los Estándares		
Estándares de Seguridad de las TIC		
Estándares en Adquisiciones		
Estándares en el Desarrollo de Software		
5-2 Resiliencia de la Infraestructura de Internet		
Resiliencia de la infraestructura de Internet		
5-3 Calidad del Software		
Calidad del Software		
5-4 Controles Técnicos de Seguridad		
Controles Técnicos de Seguridad		
5-5 Controles Criptográficos		
Controles Criptográficos		
5-6 Mercado de Seguridad Cibernética		
Tecnologías de Seguridad Cibernética		
Seguro Cibernético		
5-7 Divulgación Responsable		
Divulgación Responsable		

Uruguay

Habitantes

*Ref: Banco Mundial**

2017

3.436.646

Abonos a teléfonos celulares

*Ref: ITU***

2017

5.097.569

Personas con acceso a Internet

2017

2.346.530

Porcentaje de penetración de Internet

*Ref: ITU***

2017

68%

Uruguay cuenta con un marco de ciberseguridad, aunque no sea una estrategia nacional de seguridad cibernética. Se trata de un marco organizado con referencia a estándares internacionales aplicables a las regulaciones nacionales para la mejora de la seguridad cibernética de infraestructura crítica y organizaciones públicas.[337] Además, el país tiene un CSIRT nacional, CERTuy, que se encuentra bajo la órbita de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC).[338] Por otra parte, a través del proyecto "Fortalecimiento de la Ciberseguridad en Uruguay", esta nación se ha convertido en el primer país de la región en acceder a apoyo técnico y financiero por intermedio de una operación de préstamo del BID enfocada exclusivamente en el fortalecimiento de la ciberseguridad a nivel nacional.[339] A su vez, AGESIC recibió asesoría técnica liderada por el BID para el diseño de un Centro Nacional de Formación en Ciberseguridad y apoyo para el Centro de Operaciones de Seguridad Gubernamental (GSOC). CERTuy también es miembro de la red CSIRT Américas, por lo que puede aprovechar la naturaleza colaborativa de la red.

Si bien Uruguay no define qué se entiende por "infraestructura nacional crítica", la responsabilidad sobre su protección recae en el D-CSIRT, el CSIRT perteneciente al Ministerio de Defensa según el Decreto N° 36/015 que lo creó.[340] Además, el presupuesto AGESIC 2018 asignó una cantidad considerable de fondos para el fortalecimiento de la seguridad de la información.[141]

Uruguay tiene algunos proveedores de servicios de seguridad cibernética, y parece haber una buena conciencia general sobre cuestiones de seguridad cibernética por parte del sector privado, pero es el gobierno el que parece estar brindando más servicios de seguridad cibernética y capacitación. Para empezar, el gobierno ofrece cursos de seguridad cibernética y defensa cibernética, que están disponibles para participantes del sector público y privado.[342] Además, CERTuy presenta una serie de guías y buenas prácticas en su sitio web, las cuales proporcionan recursos para cualquiera que quiera estar más informado sobre seguridad cibernética.[343] De manera conjunta, hay varias universidades que ofrecen capacitaciones y cursos sobre seguridad cibernética.

Con respecto al marco legal y regulatorio, hay algunos proyectos de ley sobre delito cibernético enfocados en proporcionar tanto la ley sustantiva como la procesal para enjuiciar el delito cibernético una vez que se pruebe.[344] Por otro lado, el país cuenta con legislación sobre la protección de datos personales y privacidad, cifrada en la Ley N° 18.331, que se aplica a las bases de datos de los sectores público y privado.[345]

Uruguay ha establecido su Plan de Gobierno Electrónico 2020, cuyo objetivo es crear valor público a través de servicios que satisfagan las necesidades, expectativas y preferencias de los ciudadanos de una manera abierta, colaborativa, inteligente, eficiente, integrada y confiable.[346] Además, el gobierno electrónico se incluyó en la Agenda Digital 2020 como parte del pilar relativo a la innovación de la relación entre el gobierno y sus ciudadanos.[347] Actualmente, Uruguay tiene un portal gubernamental, Uruguay. gub.uy, que brinda una serie de servicios para seguir el estado de varios procesos y agregar citas con instituciones gubernamentales, para el uso de firmas electrónicas y para obtener información relevante.[348]

Indicadores: Uruguay

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia	3	4
Organización	3	4
Contenido	2	3
1-2 Respuesta a Incidentes		
Identificación de Incidentes	4	4
Organización	4	5
Coordinación	4	5
Modo de Operación	0	4
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación	2	2
Organización	2	3
Gestión de Riesgos y Respuesta	2	3
1-4 Manejo de Crisis		
Manejo de Crisis	2	3
1-5 Defensa Cibernética		
Estrategia	2	3
Organización	3	3
Coordinación	3	3
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones	3	4

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno	4	5
Sector Privado	3	3
Usuarios	3	3
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario	4	4
Confianza del Usuario en los Servicios de Gobierno Electrónico	5	5
Confianza del Usuario en los Servicios de Comercio Electrónico	4	4
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea	0	4
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia	0	4
2-5 Medios y Redes Sociales		
Medios y Redes Sociales	0	3

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

Venezuela

Habitantes

*Ref: Banco Mundial**

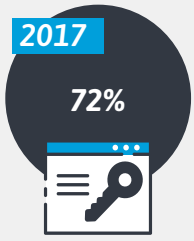
Abonos a teléfonos celulares

*Ref: ITU***

Personas con acceso a Internet

Porcentaje de penetración de Internet

*Ref: ITU***



Según datos del 2017, Venezuela actualmente no tiene una estrategia nacional de seguridad cibernética.Sin embargo, existe un sistema nacional de seguridad informática cuya aplicación es responsabilidad de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), según lo dispuesto por el artículo 54 de la Ley de Infogobierno. El objetivo de este sistema es crear condiciones que generen confianza en el uso de las TIC en manos de quienes están en el poder e implementar medidas que proporcionen niveles adecuados de seguridad para las TIC.[349] Además, existe cierta conciencia de que es necesaria una estrategia nacional de seguridad cibernética, como lo mencionó el superintendente de SUSCERTE en una ceremonia para la primera camada de graduados en informática forense en agosto de 2016.[350] SUSCERTE también es sede del CSIRT nacional de Venezuela, VenCERT, cuyo principal objetivo es prevenir, detectar y gestionar incidentes en los sistemas de información de la administración pública nacional y las entidades públicas a cargo de la gestión de infraestructura crítica.[351]

VenCERT tiene como una de sus tareas proporcionar capacitación en seguridad cibernética.[352] Durante la conferencia internacional Venezuela Digital 2017, el superintendente de SUCERTE destacó que durante 2016 se capacitaron 687 personas en seguridad cibernética en Venezuela, aunque no mencionó quien realizó dicha capacitación.[353] Además, aunque no parece haber oportunidades para que los venezolanos continúen su educación específicamente en seguridad cibernética, hay muchas opciones en temas relacionados, como informática o ingeniería de sistemas.

Hay algunas compañías privadas que brindan servicios de seguridad de la información. Sin embargo, el número de empresas y el alcance de los servicios que ofrecen son limitados. Asimismo, parece haber una falta general de conocimiento del sector privado con respecto a la seguridad cibernética, aunque algunas empresas líderes han comenzado a priorizarla.

