# Gobernanza en ciberseguridad: experiencia internacional

**Autor**

Juan Pablo Jarufe Bader
Email: jjarufe@bcn.cl
Tel.: (56) 32 226 3173
(56) 22 270 1850

Nº SUP: 134291

**Resumen**

En el ejemplo colombiano, el Plan Nacional de Protección de Infraestructura Crítica Cibernética, define un marco de gobierno, roles y responsabilidades, además de un conjunto de niveles de alertas, actuaciones, notificaciones y respuestas frente a eventos de ciberseguridad asociados a sectores críticos.

En España, en tanto, existe un Sistema de Protección de Infraestructuras Críticas, que se articula en torno a la conformación del Centro Nacional para la Protección de las Infraestructuras Críticas, orgánica en la cual coexisten y trabajan mancomunadamente actores públicos y privados.

Estados Unidos, a su vez, cuenta con el llamado *National Infrastructure Coordinating Center*, que forma parte de la División de Seguridad e Infraestructura, de la *Cybersecurity and Infrastructure Security Agency*, así como del Centro de Operaciones Nacionales del Departamento de Seguridad Interior, con un funcionamiento permanente y coordinado, que permite compartir información situacional sobre la infraestructura crítica federal.

En cuanto a la institucionalidad estonia, el *Cyber Security Council* es el encargado de aportar a una cooperación más fluida entre diversos organismos públicos del país, al tiempo de velar por el cumplimiento de las metas de la Estrategia de Ciberseguridad.

En cuanto al Reino Unido, el *National Cyber Security Centre* respalda a las organizaciones críticas del Estado, activando protocolos de respuesta inmediata ante ciberincidentes que pudiesen amenazar la continuidad de los activos críticos y las redes del aparato público y de la industria.

En España, el INCIBE-CERT es el centro de respuesta a incidentes de seguridad, cuya acción se enfoca en los ciudadanos y organismos de derecho privado. Un esquema análogo al de Estonia, donde el CERT-EE gestiona los incidentes de ciberseguridad que afectan a las redes nacionales.

Finalmente, en Uruguay, el D-CSIRT es un Equipo de Respuesta a Incidentes de Seguridad Informática de Defensa, cuya tarea es “participar de forma eficaz y eficiente en la respuesta a incidentes cibernéticos sobre infraestructuras críticas y servicios esenciales de la comunidad objetivo, así como desarrollar capacidades de prevención y detección temprana de incidentes”.

## Introducción

El presente informe da cuenta de la gobernanza en ciberseguridad en países como Colombia, España, Estados Unidos (EE.UU.), Estonia, Reino Unido y Uruguay.

El documento recoge información de los siguientes informes: Jarufe, Juan Pablo. (2020, octubre). "Protección de infraestructura crítica en la experiencia internacional". Disponible en: http://bcn.cl/3046i; Jarufe, Juan Pablo. (2020, diciembre). "Políticas de ciberseguridad en la experiencia internacional". Disponible en: http://bcn.cl/3046o; y Jarufe, Juan Pablo. (2019, julio). "Modelos de gobernanza en ciberseguridad: Experiencia internacional". Disponible en: http://bcn.cl/2kr0p.

Se deja constancia de que, en relación con los presupuestos y dotaciones vinculados con la ciberseguridad, solo fue posible obtener información parcial de algunos de los países analizados.

## I. Protección de activos y estructuras críticas

### 1. Colombia

En el ejemplo colombiano, el Plan Nacional de Protección de Infraestructura Critica Cibernética, define un marco de gobierno, roles y responsabilidades, además de un conjunto de niveles de alertas, actuaciones, notificaciones y respuestas frente a eventos de ciberseguridad asociados a sectores críticos, en consonancia con cinco principios básicos en materia de protección y resiliencia a corto, mediano y largo plazo (Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia, 2017: 8).

Esta directriz tiene por norte identificar a los responsables y la definición del esquema de coordinación que permita activar y articular las capacidades estratégicas y operativas de las instituciones del Estado encargadas de preservar la seguridad y defensa de las Infraestructuras Críticas Cibernéticas Nacionales (ICCN), así como de los operadores o propietarios de estas últimas.

El objetivo general de este plan es incrementar el grado de protección de las infraestructuras criticas cibernéticas, mediante la coordinación y articulación de las entidades responsables, a objeto de aminorar el peligro y las vulnerabilidades, junto con optimizar la prevención, alistamiento y respuesta ante el riesgo, robusteciendo la resiliencia y aportando al fortalecimiento del desarrollo económico, la seguridad y la defensa nacional del país en el plano cibernético.

Entre los objetivos específicos, en tanto, se cuentan (Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia, 2017: 9-10):

- El establecimiento de una estructura intersectorial para conducir o coordinar actuaciones necesarias para proteger las infraestructuras críticas cibernéticas, a objeto de movilizar y articular las capacidades logísticas, operativas y técnicas, para la toma de decisiones y respuesta frente a incidentes cibernéticos.

- La identificación y análisis de amenazas, vulnerabilidades, impactos e incidencia de ataques cibernéticos sobre la infraestructura crítica nacional, para determinar los niveles de seguridad y los criterios de activación de acciones de respuesta.

