

Experiencias avanzadas en políticas y prácticas de ciberseguridad

**Panorama general de Estonia, Israel,
República de Corea y Estados Unidos**

Autor:
James Andrew Lewis

Editores:
Miguel Angel Porrúa
Ana Catalina García de Alba Díaz

**Instituciones para el
Desarrollo**

**División de Capacidad
Institucional del Estado**

**DOCUMENTO PARA
DISCUSIÓN N°
IDB-DP-457**

Experiencias avanzadas en políticas y prácticas de ciberseguridad

**Panorama general de Estonia, Israel,
República de Corea y Estados Unidos**

Autor:

James Andrew Lewis

Editores:

Miguel Angel Porrúa

Ana Catalina García de Alba Díaz

Julio de 2016



BID

Banco Interamericano
de Desarrollo

<http://www.iadb.org>

Copyright © 2016 Banco Interamericano de Desarrollo. Esta obra se encuentra sujeta a una licencia Creative Commons IGO 3.0 Reconocimiento-NoComercial-SinObrasDerivadas (CC-IGO 3.0 BY-NC-ND) (<http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode>) y puede ser reproducida para cualquier uso no-comercial otorgando el reconocimiento respectivo al BID. No se permiten obras derivadas.

Cualquier disputa relacionada con el uso de las obras del BID que no pueda resolverse amistosamente se someterá a arbitraje de conformidad con las reglas de la CNUDMI (UNCITRAL). El uso del nombre del BID para cualquier fin distinto al reconocimiento respectivo y el uso del logotipo del BID, no están autorizados por esta licencia CC-IGO y requieren de un acuerdo de licencia adicional.

Note que el enlace URL incluye términos y condiciones adicionales de esta licencia.

Las opiniones expresadas en esta publicación son de los autores y no necesariamente reflejan el punto de vista del Banco Interamericano de Desarrollo, de su Directorio Ejecutivo ni de los países que representa.



Contacto: Miguel Angel Porrúa, mporrua@iadb.org.

Experiencias avanzadas en políticas y prácticas de ciberseguridad

Panorama general de Estonia, Israel,
República de Corea y Estados Unidos



Resumen

El acceso a Internet provoca un aumento de la productividad, del ingreso nacional y del empleo, y el acceso a la información cataliza el crecimiento. Sin embargo, estas oportunidades también conllevan ciertos riesgos. Las tecnologías digitales no están maduras y delincuentes y adversarios pueden aprovecharse de ellas fácilmente. Este documento de debate analiza la experiencia de cuatro de los países más avanzados en seguridad cibernética —Estonia, Israel, República de Corea y Estados Unidos—, y permitirá conocer la forma en que han abordado el problema y las lecciones que pueden extraerse de su experiencia. A fin de ofrecer una evaluación estructurada, el Centro de Estudios Estratégicos e Internacionales (CSIS) —bajo la dirección de James A. Lewis— ha basado la presente revisión en el Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM), aplicado originalmente en el “Informe Ciberseguridad 2016: ¿Estamos preparados en América Latina y el Caribe?” El CMM toma en cuenta las consideraciones de seguridad cibernética a través de cinco dimensiones de capacidad y las evalúa atendiendo a cinco etapas de madurez para cada uno de sus 49 indicadores. Este documento complementará el Informe Ciberseguridad 2016, proporcionando una visión general de las experiencias de estos destacados países, y describirá cómo han abordado la cuestión de la seguridad cibernética y cómo han evolucionado sus políticas. Por otro lado, servirá de guía para otros países a medida que vayan desarrollando sus propias estrategias nacionales de ciberseguridad.

Códigos JEL: F52, O33, O38

Palabras clave: ciberseguridad, estrategia cibernética, infraestructura crítica nacional, defensa cibernética, confianza en el uso de Internet, marcos jurídicos, respuesta a incidentes, redundancia digital, resiliencia, delincuencia cibernética

Tabla de contenidos

- Resumen ejecutivo..... 5**
- Introducción..... 8**
- República de Estonia 10**
 - Principales desafíos de ciberseguridad..... 10
 - Política y estrategia de ciberseguridad 12
 - Cultura cibernética y sociedad 13
 - Educación, formación y competencias en seguridad cibernética..... 15
 - Marco jurídico y reglamentario 17
 - Normas, organizaciones y tecnologías 18
- Estado de Israel 22**
 - Principales desafíos de ciberseguridad..... 22
 - Política y estrategia de ciberseguridad 24
 - Cultura cibernética y sociedad 26
 - Educación, formación y competencias en seguridad cibernética..... 27
 - Marco jurídico y reglamentario 29
 - Normas, organizaciones y tecnologías 30
- República de Corea 36**
 - Principales desafíos de ciberseguridad 36
 - Política y estrategia de ciberseguridad 38
 - Cultura cibernética y sociedad 39
 - Educación, formación y competencias en seguridad cibernética..... 40
 - Marco jurídico y reglamentario 41
 - Normas, organizaciones y tecnologías 43

Estados Unidos	46
Principales desafíos de ciberseguridad.....	46
Política y estrategia de ciberseguridad	48
Cultura cibernética y sociedad	49
Educación, formación y competencias en seguridad cibernética.....	50
Marco jurídico y reglamentario	52
Normas, organizaciones y tecnologías	55
Conclusiones	59

El set de datos puede ser descargado en formato abierto en: <https://mydata.iadb.org/idb/dataset/a9yc-jpsa>.

Resumen ejecutivo

El acceso a Internet y a la banda ancha provoca un aumento de la productividad, del ingreso nacional y del empleo, y el acceso a la información cataliza el crecimiento. Sin embargo, estas oportunidades también conllevan ciertos riesgos. Las tecnologías digitales no están maduras y delincuentes y adversarios pueden aprovecharse de ellas fácilmente. Así, las políticas públicas deben lograr que los países gestionen el riesgo sin sacrificar la oportunidad. Este estudio se centra en la experiencia de cuatro de los países más avanzados en seguridad cibernética —Estonia, Israel, República de Corea y Estados Unidos— para conocer de qué forma han abordado esta cuestión. Todos ellos han logrado avances significativos en ciberseguridad y su experiencia puede ofrecer lecciones útiles.

Pese a las grandes diferencias de tamaño y riqueza, estos países presentan puntos en común. Sus políticas de ciberseguridad son avanzadas porque no tardaron en aprovechar las oportunidades económicas derivadas de Internet y de la banda ancha. A su vez, todos se enfrentan a riesgos significativos. Esta combinación hace que la ciberseguridad sea esencial para ellos. La mayoría de los países no se enfrenta a amenazas similares, pero a medida que los servicios de Internet y de banda ancha se han ido convirtiendo en algo esencial para las economías nacionales, la necesidad de mejorar la ciberseguridad se ha vuelto algo no menos esencial.

Con el objetivo de ofrecer una evaluación estructurada, hemos basado nuestro análisis en el Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM), desarrollado conjuntamente por la Organización de los Estados Americanos, el Banco Interamericano de Desarrollo y la Universidad de Oxford. Los modelos de madurez de la capacidad tienen muchas aplicaciones en el mundo empresarial y en la investigación. Lo que hacen es evaluar las capacidades en una escala de complejidad, exhaustividad y sofisticación de los esfuerzos nacionales. Estas dimensiones cubren desde los esfuerzos iniciales, que tienden a ser reactivos y *ad hoc*, hasta los esfuerzos estratégicos y dinámicos, cuando los gobiernos ya han tomado decisiones en relación con políticas y asignación de recursos. Este CMM utiliza cinco niveles de madurez: inicial, formativo, establecido, estratégico y dinámico.¹ Cada nivel indica un mayor grado de sofisticación y capacidad. De esta forma, el modelo proporciona un amplio conjunto de factores para medir la madurez de los esfuerzos en materia de ciberseguridad.

Para mejorar la ciberseguridad es necesario crear estrategias, reglas e instituciones a fin de lograr que el ciberespacio sea un lugar más estable y seguro, de manera que permita el crecimiento económico y la maximización de los beneficios de las tecnologías de la información. El modelo de madurez se fija en cinco categorías de actividad: (i) Políticas y estrategia nacional de seguridad cibernética; (ii) Cultura cibernética y sociedad; (iii) Educación, formación y competencias en seguridad cibernética; (iv) Marco jurídico y reglamentario, y (v) Normas, organizaciones y tecnologías. Aunque todas son importantes, los gobiernos tendrán que establecer prioridades. Algunas mejores prácticas recomendadas pueden alcanzarse a corto plazo, mientras que para otras se necesitarían años. Los cuatro países fueron capaces de crear una estrategia de ciberseguridad en cuestión de meses; sin embargo, pese a años de esfuerzo, siguen haciendo frente a dificultades relacionadas con la mano de obra, la cultura y las normas cibernéticas.

Algunas categorías de acción mejoran la ciberseguridad de manera inmediata. La experiencia de estos países sugiere que otros países podrían centrar sus esfuerzos iniciales en tres áreas.

La primera y fundamental mejor práctica para la ciberseguridad es desarrollar una estrategia nacional. Tal estrategia proporciona un marco normativo bajo el cual los países pueden organizar sus iniciativas de ciberseguridad. Su desarrollo también puede proporcionar un mecanismo que permita una amplia coordinación gubernamental transversal.

La segunda mejor práctica es crear una estructura organizativa que asigne responsabilidades claras a los organismos gubernamentales respecto de la ciberseguridad. Un aspecto importante de esta práctica organizativa es crear una autoridad central de coordinación. La ciberseguridad es responsabilidad de muchos organismos y a veces puede darse un solapamiento de atribuciones. Para supervisar la ciberseguridad los cuatro países de referencia crearon nuevas entidades de alto nivel bajo la égida de la oficina del presidente o del primer ministro. Se trata de un paso esencial si se quiere evitar que la estrategia quede en papel mojado.

La tercera mejor práctica es la adopción de leyes y normativas en materia de ciberdelincuencia, infraestructuras críticas y protección de datos. El marco jurídico y regulatorio es crucial para la ciberseguridad. Las leyes inadecuadas dificultan los esfuerzos del gobierno, perjudican a las empresas y fomentan la delincuencia informática. Existen diferencias considerables entre los marcos jurídicos y reglamentarios de los cuatro países. Cada uno consta de un mosaico de leyes existentes y nuevas autoridades. Los cuatro consideraron necesario ampliar las autoridades legales para hacer frente a la delincuencia informática. Habida cuenta de las diferentes aplicaciones de la ciberseguridad en distintos ámbitos de la economía, con requisitos y funciones diferentes, este enfoque fragmentado podría ser más adecuado que tratar de redactar una ley única global.

La estrategia, la organización y las reglas son la primera prioridad. Una de las lecciones que puede extraerse de la experiencia de los cuatro países de referencia es que es mejor tomar medidas inmediatas antes que esperar a tener la estrategia perfecta o la ley perfecta, pues no hay estrategias perfectas. Las organizaciones siguen evolucionando según su experiencia y aprovechando las mejores prácticas de otros países. El historial de cada país muestra que la repetición y la evolución son parte de los esfuerzos nacionales para mejorar la ciberseguridad. La estrategia ha de considerarse como el inicio de un proceso que conducirá a una mejor ciberseguridad y no al fin del debate.

Todos estos países desplegaron grandes esfuerzos para incluir y hacer participar al sector privado. Estados Unidos, Estonia e Israel hicieron de la participación del sector privado un elemento fundamental de sus iniciativas de ciberseguridad. La participación del sector privado será distinta en cada país en función de su cultura política y empresarial. Algunos países todavía mantienen la propiedad o el control de los servicios públicos, lo que cambia la naturaleza de la relación en materia de regulación. Otros han privatizado sus servicios públicos y se sirven de distintos instrumentos reglamentarios y de política para regular el comportamiento empresarial.

Cabe destacar que el término “sector privado” también puede resultar engañoso. Hay muchos sectores distintos: infraestructuras críticas, empresas internacionales, y pequeñas y medianas empresas. Si bien hay aspectos comunes respecto de la forma en que los gobiernos trabajan con las empresas en términos de ciberseguridad, cada sector puede tener diferentes requisitos y su participación deberá adaptarse para lograr satisfacer mejor las necesidades. Lo anterior añade complejidad a cualquier iniciativa nacional; sin embargo, un país puede comenzar con un planteamiento sencillo, el mismo para todos los casos, y luego ir adaptándolo conforme sea necesario.

Tres de los países (Estados Unidos, Israel y República de Corea) tienen sectores muy dinámicos y competitivos en tecnología de la información (TI) que producen bienes y servicios para el mercado mundial. Esto resulta útil pero no esencial para contar con una mejor ciberseguridad nacional. Los productos y servicios de ciberseguridad están ampliamente disponibles en el mercado mundial; los países pueden comprar lo que necesitan. En cuanto a la tecnología, el énfasis debe estar en lograr comprender lo que la tecnología de punta supone para la ciberseguridad y en poner en marcha los procesos para alcanzarla. Estonia ha demostrado que es posible alcanzar un nivel excelente de ciberseguridad sin contar con una destacada industria nacional de TI. Es importante destacar que las empresas en Israel y Estados Unidos no son empresas de vanguardia directamente subvencionadas por el gobierno, lo cual introduce aspectos emprendedores e innovadores en el comportamiento empresarial. Las empresas se mueven en la dirección del mercado, apoyadas por el gobierno, no al revés. Los países pueden verse tentados a adoptar políticas para crear su propia industria de ciberseguridad, pero eso puede resultar contraproducente si el resultado es depender de productos nacionales que no sean competitivos a nivel mundial y, por tanto, que tengan menor capacidad de protección.

La estrategia, las normas y la organización son necesidades urgentes, y se pueden lograr resultados inmediatos. Otras cuestiones —por ejemplo, mano de obra, educación y cultura— son igualmente importantes, pero se requerirán esfuerzos largos y sostenidos para avanzar. Todos los países estudiados tienen dificultades en relación con la mano de obra: los expertos en ciberseguridad escasean a nivel mundial. Los cuatro países tienen programas para ampliar su mano de obra en el ámbito cibernético, generalmente en colaboración con las universidades y el sector privado.

Todos los países han hecho hincapié en el desarrollo de una cultura de ciberseguridad. Los mejores utilizan programas ya desde la escuela primaria y secundaria para inculcar buenos hábitos cibernéticos. Otros recurren a campañas de concienciación, aunque estas parecen obtener resultados desiguales.

Los cuatro países han recurrido a la cooperación internacional para fomentar la confianza, compartir las mejores prácticas e información y facilitar las iniciativas internacionales para construir un entorno cibernético estable. La cooperación incluye desde actividades entre Equipos de Respuesta a Emergencias Informáticas (CERT) hasta actividades diplomáticas de alto nivel; sin embargo, es esencial y permite el acceso de los países a recursos externos técnicos y de información. Los cuatro países se han apoyado en alianzas para reforzar sus defensas cibernéticas, y Estonia, el más pequeño de ellos, ha sido el más activo a nivel internacional.

La ciberseguridad sigue siendo un ámbito en constante evolución tanto en términos de las políticas como de la práctica. Todos los países están en el segundo o tercer ciclo de su enfoque nacional. Las mejores prácticas siguen evolucionando, guiadas por la experiencia, los nuevos retos y una mayor comprensión entre los responsables de formular las políticas.

Si se tiene en cuenta lo anterior, las experiencias de estos países suponen una guía útil para otros países que irán desarrollando sus propios enfoques nacionales sobre ciberseguridad. Estas breves evaluaciones describen de qué manera los principales países han abordado el problema de la ciberseguridad y cómo han evolucionado sus enfoques. Todos comparten el objetivo de gestionar el riesgo cibernético a fin de maximizar los beneficios del ciberespacio para sus ciudadanos y sus empresas.

Notas

1. Cybersecurity Capability Maturity Model (CMM) Pilot, diciembre de 2014 (<https://www.sbs.ox.ac.uk/cybersecurity-capacity>).

Introducción

El acceso a Internet y a la banda ancha ha aumentado la productividad, el ingreso nacional y el empleo en todo el mundo. Es un factor catalizador del crecimiento y desempeña un papel clave en cualquier estrategia moderna de desarrollo. Sin embargo, conlleva también ciertos riesgos. Las tecnologías digitales no están maduras y delincuentes y adversarios pueden aprovecharse de ellas. El acceso a Internet crea problemas de seguridad pública que requieren la acción del gobierno. Entre los mayores riesgos se encuentran la delincuencia financiera y la estabilidad de los sistemas financieros, el robo de información comercial y personal de carácter confidencial y la perturbación de los servicios críticos. Las políticas públicas deben lograr que los países gestionen el riesgo sin sacrificar la oportunidad.

Este estudio se centra en la experiencia de cuatro de los países más avanzados en seguridad cibernética, como parte de amplios esfuerzos nacionales para aprovechar el acceso a Internet y mejorar el desempeño económico y la prestación de servicios públicos. A medida que han ido avanzando, los cuatro países se han dado cuenta de la importancia de una adecuada ciberseguridad. Su experiencia permite extraer lecciones útiles que podrán tener en cuenta los países de América Latina y el Caribe.

Definimos el ciberespacio como el conjunto de dispositivos conectados a través de redes basadas en IP, no solo Internet. La ciberseguridad requiere la creación de estrategias, normas e instituciones para hacer del ciberespacio un espacio más estable y seguro, y busca proteger la información y los datos (información personal, de propiedad intelectual y de comunicaciones) y reducir el riesgo de perturbaciones en el entorno cibernético y en las infraestructuras y los servicios críticos que dependen de él.

No se puede depender exclusivamente de la tecnología para hacer frente a los retos de ciberseguridad. Con el tiempo, todos estos países han ido desarrollando y poniendo en práctica estrategias complejas para reducir el riesgo. En todos, el desarrollo ha sido gradual y se ha realizado sobre la base de la experiencia y la práctica. A partir de su experiencia, podemos sacar lecciones útiles en materia de estrategia, organización, política y regulación para aumentar la utilidad de Internet y el acceso a la banda ancha, y promover la seguridad ciudadana.

Con el fin de ofrecer una evaluación estructurada, el análisis se llevó a cabo tomando como base un Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM), desarrollado conjuntamente por la Organización de los Estados Americanos, el Banco Interamericano de Desarrollo y la Universidad de Oxford. Los modelos de madurez de capacidad, originalmente desarrollados para simplificar y mejorar el desarrollo de software, tienen ahora numerosas aplicaciones en el mundo empresarial y en la investigación. La madurez, tal como se define para este fin, se refiere al grado de formalidad del comportamiento, la práctica y los procesos en cinco áreas de capacidad: (i) Políticas y estrategia nacional de seguridad cibernética; (ii) Cultura cibernética y sociedad; (iii) Educación, formación y competencias en seguridad cibernética; (iv) Marco jurídico y reglamentario, y (v) Normas, organizaciones y tecnologías.

Los modelos de madurez evalúan las capacidades en una escala de complejidad, exhaustividad y sofisticación de los esfuerzos nacionales. Estos cubren desde los esfuerzos iniciales, que tienden a ser reactivos y *ad hoc*, hasta los esfuerzos estratégicos y dinámicos, cuando los gobiernos ya han tomado decisiones en relación con políticas y asignación de recursos. Estas decisiones pueden modificarse si las circunstancias cambian. El CMM utiliza cinco niveles de madurez: inicial, formativo, establecido, estratégico y dinámico.¹ Cada nivel indica un grado de sofisticación y capacidad. El nivel más bajo implica un nivel de capacidad *ad hoc*, mientras que el más alto indica un enfoque dinámico, capaz de responder rápidamente a nuevas exigencias.

Para decidir en qué nivel se encuadra un país hay que identificar las acciones concretas que haya adoptado y los atributos de los que goza. En el caso del desarrollo del mercado de la ciberseguridad, por ejemplo, el CMM indica el nivel de madurez mediante una escala progresiva de indicadores, que oscila entre tener acceso escaso o nulo a la tecnología y producir tecnología de la información para el mercado mundial. Cada categoría tiene indicadores específicos que se pueden utilizar para evaluar la madurez.²

En los cuatro países de referencia, el desarrollo de los esfuerzos nacionales en términos de ciberseguridad se dio de manera progresiva, y empezó a partir de legislación e instituciones existentes y fue modificándose o ampliándose con el tiempo según las necesidades mediante la creación de nuevas políticas, reglamentos, leyes e instituciones. Cabe destacar que los países continúan modificando y ajustando el enfoque nacional sobre ciberseguridad en función de la experiencia.

Una evaluación de los cuatro países analizados sugiere que todos se encuentran en algún punto entre el nivel “estratégico” y el “dinámico” en cuanto a sus capacidades de seguridad cibernética. Ninguno es completamente dinámico. En muchos aspectos lo anterior refleja la lentitud de los procesos democráticos para modificar leyes o crear nuevas organizaciones; sin embargo, todos han tenido en cuenta los requisitos en materia de ciberseguridad nacional y han tomado decisiones. En cambio, la mayoría de los países de América Latina y el Caribe están en el nivel “formativo”. Por lo tanto, este estudio se ofrece con la intención de orientar los esfuerzos nacionales para mejorar la capacidad en términos de ciberseguridad.