En materia legislativa, desde octubre de 2001, Venezuela cuenta con la Ley Especial contra los Delitos Informáticos, que persigue el objetivo de proteger los sistemas que utilizan las TI, así como también prevenir y sancionar los delitos cometidos contra dichos sistemas.[354] Sin embargo, no existe legislación para la privacidad y protección de datos.[355] Las únicas disposiciones legales en esta materia conciernen a los artículos 28 y 60 de la Constitución, los cuales hacen referencia al derecho de acceder, recuperar, cambiar o destruir información personal en bases de datos privadas o públicas, y el derecho a la protección del honor y la vida privada, entre otros bienes.[356]

Indicadores: Venezuela

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia		
Organización		
Contenido		
1-2 Respuesta a Incidentes		
Identificación de Incidentes		
Organización		
Coordinación		
Modo de Operación		
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación		
Organización		
Gestión de Riesgos y Respuesta		
1-4 Manejo de Crisis		
Manejo de Crisis		
1-5 Defensa Cibernética		
Estrategia		
Organización		
Coordinación		
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones		

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno		
Sector Privado		
Usuarios		
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario		
Confianza del Usuario en los Servicios de Gobierno Electrónico		
Confianza del Usuario en los Servicios de Comercio Electrónico		
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea		
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia		
2-5 Medios y Redes Sociales		
Medios y Redes Sociales		

D3 Formación, Capacitación y Habilidades de Seguridad Cibernética

2016 | 2020

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la Capacitación Profesional

- Provisión
- Apropiación

D4 Marcos Legales y Regulatorios

2016 | 2020

4-1 Marcos Legales

- Marcos Legislativos para la Seguridad de las TIC
- Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
- Legislación Sobre Protección de Datos
- Protección Infantil en Línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación Sustantiva Contra el Delito Cibernético
- Legislación Procesal Contra el Delito Cibernético

4-2 Sistema de Justicia Penal

- Fuerzas del Orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético

- Cooperación Formal
- Cooperación Informal

D5 Estándares, Organizaciones y Tecnologías

2016 | 2020

5-1 Cumplimiento de los Estándares

- Estándares de Seguridad de las TIC
- Estándares en Adquisiciones
- Estándares en el Desarrollo de Software

5-2 Resiliencia de la Infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del Software

- Calidad del Software

5-4 Controles Técnicos de Seguridad

- Controles Técnicos de Seguridad

5-5 Controles Criptográficos

- Controles Criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

Apéndice

CSIRT

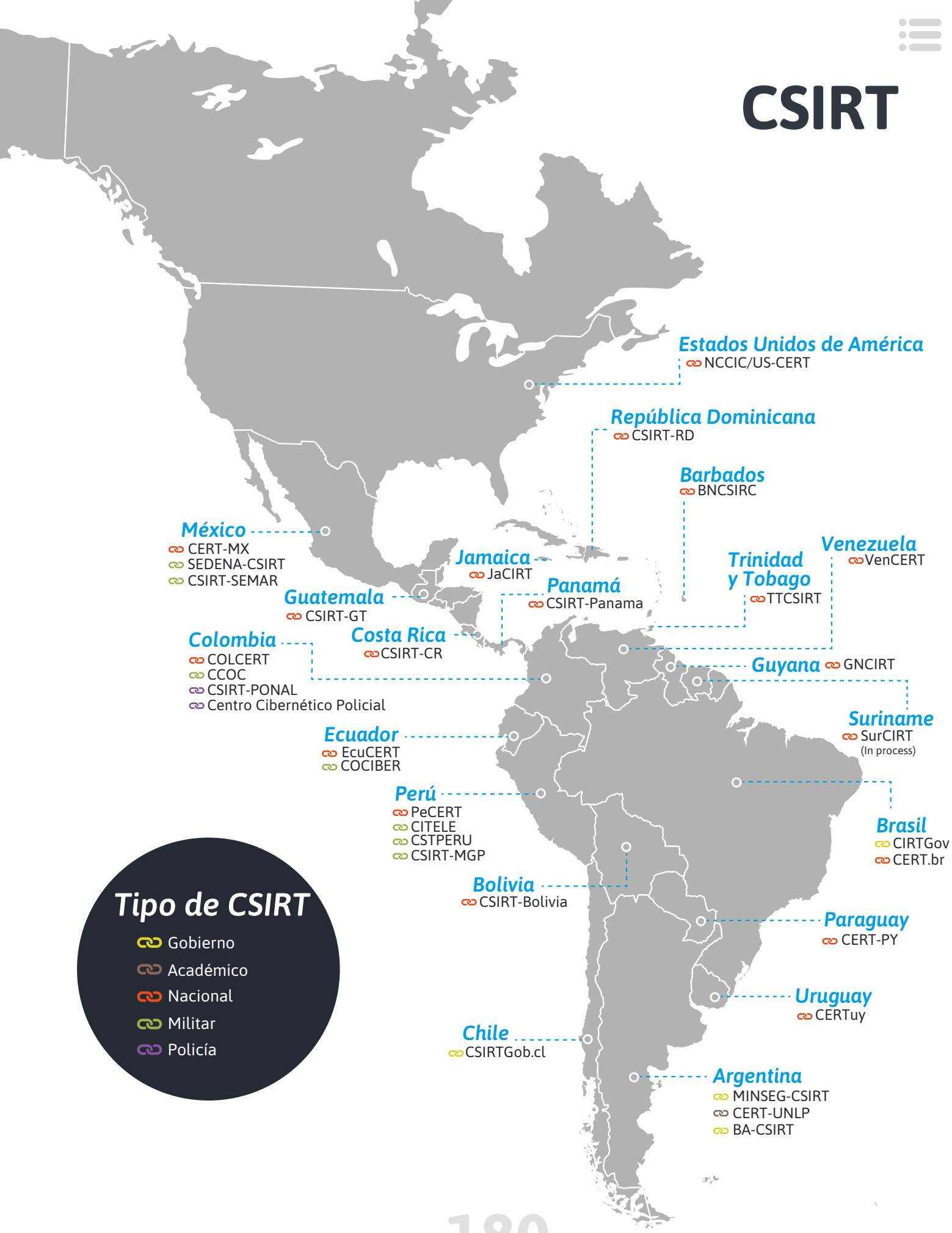
Lista de países con NCS

Convención de Budapest

Acrónimos

Referencias

CSIRT


Estados Unidos de América
NCCIC/US-CERT
República Dominicana
CSIRT-RD
Barbados
BNCSIRC
México
CERT-MX
SEDENA-CSIRT
CSIRT-SEMAR
Jamaica
JaCIRT
Venezuela
VenCERT
Trinidad y Tobago
TTCSIRT
Panamá
CSIRT-Panama
Guatemala
CSIRT-GT
Costa Rica
CSIRT-CR
Colombia
COLCERT
CCOC
CSIRT-PONAL
Centro Cibernético Policial
Guyana
GNCIRT
Suriname
SurCIRT
(In process)
Ecuador
EcuCERT
COCIBER
Perú
PeCERT
CITELE
CSTPERU
CSIRT-MGP
Brasil
CIRTGov
CERT.br
Bolivia
CSIRT-Bolivia
Paraguay
CERT-PY
Uruguay
CERTuy
Chile
CSIRTGob.cl
Argentina
MINSEG-CSIRT
CERT-UNLP
BA-CSIRT
Tipo de CSIRT
Gobierno
Académico
Nacional
Militar
Policía

Lista de CSIRT

Argentina

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Gobierno	BACSIRT	https://www.ba-csirt.gob.ar/	Ciudad de Buenos Aires	Sí
Académico	CERTUNLP	http://www.cespi.unlp.edu.ar/cert	Universidad Nacional de la Plata	Sí

Barbados

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	CIRT_BB	N-A	Barbados National Cyber Security Incidence Response Centre	Sí

Bolivia

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	CSIRT-Bolivia	http://www.csirt.gob.bo/	N-A	Sí

Chile

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Gobierno	CSIRTGob.cl	http://www.csirt.gob.cl/	Ministerio del Interior y Seguridad Pública	Sí