- La fijación de fórmulas para prevenir y reportar incidentes, gestionar crisis, respuestas y recuperación para la protección de la infraestructura crítica cibernética.

- El estímulo a la generación de conocimiento, sustentado en la colaboración intersectorial.

- El mejoramiento de la capacidad de resiliencia cibernética nacional, por medio de la planificación anticipada y el uso de mecanismos de protección, para una pronta recuperación de los servicios esenciales del país.

El Plan es elaborado, gestionado y salvaguardado por el Ministerio de Defensa, mediante el Grupo de Respuesta a Emergencias Cibernéticas, el Comando Conjunto Cibernético y el Centro Cibernético Policial, siendo objeto de revisión cada cuatro años (Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia, 2017: 17).

Colombia también ha procurado proteger sus activos, mediante el reforzamiento de vínculos internacionales, como el que mantiene como Socio Global de la Organización del Tratado del Atlántico Norte (OTAN), que busca avanzar en el desarrollo de capacidades de ciberdefensa y en un marco jurídico que fortalezca esta línea de acción; en la promoción de proyectos de investigación, formación de recurso humano de alto nivel técnico; en la adopción de una doctrina conjunta que integre las capacidades en el ciberespacio, con las que se cuentan en tierra, mar y aire; así como en programas de entrenamiento, en el marco de la cooperación con países aliados (Ministerio de Defensa Nacional de Colombia, 2022a).

Asimismo, el pasado 8 de marzo, el gobierno de este país anunció la conformación de un modelo de gobernanza digital que, de acuerdo al Decreto 338, está dirigido a robustecer la coordinación entre los diversos actores presentes en este ámbito, que pasarían a articularse a partir de cinco niveles, como son los de la Coordinación Nacional de Seguridad Digital, el Comité Nacional de Seguridad Digital, los Grupos de Trabajo de Seguridad Digital, las Mesas de Trabajo Digitales y los Puestos de Mando Unificado de Seguridad Digital.

De igual modo, esta nueva matriz acota el alcance de los Equipos de Respuesta a Incidentes Cibernéticos, distinguiendo entre (“Eje 21”, 2022):

- El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), que haría las veces de punto único de contacto y respuesta nacional ante incidentes de seguridad digital, asesorando y coordinando a las partes interesadas en la materia.

- El Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT Gobierno), constituido como un grupo de reacción anate eventos de seguridad digital en el aparato público, con capacidad para prevenir y gestionar incidentes.

## 2. España

Para hacer frente a los peligros cibernéticos, España cuenta con un Sistema Nacional de Gestión de Situaciones de Crisis (SNGSC), instancia que busca lidiar con los nuevos retos a la seguridad nacional.

A nivel más específico, existe en este país un Sistema de Protección de Infraestructuras Críticas (SPIC), que se articula en torno a la conformación del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), orgánica en la cual coexisten y trabajan mancomunadamente actores públicos y privados, cuya labor

se concentra, a su vez, en la asesoría al Secretario de Estado de Seguridad, así como en la coordinación entre las reparticiones públicas y los gestores de infraestructuras esenciales para el funcionamiento del país.

Junto a lo anterior, el texto legal validó un primer Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC), directiva sancionada el 7 de mayo de 2007, lo mismo que un primer Catálogo Nacional de Infraestructuras Estratégicas y un Acuerdo sobre Protección de Infraestructuras Críticas.

Respecto al SPIC, el artículo 5 de la Ley 8, de 2011, lo conceptualiza como el sistema conformado por "una serie de instituciones, órganos y empresas, procedentes tanto del sector público como privado, con responsabilidades en el correcto andamiaje de los servicios esenciales o en la seguridad de los ciudadanos" (Ley 8, 2011: 2-3).

Entre estos actores, cabe mencionar como primer responsable a la Secretaría de Estado de Seguridad, del Ministerio del Interior, para luego continuar con el CNPIC, los ministerios integrados en el sistema, las comunidades autónomas, las ciudades con estatuto de autonomía, las corporaciones locales, la Comisión Nacional para la Protección de las Infraestructuras Críticas (en adelante, la Comisión), el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, y los propios operadores críticos del sector público y privado.

Ahora bien, en cuanto al CNPIC, el artículo 7 de la citada norma lo define como un órgano ministerial abocado a estimular, coordinar y supervisar las acciones dispuestas por la Secretaría de Estado de Seguridad, en lo atingente al resguardo de las infraestructuras críticas en el territorio nacional.

La propia Secretaría de Estado de Seguridad debe asumir la responsabilidad de mantener actualizado el Catálogo de Infraestructuras Críticas, velando porque este listado contenga todos los datos y el análisis en torno a las infraestructuras estratégicas del país, tal cual lo dispone el artículo 4 de la norma.

Otra institucionalidad propia de este sistema es la antes mencionada Comisión, que en virtud del artículo 11 del texto legal, es considerada un órgano colegiado bajo subordinación de la Secretaría de Estado de Seguridad, con facultades para visar los distintos planes estratégicos sectoriales, a la vez que para nombrar a los operadores críticos del sistema, previa propuesta del Grupo de Trabajo Interdepartamental para la Protección de Infraestructuras Críticas, al que a su vez le compete el diseño de los diferentes planes estratégicos sectoriales (Ley 8, 2011: 2-3).