Hay que recalcar que los cuatro países examinados se enfrentan a serios adversarios militares en el ciberespacio. Las amenazas a la seguridad nacional y pública son un gran incentivo y explican buena parte de la atención que los cuatro países dedican a la ciberseguridad. Afortunadamente, el contexto de las amenazas es muy diferente en los países de la región, lo cual no significa que no haya que actuar. Los gobiernos se arriesgan al ignorar la ciberseguridad; la falta de atención dañará inevitablemente las perspectivas de desarrollo y crecimiento.

Notas

1. Cybersecurity Capability Maturity Model (CMM) Pilot, diciembre de 2014 (<https://www.sbs.ox.ac.uk/cybersecurity-capacity>).

2. Cybersecurity Capability Maturity Model (CMM) V1.2, págs. 8–41 (<https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version1.2.pdf>).



República de Estonia

Política y estrategia



Cultura y sociedad



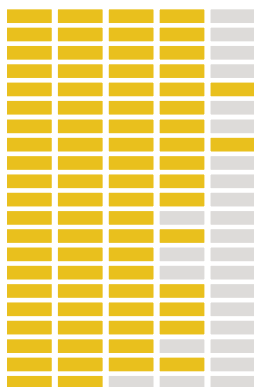
Educación



Marcos legales



Tecnología



Principales desafíos de ciberseguridad

Tras recuperar la independencia de la Unión Soviética en 1991, Estonia tenía recursos limitados para satisfacer las altas expectativas en relación con infraestructuras modernizadas y mejores servicios públicos. El vacío institucional que siguió a la independencia supuso una oportunidad única para crear tecnologías y prácticas innovadoras. Con la libertad de diseñar su propio gobierno, Estonia facilitó la pronta adopción de tecnologías de la información y la comunicación (TIC), y el gobierno adoptó de buena gana la prestación de servicios por vía electrónica. De los cuatro países analizados en esta publicación, Estonia es el que más se acerca a un enfoque “dinámico” respecto de la ciberseguridad. Sus líderes políticos han hecho de la ciberseguridad un sello distintivo de la política exterior del país.

Hoy en día, 24 años después de la independencia, la proximidad geográfica de Estonia a Rusia sigue dominando sus consideraciones de seguridad también en el ciberespacio. Adoptada en 2008, la primera estrategia de ciberseguridad de Estonia nació como respuesta a los ciberataques lanzados en 2007,¹ después de que se desplazara del centro de Tallin a un suburbio lejano una gran estatua de la era soviética que representaba a un soldado ruso. Desde entonces, la fuerte economía digital estonia y su proximidad a los centros de la ciberdelincuencia de Europa del Este la convirtieron en blanco de robos y fraudes cibernéticos. Estonia también utiliza las TIC para generar crecimiento económico, ya que incentiva a las empresas extranjeras a establecer una presencia digital en Estonia, ofreciéndoles el procesamiento en línea de servicios administrativos gubernamentales, incluidas las declaraciones de impuestos. La economía estonia en el ámbito de Internet implica flujos de datos transfronterizos, a menudo apoyándose en una infraestructura de TIC con sede fuera del país. El gobierno de Estonia hace un seguimiento de esas interdependencias de TIC para preparar sistemas de copias de seguridad y redundancias en caso de una potencial interrupción derivada de un ataque cibernético o un desastre natural.

POBLACIÓN TOTAL DEL PAÍS

1.314.545

Penetración de Internet

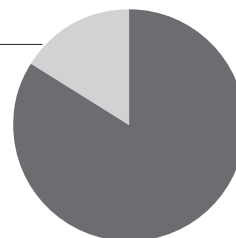
Abonos a teléfonos celulares

2.062.864

Personas con acceso a Internet

1.106.846

84%

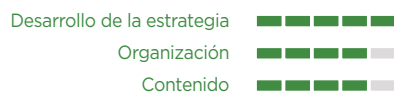


Fuente: Indicadores de Desarrollo del Banco Mundial (2014). Disponible en: <http://databank.worldbank.org/data/reports.aspx?source=2&country=USA&series=&period=>

Política y estrategia



Estrategia nacional de seguridad cibernética oficial o documentada



Defensa cibernética



Cultura y sociedad



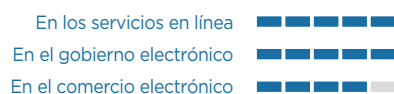
Mentalidad de seguridad cibernética



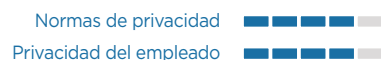
Conciencia de seguridad cibernética



Confianza en el uso de Internet



Privacidad en línea



Educación



Disponibilidad nacional de la educación y formación cibernéticas



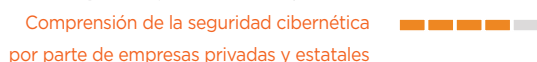
Desarrollo nacional de la educación de seguridad cibernética



Formación e iniciativas educativas públicas y privadas



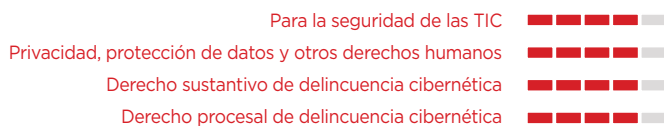
Gobernanza corporativa, conocimiento y normas



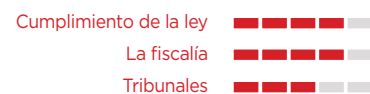
Marcos legales



Marcos jurídicos de seguridad cibernética



Investigación jurídica



Divulgación responsable de la información



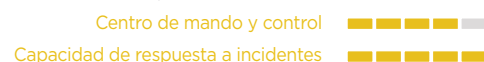
Tecnologías



Adhesión a las normas



Organizaciones de coordinación de seguridad cibernética



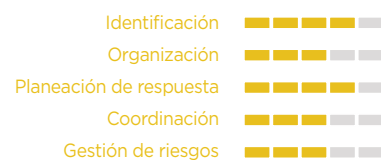
Respuesta a incidentes



Resiliencia de la infraestructura nacional



Protección de la Infraestructura Crítica Nacional (ICN)



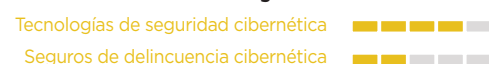
Gestión de crisis



Redundancia digital



Mercado de la ciberseguridad





INICIAL



FORMATIVO



ESTABLECIDO



ESTRATÉGICO



DINÁMICO



Política y estrategia de ciberseguridad

Dinámico

Estonia fue uno de los primeros países en elaborar una estrategia nacional de ciberseguridad. El gobierno actualizó en 2014 su estrategia de 2008, con una versión revisada que cubre el período 2014–17. La estrategia es el documento básico de planificación de la ciberseguridad y un elemento de una estrategia más amplia de seguridad nacional. La nueva estrategia se basa en su predecesora, pero vuelve a evaluar su enfoque a la luz de los cambios en el entorno de las amenazas. La estrategia estonia de ciberseguridad 2014–17 tiene varios objetivos, entre ellos:

- Revitalizar un enfoque integral y de todo el gobierno sobre la ciberseguridad.
- Crear un nivel muy alto de competencia y concienciación sobre la ciberseguridad en los organismos, las empresas y el público.
- Fortalecer la regulación para asegurar los sistemas de información.
- Apoyar los esfuerzos para poner en marcha la cooperación internacional en ciberseguridad.

La estrategia se centra en garantizar la prestación de servicios vitales, aumentando la capacidad del país para combatir la ciberdelincuencia y mejorando su capacidad de defensa nacional. Aunque la tarea se asigna a diversos organismos en el plano nacional, la perspectiva general de Estonia busca evitar la compartimentación de responsabilidades para asegurar una respuesta coordinada en caso de un incidente cibernético nacional significativo. Entre las tareas que define la estrategia se cuentan desarrollar el marco jurídico, mejorar la cooperación internacional y ampliar el número de expertos y soluciones para la ciberseguridad.

Estonia realizó cambios organizativos importantes para brindar apoyo a su estrategia de ciberseguridad. En 2009, se creó un Consejo de Seguridad Cibernética, encargado de apoyar la cooperación entre organismos y supervisar la ejecución de la estrategia, y que depende de la Comisión de Seguridad del Gobierno de la República (un cuerpo ministerial). A la Autoridad del Sistema de Información de Estonia (Riigi Infosüsteemi Amet, o RIA) se le concedieron poderes y recursos adicionales para la protección de las redes públicas. En el seno de la RIA, se creó un Departamento de Protección de las Infraestructuras Críticas de Información.

La RIA llevó a cabo un proyecto de mapeo de infraestructuras críticas para identificar los servicios vitales que dependen de medios cibernéticos y formó una comisión para promover la cooperación público-privada. Las unidades de delitos informáticos de la Dirección de la Policía y la Guardia de Fronteras se fusionaron en 2012. En 2011 se creó una Unidad de Defensa Cibernética como parte de la Liga de Defensa de Estonia, una organización voluntaria de defensa interna² que lleva su experiencia del sector privado al ámbito público.

El Consejo de Seguridad Cibernética supervisa la aplicación general de la estrategia de ciberseguridad de Estonia y cuenta con el apoyo del Ministerio de Economía y Comunicaciones, que coordina la ejecución de la política de ciberseguridad entre los organismos gubernamentales, la sociedad civil, las empresas privadas y las instituciones educativas. Todos los organismos involucrados en ciberseguridad³ presentan un informe anual al Ministerio de Economía y Comunicaciones sobre las medidas que hayan adoptado y sus resultados.

El Equipo de Respuesta ante Emergencias Cibernéticas (CERT-EE) gestiona la respuesta a incidentes. Establece prioridades entre los casos siguiendo cuatro principios:⁴ (i) el número de usuarios afectados; (ii) la gravedad del incidente; (iii) el objetivo y punto de origen del ataque, y (iv) los recursos necesarios para gestionarlo.

El CERT-EE opera en el marco de la RIA, que supervisa las vulnerabilidades de los sistemas de información de servicios vitales e infraestructuras críticas. Como tal, mantiene la plataforma X-Road, destinada al intercambio seguro de información entre los organismos gubernamentales y la población en general.⁵ Iniciada en 2001 para conectar las bases de datos del gobierno, la plataforma ofrece en la actualidad servicios de comunicaciones seguras a los agentes acreditados del sector privado.

Estonia ha llevado a cabo ejercicios nacionales de ciberseguridad en 2010, 2012 y 2015. Las universidades también pueden utilizar los dispositivos cibernéticos establecidos para fines de capacitación. Fortalecer la capacidad nacional mediante la cooperación con aliados internacionales y asociados del sector privado no es solo una medida de fomento de la confianza, sino también de reducción de costos. La concepción de la ciberseguridad de Estonia también abarca la protección del ejercicio en línea de los derechos fundamentales y la libertad de los ciudadanos.

D1-1 Estrategia nacional de seguridad cibernética oficial o documentada

Estonia actualizó su estrategia cibernética en 2014 tras la evaluación del impacto de su primer documento de planificación de 2008. El documento está diseñado para un plazo determinado (2014–17), con evaluaciones de desempeño anuales y ajustes correspondientes.

http://www.eata.ee/wp-content/uploads/2009/11/Estonian_Cyber_Security_Strategy.pdf

https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

D1-2 Consideración de la defensa cibernética

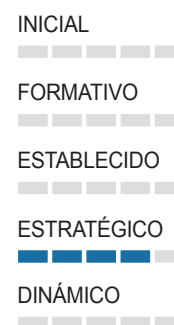
Los ejercicios regulares con aliados de la OTAN forman un elemento central de la estrategia de 2014. La creación de la Unidad de Defensa Cibernética dentro de la Liga por la Defensa de Estonia ha reforzado la cooperación entre los sectores civiles y militares en cuanto a defensa cibernética.

<https://ccdcoe.org/multimedia/cyber-defence-unit-estonian-defence-league-legal-policy-and-organisational-analysis-0.html>

Cultura cibernética y sociedad

Estratégico

Estonia se enorgullece de sus avanzados servicios de gobierno electrónico y de los buenos conocimientos tecnológicos de su población. Es líder en gobernanza electrónica, también en la autenticación digital de la identidad. Su tarjeta de identificación electrónica es el elemento clave para acceder a los servicios de gobierno electrónico. La firma digital y el certificado digital de autenticación



de la identidad almacenados en la tarjeta dan acceso a los ciudadanos a sistemas de voto por Internet, declaraciones de impuestos en línea, recetas electrónicas e historiales médicos en línea.⁶ La tarjeta de identificación sirve también como soporte para los billetes electrónicos del transporte público. Con la implementación del programa de residencia electrónica de Estonia ahora cualquier persona del mundo puede firmar documentos en línea, crear una empresa en Estonia por Internet, administrarla a distancia y hacer la declaración de la renta por Internet.⁷

Estonia fue uno de los primeros países que implantó el voto por Internet, en las elecciones parlamentarias de 2007. Las tasas de participación no han dejado de crecer en los últimos años, alcanzando el máximo histórico de 30,5% de personas que votaron en línea en 2015.⁸ La votación por Internet se ha convertido en una medida que muestra el grado de confianza que los ciudadanos depositan en la ciberseguridad.⁹

Estonia cuenta con iniciativas del sector privado apoyadas por el gobierno para avanzar en sus proyectos de ciberseguridad. Las campañas de concienciación y los cursos de formación organizados por la Fundación Look@theWorld —una red de apoyo creada por proveedores de servicios estonios y de otros países— han sido un factor clave en la promoción del uso seguro de los dispositivos de TIC. Como parte de su proyecto de seguridad informática de 2009, 400.000 personas¹⁰ recibieron capacitación sobre cómo protegerse contra los robos de identidad.¹¹ En 2014 se puso en marcha una iniciativa de seguimiento con objetivos de formación similares para los usuarios de dispositivos móviles inteligentes y firmas digitales.¹² El objetivo es llegar a 300.000 personas en 2017, lo que representa aproximadamente 70% de usuarios de dispositivos móviles inteligentes del país. Según la encuesta sobre ciberseguridad de 2015 que realiza la Comisión Europea, 47% de los encuestados estonios dijeron que se sentían bien informados acerca de los riesgos de la ciberdelincuencia.¹³

Junto con otros 26 países, Estonia forma parte de la Coalición para la Libertad de Expresión en Internet (*Freedom Online Coalition*), que aboga por la “libertad de expresión, de asociación, de reunión y la privacidad en línea”. Esta coalición coordina posiciones nacionales y declaraciones conjuntas.¹⁴ El ejercicio sin restricciones de estas libertades ha servido de inspiración para muchos de los servicios electrónicos que proporciona el gobierno de Estonia.

D2-1 Mentalidad de seguridad cibernética

Los ataques cibernéticos de 2007 hicieron que se tomara conciencia colectiva sobre las posibles vulnerabilidades a las que se enfrentaban la sociedad y la economía estonias.

D2-2 Conciencia de seguridad cibernética

Se han puesto en marcha programas de formación concertados en colaboración con iniciativas del sector privado, que se revisan periódicamente para incorporar cambios tecnológicos.

<http://www.vaatamaailma.ee/en>

<http://www.vaatamaailma.ee/en/nutikaitse>

D2-3 Confianza en el uso de Internet

La plataforma X-Road ofrece un ecosistema asegurado por el gobierno para el intercambio de datos entre ciudadanos, organismos gubernamentales y proveedores de servicios.

https://www.ria.ee/public/x_tee/xRoadOverview.pdf

D2-4 Privacidad en línea

La privacidad es una parte integral de la estrategia cibernética de Estonia, que promueve y protege el ejercicio de los derechos civiles en línea. La Ley de Protección de Datos Personales de 1996 se modificó en 2010 para cumplir con las normas de la UE.

[http://www.legaltext.ee/et/andmebaas/tekst.asp?](http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXX041K1&keel=en&pg=1&ptyyp=RT&tyyp=X&query=isikuandmete+kaitse+seadus)

[loc=text&dok=XXXX041K1&keel=en&pg=](http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXX041K1&keel=en&pg=1&ptyyp=RT&tyyp=X&query=isikuandmete+kaitse+seadus)

[1&ptyyp=RT&tyyp=X&query=isikuandmete+kaitse+seadus](http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXX041K1&keel=en&pg=1&ptyyp=RT&tyyp=X&query=isikuandmete+kaitse+seadus)

Educación, formación y competencias en seguridad cibernética

Estratégico

Estonia ha creado programas educativos en la escuela primaria y secundaria y en la universidad. La Fundación de Tecnologías de la Información para la Educación (HITSA) es la principal fuente de campañas de formación y concienciación del país, y comienza sus programas de formación con niños en edad preescolar. La HITSA celebró su primer concurso de defensa cibernética para estudiantes de secundaria en junio de 2015, con el objetivo de inspirar a la próxima generación de profesionales de la seguridad cibernética.¹⁵ Los cinco primeros clasificados fueron invitados a visitar el Ministerio de Defensa, el Centro de Excelencia para la Ciberdefensa Cooperativa (CCD-COE) de la OTAN, la Unidad de Defensa Cibernética (CDU) y la Autoridad del Sistema de Información de Estonia. Durante el verano, la HITSA acogió también la primera escuela de verano de ciberseguridad, con 70 participantes de diversos países y universidades: la Universidad de California en Berkley, la Universidad de Oxford y el University College de Londres, entre otros.¹⁶

En cuanto a la educación superior, la Facultad de Tecnologías de la Información de Estonia pondrá en marcha un nuevo programa de estudios de ingeniería de la ciberseguridad que se impartirá en inglés.¹⁷ El nuevo programa de diplomatura complementa los programas existentes a nivel de maestría. Desde 2009, la Universidad de Tecnología de Tallin y la Universidad de Tartu ofrecen un programa conjunto de maestría en ciberseguridad, con unos 50 estudiantes nuevos cada año. En 2014, la Universidad de Tecnología de Tallin, en colaboración con el Centro de Estonia 2CENTRE sobre Ciberdelincuencia, puso en marcha un programa de maestría sobre ciencia forense digital. El 2CENTRE sobre Ciberdelincuencia forma parte de una amplia red de centros de excelencia organizada por la Unión Europea, que tiene como objetivo formar profesionales que puedan combatir la ciberdelincuencia.

En 2002, el gobierno de Estonia, con el apoyo del Programa de las Naciones Unidas para el Desarrollo y el *Open Society Institute*, creó una organización no gubernamental independiente, la Academia



INICIAL

FORMATIVO

ESTABLECIDO

ESTRATÉGICO

DINÁMICO

de Gobernanza Electrónica (EGA),¹⁸ que trabaja para compartir la experiencia de este país en el desarrollo del gobierno electrónico, la democracia electrónica y los sistemas educativos para las TIC.

Pese a estas iniciativas, a Estonia le falta mano de obra en el ámbito cibernético. Un estudio encargado por la Comisión Europea sobre las condiciones del mercado laboral de las TIC estima que la fuerza de trabajo del país en el sector de las TIC ascenderá a 24.000 personas en 2015 (frente a las 23.000 de 2012).¹⁹ A pesar del crecimiento constante de las cifras desde 2001, la escasez general de los profesionales de TIC en relación con la demanda ha dado lugar a un considerable aumento de los salarios. Muchos estudiantes dejan sus estudios para aceptar empleos bien remunerados en el sector privado.

D3-1 Disponibilidad de educación y formación cibernéticas a nivel nacional

La Fundación de Tecnologías de la Información para la Educación (HITSA), en cuanto centro de enseñanza y fomento de la ciberseguridad a nivel nacional, ya comienza sus programas en la edad preescolar. Los planes de estudio de enseñanza primaria, media y secundaria contienen módulos sobre ciberseguridad.

<http://www.hitsa.ee/it-education/educational-programmes>

D3-2 Desarrollo de la educación de seguridad cibernética a nivel nacional

Estonia reconoce la necesidad de internacionalizar aún más sus esfuerzos de educación superior en ciberseguridad y busca activamente contratar a profesores expertos del extranjero. La actual escasez de profesionales formados en seguridad de las TI hace que un número significativo de estudiantes empiecen a trabajar antes de terminar sus estudios.

<http://ec.europa.eu/DocsRoom/documents/4568/attachments/1/translations/en/renditions/native>

D3-3 Formación e iniciativas educativas públicas y privadas

Cada vez hay más programas universitarios dedicados a la ciberseguridad, tanto a nivel de grado como de posgrado. Los esfuerzos por compartir la experiencia de Estonia con los países en desarrollo en cuanto a la implantación del gobierno electrónico, la democracia electrónica y los sistemas educativos para las TIC ayudan a sistematizar los logros.

<http://www.hitsa.ee/about-us/news/article-2>

<http://www.ega.ee/>

D3-4 Gobernanza corporativa, conocimiento y normas

El gobierno de Estonia, mediante el DNI electrónico, la firma digital y la plataforma X-Road, ha establecido una infraestructura de seguridad común, que también puede usar el sector privado.

Los beneficios de la armonización y el afán de ahorro de costos de las empresas han dado lugar a una rápida adopción de estas medidas.

Marco jurídico y reglamentario

Estratégico

Estonia ha desarrollado un amplio conjunto de leyes y reglamentos en materia de ciberseguridad. La ley más importante es la Ley de Emergencia de 2009,²⁰ que establece que la infraestructura crítica y su aplicación en el sector de las TIC se rige por el Reglamento de Medidas de Seguridad de los Sistemas de Información de Servicios Vitales y Activos de Información Vinculados (2013).²¹ Esta ley obliga a los proveedores de servicios vitales a notificar los incidentes cibernéticos y presentar informes a la Autoridad del Sistema de Información de Estonia una vez que se restaura la integridad del sistema.