Colombia

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	colCERT	http://www.colcert.gov.co/	Ministerio de Defensa	Sí
Militar	CCOC-ARMADA	https://ccoc.mil.co	Comando Conjunto Cibernético	Sí

Costa Rica

Tipo	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	CSIRT-CR	https://www.micit.go.cr/	Ministerio de Ciencia Tecnología y Telecomunicaciones	Sí

Ecuador

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	EcuCERT	https://www.ecucert.gob.ec/	Agencia de Regulación y Control de las Telecomunicaciones del Ecuador	Sí
Militar	COCIBER	N-A	Comando de Ciberdefensa	Sí

Estados Unidos de América

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	CISA	https://us-cert.cisa.gov/	Department of Homeland Security (DHS)	Sí

Guatemala

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	CSIRT-gt	https://www.cert.gt/	Ministerio de Gobernacion Guatemala	Sí

Guyana

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	GNCIRT	https://cirt.gy/	Ministry of Public Security	Sí

Jamaica

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	JM_CIRT	https://www.mset.gov.jm/cyber-incident-response-team-jacirt	Ministry of Science, Energy, and Technology	Sí

México

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	CERT-MX	https://www.gob.mx/sspc	Comisión Nacional de Seguridad	Sí
Militar	SEDENA-CSIRT	https://www.gob.mx/sedena	Secretaría de la Defensa Nacional	Sí
Militar	CSIRT-SEMAR	https://www.gob.mx/semar	Secretaría de Marina	Sí

Panamá

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	CSIRT-Panamá	https://cert.pa/	Autoridad Nacional para la Innovación Gubernamental	Sí

Paraguay

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	CERT-PY	https://www.cert.gov.py/	Ministerio de Tecnologías de la Informacion y Comunicación	Sí

Perú

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Militar	CITELE_EP	http://www.ejercito.mil.pe/cotele/	Comando de Telemática del Ejército del Perú	Sí
Militar	CSTPERU	https://fap.mil.pe/	Comando Conjunto de las FF.AA. del Perú	Sí
Militar	CSIRT-MGP	N-A	Marina de Guerra del Perú	Sí

República Dominicana

Tipo:	CSIRT:	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	Csirt-RD	https://csirt.gob.do/	Presidencia de la Republica	Sí

Suriname

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	SurCIRT (In process)	www.gov.sr	De Centrale Inlichting en Veiligheidsdienst (CIVD)	Sí

Trinidad y Tobago

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	CSIRT_TT	http://ttcsirt.gov.tt/	Ministry of National Security	Sí

Uruguay

Tipo:	CSIRT	Sitio web del CSIRT	Institución anfitriona	CSIRT Américas
Nacional	CERTuy	https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/	Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento	Sí
Militar	DCSIRT	https://www.gub.uy/ministerio-defensa-nacional/	Ministerio de Defensa Nacional	Sí

Países con o en desarrollo de una Estrategia Nacional de Ciberseguridad

Convención de Budapest

Acrónimos

AGESIC
Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento de Uruguay

AGETIC
Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación de Bolivia

APP
Asociación público-privada

ARCOTEL
Agencia de Regulación y Control de las Telecomunicaciones de Ecuador

BA-CSIRT
CSIRT de la Ciudad de Buenos Aires

BID
Banco Interamericano de Desarrollo

BIDC
Barbados Investment and Development Corporation

CARICOM
Comunidad del Caribe

CCTLD
Dominio de nivel superior geográfico

CdE
Consejo de Europa

CERT
Equipo de Respuesta a Emergencias de Ciberseguridad a Computadoras

CERT.br
CERT nacional de Brasil

CERT-MX
CSIRT nacional de México

CERT-PY
CSIRT nacional de Paraguay

CERTuy
CSIRT Nacional de Uruguay

CGI
Índice de Ciberseguridad Global (ITU)

CGII
Centro de Gestión de Incidentes Informáticos de Bolivia

CICCD
Centro de Defensa Cibernética de Israel del Caribe

CIRT.GY
CSIRT Nacional de Guyana

CISM
Gerente de Seguridad de Información Certificado (ISACA)

CISSP
Certificado de Seguridad de Sistemas de Información Profesional (ISC2)

CITO
Oficina Central de Tecnología de la Información de Belize

CMF
Comisión para el Mercado Financiero de Chile

CMM
Modelo de Madurez de Capacidad de Ciberseguridad para Naciones

colCERT
Equipo nacional de respuestas a incidentes de seguridad digital de Colombia

CONATEL
Consejo Nacional de Telecomunicaciones de Haití

CONATEL
Consejo Nacional de Telecomunicaciones de Honduras

CSIRTGob.cl
Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile

CSIRT
Equipos de respuesta a incidentes de seguridad cibernética

CSIRT-CR
CSIRT Nacional de Costa Rica

CSIRT-gt
CSIRT de Gobierno de Guatemala

CSIRT-RD
Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana

CSTF
Grupo de Trabajo Nacional de Ciberseguridad de Belize

D-CSIRT
CISRT del Ministerio de Defensa de Uruguay

DPSM
División de Modernización del Sector Público de Santa Lucía

ECSO
Organización Europea de Seguridad Cibernética

EcuCERT
Equipo de Respuesta antes Incidentes Cibernéticos

E-ID
Identificación electrónica

Europol
Oficina Europea de Policía

GCSCC
Centro Global de Capacidad en Seguridad Cibernética

GDPR
Reglamento Europeo de Protección de Datos

GITS
Servicios de Tecnología de la Información del Gobierno de Santa Lucía

GLACY+
Acción Global contra la Ciberdelincuencia extendida

GSOC
Centro de Operaciones de Seguridad Gubernamental

GTCSC
Grupo de trabajo para la ciberseguridad y el delito informático

HPC
Computación de alto rendimiento

I+I
Investigación e innovación

IC
Infraestructura crítica

ICCN
Infraestructura crítica cibernética nacional

ICIC
Programa Nacional de Infraestructura de Información Crítica y Ciberseguridad de Argentina

INCIBE
Instituto Nacional de Seguridad Cibernética (España)

INTERPOL
Organización Internacional de Policía Criminal

JaCIRT
CSIRT Nacional de Jamaica

MFF
Marco Financiero Plurianual

MICITT
Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica

MinTIC
Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia

MISP
Malware Information Sharing Platform and Threat Sharing

MITIC
Ministerio de Tecnologías de la Información y Comunicaciones de Paraguay

MPTC
Ministerio de Obras Públicas, Transporte y Comunicaciones de Haití

MSET
Ministerio de Ciencia, Energía y Tecnología de Jamaica

NIS
Redes y Sistemas de Información

NSC
Estrategias de Seguridad Nacional

NCS
Estrategia Nacional de Ciberseguridad

OAS
Organización de los Estados Americanos

ONGEI
Oficina Nacional de Gobierno Electrónico e Informática de Perú

OSCE
Organización para la Seguridad y la Cooperación en Europa

PBL
Préstamo basado en políticas

PeCERT
CSIRT Nacional de Perú

PUC
Comisión de Servicios Públicos de Belice

PwC
PricewaterhouseCoopers

SMEs
Pequeñas y medianas empresas

SalCERT
CSIRT de El Salvador

SERCOP
Servicio Nacional de Contratación Pública de Ecuador

SINARDAP
Sistema Nacional de Registro de Datos Públicos de Ecuador

SUSCERTE
Superintendencia de Servicios de Certificación Electrónica de Venezuela

UE
Unión Europea

UNGGE
Grupo de Expertos Gubernamentales de la ONU

TELCOR
Instituto Nicaragüense de Telecomunicaciones y Correos

TIC
Tecnologías de la información y la comunicación

TTCSIRT
CSIRT Nacional de Trinidad y Tobago

VenCERT
CSIRT nacional de Venezuela

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

Referencias

1. Informe de amenaza de cibercrimen de Metrix: una entrevista (noviembre de 2019); disponible en https://resources.infosecinstitute.com/threatmetrix-cybercrime-report-an-interview/.