Ahora bien, la operatoria del sistema aparece desglosada en el artículo 14, que hace referencia a una serie de planes de actuación, entre los que se encuentran el PNPIC, los planes estratégicos sectoriales, los planes de seguridad del operador, los planes de protección específicos y los planes de apoyo operativo.

El primero de esos ejes de acción es elaborado por la Secretaría de Estado de Seguridad, constituyendo el documento estructural para la conducción y coordinación de las diferentes funciones que a cada actor le competen en el sistema en su conjunto, frente a situaciones de amenaza a la infraestructura crítica nacional.

Por su parte, los planes estratégicos sectoriales son aprobados por la Comisión, considerando un conjunto de criterios que definen las medidas a desplegar ante un evento riesgoso; mientras los planes de apoyo operativo son elaborados por la policía estatal, debiendo incluir "las medidas de vigilancia, prevención, protección o reacción a prestar, de forma complementaria a aquellas previstas por los operadores críticos" (Ley 8, 2011: 2-3).

Por último, es dable relevar que el artículo 3 de la norma excluye de su ámbito de aplicación a los reductos bajo dependencia del Ministerio de Defensa, y de las Fuerzas y Cuerpos de Seguridad, los cuales funcionan a partir de sus propios reglamentos.

## 3. EE.UU.

En EE.UU., en tanto, la infraestructura crítica describe a los activos y sistemas físicos de vital importancia para el país, en tanto su destrucción o inhabilitación tendría un impacto sobre la economía, la salud pública o la seguridad de la Nación (*Homeland Security*, 2020).

Al respecto, el país norteamericano ha detectado una serie de áreas críticas, cuales son las del sector químico, las instalaciones comerciales, las comunicaciones, el rubro manufacturero, las represas, la base industrial de la defensa, los servicios de emergencia, la energía, la alimentación y agricultura, las oficinas de gobierno, el sector salud, los reactores nucleares, los materiales de desecho, el sistema de transporte, y los sistemas de agua (*Cybersecurity & Infrastructure Security Agency*, 2020a).

Estos sectores son cautelados por el llamado *National Infrastructure Coordinating Center* (NICC), entidad que forma parte de la División de Seguridad e Infraestructura de la *Cybersecurity and Infrastructure Security Agency* (CISA), así como del Centro de Operaciones Nacionales del Departamento de Seguridad Interior, con un funcionamiento permanente y coordinado, que permite compartir la información situacional sobre la infraestructura crítica del gobierno federal.

En caso de algún incidente contra estos reductos, el NICC se encarga de aglutinar los esfuerzos de colaboración entre el Departamento de Seguridad Interior y los operadores del rubro afectado*(Cybersecurity & Infrastructure Security Agency*, 2020b).

Respecto al ámbito legal, el 16 de noviembre de 2018, el entonces Presidente estadounidense, Donald Trump, firmó la *Cybersecurity and Infrastructure Security Agency Act*, que estableció mecanismos de cooperación público-privada, entregando asistencia técnica y emitiendo análisis a actores federales, así como a propietarios y operadores de infraestructura.

De acuerdo a la sección 2202, el Director de la CISA tiene entre sus responsabilidades (*Cybersecurity and Infrastructure Agency Act*, 2018):

- Liderar los programas de seguridad en materia de infraestructura crítica, considerando actividades de respuesta frente a incidentes asociados a activos de interés nacional.
- Articular estrategias de cooperación con agencias federales, no federales e internacionales.
- Coordinar un esfuerzo nacional para enfrentar las amenazas a la infraestructura crítica.
- Entregar análisis, experiencia y asistencia técnica a los operadores de infraestructura crítica, de manera mancomunada con otras agencias sectoriales de alcance federal.
- Desarrollar, coordinar e implementar planes estratégicos comprehensivos para las actividades de la Agencia, que cuenta con una División de Ciberseguridad, otra de Seguridad de Infraestructura y una tercera de Comunicaciones de Emergencia.

## 4. Estonia

Por su parte, la infraestructura crítica es concebida en Estonia como los sistemas de información y comunicaciones, cuya mantención, confiabilidad y seguridad son esenciales para el apropiado funcionamiento del país (*Republic of Estonia*, 2018).

Al respecto, la Estrategia de Ciberseguridad constituye un documento horizontal, que considera acuerdos y coordinación en este campo, incorporando a diversos actores, tales como las instituciones de gobierno, la

academia, los centros de pensamiento y el sector privado. Esta directriz se enfoca en cuatro objetivos principales, como son (*Cybersecurity Strategy*, 2019-2022: 14-15):

- La construcción de una sociedad digital sostenible, que descanse sobre una resiliencia y preparación frente a las emergencias, en el afán de construir una gobernanza y el desarrollo de una comunidad de ciberseguridad.
- El diseño de una industria de ciberseguridad, investigación y desarrollo competitiva a nivel global, innovadora y confiable.
- La búsqueda de liderazgo en materia de cooperación internacional en el ámbito de la ciberseguridad, mediante la promoción de un espacio sostenible alrededor del mundo.
- El desarrollo de una sociedad ciberalfabetizada, con participación del Estado, los privados y los propios ciudadanos.