La Ley de Secretos de Estado y de Información Confidencial de Estados Extranjeros de 2007 solicita una evaluación anual de la seguridad del almacenamiento digital de documentos gubernamentales clasificados como “muy secretos” y “secretos”.²² La Ley de Comunicaciones Electrónicas de 2004 (modificada en 2011)²³ autoriza a la Autoridad de Vigilancia Técnica de Estonia a que les solicite a los proveedores de servicios de TIC realizar evaluaciones de la seguridad de sus propios sistemas. La Ley de Protección de Datos Personales de 1996 (modificada en 2010)²⁴ regula el tratamiento de la correspondencia y la información personal. La Ley aplica las normas de protección de datos de la UE, distingue entre “datos personales” y “datos personales sensibles” y determina una protección ampliada para los “datos personales sensibles”.

Después de 2007, las autoridades de Estonia decidieron que las disposiciones sobre delitos informáticos del Código Penal nacional eran insuficientes para hacer frente a las acciones cibernéticas coordinadas que no buscan claramente un beneficio económico. Desde entonces una serie de enmiendas al Código Penal estonio han ampliado el espectro de hechos punibles.

En concreto, el Parlamento de Estonia ha ampliado la cobertura a la alteración, eliminación, daño o bloqueo de datos ejecutados de manera ilegal; a la interferencia u obstaculización del funcionamiento de los sistemas informáticos; a la difusión de herramientas maliciosas; a la preparación de delitos informáticos y al uso ilegal de los sistemas informáticos, estableciendo en el código penas máximas significativamente mayores para las operaciones dirigidas contra servicios o infraestructuras vitales.²⁵ Además, otros cambios en el código penal han ampliado el alcance de los actos de terrorismo, que incluyen “interferir con datos informáticos o impedir el funcionamiento de los sistemas informáticos, así como amenazar con realizar tales actos, si se cometen con el propósito de obligar al Estado o una organización internacional a una acción u omisión, o interferir de manera grave en la estructura política, constitucional, económica o social del Estado o destruirla, o interferir de manera grave en el funcionamiento de una organización internacional o destruirla, o aterrorizar gravemente a la población”.²⁶



D4-1 Marco jurídico de seguridad cibernética

El Reglamento de Medidas de Seguridad de los Sistemas de Información de Servicios Vitales y Activos de Información Vinculados (2013) define la infraestructura de información crítica en relación con la Ley de Emergencia de 2009.

https://www.ria.ee/public/KIHK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf.

Las modificaciones del Código Penal estonio introdujeron una serie de nuevos delitos específicos de seguridad cibernética.

<https://www.riigiteataja.ee/en/eli/522012015002/consolide>

D4-2 Investigación jurídica

La Oficina del Fiscal de Estonia es responsable de investigar los casos previstos en el Código Penal. Existen tratados internacionales de asistencia legal mutua, pero podrían tener escasa repercusión práctica en tiempos de tensión.

<http://www.prokuratuur.ee/en>

D4-3 Divulgación de información responsable

Los proveedores de servicios vitales, en virtud del Reglamento de Medidas de Seguridad de los Sistemas de Información de Servicios Vitales y Activos de Información Vinculados, están obligados a informar sobre cualquier incidente cibernético y a notificar a la Autoridad del Sistema de Información de Estonia una vez que se haya restaurado la integridad del sistema.

<https://www.ria.ee/en/>



INICIAL



FORMATIVO



ESTABLECIDO



ESTRATÉGICO



DINÁMICO



Normas, organizaciones y tecnologías

Estratégico

Considerando su pequeño tamaño y ubicación, Estonia ha hecho de la cooperación internacional una parte fundamental de su estrategia de ciberseguridad, y la aprovecha para mejorar su propia seguridad y aumentar su influencia internacional. Además de las asociaciones regionales con los países bálticos y nórdicos, Estonia participa activamente con la OTAN, la Unión Europea, el Grupo de Expertos Gubernamentales de las Naciones Unidas y la Organización para la Seguridad y la Cooperación en Europa (OSCE). Un componente clave de la planificación de la ciberseguridad de Estonia es el fortalecimiento de la cooperación con la OTAN, en particular albergando los ejercicios y foros cibernéticos de la alianza. Estonia ha acogido numerosos ejercicios cibernéticos internacionales, incluidos los ejercicios anuales de la OTAN denominados Escudos Bloqueados y los ejercicios de defensa cibernética de la coalición desde 2013, a fin de prepararse para ataques como el de 2007.²⁷ En una de las primeras actividades emprendidas en el marco de la Iniciativa de Ciberseguridad de la OEA, en mayo de 2015 el Equipo de Respuesta ante Emergencias Cibernéticas de Estonia organizó una capacitación de cuatro días para funcionarios gubernamentales de Costa Rica, Guyana, Jamaica,

Nicaragua, Panamá, Paraguay y Uruguay, a fin de compartir su experiencia en el desarrollo y la gestión de los CERT nacionales.²⁸

Para evitar los problemas creados por los ataques de denegación de servicio contra sitios web del gobierno en 2007, la Estrategia Cibernética de 2014–17 prevé embajadas virtuales alojadas en una nube pública en servidores basados en Estonia y centros de datos en países amigos, lo que proporcionará vías alternativas de acceso y una garantía adicional de seguridad.²⁹ Las embajadas virtuales tienen por objeto garantizar que los servicios electrónicos se mantengan incluso en caso de que se produzca un ataque físico en Estonia que pudiera interrumpir el funcionamiento del gobierno en el sentido tradicional. El concepto de la “continuidad digital del Estado”³⁰ introduce esa idea de redundancia para los servicios gubernamentales.

Estonia adoptó su propia norma de seguridad de TI basándose en el modelo de la *IT Grundschutz* (Protección Básica en las TI) desarrollada por la Oficina Federal para la Seguridad de la Información de Alemania (BSI). Obligatoria para el sector público desde 2008, la norma ISKE emplea una evaluación de tres niveles para los requisitos de seguridad de una entidad (alto, medio y bajo). La norma busca un equilibrio entre confidencialidad, integridad y disponibilidad de datos.³¹

D5-1 Adhesión a las normas

Estonia adoptó su propia norma de seguridad de TI ISKE, inspirada en la *IT Grundschutz* (Protección Básica en las TI) desarrollada por Alemania. Desde 2008, su aplicación es obligatoria para el sector público. La norma ISKE clasifica los requisitos de seguridad de una organización según un sistema de tres niveles (alto, medio y bajo).

https://www.ria.ee/public/ISKE/ISKE_english_2012.pdf

D5-2 Organizaciones de coordinación de seguridad cibernética

El Consejo de Seguridad Cibernética supervisa la aplicación de la estrategia de ciberseguridad. Le brinda apoyo el Ministerio de Economía y Comunicaciones, que guía la política de ciberseguridad y coordina su ejecución entre los organismos gubernamentales, representantes de la sociedad civil, empresas e instituciones educativas. La responsabilidad de proteger las redes gubernamentales recae en la Autoridad del Sistema de Información de Estonia (RIA).

https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

D5-3 Respuesta a incidentes

El Equipo de Respuesta ante Emergencias Cibernéticas de Estonia (CERT-EE), que opera bajo la dirección de la RIA, gestiona la respuesta a los incidentes cibernéticos. La RIA vigila directamente los sistemas de información que subyacen a los servicios vitales y las infraestructuras críticas.

<https://www.ria.ee/cert-estonia/>

D5-4 Resiliencia de la infraestructura nacional

Existen sistemas alternativos de respaldo de los servicios electrónicos y los sistemas de información vitales.

D5-5 Protección de la infraestructura crítica nacional

La RIA ha mapeado las infraestructuras críticas y los servicios vitales que dependen de sistemas de información para funcionar. Se han reducido las interdependencias transfronterizas.

https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

D5-6 Gestión de crisis

El CERT-EE asigna prioridades para la respuesta según cuatro principios: número de usuarios afectados, tipo de incidente, objetivo y punto de origen del ataque y recursos necesarios para resolverlo.

<https://www.ria.ee/cert-estonia/>.

D5-7 Redundancia digital

Estonia tiene previsto mantener embajadas virtuales en servidores situados en el país y en centros de datos en países amigos. Alojadas en nubes públicas, las embajadas virtuales proporcionan vías de acceso alternativas y una garantía adicional de seguridad. Las embajadas virtuales tienen por objeto garantizar que los servicios electrónicos se mantengan incluso en caso de un ataque físico en Estonia que pudiera interrumpir el funcionamiento del gobierno en el sentido tradicional.

https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf

D5-8 Mercado de la ciberseguridad

Se espera que el sector estonio de las TIC sea uno de los que más crezcan hasta 2022. El programa de residencia electrónica de Estonia crea un clima propicio para la inversión extranjera, permitiendo que inversores de cualquier lugar del mundo creen una empresa en Estonia por Internet, la administren a distancia y hagan la declaración de la renta por Internet. Sin embargo, las tres cuartas partes de los directivos de empresas estonias han expresado su preocupación acerca de la eficacia del gobierno para la formación de mano de obra cibernética.

<https://e-estonia.com/e-residents/about/>

http://euskilspanorama.cedefop.europa.eu/App_Controls/Documents/ShowDocument.aspx?documentid=127&

Notas

1. Ministerio de Defensa de la República de Estonia. Estrategia de ciberseguridad de Estonia 2008–13, 2008 (http://www.eata.ee/wp-content/uploads/2009/11/Estonian_Cyber_Security_Strategy.pdf).
2. Kadri, K., A-M. Osula y LTC J. Stinissen. "The Cyber Defence Unit of the Estonian Defence League." Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN, 2013 (<https://>

ccdcoe.org/multimedia/cyber-defence-unit-estonian-defence-league-legal-policy-and-organisational-analysis-0.html).

3. Entre los organismos se encuentran el Ministerio de Defensa, la Autoridad del Sistema de Información, el Ministerio de Justicia, la Dirección de la Policía y la Guardia de Fronteras, la Delegación del Gobierno, el Ministerio de Asuntos Exteriores, el Ministerio del Interior y el Ministerio de Educación e Investigación.
4. Autoridad del Sistema de Información (RIA) de la República de Estonia. "About CERT Estonia," 13 de enero de 2014 (<https://www.ria.ee/cert-estonia/>).
5. RIA. "X-Road Overview," consultado el 9 de octubre de 2015 (https://www.ria.ee/public/x_tee/xRoadOverview.pdf).
6. "e-Estonia," [estonia.eu](http://estonia.eu/about-estonia/economy-a-it/e-estonia.html) (<http://estonia.eu/about-estonia/economy-a-it/e-estonia.html>).
7. "What is e-Residency?" e-estonia.com, consultado el 9 de octubre de 2015 (<https://e-estonia.com/e-residents/about/>).
8. Comité Nacional de Elecciones de Estonia, "Statistics about Internet Voting in Estonia", consultado el 9 de octubre de 2015 (<http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics>).
9. Véase Springall, D. *et al.*, "Security Analysis of the Estonian Internet Voting System", noviembre de 2014 (<https://estoniaevoting.org/findings/paper/>) para ampliar la información sobre los aspectos de seguridad del sistema de voto electrónico de Estonia.
10. El Banco Mundial estima que Estonia tiene 1,314 millones de habitantes (2014) (<http://data.worldbank.org/country/estonia>).
11. Fundación Look@World. "Past Milestones," consultado el 9 de octubre de 2015 (<http://www.vaatamaailma.ee/en/>).
12. Fundación Look@World. "Estonia Puts Focus on Smart Device Security," consultado el 9 de octubre de 2015 (<http://www.vaatamaailma.ee/en/nutikaitse>).
13. Eurobarómetro especial 423. "Cybersecurity Report", encuesta realizada por *TNS Opinion & Social* a petición de la Dirección General de Migración y Asuntos de Interior de la Comisión Europea, febrero de 2015, 41–2 (http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf).
14. Coalición para la Libertad de Expresión en Internet. "Overview of the Freedom Online Coalition's Work and Vision to Advance Internet Freedom Globally", julio de 2015 (<https://www.freedomonlinecoalition.com/wp-content/uploads/2015/07/Freedom-Online-Coalition-Basic-facts-July-2015.pdf>).
15. Primer concurso de defensa cibernética para escolares, studyitin.ee, consultado el 9 de octubre de 2015 (<http://studyitin.ee/en/estonian>).
16. Fundación de Tecnologías de la Información para la Educación (HITSA). "Estonia Hosts the First International Cybersecurity Summer School", 10 de julio de 2015 (<http://www.hitsa.ee/about-us/news/estonia-hosts-the-first-c3s>).
17. Fundación de Tecnologías de la Información para la Educación (HITSA). "Estonian IT College is Opening a New Curriculum - Cybersecurity Engineering," 1 de junio de 2015 (<http://www.hitsa.ee/about-us/news/article-2>).
18. Academia de Gobernanza Electrónica de Estonia (<http://www.ega.ee/>).
19. Empírica. "e-Skills in Europe: Estonia Country Report," encargado por la Comisión Europea, enero de 2014 (<http://ec.europa.eu/DocsRoom/documents/4568/attachments/1/translations/en/renditions/native>).
20. Ley de Emergencia, República de Estonia, RT I 2009, 39, 262, cuya versión más reciente es RT I, 30/06/2015, 4 (<https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/504092015012/consolide>).
21. Reglamento No. 43 del 14 de marzo de 2013, República de Estonia, Reglamento de Medidas de Seguridad de los Sistemas de Información de Servicios Vitales y Activos de Información Vinculados (https://www.ria.ee/public/KIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf).
22. Ley de Secretos de Estado y de Información Confidencial de Estados Extranjeros, República de Estonia, RT I 2007, 16, 77, cuya última modificación es RT I, 22/12/2011, 2 (<https://www.riigiteataja.ee/en/eli/515112013009/consolide>).
23. Ley de comunicaciones electrónicas, RT I 2004, 87, 593, República de Estonia, cuya última modificación es la RT I, 25/03/2011, 1 (http://www.konkurentsiamet.ee/public/Electronic_Communications_Act_2011.pdf).
24. Ley de Protección de Datos Personales, República de Estonia, RT I 2007, 24, 127, cuya última modificación es la RT I, 30/12/2010, 2 (<https://www.riigiteataja.ee/en/eli/512112013011/consolide>).
25. Código Penal de la República de Estonia, RT I 2001, 61, 364, modificado por RT I, 26/02/2014, 1, párrafos 206, 207, 208, 216, 217 (http://www.wipo.int/wipolex/en/text.jsp?file_id=333555).
26. *Ibid.*, párrafo 237 (1).
27. Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN. "Estonian Defense League Sign Cooperation Agreement," 12 de febrero de 2015 (<https://ccdcoe.org/centre-estonian-defence-league-sign-cooperation-agreement.html>).
28. Cybersecurity Capacity Portal, Universidad de Oxford. "OAS and Estonia Promote Exchange of Best Practices on Cybersecurity", 5 de mayo de 2015 (<https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/oas-and-estonia-promote-exchange-best-practices-cyber-security>).
29. Ministerio de Economía y Comunicaciones de Estonia y Microsoft Corporation. 2015. "Implementation of the Virtual Data Embassy Solution" (https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf).
30. Estrategia de Ciberseguridad 2014–2017, pág. 9.
31. RIA. 2012. "Estonian Security System Overview" (https://www.ria.ee/public/ISKE/ISKE_english_2012.pdf).



Estado de Israel

Política y estrategia



Cultura y sociedad



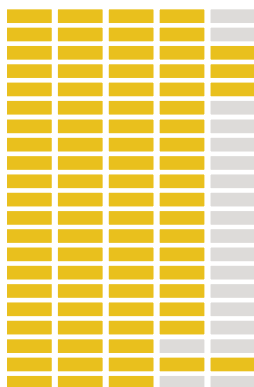
Educación



Marcos legales



Tecnología



Principales desafíos de ciberseguridad

El aparato de defensa cibernética de Israel es uno de los mejores del mundo. Un estudio comparativo de 23 países desarrollados situó a Israel como el mejor en defensa cibernética, junto con Suecia y Finlandia.¹ Pese a ello, tanto las estrategias como la organización siguen evolucionando en el país. Cada día, grupos hostiles a nivel estatal y no estatal ponen a prueba las defensas cibernéticas. Los órganos gubernamentales y las infraestructuras críticas —en particular el sector eléctrico— reciben ataques con regularidad.

Las políticas de ciberseguridad de Israel han ido cambiando en respuesta a una mayor dependencia del ciberespacio para actividades políticas, militares y económicas, lo que significa que, sin una ciberseguridad adecuada, un adversario determinado podría frustrar objetivos estratégicos clave sin enfrentarse a Israel con un ejército convencional. Israel resolvió que las estructuras organizativas civiles y militares, las responsabilidades y la normativa para proteger los sistemas informatizados —que estaban muy compartimentadas— eran insuficientes para permitir una defensa integral en el ciberespacio.²

POBLACIÓN TOTAL DEL PAÍS

8.215.700

Penetración de Internet

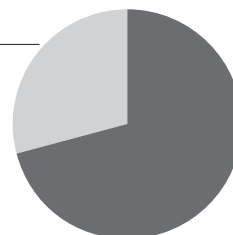
Abonos a teléfonos celulares

9.982.075

Personas con acceso a Internet

5.874.225

71%

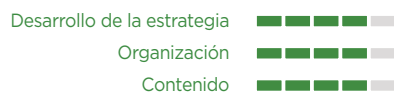


Fuente: Indicadores de Desarrollo del Banco Mundial (2014). Disponible en: <http://databank.worldbank.org/data/reports.aspx?source=2&country=USA&series=&period=>

Política y estrategia



Estrategia nacional de seguridad cibernética oficial o documentada



Defensa cibernética



Cultura y sociedad



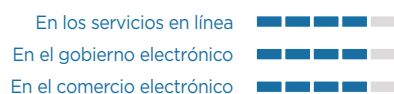
Mentalidad de seguridad cibernética



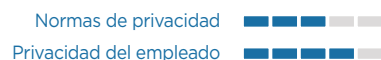
Conciencia de seguridad cibernética



Confianza en el uso de Internet



Privacidad en línea



Educación



Disponibilidad nacional de la educación y formación cibernéticas



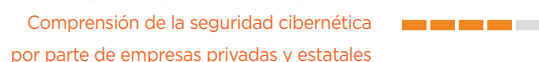
Desarrollo nacional de la educación de seguridad cibernética



Formación e iniciativas educativas públicas y privadas



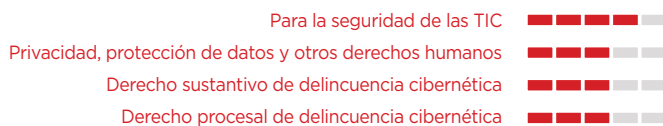
Gobernanza corporativa, conocimiento y normas



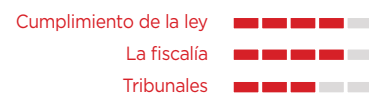
Marcos legales



Marcos jurídicos de seguridad cibernética



Investigación jurídica



Divulgación responsable de la información



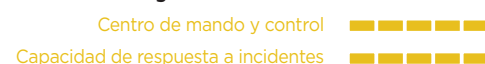
Tecnologías



Adhesión a las normas



Organizaciones de coordinación de seguridad cibernética



Respuesta a incidentes



Resiliencia de la infraestructura nacional



Protección de la Infraestructura Crítica Nacional (ICN)



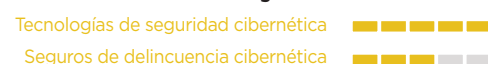
Gestión de crisis



Redundancia digital



Mercado de la ciberseguridad





INICIAL



FORMATIVO



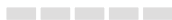
ESTABLECIDO



ESTRATÉGICO



DINÁMICO



Política y estrategia de ciberseguridad

Estratégico

Israel fue uno de los primeros países del mundo que reconoció la importancia de la defensa de sus sistemas informáticos críticos. En 1997, se puso en marcha el proyecto de gobierno electrónico israelí, denominado Tehila, con el objetivo de proteger la conexión de las oficinas gubernamentales a Internet y ofrecer un alojamiento seguro para los sitios web del gobierno. Tehila tiene como objetivo mejorar la interacción en línea entre el gobierno y los ciudadanos. Tiene la doble función de servir como proveedor de servicios de Internet (ISP) para los ministerios y de alojar sitios web y servicios del gobierno. La infraestructura de Tehila ha resistido ataques de DDoS, algunos de mayor envergadura que el de 2007 contra Estonia.³

En 2002, se aprobó la Resolución 84/B del Comité Ministerial de Seguridad Nacional sobre la responsabilidad de proteger los sistemas informáticos en el Estado de Israel. La resolución se convirtió en la política nacional de defensa cibernética civil *de facto*, proporcionando el marco inicial para los sistemas informáticos críticos (CCS) a escala nacional.⁴ El marco también identificó las áreas de responsabilidad para definir la infraestructura informática crítica y crear la Autoridad Nacional de Seguridad de la Información (NISA), que regula y asesora respecto de las infraestructuras críticas en el campo de la seguridad de la información.