2. Véase el sitio www.trends.google.com.

3. Los números representan el interés de búsqueda en relación con el punto más alto en el gráfico para la región y el tiempo dados. Un valor de 100 es la popularidad máxima del término. Un valor de 50 significa que el término es la mitad de popular. Una puntuación de 0 significa que no hubo suficientes datos para este término.

4. https://eeas.europa.eu/topics/eu-global-strategy_en.

5. JOIN (2017) 450 final-https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017JC0450&from=en.

6. COM(2015) 185 final-
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

7. JOIN (2016) 18 final-https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

8. COM (2017) 295 final- https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0295&from=EN.

9. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

10. Directiva 2013/40/EU del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información.

11. El Convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que se ocupa especialmente de las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de la red. In 2017, 55 governments had ratified or acceded to the Council of Europe Convention on Cybercrime.Disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

12. SWD (2017) 157- https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-157-F1-EN-MAIN-PART-1.PDF.

13. En septiembre de 2017 la UE mantuvo diálogos cibernéticos con Estados Unidos, China, Japón, la República de Corea e India.

14. Véase http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

15. Hintermann, Francis. 2020. 3 Powerful Ways the Pandemic Is Changing Research Forever. Consultado el 6 de julio de 2020 en https://www.accenture.com/us-en/blogs/accenture-research/3-powerful-ways-the-pandemic-is-changing-research-forever.

16. International Data Corporation. 2019. The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast. Consultado el 6 de julio de 2020 en
https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

17. FEM (Foro Económico Mundial). 2018. Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society. Consultado el 6 de julio de 2020 en WEF_Our_Shared_Digital_Future_Report_2018.pdf.
--------. 2020a. The Global Risks Report 2020. Consultado el 6 de julio de 2020 en
https://www.weforum.org/reports/the-global-risks-report-2020.

18. FEM (Foro Económico Mundial). 2020. COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications. Consultado el 6 de julio de 2020 en https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications.

19. Cybersecurity Ventures. 2019. The 2019 Official Annual Cybercrime Report. Consultado el 6 de julio de 2020 en https://www.herjavecgroup.com/resources/2019-official-annual-cybercrime-report/.

20. FEM (Foro Económico Mundial). 2018. Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society. Consultado el 6 de julio de 2020 en WEF_Our_Shared_Digital_Future_Report_2018.pdf.

21. OCDE (Organización para la Cooperación y el Desarrollo Económicos). 2019. Shaping the Digital Transformation in Latin America: Strengthening Productivity, Improving Lives. París: Publicaciones de la OCDE. Consultado el 6 de julio de 2020 en https://doi.org/10.1787/8bb3c9f1-en.

22. CEPAL (Comisión Económica para América Latina y el Caribe), Sexta Conferencia Ministerial sobre la Sociedad de la Información en América Latina y el Carib. 2018. Proposed digital agenda for Latin America and the Caribbean (eLAC2020). Consultado el 6 de julio de 2020 en https://repositorio.cepal.org/bitstream/handle/11362/43464/S1800206_en.pdf.

23. FEM (Foro Económico Mundial). 2020. Incentivizing Responsible and Secure Innovation: A Framework for Entrepreneurs and Investors. Consultado el 6 de julio de 2020 en https://www.weforum.org/reports/incentivizing-responsible-and-secure-innovation-a-framework-for-entrepreneurs-and-investors.

24. AustCyber. 2019. Australia's Cyber Security Sector Competitiveness Plan 2019: Driving Growth and Global Competitiveness. Consultado el 6 de julio de 2020 en https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019.

25. OEA (Organización de los Estados Americanos) y ASI (Alianza por la Seguridad en Internet. 2019. Cyber-Risk Oversight Handbook for Corporate Boards. Consultado el 6 de julio de 2020 en https://www.oas.org/en/sms/cicte/docs/ENG-Cyber-Risk-Oversight-Handbook-for-Corporate-Boards.pdf.

26. OCDE (Organización para la Cooperación y el Desarrollo Económicos). 2019. Shaping the Digital Transformation in Latin America: Strengthening Productivity, Improving Lives. París: Publicaciones de la OCDE. Consultado el 6 de julio de 2020 en https://doi.org/10.1787/8bb3c9f1-en.

27. El Grupo de Expertos Gubernamentales sobre los Avances en el Comportamiento Responsable del Estado en el Ciberespacio en el Contexto de la Seguridad Internacional (GGE), establecido por la Resolución 73/266 de la Asamblea General de las Naciones Unidas; y el Grupo de Expertos Gubernamentales de composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (GTCA), establecido por la Resolución 73/27 de la Asamblea General de las Naciones Unidas.

28. Comité Interamericano contra el Terrorismo. 2017. Resolución CICTE/RES. 1/17 Establecimiento de un Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio. Adoptada en la 6a sesión plenaria, sostenida el 7 de abril de 2017. Consultado el 6 de julio de 2020 en https://www.oas.org/en/sms/cicte/session_2017.asp.

29. BID (2016), disponible en https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean.

30. https://www.oxfordmartin.ox.ac.uk/cyber-security/.

31. Véase https://www.dcc.uchile.cl/seguridad.

32. Véase http://postgrados.derecho.uchile.cl/diploma-ciberseguridad-pf/.

33. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0.

34. Fuente: Global Cyber Security Capacity Centre.

35. https://technewstt.com/caribbean-cybersecurity-dev/.

36. https://www.caricom.org/media-center/communications/news-from-the-community/caribbean-nations-sign-off-on-cyber-crime-action-plan.

37. https://caricom.org/communications/view/antigua-and-barbuda-to-host-ctu-ict-week-and-symposium.

38. https://ab.gov.ag/pdf/budget/2017_Budget_Summary.pdf.

39. Encuesta en línea de la OEA.

40. https://stopthinkconnect.org.ag/.

41. https://abiit.edu.ag/programs/.

42. http://laws.gov.ag/wp-content/uploads/2019/02/a2013-14.pdf.

43. http://laws.gov.ag/wp-content/uploads/2019/02/a2013-10.pdf.

44. https://ab.gov.ag/detail_page.php?page=30.

45. https://www.youtube.com/playlist?list=PL9-4wsDIxlCBn_AKzvPD7cBjf_Q7969IA.

46. http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm.

47. Información enviada por el país.

48. Información enviada por el país.

49. Proyecto AR-L1304 - https://www.iadb.org/es/project/AR-L1304

50. https://www.state.gov/joint-statement-on-u-s-argentina-partnership-on-cyber-policy/

51. Información enviada por el país.

52. https://www.argentina.gob.ar/modernizacion/direccion-nacional-ciberseguridad/normativa.

53. https://www.pwc.com.ar/es/prensa/ciberseguridad-empresas-argentinas-no-protegen-informacion-sensible.html.

54. http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm.

55. Información enviada por el país.

56. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/country/ARG?p_auth=RS1Kx55S.

57. http://www.oas.org/juridico/PDFs/arg_ley25326.pdf.

58. http://www.oas.org/juridico/PDFs/arg_ley25326.pdf.

59. http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/105829/norma.htm.

60. https://dpicuantico.com/sitio/wp-content/uploads/2017/02/87-2017.pdf.

61. http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/316036/norma.htm.

62. http://www.thebahamasweekly.com/publish/bis-news-updates/New_Cyber_Security_Strategy_to_strengthen_data_protection_capabilities34602.shtml.

63. https://thenassauguardian.com/2018/05/11/cybercrime-up-80-percent/.

64. https://bit.ly/2QwdUs7.