Para lo anterior, la Estrategia considera una aproximación basada en riesgos y en el monitoreo permanente de cualquier intrusión en las redes, mediante un manejo interdependiente de activos digitales, considerando también aquellos de carácter transfronterizo.

Asimismo, esta hoja de ruta incluye a la defensa nacional, integrando la ciberseguridad en aquellos documentos de planificación de la seguridad del país; conduciendo ejercicios conjuntos regulares con los proveedores de servicios vitales, autoridades políticas y organizaciones militares; y desarrollando la capacidad del Comando de Ciberfuerzas de la Defensa, con aptitudes para ciberatacar y promover un modelo de ciberconscripción, con la innovación tecnológica como factor clave (*Cybersecurity Strategy*, 2019-2022: 16-18).

A su vez, la Política de Ciberseguridad de este país báltico, busca asegurar la provisión ininterrumpida de servicios y su resiliencia, para lo cual busca resguardar (*Republic of Estonia*, 2018) (*Ministry of Economic Affairs and Communications*, 2020):

- La disponibilidad y funcionamiento seguro de los servicios esenciales.
- La continuidad digital de los procesos gubernamentales.
- La gestión de la interdependencia entre servicios vitales y críticos.
- El aseguramiento de la capacidad para gestionar ciberataques que amenacen al Estado y a las empresas privadas.
- La administración de servicios ofrecidos por países extranjeros, en el caso de servicios críticos.
- La implementación de un sistema de monitoreo, análisis y reporte.
- La gestión de riesgos de seguridad de nuevas soluciones y tecnologías emergentes.

De igual forma, Estonia ha desarrollado la noción de *Critical Information Infrastructure Protection* (CIIP), principio que busca cautelar los sistemas esenciales de información y comunicación, para lo cual recolecta y administra datos, compila informes sectoriales sobre riesgos asociados, intercambia información sobre proveedores de

servicios, desarrolla medidas de seguridad, entrega análisis de riesgos a los proveedores de servicios y eleva los niveles de conciencia en torno a la ciberseguridad entre la población.

En el ámbito normativo, la sección 7 de la *Cybersecurity Act*, dispone que los proveedores de servicios críticos deben aplicar de forma permanente una serie de medidas de seguridad física y de información tecnológica, para prevenir y resolver incidentes cibernéticos, a la vez que para mitigar el impacto en la continuidad de servicios**.**

En tal sentido, el proveedor de servicios tiene que preparar un sistema de análisis de riesgos, que contemple un listado de amenazas a la seguridad de los sistemas críticos, determinando la severidad de las consecuencias de ciberincidentes asociados, monitoreando los sistemas para detectar acciones que comprometan la seguridad y los sistemas de información (*Cybersecurity Act*, 2018).

Frente a cualquier ataque ciberespacial, la Sección 8 de la norma establece que los proveedores de servicios deben notificar a la *Estonian Information System Authority*, en un plazo no mayor a 24 horas, mediante un reporte que considere las posibles causas del incidente, el tiempo de resolución del problema y las medidas aplicadas frente al evento.

Además, conforme a la Sección 11 de la ley, la notificación de un ciberincidente debe sustentarse en los criterios prescritos por el artículo 16 de la Directiva 1148, de 2016, del Parlamento Europeo, de manera que ante un incidente que llegue a tener un impacto significativo sobre la continuidad de un servicio digital en un tercer estado, la *Estonian Information System Authority* dé inmediato aviso al país que ha sido víctima del ataque.

En cuanto a la prevención de ciberataques a la infraestructura crítica, la Sección 12 del texto legal dispone que este último organismo envíe alertas a la población, permitiéndole adoptar medidas para evitar o reducir el impacto de un ciberincidente.

La siguiente Sección, en tanto, considera la existencia de un registro de incidentes ciberespaciales, entendido como una base de datos mantenida por la propia *Estonian Information System Authority*, con el fin de grabar y analizar los ciberincidentes, para luego resolverlos.

De igual forma, la Sección 16 de la ley dispone que la autoridad puede restringir el uso de o el acceso a un sistema, en caso de que el ciberincidente comprometa o dañe la seguridad de otro sistema; o cuando el administrador del mencionado servicio sea incapaz de contrarrestar la amenaza o de eliminar la perturbación originada a partir del incidente (*Cybersecurity Act*, 2018).

## 5. Reino Unido

En cuanto a la infraestructura crítica del Reino Unido, el gobierno la define, en el documento "*Public Summary of Sector Security and Resilience Plans*", de 2018, como (*UK Cabinet Office*, 2018):

*"(...) aquellos elementos tales como instalaciones, sistemas, lugares, propiedades, informaciones, personas, redes y procesos, cuya pérdida o compromiso redundaría en un impacto negativo sobre la disponibilidad, entrega e integridad de los servicios esenciales del país, conduciendo a severas consecuencias económicas o sociales, así como a la pérdida de vidas humanas. Entre estos activos, también cabe incluir algunas funciones específicas, sitios y organizaciones no considerados críticos para el mantenimiento de servicios esenciales, los cuales de todos modos requieren una protección especial, dados los potenciales peligros a los que podrían exponer a la comunidad, en caso de una emergencia de tipo nuclear o química, entre otras".*

En concreto, la infraestructura crítica del país se vincula con sectores como la industria química, energía nuclear, comunicaciones, defensa, servicios de emergencia, energía, finanzas, alimentación, gobierno, salud, espacio, transporte y agua, muchos de los cuales son de propiedad privada.