En 2010, debido al aumento de las amenazas en el ámbito cibernético, el Primer Ministro dirigió la creación de la Iniciativa Cibernética Nacional, un grupo de trabajo para formular planes nacionales con el objetivo de situar a "Israel entre los cinco países más avanzados en el campo cibernético".⁵ La iniciativa, encabezada por el presidente del Consejo Nacional de Investigación y Desarrollo, elaboró una estrategia de preparación para el ciberespacio y de cooperación entre sus componentes de seguridad económica, académica y nacional.

La Oficina Cibernética Nacional de Israel (INCB), establecida en 2010, coordina los ejercicios nacionales e internacionales. También debe trazar un panorama general de todos los órganos de inteligencia y definir el estado de la situación nacional en materia de ciberseguridad. La INCB es el resultado de los objetivos establecidos en la Iniciativa Cibernética Nacional de 2010. Las siete recomendaciones clave de esta iniciativa fueron:

1. Mejorar la educación, basándose en mejores prácticas de base y una I+D interdisciplinaria avanzada.
2. Desarrollar una infraestructura de conocimiento e I+D.
3. Crear un "escudo protector" en todo el Estado a partir de los productos de I+D nacional, y hacer frente a los problemas de privacidad.
4. Desarrollar una capacidad nacional operativa en el ciberespacio.
5. Mejorar la defensa combinando medidas legislativas técnicas y no técnicas y participando en iniciativas internacionales, especialmente con el Convenio sobre la Ciberdelincuencia del Consejo de Europa, para promover la defensa cibernética.

6. Implantar tecnologías únicas, desarrolladas a nivel nacional, y fomentar las adquisiciones locales.
7. Crear un organismo nacional para la política cibernética integral de Israel.

La INCB se encarga de promover tres áreas centrales en el ámbito cibernético:

1. Avanzar en la defensa y la construcción de la fuerza nacional en el campo cibernético.
2. Convertir a Israel en un centro de tecnologías de la información.
3. Fomentar la cooperación entre el mundo académico, la industria, el sector privado, los organismos gubernamentales y el sector de la seguridad.

La INCB, que depende directamente del Primer Ministro, aportó un nuevo énfasis interdisciplinario a la dirección y al carácter de los debates y las capacidades de la política de ciberseguridad. Fue la encargada de asesorar al Primer Ministro, al gobierno y a sus comités (con excepción de los militares y las relaciones exteriores) para consolidar, guiar y enriquecer las iniciativas y los esfuerzos del gobierno en la elaboración de la política cibernética nacional. La INCB también proporciona estimaciones de las amenazas cibernéticas a nivel nacional, promueve esfuerzos de I+D y de la industria, aumenta la conciencia pública sobre las cuestiones de ciberseguridad y facilita la cooperación nacional e internacional en temas cibernéticos.

La acción más reciente fue la creación de una Autoridad Nacional de Defensa Cibernética en febrero de 2015 en la Oficina del Primer Ministro, tras un año de luchas burocráticas sobre quién habría de ser el responsable del nuevo organismo. Finalmente, el Primer Ministro decidió no encargar esa responsabilidad al servicio de seguridad nacional israelí, el Shin Ben.⁶ Este ha sido tradicionalmente el encargado de proteger frente a ataques cibernéticos e intrusiones a los organismos estatales y las infraestructuras críticas, tales como las instituciones financieras y las encargadas del agua y la electricidad. Algunos consideraron que esta decisión supuso darle prioridad a la privacidad sobre los intereses de seguridad.

La Autoridad Nacional de Defensa Cibernética será la responsable general de la defensa cibernética. Sus oficinas están en Tel Aviv y Beerseba. Trabajarán en colaboración con la INCB, la cual seguirá definiendo la política nacional. La nueva autoridad y la oficina formarán una única dirección nacional cibernética. A la INCB se le asignó un presupuesto de ILS2.500 millones para los próximos cinco años, unos ILS500 millones anuales (US\$130 millones).⁷ La Autoridad de Defensa Cibernética desarrollará una respuesta integral frente a los ataques cibernéticos, incluidos la respuesta a las amenazas y los incidentes en tiempo real. Sus responsabilidades van más allá de las redes de infraestructuras críticas y gubernamentales y se extienden a grandes redes comerciales que hasta ahora no se consideraban infraestructuras críticas, tales como las compañías aéreas y las compañías de procesamiento de alimentos. También contará con un centro de asistencia —un Equipo de Preparación para Incidentes Cibernéticos (CERT)— a fin de fortalecer la resistencia de las organizaciones y los sectores de la economía.

Las Fuerzas de Defensa de Israel (FDI) actuarán en conjunto con la nueva Autoridad de Defensa Cibernética, pero serán responsables de los aspectos militares de la defensa cibernética. En junio de 2015, el portavoz de las FDI anunció que, en vista de los importantes desafíos que enfrentan las FDI en el ciberespacio, el jefe de gabinete había decidido establecer un comando cibernético para dirigir

las actividades operativas de las fuerzas armadas. Las FDI prevén poner en marcha este comando en un plazo de dos años. El nuevo comando examinará los medios para mejorar la eficacia operativa militar en el ciberespacio, con una mejor utilización de “las ventajas tecnológicas y humanas con las que ya cuenta Israel”.⁸

D1-1 Estrategia nacional de seguridad cibernética

La Iniciativa Cibernética Nacional fue creada en 2010, y condujo a la creación de la Oficina Cibernética Nacional de Israel (INCB) <http://sectech.tau.ac.il/cyberconference/index.php/israeli-national-cyber-bureau>

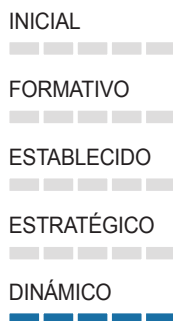
D1-2 Consideración de la defensa cibernética

La Autoridad Nacional de Defensa Cibernética se puso en marcha en febrero de 2015 para trabajar junto con la INCB. <http://mfa.gov.il/MFA/PressRoom/2015/Pages/Cabinet-approves-establishment-of-National-Cyber-Authority-15-Feb-2015.aspx>



Cultura cibernética y sociedad

Dinámico



Las necesidades de defensa de Israel y la limitación de sus recursos han contribuido al énfasis del país en la tecnología.⁹ Su dinámica democracia y su pequeño tamaño han fomentado una intensa cultura digital. Según las estadísticas de 2013 de la UIT, el 70,8% de la población israelí usa Internet.¹⁰ Un estudio realizado por la Universidad Hebrea en mayo de 2014 indica que el 81% de los israelíes mayores de 12 años navega por Internet y dos tercios se conectan varias veces al día.¹¹

La alta penetración de Internet se refleja en el sector empresarial privado israelí dedicado a la ciberseguridad, uno de los de mayor crecimiento del mundo. En los últimos cinco años, el número de este tipo de empresas se ha duplicado, llegando a las 300,¹² lo que se puede atribuir en buena parte a la abundancia de ingenieros, que provienen principalmente de dos lugares: muchos son exempleados de los 280 centros de desarrollo de alta tecnología que son propiedad de multinacionales extranjeras en Israel; y, por otro lado, se trata de miles de ingenieros que salen de las FDI cada año y aportan las habilidades necesarias para la floreciente industria de la ciberseguridad en el país.

La INCB informa que Israel exporta más productos y servicios cibernéticos que el resto de los países juntos, si se excluye a Estados Unidos.¹³ En 2014, las *startups* israelíes del sector de la ciberseguridad exportaron US\$3.000 millones en bienes cibernéticos, lo que supone 5% del mercado mundial, solo por detrás de Estados Unidos. Al menos un tercio de las exportaciones israelíes están relacionadas con las TIC, mientras que solo 7% del capital humano del país trabaja en el sector de las TIC.¹⁴ En 2013, las *startups* israelíes recibieron una inversión de US\$165 millones para su financiación, lo que representa 11% del capital global invertido en ciberseguridad. Por otra parte, casi 15% de todas las empresas del mundo que atraen inversión relacionada con productos o servicios cibernéticos son de propiedad israelí.¹⁵

La legislación israelí considera la privacidad como un derecho humano fundamental y su marco constitucional la garantiza.¹⁶ La Ley de Protección de la Privacidad de 1981 (PPA) protege la privacidad. Esta ley, forjada en varios comités de expertos durante los años setenta y principios de los ochenta, fue una de las primeras leyes de privacidad de su tipo de todo el mundo.¹⁷ El régimen israelí de privacidad de la información es muy similar al modelo europeo de protección de datos, que garantiza un derecho general a la privacidad de la información en un marco regulatorio detallado y la imposición de diversas obligaciones a los procesadores de datos personales.

D2-1 Mentalidad de seguridad cibernética

La conciencia sobre los riesgos cibernéticos es alta; hay un fuerte crecimiento del sector privado, con estrechos vínculos con el gobierno y el Ejército.

D2-2 Conciencia de seguridad cibernética

La Ciberiniciativa de 2010 ideó planes nacionales de educación dirigidos a aumentar la toma de conciencia pública sobre las amenazas informáticas.

<http://sectech.tau.ac.il/cyberconference/index.php/israeli-national-cyber-bureau>

D2-3 Confianza en el uso de Internet

El proyecto de gobierno electrónico “Tehila” se presentó en 1997 para proteger la conexión de las oficinas gubernamentales a Internet y ofrecer alojamiento seguro. El 81,2% de los israelíes mayores de 12 años se conecta a Internet.

<http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/Background.aspx>

D2-4 Privacidad en línea

La legislación israelí considera la privacidad como un derecho humano fundamental y su marco constitucional la garantiza. También está protegida por la Ley de Protección de la Privacidad de 1981.

<http://www.loc.gov/law/help/online-privacy-law/israel.php>

Educación, formación y competencias en seguridad cibernética

Dinámico

Un objetivo central de la Iniciativa Cibernética Nacional de 2010 fue idear planes nacionales de educación dirigidos a aumentar la conciencia pública sobre las amenazas informáticas. Israel está acelerando rápidamente sus esfuerzos para formar y contratar a los expertos cibernéticos necesarios para llevar ventaja sobre las numerosas amenazas que aumentan a escala global. Israel invierte considerablemente en la educación de las habilidades técnicas necesarias en términos de ciberseguridad.



INICIAL

FORMATIVO

ESTABLECIDO

ESTRATÉGICO

DINÁMICO



Como parte de una importante iniciativa nacional para desarrollar el sur de Israel, el país está intentando convertir Beerseba en un centro cibernético líder en I+D. El país cuenta también con centros de investigación y desarrollo de muchas de las principales multinacionales de alta tecnología,¹⁸ con líderes de la industria cibernética tales como EMC, Lockheed Martin, Deutsche Telekom, IBM y JVP. También cuenta con destacados investigadores académicos industriales en la Universidad Ben-Gurión (BGU) e importantes organismos gubernamentales, como la INCB y el CERT nacional (IL-CERT).¹⁹

La estrategia israelí para formar a la próxima generación de talentos cibernéticos es integrar el mundo académico, la industria de alta tecnología y el Ejército. El servicio militar obligatorio para los adultos jóvenes crea un flujo constante de personas con experiencia cibernética. La Unidad 8200 de las FDI es una incubadora de tecnología con énfasis particular en la ciberseguridad, y encuentra a sus mayores talentos visitando escuelas secundarias de todo el país para identificar candidatos de alto potencial a una edad temprana. Buscan estudiantes con altas capacidades analíticas que puedan tomar decisiones rápidas y trabajar bien en equipo. Los técnicos de la Unidad 8200 trabajan directamente con sus clientes para desarrollar productos innovadores y aprender habilidades fundamentales para las *startups*. La asociación de alumnos de la unidad ha fundado muchas empresas líderes israelíes.

El programa extracurricular *Magshimim* (Estudiantes destacados) es fruto de un esfuerzo cooperativo entre las FDI, el Ministerio de Educación y varias ONG, y se centra en la formación y el desarrollo de habilidades cibernéticas en la escuela secundaria. El programa *Gvachim* (Alturas) tiene como objetivo enseñarle a los estudiantes de secundaria los fundamentos de la defensa cibernética, elevar el nivel de la educación cibernética en Israel y preparar estudiantes para un examen de matriculación en ciberseguridad.²⁰ Los 400 estudiantes que participan en el Programa *Gvachim* se enfrentan a una considerable carga de trabajo de 900 horas. Todos los días aprenden lenguajes de programación, infraestructuras de red y cómo hacer frente a las amenazas informáticas.²¹

La institución israelí más emblemática para la cooperación público-privada en materia de formación en ciberseguridad es la Universidad Ben Gurión (BGU), situada en Beerseba, al sur del país. Alrededor de 1.000 de los 20.000 estudiantes que asisten a la BGU se especializan en informática o carreras relacionadas con las TI. La BGU fue la primera universidad israelí que ofreció un programa universitario de ciberseguridad, hace ya varios años.²² Israel cuenta con numerosas iniciativas para reforzar la formación y la educación de los trabajadores y los ciudadanos en cuestiones de ciberseguridad. Además de los programas de formación de las FDI, la inversión privada no deja de aumentar.²³

En marzo de 2015, el Ministerio de Educación israelí anunció una asociación con Lockheed Martin para crear un plan de estudios nacional de ciberseguridad para los estudiantes de secundaria de Israel.²⁴ La iniciativa compartirá las mejores prácticas y colaborará con otras iniciativas para poner en marcha talleres y concursos. En 2014, en Beerseba, durante la conferencia CyberTech, IBM estableció su Centro de Excelencia de Ciberseguridad (CCoE) en el campus de la Universidad Ben Gurión. El CCoE observa las tendencias tecnológicas y de mercado —incluidas la nube, los dispositivos móviles, la web, las redes sociales y las TI— e investiga los riesgos de seguridad que estas crean y cómo disminuirlos.²⁵

D3-1 Disponibilidad de educación y formación cibernéticas a nivel nacional

Hay una fuerte inversión en la educación de habilidades técnicas. Uno de los niveles de formación per cápita más altos del mundo en ciberseguridad.

D3-2 Desarrollo de la educación de seguridad cibernética a nivel nacional

El Ministerio de Relaciones Exteriores, las FDI y la educación superior desarrollan programas nacionales de formación cibernética. En 2013, las FIL implementaron el Programa Gvachim, un programa de educación de defensa cibernética de alto nivel para los estudiantes de 10.º a 12.º grado.

<https://www.idfblog.com/blog/2014/06/08/educating-future-cyber-warfare-next-generation-soldier/>

D3-3 Formación e iniciativas educativas públicas y privadas

La estrategia es integrar al mundo académico, a la industria de alta tecnología y al Ejército para formar a la próxima generación de mano de obra cibernética.

<http://www.c4isrnet.com/story/military-tech/cyber/2014/12/12/lockheed-forms-israeli-cyber-research-group/20299707/>

D3-4 Gobernanza corporativa, conocimiento y normas

Los directivos y los ejecutivos tienen un buen conocimiento de los problemas cibernéticos y de las normas. Sin embargo, aún no es completa su aplicación en todos los niveles de las empresas.

Marco jurídico y reglamentario

Establecido

La legislación israelí en materia de ciberseguridad se ha desarrollado lentamente. Los esfuerzos legales y reglamentarios israelíes prestan especial atención a la ciberdelincuencia y la protección de la privacidad. El mecanismo utilizado para procesar las violaciones con respecto a las TIC es la Ley de Informática de 1995, según la cual cualquier cambio, distorsión o daño provocado a los programas informáticos, cualquier violación de los permisos de acceso en el uso de una computadora o cualquier presentación de información de pantalla falsa constituye un delito punible de hasta cinco años de prisión.²⁶

Israel modificó su legislación informática en julio de 2012 para ponerla en línea con el Convenio sobre Ciberdelincuencia de Budapest, el primer tratado internacional sobre delitos cometidos a través de Internet.²⁷ Se creó una nueva sección 6, que considera delito crear o distribuir software para infiltrarse en un equipo, hacer que la computadora imprima información falsa o con el propósito de violar la privacidad de terceros o realizar escuchas ilegales, incluso si no llegan a causar daños o interferencias al sistema comprometido. También analiza la Convención de Budapest para exigir intencionalidad en el caso de los delitos enumerados en la sección 6.²⁸



INICIAL

FORMATIVO

ESTABLECIDO

ESTRATÉGICO

DINÁMICO

En noviembre de 2012, la policía israelí anunció la creación de una unidad de 60 personas para luchar contra los delitos informáticos, situada en el Ministerio de Seguridad Pública.²⁹ En el ámbito civil, la legislación y las políticas gubernamentales se han centrado históricamente en la seguridad de la información: protección de datos y sistemas informáticos.

En el último tiempo, los reguladores financieros de Israel han estado muy activos en el desarrollo de nuevas normas. En 2014, el Banco Central publicó directrices sobre la gestión de los riesgos en la nube. En 2015, el Supervisor Bancario emitió una circular que ordenaba a los bancos hacer hincapié en la gestión de los riesgos relacionados con la cibernética y adoptar medidas para reducir tales riesgos.³⁰

D4-1 Marco jurídico de seguridad cibernética

La Ley de Informática de 1995 persigue las violaciones de las TIC. Se modificó la ley en julio de 2012 para ponerla en consonancia con el Convenio sobre la Ciberdelincuencia de Budapest. La Ley de Protección de la Privacidad de 1981 (PPA) fue una de las primeras leyes de privacidad de su tipo del mundo.

http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403293_text

D4-2 Investigación jurídica

En noviembre de 2012, se creó, en relación con la IL-CERT, una unidad de 60 personas para hacer frente a la ciberdelincuencia, con sede en el Ministerio de Seguridad Pública.

<http://www.jpost.com/National-News/Israel-Police-to-tackle-cyber-crime-with-new-unit>

D4-3 Divulgación de información responsable

La INCB es responsable de comunicar incidentes cibernéticos y de informar al respecto al gobierno y al sector privado.

<http://sectech.tau.ac.il/cyberconference/index.php/israeli-national-cyber-bureau>



INICIAL

FORMATIVO

ESTABLECIDO

ESTRATÉGICO

DINÁMICO

Normas, organizaciones y tecnologías

Estratégico

Los intentos de Israel de regular la ciberseguridad para el sector privado se limitan principalmente al establecimiento de normas tecnológicas y a la cooperación entre gobierno e industria. En la actualidad, destacan dos iniciativas: las normas ISO 27001 e ISO 27002 de la Organización Internacional de Normalización (ISO). Ambas son normas de ciberseguridad que ofrecen certificaciones voluntarias ISO/IEC para empresas. También es digna de mención la Norma de Buenas Prácticas para la Seguridad del Foro de Seguridad de la Información (ISF), que cubre una amplia gama de marcos

de seguridad de la información para reducir los riesgos de las empresas asociadas a sistemas de información.³¹

La recomendación central de la Iniciativa Cibernética Nacional fue establecer una oficina cibernética nacional con estatus de órgano consultivo al servicio del gobierno y del jefe del gobierno. Las principales actividades de la oficina se relacionarían con políticas y acciones gubernamentales en el ámbito cibernético, incorporando aspectos tanto civiles como militares. El 7 de agosto de 2011, el Gobierno de Israel aprobó la creación de la Oficina Cibernética Nacional y determinó que tendría la función de propagador de políticas cibernéticas y órgano de coordinación, que mejoraría la protección de la infraestructura nacional frente a ataques cibernéticos y que haría avanzar la investigación cibernética en la esfera industrial.

En febrero de 2015, Israel anunció la creación de una nueva autoridad nacional de defensa cibernética. Sus principales funciones serían las siguientes:³²

1. Gestionar, controlar y llevar a cabo esfuerzos operativos a nivel nacional para proteger el ciberespacio, gracias a un enfoque sistémico que ofrezca soluciones defensivas completas y constantes frente a los ataques cibernéticos.
2. Operar un equipo de respuesta ante emergencias cibernéticas (CERT).
3. Consolidar y fortalecer la resistencia de la economía mediante medidas de preparación y regularización.
4. Diseñar y poner en práctica una doctrina nacional de defensa cibernética.
5. Realizar las tareas que el Primer Ministro pudiera determinar, en consonancia con la misión designada por la Autoridad.

Según la decisión programada, una Dirección Cibernética Nacional incluiría las sedes cibernéticas nacionales, como unidades independientes en la Oficina del Primer Ministro. La autoridad tendrá la responsabilidad de lograr sus objetivos y llevar a cabo su misión, mientras que las sedes cibernéticas nacionales dirigirán los ámbitos de la política y la estrategia nacional sobre competencia cibernética y reforzarán el papel de Israel en cuanto país a la vanguardia mundial en el campo de la ciberseguridad.³³

El IL-CERT (Equipo de Respuesta a Emergencias Informáticas de Israel) es el centro civil nacional para hacer frente a incidentes cibernéticos y de seguridad de la información. Se trata de una organización profesional independiente que proporciona una dirección para que personas y organizaciones de Israel y de todo el mundo puedan informar sobre incidentes relacionados con Internet en Israel. El IL-CERT es responsable de coordinar de manera proactiva las actividades que abordan incidentes de seguridad, compartiendo información y sensibilizando al público sobre cuestiones de seguridad de la información y la privacidad.³⁴ Realiza la gestión de crisis en Israel en caso de problemas cibernéticos, bajo la égida de la INCB. También investiga incidentes de seguridad de la información y publica información sobre el abordaje de incidentes futuros y sobre herramientas de defensa; a su vez, ofrece evaluaciones y recomendaciones de calidad para el público en general.³⁵

El trabajo de fortalecimiento de la resiliencia de la infraestructura nacional es responsabilidad de la nueva autoridad nacional de ciberseguridad (NCSA), creada por el Primer Ministro en 2015.