65. http://www.tribune242.com/news/2017/jul/21/bahamas-must-do-more-to-combat-cyber-crime/.

66. http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf.

67. http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0003/DataProtectionPrivacyofPersonalInformationAct_1.pdf.

68. BH-L1045 https://www.iadb.org/en/project/BH-L1045.

69. https://www.securehost.com/wp-content/uploads/docs/EBusinessPolicy.pdf.

70. http://www.vision2040bahamas.org/media/uploads/Draft__National_Development_Plan_01.12.2016_for_public_release.pdf, p. 52.

71. https://www.bahamas.gov.bs/wps/portal/public/gov/government/eServices/!ut/p/b0/04_Sj9CPykssy0xPLMnMz0vMAfGjzOKN3f19A51NLHwtAhxdDTwNQ_z9Ag19DP2djPULsh0VAZl2VXA!/.

72. https://www.bibtbahamas.com/copy-of-mp-business.

73. https://www.bifs-edu.com/cyber-security-.

74. http://www.centralbankbahamas.com/news.php?cmd=view&id=16419.

75. http://gisbarbados.gov.bb/blog/cybersecurity-strategy-for-barbados/.

76. BA-L1046 - https://www.iadb.org/es/project/BA-L1046.

77. https://www.intgovforum.org/multilingual/system/files/filedepot/21/barbados_igf_annual_2017_report.pdf.

78. http://gisbarbados.gov.bb/blog/stronger-cyber-security-paramount/.

79. https://www.caribbeancsc.com/. https://advantagecaribbean.com/cyber-security/.

80. http://www.oas.org/juridico/spanish/cyb_bbs_computer_misuse_2005.pdf.

81. https://www.barbadosparliament.com/bills/details/396

82. https://www.barbadosparliament.com/htmlarea/uploaded/File/Resolutions/Resolution_E_Government_Strategy_2006.pdf.

83. https://www.blp.org.bb/wp-content/uploads/2017/07/bb_National_ICT_Strategic_Plan_Final_2010.pdf. https://repositorio.cepal.org/bitstream/handle/11362/39858/S1501269_en.pdf?sequence=1.

84. http://gisbarbados.gov.bb/blog/government-pushing-digital-technology/.

85. http://www.caribbean360.com/business/barbados-moves-to-introduce-digital-payment-network.

86. https://www.intgovforum.org/multilingual/system/files/filedepot/21/barbados_igf_annual_2017_report.pdf.

87. http://www.cavehill.uwi.edu/programmes/#FacultyAnchor.

88. https://businessviewcaribbean.com/belize-cyber-crimes-security-symposum-raises-awareness/.

89. https://www.ub.edu.bz/academics/academic-faculties/faculty-of-science-and-technology/.

90. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

91. http://www.siliconcaribe.com/2017/05/05/belize-leads-caribbean-race-to-cyberattack-preparedness/.

92. https://developernetwork.azurewebsites.net/cito.gov.bz/egovpolicy/BelizeNatleGovPolicy2015.pdf

93. https://web.senado.gob.bo/prensa/noticias/aprueban-pl-que-declara-prioridad-nacional-la-elaboraci%C3%B3n-e-implementaci%C3%B3n-de-la.

94. https://www.cgii.gob.bo/es/normativa.

95. https://www.cgii.gob.bo/es/acerca-del-cgii.

96. https://www.csirtamericas.org/.

97. Encuesta virtual de la OEA.

98. Art. 363 del Código Penal.

99. Decreto Supremo N° 28168 Acceso a la Informacion-
https://www.comunicacion.gob.bo/?q=20130725/decreto-supremo-n%C2%BA-28168-acceso-la-informacion.

100. https://coplutic.gob.bo/IMG/pdf/plan_gobierno_electronico_.pdf.

101. Ley N° 1.080/2018: Ley de Ciudadanía Digital.

102. http://www.in.gov.br/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419

103. Propuesta de Enmienda a la Constitución N° 17 de 2019; disponible en https://www25.senado.leg.br/web/atividade/materias/-/materia/135594 (página visitada el 10 de enero de 2020).

104. Código Penal de Brasil (1940) Decreto-Ley N° 2.848 del 7 de diciembre de 1940; disponible en http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm (página visitada el 11 de mayo de 2018).

105. Código de Protección al Consumidor (Ley N° 8.078/1990); disponible en https://www.emergogroup.com/sites/default/files/file/lei_8.078_1990_consumer_protection_code.pdf (página visitada el 14 de mayo de 2018).

106. http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.

107. https://www.csirt.gob.cl/.

108. https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf.

109. CH-L1142 - https://www.iadb.org/es/project/CH-L1142.

110. CH-L1142 - https://www.iadb.org/es/project/CH-L1142.

111. http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.

112. http://www.ciberseguridad.gob.cl/consulta-ciudadana/.

113. https://alianzaciberseguridad.cl/.

114. https://www.latercera.com/pulso/noticia/gobierno-evalua-exigir-inversion-ciberseguridad-algunas-actividades-del-sector-privado/201537/.

115. https://www.leychile.cl/Navegar?idNorma=30590.

116. https://www.leychile.cl/Navegar?idNorma=141599.

117. http://www.senado.cl/proteccion-a-los-datos-personales-como-derecho-constitucional-sera-una/senado/2018-05-15/181511.html.

118. https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07

119. https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=12192-25

120. https://www.unescap.org/sites/default/files/E-Government%20Survey%202018_FINAL.pdf.

121. http://www.agendadigital.gob.cl/files/Agenda%20Digital%20Gobierno%20de%20Chile%20-%20Capitulo%203%20-%20Noviembre%202015.pdf.

122. http://www.agendadigital.gob.cl/files/Agenda%20Digital%20Gobierno%20de%20Chile%20-%20Capitulo%203%20-%20Noviembre%202015.pdf.

123. https://digital.gob.cl/instructivo/acerca-de.

124. https://www.leychile.cl/Navegar?idNorma=1138479.

125. http://www.internetsegura.cl/quienes-somos/.

126. CONPES 3701 DE 2011 Lineamientos de ciberseguridad y ciberdefensa, julio de 2011; disponible en https://www.mintic.gov.co/portal/604/w3-article-3510.html.

127. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

128. En el Comité de Seguridad Digital se estudian las siguientes temáticas: Política y Normatividad para la Seguridad Digital, Protección y Defensa de la Infraestructura Crítica Cibernética Nacional, Gestión de Riesgos de Seguridad Digital, Crisis y Seguimiento a Amenazas Cibernéticas, Protección de Datos Personales, Asuntos Internacionales de Seguridad Digital y Comunicaciones Estratégicas para la Seguridad Digital.

129. http://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=83433; https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

130. Esta función es llevada a cabo de forma colaborativa junto con el Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares y el Centro Cibernético Policial (CCP) de la Policía Nacional, el CSIRT de Gobierno, el CSIRT Financiero, la Fiscalía General de la Nación, enlaces sectoriales de seguridad digital y demás iniciativas de CSIRTS sectoriales y privados, así como entidades de orden nacional o enlaces con equipos de respuesta de otros países y organismos internacionales que por su misión puedan realizar aportes en cuanto a la respuesta a incidentes cibernéticos. Asimismo, y en caso de que se detecte un incidente que pueda llevar a una crisis nacional, el colCERT reporta de manera inmediata al Coordinador Nacional de Seguridad Digital, para activar el Comité de Seguridad Digital de modo de manejar así la crisis.

131. Asimismo, se expidió la Guía de administración de riesgos, corrupción y seguridad digital , dirigida a todas las entidades de la rama ejecutiva, mediante la cual se suministra una metodología que permita gestionar de manera efectiva los riesgos que afectan el logro de los objetivos estratégicos y de proceso, entre ellos los asociados a la seguridad digital. Igualmente, la Comisión de Regulación de Comunicaciones (CRC) expidió la Resolución N° 5.569 de 2018 "Por la cual se modifica el artículo 5.1.2.3 del Capítulo I del Título V de la Resolución CRC 5050 de 2016 en materia de gestión de seguridad en redes de telecomunicaciones y se dictan otras disposiciones".