Varios de estos sectores contemplan, a su vez, subdepartamentos como los de policía, salud y bomberos, en el caso de los servicios de emergencia.

Respecto a la política referida a la infraestructura más sensible del país, la Oficina del Gabinete Presidencial lidera los departamentos gubernamentales responsables de los trece sectores calificados como críticos, en aras de generar los denominados Planes de Resiliencia y Seguridad Sectorial, que describen (*UK Cabinet Office*, 2018):

- Las aproximaciones de cada departamento al manejo de seguridad de infraestructura crítica.
- El análisis de riesgos significativos para cada sector.
- Las actividades implementadas para mitigar riesgos.

El análisis gubernamental de amenazas y riesgos, se basa en un ciclo continuo de lecciones aprendidas, en base a eventos reales, construyéndose en función de la evidencia y la mejora de las fórmulas para calcular los potenciales impactos o consecuencias de las amenazas.

Los posibles riesgos definidos en el informe oficial, incluyen el ataque de terceros estados hostiles; los ciberataques; los actos de terrorismo o crimen organizado; y el espionaje político, militar o comercial.

En relación con el nivel de exposición frente a las amenazas, el texto considera limitada la posibilidad de un ataque terrorista sobre la infraestructura, aunque sí define al sector transporte como un ámbito que enfrenta mayores niveles de vulnerabilidad.

A su vez, existen varios riesgos naturales, como las inundaciones, el cambio climático y las tormentas, que pueden lesionar el funcionamiento diario de la infraestructura del país. Adicionalmente, el reporte menciona el desorden público y la presión social, así como la ausencia del aparato estatal y las pandemias, como factores que pueden llevar a la clausura temporal o a la reducción de servicios (*UK Cabinet Office*, 2018).

Por lo mismo, el objetivo central del gobierno apunta a reducir la vulnerabilidad, construyendo una capacidad de infraestructura resistente, que pueda recuperarse rápidamente tras posibles ataques.

Finalmente, la directriz sindica como responsables de la seguridad de los sectores críticos del país, a los propios propietarios y operadores de la infraestructura en cuestión, los legisladores, los servicios de emergencia, así como al gobierno local y central.

En el primer caso, el deber apunta a mantener la operación de las instalaciones en el día a día, efectuando un análisis de riesgos a nivel de activos; y tomando decisiones sobre mantenimiento, capacitación e inversión, a fin de mejorar la seguridad organizacional y la resiliencia de cada sector.

Respecto a las autoridades locales y los servicios de emergencia, la *Civil Contingencies Act*, de 2004, les delega la función de identificar y analizar la probabilidad de impacto de potenciales emergencias que podrían afectar a la sociedad en sus áreas de jurisdicción, así como el deber de desarrollar planes de respuesta ante emergencias.

En cuanto a las agencias de gobierno, finalmente, estas proveen asesoría a los actores ya mencionados, como por ejemplo en el caso del *Centre for the Protection of National Infrastructure*, que entrega apoyo en seguridad a

organizaciones y empresas vinculadas a la infraestructura crítica del país, en el afán de reducir riesgos y vulnerabilidades frente al terrorismo, espionaje y otras amenazas (*UK Cabinet Office*, 2018).

### 6. Uruguay

En el paradigma uruguayo, el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) fue creado en 2008, a partir de la publicación de la Ley 18.362, con el objetivo de proteger los activos de información críticos del Estado y promover el conocimiento en seguridad de la información, de manera de prevenir y responder a los incidentes de seguridad.

El CERTuy está conformado por un grupo de expertos responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

Sus principales objetivos son (Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento, 2022a):

- Centralizar, coordinar y optimizar los procesos de respuesta a incidentes en seguridad de la información.
- Realizar tareas preventivas.
- Difundir mejores prácticas en seguridad de la información.

El primer objetivo es abordado por el *Computer Emergency Response Team / Coordination Center*, un equipo de respuesta y un centro de coordinación de emergencias informáticas que actúa cuando ocurre un incidente informático, como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información del organismo.

Por su parte, el Centro de Operaciones de Ciberseguridad tiene la función de detectar en tiempo real eventos e incidentes de ciberseguridad en los Activos de Información Críticos del Estado, así como colectar y analizar información de ciberseguridad, para prevenir y detectar incidentes de ciberseguridad.

## II. Dependencia dentro de la estructura del Estado

### 1. Colombia

Colombia cuenta con diversos organismos públicos nacionales, que velan por generar un marco legal adecuado, para garantizar la progresiva incorporación de la ciberseguridad industrial en las estructuras de las empresas con presencia nacional (principalmente infraestructuras críticas). Entre ellos, cabe destacar (Centro de Ciberseguridad Industrial, 2022a):

- ColCERT.
- Comando Conjunto Cibernético.

- Centro Cibernético Policial.
- Ministerio de Tecnologías de la Información y las Comunicaciones (MINTICS).
- Ministerio de Defensa Nacional.

Este país ha buscado consolidar una visión rectora en materia de ciberseguridad, a partir del documento "CONPES 3701", que esboza los lineamientos de política nacional en este ámbito.