Su objetivo clave es fortalecer la resiliencia cibernética nacional consolidando estrategias y compartiendo información relevante con todas las organizaciones. La NCSA también es responsable del mantenimiento del IL-CERT y todos los esfuerzos operativo-defensivos nacionales.

Proteger la información sensible y los sistemas informáticos no son desafíos nuevos para Israel. El marco para la protección de infraestructuras críticas se previó en la decisión B/84 del Comité Ministerial de Seguridad Nacional, “La responsabilidad de proteger los sistemas informáticos en el Estado de Israel”, el 11 de diciembre de 2002. Si bien las amenazas han ido evolucionando, la decisión continúa sirviéndole de base al país al momento de responder a amenazas informáticas a la infraestructura crítica.³⁶ La decisión contempla la creación de un comité de dirección para identificar qué instituciones es fundamental proteger, y el establecimiento de una unidad de gobierno para proteger la infraestructura civil informatizada, la Autoridad de Seguridad de la Información (Re'em).³⁷ Esta fue establecida por el Shin Bet para cumplir con las restricciones legales sobre la intervención del gobierno en los negocios, ya que por ley solo las autoridades civiles, como la policía o el Servicio General de Seguridad, pueden intervenir en empresas privadas. Re'em supervisa la seguridad de TI en las instituciones definidas como críticas: proporciona orientación, supervisa la aplicación y establece sanciones contra quienes violen sus directrices. Las instituciones asumen los costos de la protección requerida.

El mercado de la ciberseguridad de Israel es uno de los que más rápido crecen en el mundo. En 2014, las empresas israelíes vendieron alrededor de US\$6.000 millones de software de seguridad de Internet, lo que equivale aproximadamente a una décima parte de las ventas mundiales. Gran parte se debe a Check Point, conocida por su software antivirus ZoneAlarm para computadoras personales, así como a una amplia gama de productos de seguridad empresarial en línea.³⁸ Israel también está propiciando el desarrollo de diversas *startups* de ciberseguridad. El año pasado se vendieron ocho de ellas a inversores extranjeros por un total de US\$700 millones.³⁹ Además, en Israel, los seguros cibernéticos tienen ya un pequeño mercado, que sigue creciendo.

D5-1 Adhesión a las normas

El sector privado aplica las normas ISO 27001 e ISO 27002. Ambas son normas de ciberseguridad que ofrecen certificaciones voluntarias de ISO/IEC para empresas. <http://www.27000.org/iso-27001.htm>

D5-2 Organizaciones de coordinación de seguridad cibernética

La INCB y la nueva Autoridad de Defensa Cibernética son responsables de la coordinación de la política cibernética. El centro de mando y control se encuentra dentro del Cuerpo C4I. <https://www.idfblog.com/about-the-idf/idf-units/c4i-computers-and-communications/>

D5-3 Respuesta a incidentes

La IL-CERT hace frente a incidentes cibernéticos y de TIC. Es responsable de coordinar las actividades que abordan incidentes de seguridad de manera proactiva antes de que ocurran, y de intercambiar información y concienciar al público sobre las cuestiones de seguridad de la información y la privacidad.

<https://il-cert.org.il/>

D5-4 Resiliencia de la infraestructura nacional

La infraestructura tecnológica nacional se gestiona a través de la INCB y la Autoridad de Seguridad de la Información (Re'em), que forma parte de la Agencia de Seguridad de Israel.

<http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx>

D5-5 Protección de la infraestructura crítica nacional

El marco para la protección de infraestructuras críticas de Israel se previó en la decisión B/84 del Comité Ministerial de Seguridad Nacional, "La responsabilidad de proteger los sistemas informáticos en el Estado de Israel", el 11 de diciembre de 2002.

http://sectech.tau.ac.il/sites/default/files/publications/article_3_12_-_chaire_cyberdefense.pdf

D5-6 Gestión de crisis

La gestión de crisis de naturaleza cibernética está específicamente en manos de la IL-CERT, bajo la tutela de la INCB. También investiga los incidentes de seguridad de la información y publica información sobre el abordaje de incidentes futuros y sobre herramientas de defensa, y ofrece evaluaciones y recomendaciones de calidad para el público en general.

<https://il-cert.org.il/>

D5-7 Redundancia digital

Los organismos dependientes de la INCB son responsables de los sistemas cibernéticos redundantes.

D5-8 Mercado de la ciberseguridad

El mercado de la ciberseguridad de Israel es uno de los que más rápido crecen en el mundo. En 2014, las empresas israelíes vendieron alrededor de US\$6.000 millones de software de seguridad de Internet, lo que equivale aproximadamente a una décima parte de las ventas mundiales.

Notas

1. Informe de la Agenda de Seguridad y Defensa (SDA), Cyber-Security: The Vexed Question of Global Rules (30 de enero de 2012): 66–67.
2. Raska, M. 2015. "Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defense Strategy." Universidad Tecnológica de Nanyang de la RSIS, enero de 2015.
3. Tabansky, L. and I. B. Israel. 2015. *Cybersecurity in Israel*. New York, NY: Springer.
4. "National Cyber Bureau," consultado el 10 de octubre de 2015 (<http://sectech.tau.ac.il/cyberconference/index.php/israeli-national-cyber-bureau>).
5. <http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/Background.aspx>.
6. "How Israel Balances Cybersecurity, Privacy - Al-Monitor: The Pulse of the Middle East." *Al-Monitor*, consultado el 9 de octubre de 2015 (<http://www.al-monitor.com/pulse/originals/2015/06/israel-national-cyber-bureau-shin-beth-civil-rights-privacy.html>).
7. Tabansky, L. 2013. "Cyberdefense Policy of Israel: Evolving Threats and Responses." *Yuval Ne'eman Workshop for Science, Technology and Security*. Enero de 2013 (http://sectech.tau.ac.il/sites/default/files/publications/article_3_12_-_chaire_cyberdefense.pdf).
8. Elban, M. y G. Siboni, "Establishing an IDF Cyber Command," *INSS Insight*. 8 de julio de 2015 (<http://www.inss.org.il/index.aspx?id=4538&articleid=10007>).
9. Sugarman, E. 2014. "What The United States Can Learn From Israel About Cybersecurity." *Forbes*. Octubre de 2014 (<http://www.forbes.com/sites/elisugarman/2014/10/07/what-the-united-states-can-learn-from-israel-about-cybersecurity/>).
10. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Israel.pdf.
11. Dror, Y. "Online Privacy in Israel." Facultad de Estudios de Gestión Académica, Universidad Hebrea, mayo de 2014 (http://www.colman.ac.il/research/research_institute/israel_project_Digital/Documents/digital_research_2014_eng.pdf).
12. "Cyber-Boom or Cyber-Bubble?" *The Economist*, 1 de agosto de 2015 (<http://www.economist.com/news/business/21660112-internet-security-has-become-bigger-export-earner-arms-cyber-boom-or-cyber-bubble>).
13. <http://sectech.tau.ac.il/cyberconference/index.php/israeli-national-cyber-bureau>.
14. Tabansky e Israel, *Cybersecurity in Israel*.
15. Raska, M. "The Israeli Experience." 2015. *The Straits Times*, 24 de junio de 2015 (<http://www.straitstimes.com/opinion/the-israeli-experience>).
16. "Basic Law: Human Dignity and Liberty (1992)," consultado el 9 de octubre de 2015 (<http://www.israelawresourcecenter.org/israelaws/fulltext/basiclawhumandignity.htm>).
17. Birnhack, M. y K. Niva Elkin. 2011. "Does Law Matter Online? Empirical Evidence on Privacy Law Compliance," *Michigan Telecommunications and Technology Law Review*, 17(2): 337–84.
18. Tabansky e Israel, *Cybersecurity in Israel*.
19. Raska, M. "Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defense Strategy." Universidad Tecnológica de Nanyang de la RSIS, enero de 2015.
20. Tabansky e Israel, *Cybersecurity in Israel*.
21. "Educating for the Future: Cyber Warfare and the Next Generation," *IDF Blog | The Official Blog of the Israel Defense Forces*, consultado el 9 de octubre de 2015 (<https://www.idfblog.com/blog/2014/06/08/educating-future-cyber-warfare-next-generation-soldier/>).
22. "Why Israel Could Be the next Cybersecurity World Power," *ITworld*, 9 de marzo de 2015 (<http://www.itworld.com/article/2894051/why-israel-could-be-the-next-cybersecurity-world-power.html>).
23. "Why Israel Could Be the next Cybersecurity World Power."
24. "Lockheed Martin Partners with Israel on National Cyber Curriculum," consultado el 7 de octubre de 2015 (<http://www.israeldefense.co.il/en/content/lockheed-martin-partners-israel-national-cyber-curriculum>).
25. "Why Israel Could Be the next Cybersecurity World Power."
26. Fish, J. "Israel Law Blog: Israel Updates Its Computer Law to Comply with the Budapest Convention," *Israel Law Blog*, July 26, 2012 (<http://israelawblog.blogspot.com/2012/07/israel-updates-its-computer-law-to.html>).
27. Levush, R. "Global Legal Monitor: Israel: Criminalization of Certain Activities Involving Computer Software | Global Legal Monitor | Law Library of Congress | Library of Congress" webpage, 21 de agosto de 2012 (http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403293_text).
28. Fish, J. "Israel Law Blog."
29. "Israel Police to Tackle Cyber Crime with New Unit." *The Jerusalem Post | JPost.com*, consultado el 9 de octubre de 2015 (<http://www.jpost.com/National-News/Israel-Police-to-tackle-cyber-crime-with-new-unit>).
30. "Israel Supervisor of Banks Issues Cyber Defense Circular," consultado el 28 de octubre de 2015 (http://www.law.co.il/en/news/israeli_internet_law_update/2015/03/20/banking-supervisor-issues-cyber-defense-circular/).

31. "Towards a Cybersecurity Policy Model – Israel National Cyber Bureau (INCB) Case Study," 7 de enero de 2015 (https://publixphere.net/i/noc/page/IG_Case_Study_Towards_a_Cyber_Security_Policy_Model_Israel_National_Cyber_Bureau_INCB).
32. "Cabinet Approves Establishment of National Cyber Authority 15 Feb 2015," consultado el 28 de octubre de 2015 (<http://mfa.gov.il/MFA/PressRoom/2015/Pages/Cabinet-approves-establishment-of-National-Cyber-Authority-15-Feb-2015.aspx>).
33. "Broad Powers to a New Israeli National Cyber Defense Authority," consultado el 9 de octubre de 2015 (http://www.law.co.il/en/news/israeli_internet_law_update/2015/01/09/Broad-Powers-to-new-National-Cyber-Defense-Authority/).
34. "IL-CERT." *IL-CERT*, consultado el 9 de octubre de 2015 (<https://il-cert.org.il/>).
35. *Ibid.*
36. Tabansky, L. 2011. "Critical Infrastructure Protection against Cyber Threats," *Military and Strategic Affairs* 3(2). Noviembre: 72.
37. <http://www.shabak.gov.il/about/units/reem/Pages/default.aspx>.
38. "Cyber-Boom or Cyber-Bubble?"
39. "US IPO Pricing Recap: CyberArk Software Pops 85% and Year's Second Largest IPO Trades Up." *NASDAQ.com*, consultado el 28 de octubre de 2015 (<http://www.nasdaq.com/article/us-ipo-pricing-recap-cyberark-software-pops-85-and-years-second-largest-ipo-trades-up-cm396042>).



República de Corea

Política y estrategia



Cultura y sociedad



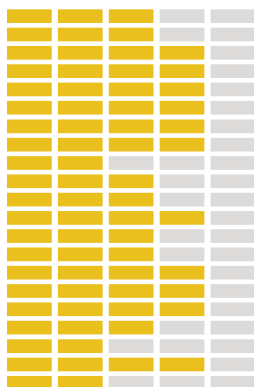
Educación



Marcos legales



Tecnología



Principales desafíos de ciberseguridad

La postura de ciberseguridad de la República de Corea refleja el desafío que plantea Corea del Norte. El ciberespacio se ha convertido en un nuevo escenario de conflicto en la península coreana. La creciente capacidad cibernética de Corea del Norte hace que la República de Corea se esfuerce por mejorar su seguridad cibernética.

El Libro Blanco de la Defensa de la República de Corea de 2014 subraya que “Corea del Norte cuenta en la actualidad con unos 6.000 soldados de guerra cibernética y lleva a cabo una guerra cibernética, que incluye la perturbación de operaciones militares y ataques contra las grandes infraestructuras nacionales con el fin de causar una parálisis psicológica y física en el Sur”.¹ Según un informe de 2015, los ataques cibernéticos procedentes de Corea del Norte han acarreado daños económicos para el vecino del sur que ascienden a 800.000 millones de won (US\$706 millones).² Son ejemplos de acciones cibernéticas de Corea del Norte los ataques de 2013 que interrumpieron el servicio de varias cadenas de televisión y dos bancos surcoreanos.³ Las investigaciones de la República de Corea sobre una falla en el sistema de información de un operador de una planta nuclear en diciembre de 2014 apuntan a una intrusión norcoreana.⁴ Los atacantes no pusieron en peligro ningún sistema crítico para la gestión de la operación de los reactores, pero obtuvieron proyectos y datos de pruebas que podrían ser útiles para planificar futuros ataques. Estados Unidos y los organismos de defensa surcoreanos suponen que, en caso de un conflicto de envergadura, Corea del Norte lanzará ataques cibernéticos contra infraestructuras críticas de la República de Corea y sus redes de comando y control.

POBLACIÓN TOTAL DEL PAÍS

50.423.955

Penetración de Internet

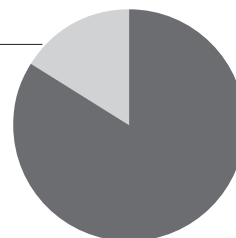
Abonos a teléfonos celulares

58.340.515

Personas con acceso a Internet

42.507.394

84%

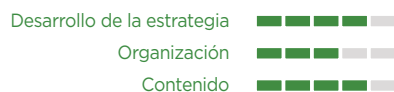


Fuente: Indicadores de Desarrollo del Banco Mundial (2014). Disponible en: <http://databank.worldbank.org/data/reports.aspx?source=2&country=USA&series=&period=>

Política y estrategia



Estrategia nacional de seguridad cibernética oficial o documentada



Defensa cibernética



Cultura y sociedad



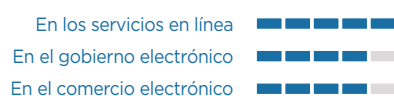
Mentalidad de seguridad cibernética



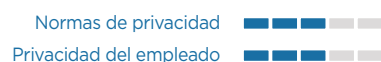
Conciencia de seguridad cibernética



Confianza en el uso de Internet



Privacidad en línea



Educación



Disponibilidad nacional de la educación y formación cibernéticas



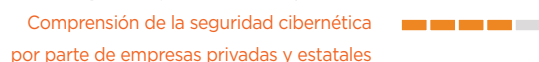
Desarrollo nacional de la educación de seguridad cibernética



Formación e iniciativas educativas públicas y privadas



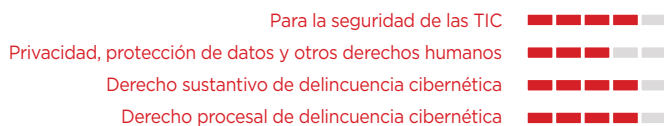
Gobernanza corporativa, conocimiento y normas



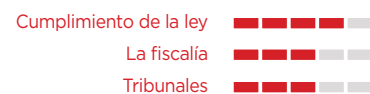
Marcos legales



Marcos jurídicos de seguridad cibernética



Investigación jurídica



Divulgación responsable de la información



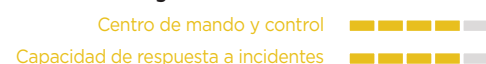
Tecnologías



Adhesión a las normas



Organizaciones de coordinación de seguridad cibernética



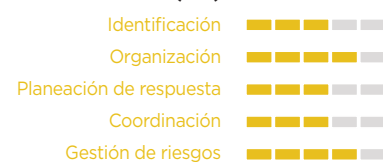
Respuesta a incidentes



Resiliencia de la infraestructura nacional



Protección de la Infraestructura Crítica Nacional (ICN)



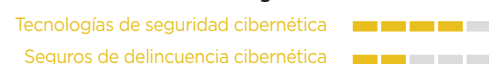
Gestión de crisis



Redundancia digital



Mercado de la ciberseguridad





INICIAL



FORMATIVO



ESTABLECIDO



ESTRATÉGICO



DINÁMICO



Política y estrategia de ciberseguridad

Estratégico

La primera política de ciberseguridad de la República de Corea se encuadró en una estrategia más amplia que buscaba digitalizar su economía. La creación en 1996 del Centro Coreano de Seguridad de la Información —la actual Agencia Coreana de Internet y Seguridad (KISA)— fue uno de los primeros pasos del país en el ámbito de la ciberseguridad. Desde entonces, sus políticas de ciberseguridad han pasado por varios ciclos. En 2011, la República de Corea anunció un “plan maestro” nacional de ciberseguridad para responder a los ataques cibernéticos.⁵ Desarrollado en conjunto por 15 organismos gubernamentales, el plan adopta un enfoque global de la ciberseguridad nacional, que considera al ciberespacio una parte más del territorio nacional que necesita un sistema de defensa a escala nacional. En el marco del plan maestro, el Centro Nacional de Ciberseguridad, dirigido por el Servicio Nacional de Inteligencia, coordina las iniciativas contra los ataques informáticos entre los organismos gubernamentales. La estrategia insta a los organismos gubernamentales y a las empresas privadas a cifrar los datos importantes y hacer copias de seguridad de ellos, así como a instalar programas informáticos que eviten ataques cibernéticos. Para supervisar su aplicación y coordinación, en marzo de 2015 la República de Corea anunció el nombramiento de un nuevo consejero presidencial dedicado a cuestiones de ciberseguridad.⁶

El Plan Maestro Nacional de Ciberseguridad se basa en tres pilares: la inversión en capacidades de seguridad, el desarrollo de un marco jurídico y la cooperación internacional. Las tareas emprendidas en su puesta en práctica se agrupan en cinco planes de acción:

6. Establecer un sistema de respuesta conjunta de los sectores privado, público y militar.
7. Fortalecer la seguridad de las infraestructuras críticas y mejorar la protección de los secretos.
8. Detectar y bloquear los ataques cibernéticos a nivel nacional.
9. Poner en marcha medidas disuasorias contra la provocación cibernética y fortalecer la cooperación internacional.
10. Crear infraestructuras de ciberseguridad.

D1-1 Estrategia nacional de seguridad cibernética

En abril de 2015, la República de Corea nombró a su primer asesor cibernético del presidente dentro de la Oficina Nacional de Seguridad. El puesto representa una “torre de control” del país para favorecer respuestas eficaces a las amenazas informáticas.

<http://english1.president.go.kr/government/office-of-national-security.php>

D1-2 Consideración de la defensa cibernética

El Cibercomando fue creado en 2010. El Ejército coreano posee tanto capacidades cibernéticas ofensivas como defensivas, desarrolladas principalmente para contrarrestar la capacidad cibernética de Corea del Norte.

http://m.mnd.go.kr/cop/pblicttn/selectPublicationUser.do?siteId=mnd_eng&componentId=51&categoryId=0&publicationSeq=689&pageIndex=1&id=mnd_eng_021400000000

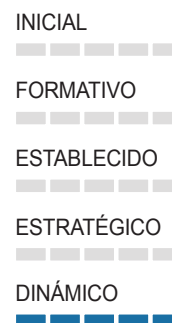
Cultura cibernética y sociedad

Dinámico

La República de Corea es un líder mundial en TI. Más de 75% de los coreanos tienen teléfonos móviles. Además, está por delante de Estados Unidos y Europa en términos de penetración de la banda ancha: las tres cuartas partes de los hogares coreanos tienen banda ancha de alta velocidad. Dos tercios de los coreanos menores de 30 años utilizan dispositivos inalámbricos para acceder a Internet. El acceso de banda ancha está muy subvencionado, y el gobierno promueve activamente el uso de Internet como parte de una estrategia de innovación más amplia.⁷

A fin de promover una cultura cibernética resiliente, la República de Corea se esfuerza por aumentar la concienciación general sobre la ciberseguridad, compartir las mejores prácticas y enviar alertas de amenazas específicas. Además del Mes de Concienciación sobre Seguridad de la Información, en octubre de 2013 la Comisión de Comunicaciones de Corea puso en marcha la campaña de Mantenimiento de la Seguridad en Internet, donde conocidos personajes hablaron en televisión y radio sobre la protección de datos personales. También se instalaron pancartas y se publicaron anuncios en subterráneos, autobuses, centros comerciales y salas de juego.⁸

Como parte de este esfuerzo público, la KISA dirige un “programa de vacunación cibernética”, en colaboración con los proveedores de servicios de Internet, a fin de identificar y contactar a los usuarios cuyos equipos hayan sido secuestrados por una *botnet*. También se ofrecen herramientas gratuitas en línea para eliminar el *malware* que agrega computadoras a los ataques en red. A medida que los usuarios van usando cada vez más los dispositivos móviles inteligentes, las soluciones de seguridad gubernamentales han ampliado la cobertura del espectro. La aplicación *Phone Keeper* analiza los teléfonos en busca de *malware* e impide que un usuario abra accidentalmente enlaces de texto de *phishing* que conduzcan a sitios web infectados.⁹



D2-1 Mentalidad de seguridad cibernética

La República de Corea se considera el país más conectado del mundo, por lo que en los medios tradicionales, en los medios sociales y en los debates académicos se habla con frecuencia de los problemas y las políticas de ciberseguridad. Los medios digitales tienen cada vez más peso como fuente de opinión para los surcoreanos.