132. CO-L1233 - https://www.iadb.org/en/project/CO-L1233.

133. https://www.mintic.gov.co/portal/604/w3-article-15119.html.

134. https://www.mintic.gov.co/portal/604/w3-article-11319.html.

135. http://www.oas.org/es/sap/dgpe/escuelagob/novedades_OEA-capacita-estudiantes-seguridad-digital.asp.

136. https://www.enticconfio.gov.co/quienes-somos.

137. http://www.oas.org/juridico/spanish/cyb_col_ley1273.pdf.

138. https://www.dnp.gov.co/programa-nacional-del-servicio-al-ciudadano/Paginas/Proteccion-de-datos-personales.aspx.

139. http://www.sic.gov.co/sites/default/files/files/Superintendente_Proteccion_Datos_Personales.pdf.

140. https://www.interpol.int/en/Who-we-are/Member-countries/Americas/COLOMBIA; https://www.europol.europa.eu/agreements/colombia

141. Naciones Unidas: Comisión de Prevención del Delito y Justicia Penal, Grupos de Expertos y de Composición Abierta; Grupo de Trabajo de Medidas de Confianza de la Organización de Estados Americanos (OEA) (en 2018 Colombia ejerció la Presidencia del Grupo); Alianza Pacífico; Convenio de Budapest-Consejo de Europa; Centro Europeo contra el cibercrimen (EC3), Organización del Tratado del Atlántico Norte (OTAN); EUROPOL e INTERPOL.

142. http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf.

143. http://estrategia.gobiernoenlinea.gov.co/623/articles-7929_recurso_1.pdf; http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf.

144. https://www.micit.go.cr/files/estrategia-nacional-ciberseguridad.

145. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=72316&nValor3=88167&strTipM=TC.

146. Encuesta en línea de la OEA.

147. Por ejemplo, https://www.tec.ac.cr/fundatec/especialista-gestion-ciberseguridad-empresarial

148. https://presidencia.go.cr/comunicados/2018/02/expertos-espanoles-estan-en-costa-rica-para-capacitar-a-funcionarios-publicos-sobre-ciberseguridad/.
https://micit.go.cr/index.php?option=com_content&view=article&id=10337:estudiantes-costarricenses-reciben-capacitacion-en-seguridad-digital-de-la-oea&catid=40&Itemid=630.

149. https://www.imprentanacional.go.cr/pub/2012/11/06/ALCA172_06_11_2012.pdf.

150. https://www.elfinancierocr.com/economia-y-politica/costa-rica-enfrenta-el-cibercrimen-con-armas-oxidadas/RIDQNOWPORGAJEES3DRE7KKEPE/story/.

151. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC.

152. http://www.firma-digital.cr/plan_maestro_gob_digital.pdf.

153. https://dsc.dm/programmes/.

154. https://www.dominicavibes.dm/education-175314/.

155. http://www.dominica.gov.dm/laws/2010/Electronic%20Evidence%20no.%2013.pdf.

156. http://www.dominica.gov.dm/laws/2013/Electronic%20Filing,%202013%20ACT%2020%20of%202013.pdf.

157. http://www.dominica.gov.dm/laws/2013/Electronic%20Funds%20Transfer%20Act,%202013%20ACT%2017%20of%202013.pdf.

158. http://www.dominica.gov.dm/laws/2013/Electronic%20Transactions%20Act,%202013%20Act%2019%20of%202013.pdf.

159. https://www.ecucert.gob.ec/nosotros.html.

160. http://www.oas.org/juridico/pdfs/mesicic4_ecu_estat.pdf, página 24.

161. https://www2.deloitte.com/ec/es/pages/risk/articles/cyber-risk-2018.html.

162. https://www.cci-es.org/web/cci/detalle-pais/-/journal_content/56/10694/445446.

163. http://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf.

164. https://vlex.ec/vid/codigo-organico-integral-penal-631464447?_ga=2.104058179.2107735450.1529940398-1975001013.1529940398#section_35.

165. Artículo 66, parágrafo 19 de la Constitución.

166. La Ley Orgánica de Comunicación, la Ley Orgánica de Telecomunicaciones, y el Reglamento a la Ley Orgánica de Telecomunicaciones tienen artículos relacionados a la protección de datos personales.

167. https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/250%20protec-intimidad-grivadeneira-12-07-2016/PP-protec-intimidad-grivadeneira-12-07-2016.pdf.

168. Fuente: Estado Miembro.

169. https://ec.okfn.org/files/2014/12/PlanGobiernoElectronicoV1.pdf.

170. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/09/PNGE_2018_2021sv2.pdf.

171. Articulo 10 (5 y 11), Ley Orgánica Del Sistema Nacional de Contratación Pública; disponible en https://www.epn.edu.ec/wp-content/uploads/2018/08/Ley-Org%C3%A1nica-de-Contrataci%C3%B3n-P%C3%BAblica.pdf.

172. https://www.gobiernoelectronico.gob.sv/wp-content/uploads/2018/09/Estrategia-de-Gobierno-Digital-2022.pdf.

173. http://www.secretariatecnica.gob.sv/category/transformacion-del-estado/gobierno-electronico/.

174. Informaciones enviadas por agentes del país.

175. https://www.theknowledgeacademy.com/sv/courses/cisa-training/

176. https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073646641_archivo_documento_legislativo.pdf.

177. https://www.asamblea.gob.sv/decretos/details/166.

178. https://www.gobiernoelectronico.gob.sv/wp-content/uploads/2018/09/Estrategia-de-Gobierno-Digital-2022.pdf.

179. http://www.secretariatecnica.gob.sv/gobierno-lanza-politica-de-datos-abiertos-y-presenta-portal-datos-gob-sv/ http://www.secretariatecnica.gob.sv/lanzan-el-sistema-integrado-de-gestion-administrativa-siga/.

180. http://tenoli.gobiernoelectronico.gob.sv/.

181. https://www.gobiernoelectronico.gob.sv/?p=483.

182. http://www.nowgrenada.com/2014/02/cyber-security-strategy-needed-fight-cyber-crimes/.

183. Encuesta en línea de la OEA.

184. http://www.gov.gd/egov/pdf/electronic_crime.pdf.

185. https://www.oecs.org/en/procurement/e-gov/data-protection-act.

186. http://www.gov.gd/egov/docs/ict_egov/ICT_strategy_grenada.pdf.

187. http://www.gov.gd/egov/docs/ict_egov/draft_2010_2014_CARICOM_egovernment_strategy.pdf.

188. Encuesta en línea de la OEA.

189. http://mingob.gob.gt/wp-content/uploads/2018/06/version-digital.pdf.

190. https://www.cert.gt/

191. https://www2.deloitte.com/gt/es/pages/risk/articles/cyber-risk.html; https://www.widefense.com/contacto/; https://www.cyberseg.com/.

192. https://www.linkedin.com/company/soluciones-seguras?originalSubdomain=gt ; https://www.facebook.com/events/ministerio-de-gobernaci%C3%B3n-guatemala/guatemala-mes-de-la-ciberseguridad/389628648376004/ ; https://www.solucionesseguras.com/noticias/soluciones-seguras-cybersecurity-magazine#edicion8 .

193. https://www.isoc.org.gt/ciberseguridad/grupo-de-trabajo-de-ciberseguridad/.

194. http://mingob.gob.gt/viceministerio-de-tecnologia-realiza-capacitacion-sobre-ciberamenazas/.