Al respecto, esta fuente define la ciberseguridad como "la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética" (MINTICS, 2014: 4-5).

El texto establece un conjunto de vectores de desarrollo, compuestos a su vez por líneas temáticas, que tienen por norte robustecer la posición del país en el plano de la ciberseguridad, mediante un enfoque colaborativo entre los actores estatales y privados, considerando igualmente la participación de la academia y el sector empresarial.

Lo anterior, en aras de generar proyectos innovadores de política pública, dirigidos a consolidar la posición del país en cuanto a gestión de seguridad de la información, salvaguarda de la infraestructura crítica, aseguramiento de sistemas, y definición de rangos mínimos de control de riesgos y amenazas cibernéticas contra la soberanía nacional y los principios constitucionales del Estado.

Entre los vectores incorporados, se pueden mencionar los delitos cibernéticos, como factor decisivo de las políticas y normas que pretenden cohesionar al país en su propósito de reconocer estos actos en los procesos jurídicos, constitucionales y penales; la generación de directrices que cautelen la reserva e integridad de la información más sensible del Estado colombiano, mediante la implementación de esquemas tecnológicos; y el estímulo a directivas que avancen en el establecimiento de alianzas y acuerdos de cooperación internacional en el combate a las ciberamenazas y el fortalecimiento de la defensa nacional en el ciberespacio.

Este esquema tiene por finalidad instaurar procesos de innovación, dirigidos a la integración de datos vinculados con las incidencias cibernéticas que se produzcan a lo largo del país, estimulando la interoperabilidad y el intercambio de información.

Asimismo, esta estrategia apunta a satisfacer una serie de requerimientos temáticos, entre los que cabe mencionar (MINTICS, 2014: 10-11):

- La estructuración, diseño, desarrollo e implementación de modelos de medición de riesgos, amenazas y vulnerabilidades presentes en los sistemas oficiales de información, permitiendo una mejor toma de decisiones en materia de prevención, protección y detección temprana de incidentes.
- El armado y puesta en vigor de modelos para la gestión federada de incidentes, dirigidos al desarrollo de sistemas integrados para el monitoreo, detección, prevención, información, respuesta y alerta temprana ante problemas de naturaleza cibernética.
- La disposición de controles operativos para el empleo de activos críticos y medios tecnológicos del Estado, a fin de reducir vulnerabilidades asociadas al transporte, procesamiento y almacenamiento de datos de alta sensibilidad.

- La definición, coordinación, entrenamiento e implementación de centros y equipos de respuesta de alcance nacional, regional y local, para hacer frente a incidentes cibernéticos.

Por otra parte, la Política Nacional de Seguridad Digital busca que el gobierno, las entidades públicas y privadas, los centros de estudios, y la sociedad civil, utilicen responsablemente un entorno digital abierto, seguro y confiable, mediante el robustecimiento de sus capacidades para reconocer, administrar y aminorar los riesgos vinculados a a las actividades digitales (CONPES, 2016: 11-13).

De igual modo, el gobierno colombiano ha apuntado hacia el fortalecimiento de las capacidades administrativas y operativas del Comando Conjunto Cibernético, las unidades cibernéticas de las Fuerzas Militares y los órganos de inteligencia del Estado.

De forma adicional, la Política ha avanzado en una actualización del catálogo de infraestructura crítica nacional y en la estructuración de guías de riesgo operacional para optimizar la resiliencia de estas instalaciones.

Además, el gobierno ha procurado implementar una agenda estratégica de cooperación y asistencia nacional e internacional en materia digital, revisando el marco jurídico vigente, a fin de poner en marcha un esquema de diplomacia digital en el país.

Por último, la autoridad ha buscado generar redes internacionales de intercambio de información en el plano de la seguridad digital (CONPES, 2016: 72-75).

## 2. España

La estructura de la ciberseguridad en el marco del Sistema de Seguridad Nacional español, está constituida por los siguientes componentes (Estrategia Nacional de Ciberseguridad de España, 2019: 61-64):

- El Consejo de Seguridad Nacional: es el órgano al que corresponde asistir al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional. Actúa, a través del Departamento de Seguridad Nacional, como punto de contacto único para ejercer una función de enlace y garantizar la cooperación transfronteriza con otros países de la Unión Europea.

- El Comité de Situación: tiene carácter único para el conjunto del Sistema de Seguridad Nacional y actuará, apoyado por el Departamento de Seguridad Nacional, de acuerdo con las directrices político-estratégicas dictadas por el Consejo de Seguridad Nacional en materia de gestión de crisis.

- El Consejo Nacional de Ciberseguridad: da apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad. Entre sus funciones, se encuentra el reforzamiento de las relaciones de coordinación, colaboración y cooperación entre las distintas administraciones públicas con competencias en materia de ciberseguridad, así como entre los sectores público y privado, en pos de facilitar la toma de decisiones del propio Consejo, mediante el análisis, estudio y propuesta de iniciativas, tanto en el ámbito nacional como internacional. De igual modo, puede valorar los riesgos y amenazas, analizar los posibles escenarios de crisis, estudiar su posible evolución, elaborar y mantener actualizados los planes de respuesta, y formular directrices para la realización de ejercicios de gestión de crisis en el ámbito de la ciberseguridad, evaluando los resultados de su ejecución, todo ello en coordinación con los órganos y autoridades directamente competentes.