D2-2 Conciencia de seguridad cibernética

La KISA y la Comisión de Comunicaciones de Corea han puesto en marcha campañas de concienciación cibernética para promover la resiliencia entre la población. <http://isis.kisa.or.kr/eng/ebook/EngWhitePaper2014.pdf>



INICIAL



FORMATIVO



ESTABLECIDO



ESTRÁTÉGICO



DINÁMICO



D2-3 Confianza en el uso de Internet

Se estima que un 85% de los surcoreanos están conectados a Internet, lo que influye en el comercio de forma determinante.

D2-4 Privacidad en línea

Las protecciones para la privacidad en la actividad en línea son débiles, y se ha criticado al gobierno por tratar de controlar contenidos críticos hacia la política gubernamental.

Educación, formación y competencias en seguridad cibernética

Estratégico

El enfoque de la República de Corea sobre educación y formación en ciberseguridad busca aprovechar su servicio militar nacional obligatorio, su ingeniería e informática de primer nivel y su sólido sector empresarial. El ejército de la República de Corea ha creado numerosos programas educativos y de capacitación para formar expertos en cuestiones cibernéticas. En colaboración con el Ministerio de Ciencia, TIC y Planificación del Futuro, los militares crearon en 2015 un programa para contratar profesionales directamente del sector privado. La Universidad de Corea también ha creado el Departamento de Defensa Cibernética, que fomenta la formación de expertos cibernéticos especializados.¹⁰ La normativa que obliga a las grandes empresas a contratar jefes de seguridad de los servicios de información ha conllevado un aumento de la demanda de profesionales especializados en cuestiones cibernéticas.

La KISA apoya la formación de asociaciones entre universidades y empresas privadas para modernizar el programa académico según las necesidades de las empresas y garantizarles empleo a los estudiantes desde el comienzo de su formación. Otra iniciativa de la KISA fue la creación de la Academia de Seguridad del Conocimiento y la Información, diseñada para hacer frente al déficit de profesionales en diversas disciplinas tales como ciencia forense digital, biorreconocimiento, aplicación de RFID/USN para la seguridad y consultoría sobre seguridad de la información.¹¹ Los altos costos de inversión inicial en estos campos han dado lugar a un desajuste entre las limitadas oportunidades de formación en las instituciones existentes y una mayor demanda de expertos en estas áreas en el mercado laboral.¹²

Desde 2005, la KISA, a través del Curso de Formación de Asia y el Pacífico sobre Seguridad de la Información, ha ayudado a países en desarrollo a elaborar sus CERT nacionales. Los empleados gubernamentales reciben guías de mejores prácticas en el Centro de Formación sobre la Información, dirigido por el Departamento de Desarrollo de Recursos Humanos de Informatización, dependiente del Ministerio de Seguridad y Administración Pública.¹³

En 2008, el Ministerio de Educación creó el Centro de Formación en Ciberseguridad (CECA) para ayudar a mejorar las normas de seguridad relativas al desarrollo de la propiedad intelectual en

las universidades de investigación. En 2013, participaban 406 instituciones, 308 de las cuales han establecido centros de control locales. El CECA intercambia información y coordina la respuesta a incidentes con el KrCERT y el Centro Nacional de Ciberseguridad.¹⁴

D3-1 Disponibilidad de educación y formación cibernéticas a nivel nacional

La KISA ha puesto en marcha la Academia de Seguridad del Conocimiento y la Información, y el Ministerio de Información y Comunicación organiza campañas de formación de expertos todos los años.

<https://www.kisa.or.kr/eng/main.jsp>

D3-2 Desarrollo de la educación de seguridad cibernética a nivel nacional

Parte de la estrategia de la República de Corea para establecer una base de conocimientos de TIC implica ser un "país impulsado por las personas", por lo que siguen creciendo las oportunidades de educación en materia de seguridad de la información.

<http://www.klink.or.kr/pages/program/program.jsp>

D3-3 Formación e iniciativas educativas públicas y privadas

El sector de las TIC de la República de Corea mantiene una estrecha relación con el gobierno, y las iniciativas público-privadas están creciendo. La Alianza Nacional de Seguridad de la Información (NISA) está compuesta por representantes del sector público y privado e instituciones académicas.

http://itlaw.wikia.com/wiki/National_Information_Security_Alliance

D3-4 Gobernanza corporativa, conocimiento y normas

Una estrecha relación entre la industria y el gobierno ha fomentado el crecimiento del comercio electrónico y la aplicación de normas eficaces para la información cibernética.

http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=PRC_K1V4V0O2U2M7N0L0Z3B1T3J8X6Z0E9

Marco jurídico y reglamentario

Establecido

La República de Corea no tiene una legislación general de ciberseguridad ni de infraestructuras críticas, sino una serie de leyes y reglamentos en materia de protección de la información, incluidas leyes sobre secretos militares, telecomunicaciones, delitos informáticos, gobierno electrónico y protección de las infraestructuras de la información. Las más importantes son la Ley Nacional de Prevención del Terrorismo Cibernético, la Ley de Protección de la Infraestructura de la Información y las Comunicaciones, la Ley sobre la Privacidad, y el Reglamento de Gestión de la Ciberseguridad Nacional (directiva presidencial 141).



INICIAL



FORMATIVO



ESTABLECIDO



ESTRATÉGICO



DINÁMICO



La primera ley de la República de Corea que se dedicó a la ciberseguridad data de 1995, cuando la Ley Marco de Promoción de la Informatización¹⁵ convirtió la seguridad de la información en una responsabilidad gubernamental.¹⁶ La ley describe las responsabilidades de la KISA, así como los requisitos de información para los proveedores de servicios de información y comunicación. Luego le siguieron la Ley de Protección de la Infraestructura de Información y Comunicación (2002) y la Ley de Promoción del Uso de la Información y las Redes de Comunicación y de la Protección de la Información (2003), que constituyen la base legislativa para la aplicación de la legislación sobre delitos cibernéticos en la República de Corea.¹⁷

La Ley de Prevención de la Divulgación y de Protección de la Tecnología Industrial¹⁸ dispuso la suspensión y prohibición total de la exportación de tecnologías cuando se considere que socava la seguridad nacional de la República de Corea. La Ley de Promoción de la Industria de la Tecnología de la Información y de las Comunicaciones de 2009, que busca crear un entorno nacional propicio para el sector de las TIC, incluye una sección sobre el fortalecimiento de la seguridad de la información. La Ley de la Firma Digital regula la distribución de certificados públicos.

La Ley de Gobierno Electrónico¹⁹ esboza los procedimientos de autenticación y los certificados aceptados para garantizar la seguridad en la provisión digital de servicios gubernamentales. Los problemas de privacidad no tratados por esta ley se abordan en la Ley de Protección de Datos Personales Almacenados y Mantenidos por Organismos Públicos.

La Ley sobre el Desarrollo de la Computación en la Nube y la Protección de los Usuarios —en vigor desde septiembre de 2015— es la primera de este tipo. Los proveedores de servicios en la nube están obligados a informar a los usuarios afectados de cualquier fuga de datos que se produzca. Además, la ley prohíbe explícitamente compartir información personal con proveedores de servicios y obliga a destruir tales registros de información tras la interrupción del servicio. También hace responsables a los proveedores de servicios de los daños causados a los usuarios en caso de intrusiones en la red.²⁰

D4-1 Marco jurídico de seguridad cibernética

La Ley Penal, la Ley de Promoción del Uso de la Información y las Redes de Comunicación y de la Protección de la Información, la Ley de Protección de Datos Personales y la Ley de Protección de la Infraestructura de la Información y la Comunicación forman la base legislativa para la aplicación de la legislación penal cibernética en la República de Corea.

<http://www.worldlii.org/int/other/PrivLRes/2005/2.html>

D4-2 Investigación jurídica

La Oficina Cibernética de la Agencia Nacional de Policía se fundó en junio de 2014, aunque la primera vez que se formó un equipo de investigación de delitos informáticos fue en 1997.

www.netan.go.kr/eng/index.jsp

D4-3 Divulgación de información responsable

La Comisión de Comunicaciones de Corea (KCC) es el órgano regulador responsable de reportar incidentes de violación de datos cibernéticos. Recientes modificaciones en relación con la violación de datos (Ley No. 10479) en la legislación sobre protección de datos surcoreana aumentan las multas, disminuyen el umbral de responsabilidad que han de cumplir los reguladores para imponer multas, permiten compensar a los demandantes individuales sin probar los daños y obligan a la notificación de las personas afectadas en un plazo de 24 horas tras descubrirse una violación.

http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=PRC_K1V4V0O2U2M7N0L0Z3B1T3J8X6Z0E9

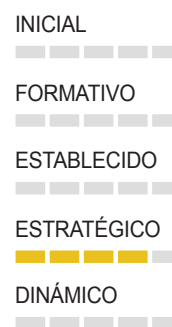
Normas, organizaciones y tecnologías

Estratégico

La República de Corea tiene diversos órganos con responsabilidades en el ámbito de la ciberseguridad, entre los que destacan el Ministerio de Defensa Nacional (que incluye el Cibercomando de Corea), el Ministerio de Ciencia, TIC y Planificación del Futuro, el Servicio Nacional de Inteligencia y el Ministerio de Seguridad y Administración Pública. La KISA se encarga de la sensibilización sobre las amenazas y el intercambio de información con el sector privado.

El Centro Nacional de Ciberseguridad (NSCS), que forma parte del Servicio de Inteligencia Nacional, es el principal órgano para investigar y analizar los incidentes de ciberseguridad en la República de Corea. Durante las crisis, el Equipo Nacional de Respuesta ante las Amenazas Cibernéticas, formado por militares y entidades civiles y del sector privado, colabora con el Centro. La gestión de incidentes cibernéticos —públicos y privados— es responsabilidad del Equipo de Respuesta a Incidentes de Seguridad Informática/Centro de Coordinación (KnCERT/CC).

La República de Corea no cuenta con normas de ciberseguridad ni requisitos de certificación específicos para las adquisiciones públicas. Cuando se han establecido requisitos generales de contratación TI, a veces se incluyen requisitos locales específicos. La República de Corea también ha introducido requisitos en cuestión de pruebas nacionales para productos que ya han recibido una acreditación internacional. Aunque la República de Corea participa en el Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes (CCRA), en la práctica se da una combinación de requisitos locales únicos y de requisitos de pruebas adicionales, lo que supone un obstáculo para la correcta aplicación del CCRA.²¹ La República de Corea tiene su propio Sistema de Evaluación y Certificación (KECS) para promover el uso de productos y sistemas de TI certificados y validados a fin de mejorar el nivel de seguridad de las redes nacionales de información y comunicaciones. Estos requisitos se están formalizando en todas las políticas de adquisiciones públicas.²²



D5-1 Adhesión a las normas

La República de Corea participa en el CCRA, pero en la práctica se da una combinación de requisitos locales únicos y requisitos de pruebas adicionales que supone un obstáculo para la correcta aplicación del CCRA. La República de Corea tiene su propio Sistema de Evaluación y Certificación para promover el uso de productos y sistemas de TI certificados y validados.

<https://www.commoncriteriaportal.org/ccra/members/>

<http://www.ipa.go.jp/event/iccc2005/pdf/B1-09B.pdf>

D5-2 Organizaciones de coordinación de seguridad cibernética

En abril de 2015, el presidente Park nombró al general de brigada Shin In-Seop como coordinador de ciberseguridad de la República de Corea dentro de la Oficina Nacional de Seguridad. El puesto está diseñado para fortalecer aún más la "torre de control" del país y favorecer una respuesta más eficaz a las amenazas cibernéticas.

<http://english1.president.go.kr/government/office-of-national-security.php>

D5-3 Respuesta a incidentes

La República de Corea mantiene una capacidad efectiva en su CERT. El KrCERT, que depende de la KISA, trabaja con el sector privado, mientras que el KnCERT es responsable de las respuestas del sector público como parte del Centro Nacional de Ciberseguridad, y del vínculo con los CERT privados.

<http://eng.krcert.or.kr/main/main.jsp>

D5-4 Resiliencia de la infraestructura nacional

Esta cuestión no se ha tratado de manera explícita.

D5-5 Protección de la infraestructura crítica nacional

La infraestructura crítica es protegida por la oficina del Primer Ministro de Corea, el Centro Nacional de Ciberseguridad (NSCS) y el Ministerio de Ciencia, TIC y Planificación del Futuro.

<https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/presentations/dr-so-jeong-kim-national-security-research-institute-s-korea-cyber-security-in-the-republic-of-south-korea>

D5-6 Gestión de crisis

El KnCERT y el KrCERT son responsables de la gestión de las crisis cibernéticas.

<http://service1.nis.go.kr>

D5-7 Redundancia digital

Esta cuestión no se ha tratado de manera explícita.

D5-8 Mercado de la ciberseguridad

La comunidad empresarial de la República de Corea mantiene una estrecha relación con el gobierno, que apoya los esfuerzos que hacen las empresas por crecer. Esto se ha extendido a la economía digital, donde la financiación del gobierno apoya a un fuerte sector de *startups*.

Notas

- Ministerio de Defensa de la República de Corea. 2015. *Libro Blanco de la Defensa, 2014* (http://m.mnd.go.kr/cop/pblict/selectPublicationUser.do?siteId=mnd_eng&componentId=51&categoryId=0&publicationSeq=689&pageIndex=1&id=mnd_eng_021400000000).
- "Cybercrime in Asia: A Changing Regulatory Environment. Marsh Asia," consultado el 23 de octubre de 2015, (<http://asia.marsh.com/NewsInsights/ID/41587/Cybercrime-in-Asia-A-Changing-Regulatory-Environment.aspx>).
- Cluley, F. 2013. "DarkSeoul: SophosLabs Identifies Malware Used in South Korean Internet Attack," *nakedsecurity.sophos.com*, 20 de marzo de 2013 (<https://nakedsecurity.sophos.com/2013/03/20/south-korea-cyber-attack/>); "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War," Blog Oficial de Symantec, 26 de junio de 2013 (<http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>).
- Park, J.-M. y M. Cho. 2015. "South Korea Blames North Korea for December Hack on Nuclear Operator," 17 de marzo de 2015 (<http://www.reuters.com/article/2015/03/17/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317>).
- Disponible en: https://ccdc.co.kr/sites/default/files/strategy/KOR_NCSS_2011.pdf.
- "South Korea Beefs Up Cybersecurity With an Eye on North Korea." *The Diplomat*, consultado el 22 de octubre de 2015 (<http://thediplomat.com/2015/04/south-korea-beefs-up-cyber-security-with-an-eye-on-north-korea/>).
- "Why Internet Connections Are Fastest in South Korea – CNN.com," consultado el 27 de octubre de 2015 (<http://edition.cnn.com/2010/TECH/03/31/broadband.south.korea/>).
- Ministerio de Ciencia, TIC y Planificación Futura de la República de Corea y Agencia de Internet y Seguridad de Corea. 2014. *Korea Internet White Paper*, 93–4 (<http://isis.kisa.or.kr/eng/ebook/EngWhitePaper2014.pdf>).
- "South Korean Schools Are Remotely Disabling Students' Smartphones." *The Verge*, consultado el 27 de octubre de 2015 (<http://www.theverge.com/2014/3/20/5528842/korean-schools-block-smartphones-in-class-smartkeeper>).
- Instituto para el Desarrollo de Corea y Ministerio de Estrategia y Finanzas de la República de Corea. 2011. "Eight Key Areas of ICT Development in Korea and Three High Priority Initiatives in Abu Dhabi's ICT Development." Mayo de 2011, 276 (http://cid.kdi.re.kr/cid_eng/public/report_read05.jsp?1=1&pub_no=12035).
- La sigla corresponde a "identificación por radiofrecuencia/red de sensores ubicuos."
- Eight Key Areas of ICT Development in Korea*, 279.
- Ibid.*, 267.
- 2013 White Paper on ICT in Education Korea*, 106.
- Rebautizada en 2009 Ley Marco de Promoción de la Informatización.
- En el Libro Blanco de Internet de Corea de 2014 (pág. 95) figura una descripción completa de las leyes relacionadas con Internet que se encuentran en vigor (a junio de 2014).
- La Ley de Promoción del Uso de la Información y las Redes de Comunicación se rebautizó como Ley de Promoción del Uso de la Información y las Redes de Comunicación y de la Protección de la Información, etc.
- Ley de Prevención de la Divulgación y para la Protección de la Tecnología Industrial, República de Corea, la Ley No. 8062, del 27 de octubre de 2006, modificada por la Ley No. 11690 del 23 de marzo de 2013 (<http://www.wipo.int/wipolex/en/details.jsp?id=13745>).
- Ley de Gobierno Electrónico, República de Corea, Ley No. 8171, del 3 de enero de 2007, modificada por la Ley No. 11461 del 1 de junio de 2012 (http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=25509&type=new&key).
- Galeote, R. 2015. "South Korea: National Assembly Passes 'World-first' Cloud Computing Act," *DataGuidance.com*, 19 de marzo de 2015 (http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=3459).
- "Members of the CCRA: New CC Portal," consultado el 23 de octubre de 2015 (<http://www.commoncriteriaportal.org/ccra/members/>).
- "Welcome to ITSCC," consultado el 23 de octubre de 2015 (<http://www.itsc.kr/eng/main.asp>).



Estados Unidos

Política y estrategia



Cultura y sociedad



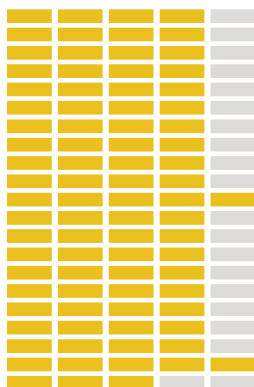
Educación



Marcos legales



Tecnología



Principales desafíos de ciberseguridad

Estados Unidos tiene un complejo conjunto de normas, instituciones y políticas para administrar el desafío de la ciberseguridad. Las iniciativas comenzaron hace casi 20 años, en la década del noventa, pero en los últimos seis años ha surgido un enfoque compacto e integrado. Las autoridades estadounidenses consideran a las amenazas cibernéticas como la principal amenaza estratégica a la que se enfrenta el país.¹ Estados Unidos ha experimentado una campaña continua de espionaje económico y delitos financieros a través de Internet y se enfrenta a un riesgo de ataques a sus infraestructuras y servicios críticos. Las pérdidas para la economía estadounidense se elevan a miles de millones de dólares cada año. El último año ha sido particularmente difícil, con ataques coercitivos dirigidos contra Sony Pictures, el Casino Sands y Github, un servicio de alojamiento. Estados Unidos ha detectado que diversos países han examinado su infraestructura crítica en busca de vulnerabilidades con vistas a un ataque cibernético.

POBLACIÓN TOTAL DEL PAÍS

318.857.056

Penetración de Internet

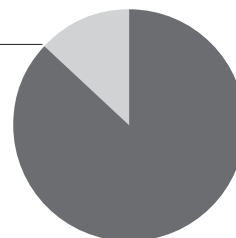
Abonos a teléfonos celulares

351.380.475

Personas con acceso a Internet

278.681.066

87%

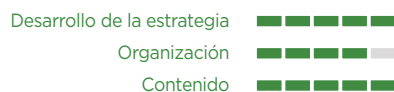


Fuente: Indicadores de Desarrollo del Banco Mundial (2014). Disponible en: <http://databank.worldbank.org/data/reports.aspx?source=2&country=USA&series=&period=>

Política y estrategia



Estrategia nacional de seguridad cibernética oficial o documentada



Defensa cibernética



Cultura y sociedad



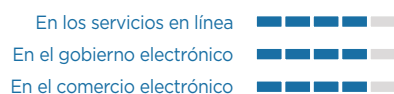
Mentalidad de seguridad cibernética



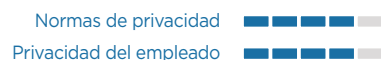
Conciencia de seguridad cibernética



Confianza en el uso de Internet



Privacidad en línea



Educación



Disponibilidad nacional de la educación y formación cibernéticas



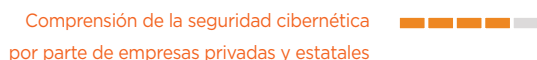
Desarrollo nacional de la educación de seguridad cibernética



Formación e iniciativas educativas públicas y privadas



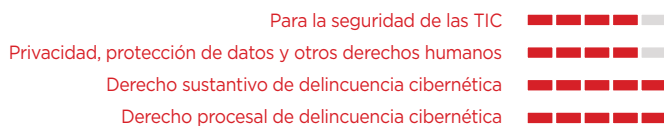
Gobernanza corporativa, conocimiento y normas



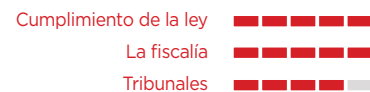
Marcos legales



Marcos jurídicos de seguridad cibernética



Investigación jurídica



Divulgación responsable de la información



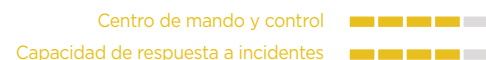
Tecnologías



Adhesión a las normas



Organizaciones de coordinación de seguridad cibernética



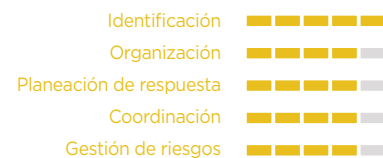
Respuesta a incidentes



Resiliencia de la infraestructura nacional



Protección de la Infraestructura Crítica Nacional (ICN)



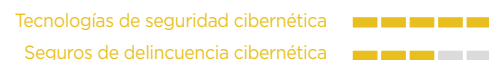
Gestión de crisis



Redundancia digital



Mercado de la ciberseguridad





Política y estrategia de ciberseguridad

Estratégico

La Comisión de la Casa Blanca sobre la Protección de las Infraestructuras Críticas de 1998 predijo que el hecho de depender cada vez más de sistemas de información cibernéticos crearía “una nueva dimensión de vulnerabilidad”.² El informe determinó que los ataques cibernéticos a infraestructuras y sistemas de información podrían perjudicar seriamente a la economía y a la seguridad de Estados Unidos.