195. http://mingob.gob.gt/personal-de-gobernacion-recibe-capacitacion-para-formacion-del-primer-centro-de-respuesta-ante-incidentes-informaticos/.

196. https://www.congreso.gob.gt/assets/uploads/info_legislativo/iniciativas/Registro5254.pdf.

197. Artículo 1 de la iniciativa de ley N° 5.254 de 2017.

198. http://www.oas.org/es/sla/ddi/docs/G7%20Iniciativa%204090-2009.pdf

199. http://www.transparencia.gob.gt/ejes-de-accion/gobierno-electronico/.

200. https://cirt.gy/about.

201. https://cirt.gy/.

202. Encuesta en línea de la OEA.

203. https://www.kaieteurnewsonline.com/2019/04/06/guyana-gets-uk-help-to-fight-cyber-crime/.

204. http://dpi.gov.gy/gpf-launches-zara-cyber-security-centre-lauded-as-exemplary-publicprivate-partnership/; https://guyanachronicle.com/2017/03/22/first-cyber-security-centre-to-be-launched-in-georgetown-thousands-benefit-from-ict-training.

205. https://www.kaieteurnewsonline.com/2018/08/20/president-assents-to-cybercrime-bill/.

206. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

207. http://parliament.gov.gy/documents/bills/6033-cybercrime_bill_2016_-_no._17_of_2016.doc.

208. https://dpi.gov.gy/tag/cyber-crime-bill/.

209. https://doe.gov.gy/gsds.

210. http://conatel.gouv.ht/node/188.

211. http://www.haitilibre.com/article-24457-haiti-technologie-vers-un-centre-d-alerte-en-matiere-de-cybersecurite.html.

212. https://lenouvelliste.com/article/189514/haiti-laudit-informatique-une-necessite-pour-nos-entreprises-aujourdhui.

213. https://www.lenouvelliste.com/article/171291/cyberattaque-sommes-nous-proteges-ou-en-sommes-nous-en-haiti.

214. https://www.haiticybercon.com/.

215. Informe de país de Haití: actividades cibernéticas por año.

216. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

217. http://www.ht.undp.org/content/dam/haiti/docs/Gouvernance%20d%C3%A9mocratique%20et%20etat%20de%20droit/UNDP_HT_PLAN%20STRAT%C3%89GIQUE%20de%20developpement%20Haiti_tome1.pdf.

218. http://primature.gouv.ht/?page_id=36

219. Encuesta en línea de la OEA.

220. http://congresonacional.hn/index.php/2018/02/08/dictamen/.

221. http://www.sre.gob.hn/portada/2016/Diciembre/08-12-16/Honduras%20da%20%E2%80%9Cun%20gran%20salto%E2%80%9D%20en%20esta%20alianza%20con%20Israel.pdf.

222. HO-L1202 - https://www.iadb.org/es/project/HO-L1202.

223. Con base en las respuestas recibidas por la encuesta virtual de la OEA.

224. http://www.latribuna.hn/2018/02/09/mexico-apoyara-honduras-materia-ciberseguridad/.

225. https://ceabad.com/honduras-taller-local-ciberseguridad-como-estrategia-nacional/.

226. http://www.elheraldo.hn/pais/1168270-466/congreso-nacional-honduras-continua-aprobacion-ley-de-proteccion-datos.

227. https://cei.iaip.gob.hn/doc/Ley%20de%20Proteccion%20de%20Datos%20Personales.pdf.

228. http://agendadigital.hn/wp-content/uploads/2013/10/AgendadigitalCOR.pdf.

229. https://www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf.

230. https://jis.gov.jm/cyber-incident-response-team-fully-equipped-and-operational/.

231. https://mof.gov.jm/documents/documents-publications/document-centre/file/1643-estimates-of-expenditure-2018-2019.html.

232. https://www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf.

233. https://www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf.

234. https://www.pwc.com/jm/en/press-room/boards-and-cyber-attacks.html.

235. https://jis.gov.jm/media/Andrew-Wheatley-Sectoral-Presentation-2017.pdf.

236. https://jis.gov.jm/media/Andrew-Wheatley-Sectoral-Presentation-2017.pdf;
https://jis.gov.jm/government-employees-trained-cybersecurity/.

237. https://moj.gov.jm/sites/default/files/laws/Cybercrimes%20Act.pdf.

238. https://moj.gov.jm/laws/cybercrimes-act.

239. http://www.japarliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf.

240. https://www.japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202017----.pdf.

241. https://planipolis.iiep.unesco.org/en/2009/vision-2030-jamaica-information-and-communications-technology-ict-sector-plan-2009-2030-final.

242. https://www.mset.gov.jm/policies-glance-0.

243. https://japarliament.gov.jm/attachments/article/339/The%20National%20Identification%20and%20Registration%20Act,%202017--.pdf.

244. https://www.nidsfacts.com/.

245. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

246. https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es; http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1348059.

247. https://www.pwc.com/mx/es/archivo/2019/20190402-digital-trust-pt1.pdf?utm_source=Website&utm_medium=SiteDTrust&utm_content=DescargaPDF1.

248. https://www.gob.mx/cms/uploads/attachment/file/274782/Resumen-Ciberseguridad.pdf.

249. https://www.gob.mx/policiafederal/es/articulos/manual-basico-de-ciberseguridad-para-la-micro-pequena-y-mediana-empresa?idiom=es

250. http://www.informatica-juridica.com/codigo/articulo-211-codigo-penal-federal-mexicano/.

251. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

252. https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf.

253. https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf.

254. https://www.gob.mx/.

255. http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d.

256. https://www.poderjudicial.gob.ni/pjupload/noticia_reciente/CP_641.pdf.

257. https://www.gacetaoficial.gob.pa/pdfTemp/27289_A/GacetaNo_27289a_20130517.pdf.

258. **ibíd.**

259. **ibíd.**

260. https://www.gacetaoficial.gob.pa/pdfTemp/26880/34793.pdf.

261. https://cert.pa/sobre-nosotros/.

262. **PN-L1114 -** https://www.iadb.org/es/project/PN-L1114.

263. https://yabt.net/news.php?n=cyberseguirdad-panama-2017.

264. https://cert.pa/cursos/.

265. http://www.organojudicial.gob.pa/wp-content/uploads/2016/11/Texto-%C3%9Anico-del-C%C3%B3digo-Penal-2010.pdf.

266. http://www.asamblea.gob.pa/proyley/2017_P_558.pdf.

267. https://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2010/2013/2013_606_1726.pdf

268. https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf.

269. http://innovacion.gob.pa/descargas/Agenda_Digital_Estrategica_2014-2019.pdf.

270. https://www.mitic.gov.py/materiales/publicaciones/plan-nacional-de-ciberseguridad-paraguay; https://www.presidencia.gov.py/archivos/documentos/DECRETO7052_5cq17n8g.pdf.

271. https://www.cert.gov.py/index.php . https://www.presidencia.gov.py/archivos/documentos/DECRETO2274_30nobos1.PDF. https://www.cert.gov.py/application/files/4115/6642/8626/MITIC_Iniciativas_Ciberseguridad_PY.pdf.

272. PR-L1153 - https://www.iadb.org/es/project/PR-L1153 y https://www.mitic.gov.py/agenda-digital/documentos.

273. Plan Nacional de Ciberseguridad, página 26.

274. Plan Nacional de Ciberseguridad, página 26.

275. http://www.paraguay.com/nacionales/lanzan-campana-de-ciberseguridad-conectate-seguro-py-105453; https://www.conectateseguro.gov.py/.

276. http://fiadi.org/wp-content/uploads/2017/10/LEY-4439-DELITOS-INFORMATICOS.pdf.

277. http://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado.

278. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

279. http://gestordocumental.senatics.gov.py/share/s/kSvUFg7rSdmez7fA8OTaOA.