- La Comisión Permanente de Ciberseguridad: se establece con objeto de facilitar la coordinación interministerial a nivel operacional, en el ámbito de la ciberseguridad. Presidida por el Departamento de Seguridad Nacional, se compone de aquellos órganos y organismos representados en el Consejo Nacional de Ciberseguridad con responsabilidades operativas. Es el órgano al que corresponde asistir al Consejo Nacional de Ciberseguridad sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad. El funcionamiento de la Comisión se enmarca en el procedimiento de gestión de crisis de ciberseguridad, que busca detectar y valorar los riesgos y amenazas, facilitar el proceso de toma de decisiones, y asegurar una respuesta óptima y coordinada de los recursos del Estado. Además, incluye los diferentes niveles de activación del Sistema de Seguridad Nacional, junto a instrucciones para la gestión de la comunicación pública.

- El Foro Nacional de Ciberseguridad: actuará en la potenciación y creación de sinergias público-privadas, particularmente en la generación de conocimiento sobre las oportunidades, desafíos y amenazas a la seguridad en el ciberespacio. La puesta en marcha de esta instancia y la armonización de su funcionamiento con los órganos existentes, se realiza mediante la aprobación de las disposiciones normativas necesarias, con el objetivo de alcanzar el funcionamiento coordinado y eficiente de estos componentes en el Sistema de Seguridad Nacional.

El marco estratégico e institucional de la ciberseguridad se complementa con las autoridades públicas competentes en materia de seguridad de las redes y sistemas de información, así como con los CSIRT de referencia nacional que aparecen recogidos en el marco jurídico nacional.

Asimismo, los CSIRT de las comunidades autónomas, de las ciudades autónomas, de las entidades locales y sus organismos vinculados o dependientes, los de los organismos privados, la red de CSIRT.es y otros servicios de ciberseguridad relevantes, deben estar coordinados con los anteriores, en función de las competencias de cada cual (Estrategia Nacional de Ciberseguridad, 2019: 61-64).

Por otra parte, la gobernanza en ciberseguridad de este país contempla la existencia del Instituto Nacional de Ciberseguridad de España (INCIBE), conocido hasta 2014 como Instituto Nacional de Tecnologías de la Comunicación. Se trata de una entidad subordinada al Ministerio de Economía y Empresa, que tiene a su cargo el desarrollo de la ciberseguridad, tanto en lo que respecta a la situación de la sociedad civil, la academia y las compañías privadas, como a la realidad de los sectores estratégicos.

Al respecto, este organismo sustenta su trabajo en la investigación y coordinación con actores competentes en la materia, tanto a nivel nacional como internacional.

En esta línea, se trata de un ente oficial para el desarrollo de la ciberseguridad, “como motor de transformación social y oportunidad para la innovación” (INCIBE, 2019a), que cuenta con un centro de respuesta a incidentes de seguridad, tanto en el caso de ciudadanos comunes como de empresas.

En cuanto a la situación de eventos que afecten a operadores críticos del sector privado, esta última unidad es manejada en conjunto por el INCIBE y el CNPIC, respectivamente.

Así, este módulo se transforma en uno de los equipos de respuesta que trabaja en mancomunión con otros agentes de alcance nacional e internacional, en el ánimo de optimizar la eficacia en el combate a los delitos informáticos de connotación pública.

En tal sentido, el objetivo del INCIBE es reforzar la protección de datos, así como la privacidad de los servicios prestados por medios digitales, en base a cuatro principios básicos, a saber (INCIBE, 2019a):

- La promoción de servicios de ciberseguridad, que posibiliten un aprovechamiento de las tecnologías de información y un incremento de la confianza digital. Esto último, a través de fórmulas de prevención y reacción frente a incidentes informáticos, a la vez que por medio del estímulo a una cultura de la seguridad de la información, mediante campañas de sensibilización.

- La promoción de iniciativas innovadoras, que cuenten con la capacidad para producir inteligencia en ciberseguridad.

- La generación de talento e investigación avanzada en el ámbito de la ciberseguridad, de modo de propiciar un mercado de productos de referencia internacional.

- La participación en redes nacionales e internacionales de colaboración, que contribuyan a "facilitar la inmediatez, globalidad y efectividad a la hora de desplegar una actuación en el ámbito de la ciberseguridad" (INCIBE, 2019b).

### 3. Estonia

En cuanto a la institucionalidad estonia, el *Cyber Security Council*, creado en 2009 y presidido por el Secretario General del Ministerio de Asuntos Económicos y Comunicaciones, es el encargado de aportar a una cooperación más fluida entre diversos organismos públicos del país, al tiempo de velar por el cumplimiento de las metas de la Estrategia de Ciberseguridad.

A su vez, la *Information System Authority* es la entidad subordinada al Ministerio de Asuntos Económicos y Comunicaciones, que organiza los niveles nacionales de protección para las redes y sistemas informáticos de los sectores público y privado, que resulten esenciales para el funcionamiento del Estado (*Republic of Estonia*, 2018).