En respuesta, la Casa Blanca creó la Directiva de Decisión Presidencial 63 (PDD-63), que recomienda a los organismos que tomen todas las medidas necesarias para garantizar la continuidad y la viabilidad de las infraestructuras críticas. La PDD-63 creó la figura de un Coordinador Nacional para la Seguridad, la Protección de las Infraestructuras y el Contraterrorismo (un alto funcionario de la Casa Blanca). La decisión también creó alianzas público-privadas. El presidente designó a organismos del gobierno federal que encabezarían la acción respecto a determinadas infraestructuras críticas. Aunque la PDD-63 solicitó la creación de un Centro de Análisis e Intercambio de Información único, diversos sectores de infraestructuras críticas crearon sus propios centros específicos del sector. La eficacia varía según los sectores, pero algunos, como el de Servicios Financieros, se destacaron por sus éxitos. El Centro Pluriestatal de Análisis e Intercambio de Información proporciona información a los gobiernos locales y estatales en los 50 estados y en territorios y distritos de los EE.UU.³ Sin embargo, las medidas resultaron ser insuficientes, lo que llevó a la Casa Blanca a crear en 2008 la Iniciativa Integral de Ciberseguridad Nacional (CNCI).⁴ Entre sus atribuciones se encuentran:⁵

- La gestión de las redes del gobierno de manera unificada mediante el programa “*Trusted Internet Connections*”.
- La puesta en marcha de sistemas de detección y prevención de intrusiones en todo el gobierno.
- La coordinación de los esfuerzos en I+D.
- La conexión de los centros federales de operaciones cibernéticas.
- El desarrollo y la aplicación de un plan de contrainteligencia cibernética que abarque a todo el gobierno.
- El aumento de la seguridad de las redes confidenciales.
- La expansión de la educación cibernética.
- El desarrollo de estrategias y programas de disuasión.
- La gestión de riesgos de la cadena de suministro.
- La definición del papel del Gobierno federal en materia de ciberseguridad de las infraestructuras críticas.

Solo unas pocas de estas iniciativas tuvieron éxito. Poco después de asumir el cargo en 2009, el Presidente Obama ordenó una revisión de las iniciativas federales, como la CNCI, y pidió al Consejo de Seguridad Nacional que desarrollara un enfoque global sobre ciberseguridad. La Revisión de la Política Cibernética resultante recomendó la adopción de varias medidas:⁶

- Crear un puesto de coordinador de ciberseguridad.
- Trabajar con las administraciones estatales y locales y con el sector privado para ofrecer una respuesta unificada a futuros incidentes cibernéticos.

- Fortalecer las alianzas público-privadas.
- Invertir en una I+D de punta.
- Iniciar una campaña para promover la sensibilización sobre la ciberseguridad y la formación de mano de obra digital.

En 2011, el gobierno del Presidente Obama elaboró también una Estrategia Internacional para el Ciberespacio, haciendo hincapié en la “estabilidad a través de normas”, y creó el cargo de Coordinador de Ciberseguridad del Departamento de Estado.⁷

D1-1 Estrategia nacional de seguridad cibernética

La Estrategia Nacional Integral de Seguridad Cibernética de 2008 y la Revisión de la Política Cibernética de 2009 definen la estrategia cibernética de Estados Unidos.

<https://www.whitehouse.gov/node/233086>

https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

D1-2 Consideración de la defensa cibernética

La estrategia se resume en la Estrategia Cibernética de 2015 del Departamento de Defensa.

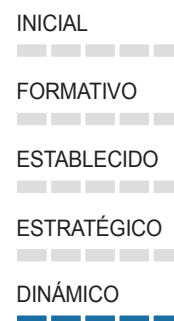
http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Cultura cibernética y sociedad

Dinámico

Estados Unidos tiene una de las culturas cibernéticas más dinámicas del mundo. En los últimos años, una serie de vulneraciones de ciberseguridad de gran repercusión mediática ha traído al primer plano la cuestión de la sensibilización pública. Distintas iniciativas han fomentado la sensibilización. La Comisión Federal de Comercio (FTC) proporciona a las empresas informes sobre la seguridad de los datos.⁸ El Sistema Nacional de Concienciación Cibernética, que forma parte del Equipo de Respuesta ante Emergencias Cibernéticas, supervisa el entorno de las amenazas y emite alertas oportunas sobre las tendencias.⁹ La Base de Datos Nacional sobre Vulnerabilidades (NVD) ofrece un repositorio mantenido por el gobierno sobre todas las vulnerabilidades conocidas.¹⁰ El protocolo de automatización del contenido de seguridad creado bajo la égida del Instituto Nacional de Normas y Tecnología (NIST) hace operativa la información recopilada en la NVD, estableciendo las configuraciones de los sistemas operativos y las aplicaciones acordes a las normas de seguridad.

El Mes de Concienciación sobre la Ciberseguridad Nacional —creado en 2004 por la Alianza Nacional de Ciberseguridad, un grupo del sector privado y el Departamento de Seguridad Nacional (DHS)— tiene lugar todos los años con el objetivo de promover una cultura de ciberseguridad en el trabajo y el uso seguro de dispositivos conectados a Internet, y de servir de inspiración a los estudiantes para que opten por una carrera en el ámbito de la ciberseguridad.¹¹ A su vez, puso en marcha la campaña *Stop. Think. Connect*¹² a fin de explicar los requisitos de ciberseguridad necesarios.



D2-1 Mentalidad de seguridad cibernética

Estados Unidos tiene una de las culturas cibernéticas más dinámicas del mundo. En los últimos años, una serie de vulneraciones de ciberseguridad de gran repercusión mediática han traído al primer plano la cuestión de la sensibilización pública.

D2-2 Conciencia de seguridad cibernética

El Sistema Nacional de Concienciación Cibernética, creado con el Equipo de Respuesta a Emergencias Cibernéticas, supervisa el entorno de las amenazas y emite alertas oportunas sobre las tendencias.

<https://www.us-cert.gov/ncas>

https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf

La FTC proporciona a las empresas informes sobre la seguridad de los datos.

D2-3 Confianza en el uso de Internet

La confianza en el uso de Internet es alta, a pesar de las numerosas vulneraciones de ciberseguridad de gran repercusión mediática que han afectado a datos corporativos y personales en los últimos años.

D2-4 Privacidad en línea

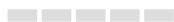
Estados Unidos no tiene una ley global de ciberseguridad; no obstante, diversos estados han aprobado leyes para la protección de los usuarios de Internet.



Educación, formación y competencias en seguridad cibernética

Estratégico

INICIAL



FORMATIVO



ESTABLECIDO



ESTRATÉGICO



DINÁMICO



Estados Unidos ofrece sólidos programas universitarios sobre ciberseguridad, tanto en su vertiente técnica como de políticas. El Departamento de Educación y la Fundación Nacional de Ciencias (NSF) colaboran en la formación de la próxima generación de profesionales del ámbito de la ciberseguridad. El componente de ciberseguridad de los programas de Educación Tecnológica Avanzada (ATE)¹³ ofrecido por la NSF forma técnicos. Los centros de educación tecnológica avanzada comparten su experiencia y recursos para facilitar los programas de seguridad informática en los centros universitarios.¹⁴

La Agencia Nacional de Seguridad (NSA) y el DHS han construido una red de Centros Nacionales de Excelencia Académica en las áreas de defensa cibernética¹⁵ y de operaciones cibernéticas,¹⁶ con universidades de todo el país. Bajo los auspicios de la Iniciativa Nacional para la Educación sobre

Ciberseguridad (NICE), estos programas buscan solventar la escasez de personal con conocimientos de ciberseguridad —ampliando el alcance y mejorando el nivel de las iniciativas de formación— y proporcionar asistencia temprana en el desarrollo de la carrera para atraer a una cantidad mayor de talentos a esta disciplina.¹⁷ Uno de los objetivos de la iniciativa es elevar la proporción de personas de poblaciones insuficientemente representadas con el fin de aumentar la diversidad. Asimismo se han creado diversas becas en materia de ciberseguridad.¹⁸

La iniciativa NICE proporciona herramientas analíticas que ayudan a empresas y organismos a planificar su plantilla¹⁹ mediante la evaluación de sus necesidades de capital humano teniendo en cuenta la capacidad, la madurez y el déficit de conocimiento especializado de la institución.²⁰ El catálogo de la educación y formación de la Iniciativa Nacional de Carreras y Estudios en Ciberseguridad (NICCS) ayuda a los empleados en su desarrollo profesional y actualmente ofrece más de 1.300 cursos.²¹ El Equipo de Respuesta ante Emergencias Cibernéticas en los Sistemas de Control Industrial (ICS-CERT) ofrece oportunidades de formación regulares en su portal virtual de aprendizaje, que está específicamente dirigido al personal de seguridad del ICS.²²

La mayoría de las decisiones sobre el contenido y la estructura de los planes de estudio en Estados Unidos las toman instituciones educativas privadas o se definen a nivel estatal. Por tanto, la política federal tiene un efecto limitado; la estrategia federal para mejorar la posición de la ciberseguridad dentro de los programas educativos ha sido entonces proporcionar un marco informal a través de concursos cibernéticos nacionales²³ y material de formación gratuito. La rama de Educación y Concienciación sobre la Ciberseguridad del DHS ha desarrollado programas de estudio orientados a las disciplinas de ciencia, tecnología, ingeniería y matemáticas para los profesores de enseñanzas medias, que incluyen aspectos de ciberseguridad²⁴ y cuentan con el apoyo del Programa de Asistencia para la Educación y la Formación en Ciberseguridad.²⁵

D3-1 Disponibilidad de educación y formación cibernéticas a nivel nacional

La NSA y el DHS han construido una red de Centros Nacionales de Excelencia Académica en las áreas de defensa cibernética y operaciones cibernéticas con universidades de todo el país. Bajo los auspicios de la NICE, estos programas buscan solventar la escasez de personal con conocimientos de ciberseguridad.

http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf

D3-2 Desarrollo de la educación de seguridad cibernética a nivel nacional

La NICE se ocupa de la educación y el desarrollo de mano de obra para la ciberseguridad.

http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf

A nivel local, se han realizado esfuerzos para integrar la ciberseguridad en los planes de estudios generales, pero no existe una orientación federal.

D3-3 Formación e iniciativas educativas públicas y privadas

La NICE proporciona herramientas analíticas que ayudan a empresas y organismos mediante la evaluación de sus necesidades de capital humano. <https://niccs.us-cert.gov/education/scholarship-opportunities>

El catálogo de la educación y formación de la Iniciativa Nacional de Carreras y Estudios en Ciberseguridad ayuda a los empleados en su desarrollo profesional, y actualmente ofrece más de 1.300 cursos.

El Equipo de Respuesta ante Emergencias Cibernéticas en los Sistemas de Control Industrial (ICS-CERT) ofrece oportunidades de formación regulares en su portal virtual de aprendizaje dirigido específicamente al personal de seguridad del ICS.

D3-4 Gobernanza corporativa, conocimiento y normas

Luego de varios incumplimientos de empresas muy conocidas en los últimos años, el nivel de conciencia sobre los problemas de seguridad cibernética es muy alto entre las empresas estadounidenses. La adhesión a las normas es considerable en el sector financiero y mejora en otros ámbitos. <http://www.ponemon.org/library/2014-a-year-of-mega-breaches>



Marco jurídico y reglamentario

Dinámico

INICIAL



FORMATIVO



ESTABLECIDO



ESTRATÉGICO



DINÁMICO



Estados Unidos no tiene una ley global de ciberseguridad, sino una variedad de regímenes regulatorios y marcos jurídicos, en su mayoría específicos de un sector. La industria financiera ha sido uno de los sectores más activos en esta área, y las directrices elaboradas en los últimos años han estado en manos de la Oficina de Control de la Moneda, la Comisión de Bolsa y Valores (SEC), el Consejo Federal de Vigilancia de las Instituciones Financieras, la Reserva Federal y la Autoridad de Regulación Financiera.²⁶ En 2006, la Reserva Federal publicó la "Circular operativa No. 5: Acceso electrónico", que describe los requisitos de ciberseguridad para las empresas que se conectan a los sistemas de pago de la Reserva Federal.²⁷

De las normas de cumplimiento obligado, la Ley de Secreto Bancario de 1970 exige que las empresas pongan en marcha sistemas de gestión de TI para evitar transacciones ilícitas y notificar a la Red de Control de Delitos Financieros sobre cualquier actividad sospechosa que se conozca o se sospeche.²⁸

La Ley Gramm-Leach-Bliley de 1999 (GLBA) creó requisitos de seguridad de datos personales para el sector financiero. Dicha ley prevé una “regla de salvaguardias”, por la que las empresas financieras deberán elaborar un plan de seguridad de la información para proteger y evitar la divulgación no autorizada de los datos personales de los consumidores.²⁹ En 2003, el Congreso aprobó la Ley de Operaciones de Crédito Justas y Exactas (FACTA), que se centró en normas de seguridad de la información a fin de prevenir robos de identidad mediante el requisito de eliminación de datos en informes y registros de los consumidores a partir de junio de 2005.³⁰

La Ley de Política Energética de 2005 facultó a la Comisión Federal Reguladora de la Energía (FERC) para que supervise la fiabilidad de la red de transporte de energía eléctrica³¹ y para que apruebe normas fiables obligatorias sobre ciberseguridad. La Corporación para la Fiabilidad de la Red Eléctrica Norteamericana (NERC), certificada por la FERC como organización que se ocupa de la fiabilidad de la red eléctrica del país, desarrolló normas de protección de infraestructuras críticas, aprobadas en enero de 2008.³² Al desarrollar una tecnología de redes inteligentes en Estados Unidos, la Ley de Independencia Energética y Seguridad de 2007 (EISA) les otorgó a la FERC y al NIST responsabilidades para coordinar la elaboración de directrices y normas.³³

Las competencias de la FTC incluyen vigilar las prácticas anticompetitivas relacionadas con la seguridad de los datos y la privacidad; a su vez, la FTC ha iniciado acciones legales contra organizaciones que han violado los derechos de privacidad de los consumidores o no han protegido la información sensible de los consumidores. En muchos de estos casos, la FTC ha acusado a los demandados de violar la Sección 5 de la Ley de la FTC, que prohíbe los actos y prácticas desleales y engañosas en el comercio. Además, vela por el cumplimiento de otras leyes federales relativas a la privacidad y la seguridad de los consumidores.³⁴

La Ley de Portabilidad y Responsabilidad del Seguro Sanitario de 1996 (HIPAA) obliga a que se establezcan normas nacionales para las transacciones electrónicas relacionadas con la atención médica, así como identificadores nacionales para los proveedores, los planes de seguro de salud y los empleadores. La HIPAA define políticas, procedimientos y directrices para mantener la privacidad y la seguridad de la información de identificación personal de salud, y describe numerosos delitos relacionados con la atención de la salud, además de establecer sanciones civiles y penales en caso de que no se cumplan tales principios.³⁵

La principal ley federal contra la piratería es la Ley de Fraude y Abuso Informáticos (CFAA) de 1986, que define como delito acceder intencionadamente a una computadora “sin autorización” o “más allá de lo que se ha autorizado”.³⁶ La Ley de Espionaje Económico de 1996 considera como delito el robo o apropiación indebida de un secreto comercial. Hay numerosas otras leyes federales sobre delitos informáticos relacionadas con el fraude en Internet, incluidos el fraude electrónico y el fraude por correo electrónico, el fraude con tarjetas de crédito y el lavado de dinero; la pornografía infantil en línea; la venta por Internet de medicamentos u otras sustancias controladas, armas de fuego, alcohol y juegos de azar; así como la piratería de software y el robo de la propiedad intelectual. Estas leyes han sido reforzadas por órdenes ejecutivas para la protección de infraestructuras críticas, el intercambio de información³⁷ y las sanciones cibernéticas.³⁸ En febrero de 2013, el Presidente Obama firmó la Orden Ejecutiva 13636, con miras a mejorar la ciberseguridad de las infraestructuras críticas, y elevar el nivel de las capacidades básicas para la gestión del riesgo cibernético en el sector de las infraestructuras críticas. La orden se centró en el intercambio de información, la privacidad y la adopción de prácticas de ciberseguridad.³⁹ También encargó al NIST que trabajara con el sector privado para identificar las normas de consenso voluntarias existentes y las mejores prácticas de la industria y las incorporara en un marco de ciberseguridad, que se puso en marcha en febrero de 2014.⁴⁰

Cuarenta y siete estados, el Distrito de Columbia, Guam, Puerto Rico y las Islas Vírgenes han aprobado leyes que obligan a las entidades privadas o gubernamentales a informar a las personas sobre violaciones a la seguridad de la información personal. La mayoría de los estados han promulgado leyes de este tipo desde 2002 en respuesta a un creciente número de violaciones a las bases de datos de consumidores que contenían datos personales. La primera ley de ese tipo —la Ley de Notificación de las Violaciones de la Seguridad de los Datos de California— se promulgó en 2002.⁴¹ En general, la mayoría de las leyes estatales siguen los principios básicos de la ley californiana original: las empresas deben informar inmediatamente a los clientes si se produjera una filtración de información, por lo general por escrito. Desde entonces, California ha ampliado su legislación y ha incluido la información médica y de seguros de salud.⁴²

En octubre de 2011, la SEC publicó una guía sobre las obligaciones de información relativas a los riesgos de ciberseguridad y a los incidentes cibernéticos. La guía señala que, aunque no hay reglas que aborden explícitamente este tema, los incidentes cibernéticos y el riesgo de incidentes de este tipo pueden, sin embargo, engendrar obligaciones de información en virtud de las normas actuales de la SEC, en particular la obligación de revelar información que un “inversor razonable consideraría importante para una decisión de inversión”, que está comprendida en la Ley de Valores de 1933 y en la Ley sobre el Mercado de Valores de 1934.⁴³

D4-1 Marco jurídico de seguridad cibernética

Estados Unidos no tiene una ley global de ciberseguridad, sino diversos regímenes regulatorios y marcos legales. La mayoría son específicos de diversos sectores.

<https://www.fas.org/sgp/crs/natsec/R42114.pdf>

La ciberdelincuencia está condenada en virtud de la Ley de Fraude y Abuso Informáticos (CFAA) de 1986. Hay otras leyes y órdenes ejecutivas que también tienen esa capacidad.

D4-2 Investigación jurídica

Diversos organismos de los Estados Unidos tienen responsabilidades en la investigación judicial de los delitos informáticos, dirigidos por el Departamento de Justicia.

<http://www.justice.gov/usao/priority-areas/cyber-crime>

D4-3 Divulgación de información responsable

En octubre de 2011, la SEC publicó una guía sobre las obligaciones de información relativas a los riesgos de ciberseguridad y a los incidentes cibernéticos.

<http://csis.org/publication/evolution-cybersecurity-requirements-us-financial-industry>

Hasta la fecha, 47 estados han aprobado leyes que obligan a las entidades privadas o gubernamentales a informar a las personas sobre violaciones de seguridad de la información personal.

Normas, organizaciones y tecnologías

Estratégico

La responsabilidad de la ciberseguridad la comparten diversos organismos, cada uno con su propio conjunto de responsabilidades y atribuciones. Los más importantes son el Departamento de Seguridad Nacional (DHS), el Departamento de Justicia y la Oficina Federal de Investigación (FBI), y los Departamentos de Estado y Defensa. El DHS es el principal organismo en materia de ciberseguridad nacional, y su Dirección de Programas y Protección Nacional (NPPD) tiene la responsabilidad operativa. La NPPD se ve obstaculizada tanto por la falta de recursos como de competencia legislativa. La NPPD alberga el Centro de Integración de la Ciberseguridad Nacional y las Comunicaciones (NCCIC), que incluye tanto el US-CERT como el ICS-CERT.⁴⁴ El US-CERT desarrolla mecanismos de detección y prevención para las instituciones federales y también proporciona información sobre el entorno de las amenazas a las organizaciones del sector privado y los asociados internacionales. El ICS-CERT opera a través de alianzas público-privadas con empresas de infraestructura crítica, ofreciendo monitoreo, servicios analíticos y asistencia de respuesta para infraestructuras críticas y organizaciones de recursos clave.