280. https://www.senatics.gov.py/application/files/2414/5200/6345/ley_4989_senatics.pdf.

281. https://www.cert.gov.py/index.php/controles-criticos-seguridad.

282. https://www.cert.gov.py/index.php/criterios-minimos-de-seguridad-de-software.

283. https://www.cert.gov.py/index.php/directivas-de-ciberseguridad-para-canales-de-comunicacion-oficiales-del-estado.

284. http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf.

285. https://busquedas.elperuano.pe/normaslegales/ley-que-modifica-el-decreto-legislativo-1141-decreto-legisl-ley-n-30618-1548998-4/.

286. https://busquedas.elperuano.pe/normaslegales/ley-que-modifica-el-decreto-legislativo-1141-decreto-legisl-ley-n-30618-1548998-4/.

287. https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-el-reglamento-para-la-identifica-decreto-supremo-n-106-2017-pcm-1585361-1/.

288. https://www.pecert.gob.pe/index.php/acerca-de-nosotros/que-es-el-pe-cert.

289. https://www.cci-es.org/web/cci/detalle-pais/-/journal_content/56/10694/301898.

290. PE-L1222 - https://www.iadb.org/es/project/PE-L1222.

291. https://elperuano.pe/noticia-expertos-analizan-desafios-y-gestion-seguridad-digital-66976.aspx.

292. Decreto Legislativo N° 1.412; disponible en https://busquedas.elperuano.pe/normaslegales/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1/.

293. https://busquedas.elperuano.pe/normaslegales/declaran-de-interes-nacional-el-desarrollo-del-gobierno-digi-decreto-supremo-n-118-2018-pcm-1718338-2/.

294. Decreto Supremo N° 118-2018; disponible en http://www.gobiernodigital.gob.pe/banco/segdi_BUSQ_NORMAS.asp.

295. https://www.gob.pe/institucion/pcm/normas-legales/289706-1412

296. http://www.leyes.congreso.gob.pe/Documentos/Leyes/30096.pdf.

297. http://www.oas.org/juridico/spanish/cyb_per_ley_27309.pdf.

298. http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf.

299. https://indotel.gob.do/media/10605/decreto-230-18.pdf.

300. http://optic.gob.do/wp-content/uploads/2019/02/Decreto-258-16.pdf.

301. http://www.oas.org/juridico/PDFs/repdom_ley5307.pdf.

302. https://indotel.gob.do/media/6200/ley_172_13.pdf.

303. Artículo 44 Párrafo 2 y Artículo 70 de la Constitución.

304. http://www.redipd.es/legislacion/common/legislacion/rep_dominicana/constitucion_dominicana_2010.pdf.

305. https://www.sknvibes.com/news/newsdetails.cfm/100223.

306. https://buzz-caribbean.com/article/st-kitts-government-wants-digital-transformation-of-local-economy/.

307. http://www.mof.gov.kn/wp-content/uploads/2017/12/Estimates-2018-Volume-II-Final-Website.pdf.

308. Información recibida directamente del país.

309. https://www.unodc.org/res/cld/document/kna/Electronic_Crimes_Act._No._27_of_2009_pmd_-_Electronic_Crimes_Act_No._27_of_2009.pdf.

310. https://www.thestkittsnevisobserver.com/local-news/st-kitts-and-nevis-legislators-pass-data-protection-bill-2018/.

311. https://unstats.un.org/unsd/dnss/docViewer.aspx?docID=2297.

312. http://timescaribbeanonline.com/st-kitts-nevis-government-launches-e-government-portal-that-promises-cost-effectiveness-and-time-efficiency/.

313. Información recibida directamente del país.

314. Evento patrocinado por el Grupo de Operadores de Redes del Caribe (CaribNOG, por sus siglas en inglés) y el Capítulo de SVG de la Internet Society: http://www.isoc.vc/news-release/st-vincent-to-host-cyber-security-forum/.

315. https://www.caribjournal.com/2017/12/19/st-vincent-moves-strengthen-cybersecurity/.

316. http://finance.gov.vc/finance/images/PDF/the_role_of_education_in_cyber_security.pdf.

317. http://www.isoc.vc/about/.

318. http://www.gov.vc/images/PoliciesActsAndBills/SVG_Electronic_Transactions_Act_2015.pdf

319. http://www.gov.vc/images/PoliciesActsAndBills/SVG_Cybercrime_Act_2016.pdf

320. http://www.assembly.gov.vc/assembly/images/stories/cybercrime%20bill%202016.pdf.

321. http://www.gov.vc/images/pdf_documents/svg_egov_development_strategy_report.pdf.

322. http://www.gov.vc/images/PoliciesActsAndBills/SVGICTStrategyAndActionPlanFinal.pdf.

323. www.govt.lc.

324. Electronic Transactions Act N° 16 de 2011.

325. http://www.govt.lc/news/senate-votes-on-data-protection-amendment.

326. https://stluciatimes.com/saint-lucia-to-strengthen-laws-to-protect-cyber-shoppers/

327. http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-555/14.

328. https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2017/20287.aspx; http://www.tas.sr/.

329. https://www.oas.org/es/sap/dgpe/gemgpe/suriname/suriname.pdf.

330. https://www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(English).pdf.

331. https://ttcsirt.gov.tt/index.php/background/.

332. https://www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(English).pdf.

333. Encuesta en línea de la OEA.

334. https://www.samtt.com/index.php/programmes/anglia-ruskin-university/msc-network-sec.

335. http://www.ttparliament.org/legislations/b2017h15g.pdf;
http://www.ttparliament.org/legislations/a2011-13.pdf.

336. http://www.ttconnect.gov.tt.

337. https://www.agesic.gub.uy/innovaportal/file/5823/1/marco-de-ciberseguridad-4.0-completo.pdf.

338. https://www.cert.uy/inicio/institucional/que_es_el_cert/;
https://www.agesic.gub.uy/innovaportal/v/33/1/agesic/que-es-agesic.html?idPadre=19.

339. UR-L1152 - https://www.iadb.org/en/project/UR-L1152.

340. https://www.impo.com.uy/bases/decretos/36-2015.

341. https://www.agesic.gub.uy/innovaportal/file/94/1/prespuesto_2018.pdf.

342. https://tramites.gub.uy/ampliados?id=3847.

343. https://www.cert.uy/seguroteconectas/recomendaciones.

344. https://parlamento.gub.uy/camarasycomisiones/representantes/documentos/repartido/48/433/0/pdf.

345. https://www.impo.com.uy/bases/leyes/18331-2008.

346. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/plan-de-gobierno-digital-uruguay-2020.

347. https://www.agesic.gub.uy/innovaportal/file/6122/1/agenda-uruguay-digital---enero-final.pdf.

348. https://www.gub.uy/.

349. http://www.suscerte.gob.ve/?p=2074.

350. https://www.mppeuct.gob.ve/actualidad/noticias/plan-nacional-de-ciberseguridad-y-ciberdefensa.

351. http://www.suscerte.gob.ve/?page_id=1736.

352. Ibíd..

353. http://www.presidencia.gob.ve/Site/Web/Principal/paginas/classMostrarEvento3.php?id_evento=4397.

354. http://www.redipd.es/legislacion/common/legislacion/venezuela/13-leydelitosinformaticos.pdf.

355. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

356. https://web.oas.org/mla/en/Countries_Intro/Ven_intro_fundtxt_esp_1.pdf

* https://data.worldbank.org/indicator/SP.POP.TOTL

** https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

www.observatoriociberseguridad.com

CIBERSEGURIDAD

RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

Reporte Ciberseguridad 2020

Reporte Ciberseguridad 2020

BID Mejorando vidas

OEA Más derechos para más gente

www.observatoriociberseguridad.com