El FBI es el organismo líder en la investigación de los delitos informáticos (el Servicio Secreto, vinculado al DHS, investiga también los delitos informáticos financieros). Tanto el FBI como la Agencia Nacional de Seguridad (que forma parte del Departamento de Defensa) apoyan al DHS en su misión de cuidar de la ciberseguridad nacional. En los últimos años, los Departamentos del Tesoro, Comercio y Energía también han desempeñado un papel activo. La FTC y la Comisión Federal de Comunicaciones, dos organismos independientes, desempeñan un papel importante en la formulación de políticas. El Coordinador de Ciberseguridad de la Casa Blanca —un puesto creado tras la Revisión de la Política Cibernética de 2009— dirige el desarrollo interinstitucional de la estrategia y la política nacional de ciberseguridad, y supervisa a los organismos en la aplicación de dichas políticas.⁴⁵ La novedad más importante es la creación del Marco de Ciberseguridad del NIST, que se creó tras un largo proceso de consulta con el sector privado y reúne las mejores prácticas para la seguridad de la red. El presidente les encargó a los organismos reguladores sectoriales que velaran por la aplicación en sus reglamentaciones de los objetivos de ciberseguridad del Marco del NIST. Por ejemplo, el Departamento de Energía puso en marcha un programa de Modelo de Madurez de Capacidad de Seguridad Cibernética. Hay servicios relacionados con los modelos de madurez de la capacidad de ciberseguridad para organizaciones de todos los tamaños, a fin de que puedan evaluar cómo están aplicando el Marco del NIST.⁴⁶ El sector financiero ha adoptado elementos clave de los marcos de normalización, en particular los del NIST en el Marco de Ciberseguridad de 2013, así como las normas ISO y de la Asociación de Auditoría y Control de los Sistemas de Información (ISACA).

Estados Unidos es un país líder en tecnología y ciberseguridad de la información. La ciberseguridad se ha convertido en una prioridad de inversión tanto para el gobierno como para el sector privado. El pasado año, empresas de capital de riesgo invirtieron más de US\$1.000 millones en *startups* de ciberseguridad. Diecisiete empresas de capital de riesgo de Silicon Valley se centran en el desarrollo de tecnologías innovadoras de ciberseguridad, y el año pasado invirtieron en más de 230 *startups* de ciberseguridad. La Agencia de Proyectos de Investigación Avanzados de Defensa y la Fundación Nacional de Ciencias realizaron también importantes inversiones en I+D en el campo de la ciberseguridad.



D5-1 Adhesión a las normas

La creación del Marco NIST ha dado un impulso a la utilización de normas de ciberseguridad.

<http://www.nist.gov/cyberframework/>

D5-2 Organizaciones de coordinación de seguridad cibernética

El Coordinador de Ciberseguridad de la Casa Blanca —un puesto creado tras la Revisión de la Política Cibernética de 2009— dirige el desarrollo interinstitucional de la estrategia y la política nacional de ciberseguridad, y supervisa la aplicación de dichas políticas por parte de los organismos.

<http://www.dhs.gov/national-cybersecurity-communications-integration-center>

<https://www.whitehouse.gov/blog/author/michael-daniel>

D5-3 Respuesta a incidentes

El Centro de Integración de la Ciberseguridad Nacional y las Comunicaciones (NCCIC) es una división del DHS y alberga tanto al US-CERT como al ICS-CERT.

<https://www.us-cert.gov/>

D5-4 Resiliencia de la infraestructura nacional

El US-CERT completa el análisis de resiliencia cibernética (CRR).

<https://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf>

En 2015, los Planes de Sectores Específicos complementaron el Plan Nacional de Protección de Infraestructuras (NIPP) en el DHS.

<http://www.dhs.gov/critical-infrastructure-security-resilience-month>

D5-5 Protección de la infraestructura crítica nacional

El Plan Nacional de Protección de Infraestructuras (NIPP) de 2013: una Alianza por la Seguridad y la Resiliencia de las Infraestructuras Críticas expone de qué manera trabajan juntos el gobierno y los participantes del sector privado de la comunidad de las infraestructuras críticas con el propósito de gestionar los riesgos y lograr resultados de seguridad y resistencia.

<http://www.dhs.gov/national-infrastructure-protection-plan>

D5-6 Gestión de crisis

Los comandos cibernéticos militares de Estados Unidos y el Equipo de Respuesta ante Emergencias Cibernéticas (US-CERT) se ocupan de las crisis cibernéticas en las fuerzas armadas y el sector de las infraestructuras críticas nacionales, respectivamente.

<https://www.us-cert.gov/>

D5-7 Redundancia digital

El US-CERT se ocupa de cuestiones de redundancia y resiliencia digital. <https://www.us-cert.gov/>

D5-8 Mercado de la ciberseguridad

Estados Unidos cuenta con un gran mercado en crecimiento en términos de tecnología de la seguridad cibernética. Los seguros cibernéticos también están ganando popularidad para poder proteger financieramente a las compañías estadounidenses en caso de incidentes.

Notas

1. "Special Report: Cyber Strategy," consultado el 13 de octubre de 2015 (http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy).
2. <http://fas.org/irp/offdocs/pdd/pdd-63.htm>
3. Cybersecurity Awareness Month and Toolkits, Multi-State Information Sharing & Analysis Center, consultado el 9 de octubre de 2015 (<http://msisac.cisecurity.org/resources/toolkit/>).
4. "The Comprehensive National Cybersecurity Initiative." *The White House*, consultado el 13 de octubre de 2015 (<https://www.whitehouse.gov/node/233086>).
5. *Ibid.*
6. "Cyberspace Policy Review." *The White House*, consultado el 11 de octubre de 2015, <https://www.whitehouse.gov/node/848>.
7. "Launching the U.S. International Strategy for Cyberspace." *Whitehouse.gov*, consultado el 13 de octubre de 2015 (<https://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace>).
8. Seguridad de los Datos, Comisión Federal de Comercio de los Estados Unidos, consultado el 9 de octubre de 2015 (<https://www.ftc.gov/datasetsecurity>).
9. Sistema Nacional de Concienciación Cibernética, US-CERT, consultado el 9 de octubre de 2015 (<http://www.us-cert.gov/ncas>).
10. Base de Datos Nacional sobre Vulnerabilidad, NIST, consultado el 9 de octubre de 2015 (<https://nvd.nist.gov/>).
11. Mes de Concienciación sobre la Ciberseguridad Nacional de 2015, Departamento de Seguridad Nacional de los Estados Unidos, 14 de octubre de 2015 (<http://www.dhs.gov/national-cyber-security-awareness-month>).
12. Campaña *Stop. Think. Connect.*, consultada el 9 de octubre de 2015 (<http://www.stopthinkconnect.org/>).
13. Programa de Educación Tecnológica Avanzada en Tecnologías de la Seguridad, consultado el 9 de octubre de 2015 (<http://www.atecenters.org/security-technologies/>).
14. O'Brien, M. y A. Kellan. 2013. "Community College Cybersecurity Program Trains 21st Century Workforce." Washington, D.C.: Fundación Nacional de Ciencias. 28 de enero (http://www.nsf.gov/news/special_reports/science_nation/cybersecurity.jsp?WT.mc_id=USNSF_51).
15. Centros Nacionales de Excelencia Académica - Defensa Cibernética, Agencia Nacional de Seguridad, 6 de julio de 2015 (<https://www.nsa.gov/academia/ncae-cd/index.shtml>).
16. Centros Nacionales de Excelencia Académica - Ciberoperaciones, Agencia Nacional de Seguridad, 9 de septiembre de 2015 (https://www.nsa.gov/academia/nat_cae_cyber_ops/index.shtml).
17. Véase el "Proyecto de Objetivos Estratégicos", Iniciativa Nacional para la Educación en Ciberseguridad (NICE), 8 de septiembre de 2015 (<http://csrc.nist.gov/nice/index.htm>); el conjunto original de objetivos se puede ver en Iniciativa Nacional para la Educación en Ciberseguridad - Strategic Plan, NICE, septiembre de 2012 (http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf).
18. Becas, Iniciativa Nacional de Carreras y Estudios en Ciberseguridad (NICCS), consultado el 9 de octubre de 2015 (<https://niccs.us-cert.gov/education/scholarship-opportunities>).
19. NICE, "Best Practices for Planning a Cybersecurity Workforce", Libro Blanco, 3 de octubre de 2012 (https://niccs.us-cert.gov/sites/default/files/publications/documents/Best%20Practices%20for%20Planning%20a%20Cybersecurity%20Workforce_05312012_v4.1_DRAFT_NICE%20branded.pdf).

20. NICE, "Cybersecurity Capability Maturity Model", Libro Blanco, 1 de julio de 2013 (https://niccs.us-cert.gov/sites/default/files/documents/files/NICE%20Capability%20Maturity%20Model%20white%20paper_06282013_FINAL_NICE%20branded_0.pdf).
21. "Introduction to the Education and Training Catalog," NICCS, consultado el 9 de octubre de 2015 (<https://niccs.us-cert.gov/training/tc/search>).
22. Portal Virtual de Aprendizaje, ICS-CERT, consultado el 9 de octubre de 2015 (<https://ics-cert-training.inl.gov/lms/>).
23. Concursos cibernéticos, NICCS, consultado el 9 de octubre de 2015 (<https://niccs.us-cert.gov/training/tc/search/cmp/new>).
24. "Desarrollo profesional para maestros", NICCS, consultado el 9 de octubre de 2015 (<https://niccs.us-cert.gov/education/professional-development-teachers>).
25. Programa de Asistencia para la Educación y la Formación en Ciberseguridad No. 97,127, Catálogo de Programas Nacionales de Asistencia Federal, 2011 (<https://www.cfda.gov/index?s=program>).
26. "The Evolution of Cybersecurity Requirements for the U.S. Financial Industry, Center for Strategic and International Studies."10,16]]]]]]], "schema": "https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}]
27. Ibid.10,16]]]]]]], "schema": "https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}]
28. "BSA/AML Examinations," 29 de diciembre de 2010 (<http://www.occ.gov/topics/compliance-ba/bsa/aml-examinations/index-aml-examinations.html>).
29. "Standards for Safeguarding Customer Information (Safeguards Rule) | Federal Trade Commission," consultado el 16 de octubre de 2015 (<https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/standards-safeguarding-customer>).
30. "FACTA Disposal Rule Goes into Effect June 1 | Federal Trade Commission," consultado el 16 de octubre de 2015 (<https://www.ftc.gov/news-events/press-releases/2005/06/facta-disposal-rule-goes-effect-june-1>).
31. "FERC: Electric Reliability: Cyber & Grid Security," consultado el 16 de octubre de 2015 (<http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp>).
32. "Critical Infrastructure Protection Committee (CIPC)," consultado el 16 de octubre de 2015 (<http://www.nerc.com/comm/cipc/pages/default.aspx>).
33. NIST US Department of Commerce, "NIST Identifies Five," consultado el 16 de octubre de 2015 (http://www.nist.gov/public_affairs/releases/smartgrid_100710.cfm).
34. "2014 Privacy and Data Security Update," Comisión Federal de Comercio, consultado el 13 de octubre de 2015 (https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf).
35. "HHS.gov," Text, *HHS.gov*, consultado el 15 de octubre de 2015 (<http://www.hhs.gov/>).
36. "18 U.S. Code Chapter 37 - ESPIONAGE AND CENSORSHIP | US Law | LII / Legal Information Institute," consultado el 15 de octubre de 2015 (<https://www.law.cornell.edu/uscode/text/18/part-I/chapter-37>).
37. "2015 Executive Orders Signed by Barack Obama," consultado el 29 de octubre de 2015 (<https://www.archives.gov/federal-register/executive-orders/2015.html>).
38. "Issuance of an Executive Order Related to Significant Malicious Cyber-Enabled Activities," consultado el 15 de octubre de 2015 (<http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20150401.aspx>).
39. "Foreign Policy Cybersecurity Executive Order 13636," *The White House*, consultado el 16 de octubre de 2015 (<https://www.whitehouse.gov/node/298406>).
40. "Launch of the Cybersecurity Framework | The White House," consultado el 28 de julio de 2014 (<http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework>).
41. "Security Breach Notification Laws," consultado el 13 de octubre de 2015 (<http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>).
42. "California Expands Breach Notification Law to Cover Online Accounts | HL Chronicle of Data Protection," consultado el 15 de octubre de 2015 (<http://www.hldataprotection.com/2013/11/articles/cybersecurity-data-breaches/california-expands-breach-notification-law-to-cover-online-accounts/>).
43. "SEC Issues New Guidance on Disclosing Cybersecurity Risks and Incidents | WilmerHale," consultado el 16 de octubre de 2015 (<https://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=95112>).
44. National Cybersecurity & Communications Integration Center, U.S. Department of Homeland Security, consultado el 19 de septiembre de 2014 (<http://www.dhs.gov/about-national-cybersecurity-communications-integration-center>).
45. "Michael Daniel," *Whitehouse.gov*, consultado el 16 de octubre de 2015 (<https://www.whitehouse.gov/blog/author/michael-daniel>).
46. Programa de Modelo de Madurez de Capacidad de Seguridad Cibernética, Departamento de Energía de los Estados Unidos, consultado el 9 de octubre de 2015 (<http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program>).

Conclusiones

La experiencia de los países analizados nos permite sacar algunas conclusiones generales sobre cómo debería ser una respuesta nacional adecuada a los retos de la ciberseguridad y qué mejores prácticas podrían adoptarse. La ciberseguridad requiere la creación de estrategias, reglas e instituciones que hagan del ciberespacio un lugar más estable y seguro, lo que permitirá aunar crecimiento económico y maximización de los beneficios de las tecnologías de la información.

La primera y fundamental mejor práctica en términos de ciberseguridad es desarrollar una estrategia nacional, ya que tales estrategias proporcionan un marco normativo bajo el cual los países pueden organizar sus iniciativas de ciberseguridad. Su desarrollo también puede proporcionar un mecanismo que permita una amplia coordinación gubernamental transversal. En tres casos, los países ya se encuentran en un segundo ciclo de tales documentos de estrategia u orientación. Para cada uno de los países examinados, las estrategias abordan las medidas necesarias para hacer del ciberespacio una plataforma estable y segura para la actividad económica y reducir los riesgos en cuanto a la seguridad pública y nacional. Al igual que con otras áreas de la ciberseguridad, un objetivo inmediato de una estrategia es elevar desde el nivel técnico al político el debate y la toma de decisiones. El proceso de desarrollo de una estrategia nacional puede ser una contribución útil para ese fin.

La segunda mejor práctica es la creación de una estructura organizativa explícita que asigne responsabilidades entre los ministerios y las oficinas para los diversos aspectos de la ciberseguridad. Las medidas organizativas más básicas, tales como la mejora de la capacidad para aplicar leyes o la creación de un equipo de respuesta ante emergencias cibernéticas (CERT) son un buen comienzo, pero de ninguna manera son suficientes. Los países que cuentan con programas de ciberseguridad más avanzados han creado nuevas organizaciones para asumir esa responsabilidad. En los cuatro países examinados se observan distintos grados de redundancia y la superposición de responsabilidades, algo inevitable y que quizá sea preferible a una estructura institucional inadecuada.

Un aspecto importante de esta mejor práctica organizativa es la creación de algún tipo de autoridad central de coordinación. La ciberseguridad es responsabilidad de muchos organismos y a veces puede darse un solapamiento de atribuciones. Todos los países estudiados crearon nuevas entidades de alto nivel adjuntas a las oficinas del presidente o del primer ministro para supervisar la ciberseguridad. A medida que los esfuerzos de ciberseguridad fueron madurando y ampliando su alcance, los cuatro países crearon un órgano central de coordinación. En todos los casos analizados los órganos de coordinación están vinculados al aparato de toma de decisiones en materia de seguridad nacional, y no a los organismos económicos o de seguridad; aunque ninguno esté a nivel ministerial, su conexión con el jefe del Ejecutivo les confiere alto rango e influencia.

Otra buena práctica es el desarrollo de un marco jurídico adecuado, basado en precedentes tomados de acuerdos internacionales y de la legislación de otros países. Contar con leyes adecuadas para los delitos informáticos, las infraestructuras críticas y la protección de datos resulta crucial para la ciberseguridad.

Si bien cada país tiene un enfoque diferente al trabajar con el sector privado, algo que refleja las diferentes legislaciones y culturas políticas nacionales, los esfuerzos nacionales de colaboración para aumentar la concienciación en la comunidad financiera y empresarial son un elemento central de las prácticas de los cuatro países, al igual que los esfuerzos para aumentar la concienciación pública sobre la forma de gestionar los riesgos de ciberseguridad.

La mayor divergencia entre los países se observa en los marcos jurídicos y reglamentarios. La mayoría aborda la ciberseguridad desde un mosaico de leyes existentes y nuevas autoridades. Teniendo en cuenta las diversas aplicaciones de la ciberseguridad en los distintos ámbitos de la economía, con requisitos y funciones diferentes, este enfoque fragmentado podría resultar conveniente, en lugar de tratar de elaborar una única ley general. Una de las áreas de coincidencia es que la mayoría de los países vieron la necesidad de ampliar la autoridad legal para hacer frente a la ciberdelincuencia.

Cada país ha prestado especial atención a unos pocos sectores de infraestructuras críticas, por lo general las finanzas, la energía eléctrica y los servicios públicos. Esta elección no fue el resultado de un proceso explícito de priorización, sino que, más bien, las infraestructuras clave requieren una buena ciberseguridad.

Todos los países examinados hacen esfuerzos en relación con los problemas de personal. Hay escasez mundial de mano de obra con conocimiento especializado en ciberseguridad, y los cuatro países analizados tienen programas para ampliar su mano de obra en el ámbito cibernético, por lo general en colaboración con las universidades y el sector privado. El ejército y el servicio militar israelíes —que tienen un gran nivel tecnológico— supusieron una ventaja en el desarrollo de esa mano de obra. Todos los países consideraron necesario crear planes de estudio y programas de ciberseguridad especiales, y no limitarse a los cursos tradicionales de informática.

Tres de los países —República de Corea, Estados Unidos e Israel— tienen sectores de TI dinámicos y competitivos que producen bienes y servicios para el mercado mundial. Eso se debe a decisiones deliberadas (tomadas hace décadas en el caso de Estados Unidos) para apoyar al sector de TI con inversiones e incentivos. Es importante destacar que las empresas israelíes y estadounidenses no son empresas nacionales de vanguardia directamente subvencionadas por el gobierno, lo que introduce aspectos emprendedores e innovadores en el comportamiento empresarial. Las empresas se mueven en la dirección del mercado, apoyadas por el gobierno, no al revés.

La cooperación internacional, el fomento de la confianza, el intercambio de mejores prácticas e información y el establecimiento de las bases para un entorno cibernético estable son también elementos comunes en las prácticas de los cuatro países. La cooperación puede abarcar desde actividades entre CERT hasta actividades diplomáticas de alto nivel, pero en todo caso es esencial y otorga a los países acceso a recursos externos técnicos y de información. Cada uno de los cuatro países recurrió a alianzas para fortalecer sus defensas cibernéticas, y Estonia, el más pequeño, fue el más activo a nivel internacional.

Estas breves evaluaciones son una descripción de cómo algunos países líderes en la materia han abordado el problema de la ciberseguridad y de qué forma han evolucionado sus enfoques. Todos comparten el objetivo de la gestión del riesgo cibernético con el propósito de lograr que el ciberespacio no sea más arriesgado que cualquier otra actividad. La manera en que cada país afronte este desafío estará determinada por su historia, su cultura y sus instituciones. En los cuatro países estudiados,

la ciberseguridad es un ámbito donde las políticas y la práctica están en constante evolución. Todos se encuentran en el segundo o tercer ciclo de un enfoque nacional. A medida que los países del mundo experimenten distintas políticas, leyes y estructuras organizativas, la ciberseguridad seguirá siendo un ámbito de políticas dinámico, donde las mejores prácticas seguirán evolucionando, guiadas por la experiencia, los nuevos retos y el desarrollo de una concepción más sofisticada por parte de los responsables políticos. Las experiencias de estos países proporcionan una guía útil para las mejores prácticas de otros países que estén desarrollando sus propias estrategias nacionales de ciberseguridad.

Este documento junto con el Informe Ciberseguridad 2016, “Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?” —elaborado por el Banco Interamericano de Desarrollo y la Organización de los Estados Americanos— constituyen la base para un estudio separado que identifique las diferencias entre la región de América Latina y el Caribe y los cuatro casos reconocidos en el ámbito de la ciberseguridad que se expusieron en este estudio. La investigación puede consultarse en: <https://publications.iadb.org/handle/11319/7449?locale-attribute=es&>.