Por su parte, un tercer actor relevante es el Cibercomando, órgano asesor del Ministerio de Defensa, que se encarga de conducir las operaciones ciberespaciales. Sus principales misiones específicas son (*Defence Forces*, 2022):

- Proveer información e infraestructura tecnológica en materia de comunicaciones y servicios.
- Planificar y ejecutar operaciones de ciberdefensa.
- Obtener, mantener y compartir análisis situacionales sobre el ciberespacio.
- Planificar y ejecutar misiones de información y comunicación estratégica.
- Entrenar, preparar y movilizar a las unidades para tiempos de guerra y reserva.

### 4. EE.UU.

En EE.UU., la CISA es el órgano de alcance federal que lidera el trabajo estratégico para fortalecer la seguridad, resiliencia y fuerza de trabajo en el ecosistema ciberespacial, con el fin de proteger los servicios críticos del Estado.

Establecida en 2018, esta agencia actúa como coordinadora nacional para la seguridad y resiliencia de la infraestructura crítica del Estado, administrando y reduciendo los riesgos ciberespaciales, conectando los operadores de sistemas con la industria, la academia, el gobierno y actores internacionales, a la vez que aglutinando los recursos, análisis y herramientas que ayuden a una mayor resiliencia y seguridad física en este ambiente.

Esta instancia opera mancomunadamente con la *Office of Management and Budget*, que es la responsable de la ciberseguridad federal en su conjunto.

También lidera las respuestas ante ciberincidentes y asegura que la información sea oportuna y compartida por todos los actores federales y no federales, así como por el sector privado (CISA, 2022a).

## 5. Reino Unido

En cuanto al Reino Unido, el *National Cyber Security Centre* (NCSC) respalda a las organizaciones críticas del Estado, activando protocolos de respuesta inmediata ante ciberincidentes que pudiesen amenazar la continuidad de los activos críticos y las redes del aparato público y de la industria.

Nacido en 2016, este organismo con sede en Londres, se nutre de la experiencia de entidades como la *National Technical Authority for Information Assurance* (CESG), el *Centre for Cyber Assessment*, el CERT-UK y el *Centre for Protection of National Infrastructure*.

En esta línea, el NCSC ofrece un solo punto de contacto para organizaciones de gran tamaño, agencias de gobierno, terceros estados y público en general (NCSC, 2022a).

## 6. Uruguay

En Uruguay, la política digital nace a partir de la “Agenda Uruguay Digital”, hoja de ruta que fija, prioriza, articula y transmite los programas de desarrollo de la sociedad de la información y el conocimiento en el sector público, mediante una visión de alcance nacional, fórmulas de seguimiento y sustentabilidad.

Esta directriz se hace operativa mediante dos grandes planes de acción, como son (Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento, 2020a):

- Plan de Gobierno Digital, que puntualiza el destino de los proyectos prioritarios de transformación digital del gobierno uruguayo, por medio de las oportunidades que entrega el empleo de las tecnologías, en un enfoque integrado entre el Estado, la ciudadanía, la industria y la academia.

- Plan de Acción de Gobierno Abierto, que tiene como fin robustecer la democracia y el Estado de Derecho, a partir de la inclusión de un saber colectivo, sustentado en principios como la transparencia, la participación ciudadana y el *accountability*.

Este esquema adquiere entidad gracias a la labor de la Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento (AGESIC), entidad con autonomía técnica, creada en virtud de la Ley 17.930, de diciembre de 2005, que se encuentra subordinada a la Presidencia del país.

El funcionamiento de este organismo aparece regulado en el artículo 2 del Decreto 205, de junio de 2006, que fija entre sus objetivos generales (Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento, 2020b):

*"(…) la mejora de los servicios al ciudadano, utilizando las posibilidades que brindan las tecnologías de la información y las comunicaciones, así como el impulso al desarrollo de la sociedad de la información en el país, con énfasis en la inclusión de la práctica digital de sus habitantes y el fortalecimiento de las habilidades de la sociedad en la utilización de las tecnologías"*.

Asimismo, el artículo 55 de la Ley 18.046, de Rendición de Cuentas, de octubre de 2006, añade como nuevas metas la planificación y coordinación de iniciativas vinculadas con el gobierno electrónico, como sustento para una mayor transparencia de los procesos estatales, y para una mejor prevención y respuesta ante incidentes que pudiesen lesionar los activos más sensibles del país.

A nivel específico, en tanto, el Decreto 184, de 14 de julio de 2015, faculta a la AGESIC para (Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento, 2020c):

- Esbozar los programas y la Estrategia Nacional de Desarrollo de Gobierno Electrónico y Gobierno Abierto.
- Sugerir medidas a los órganos estatales y no estatales, al momento de diseñar planes de gobierno electrónico.
- Normar la implementación de acciones relacionadas con la puesta en marcha de proyectos particulares de gobierno electrónico, por medio de la articulación de fórmulas tales como fondos concursables y planes directores de gobierno electrónico.
- Elaborar las directrices y la estrategia nacional de gobernanza, integración, interoperabilidad, capital humano y compras relativas a las tecnologías de la información en organismos públicos.
- Formular reglas técnicas para servicios atingentes a las tecnologías de la información en entes públicos, al tiempo de efectuar auditorías, seguimientos y análisis.
- Desarrollar planes específicos para la realización de trámites y servicios en línea, en aras de avanzar hacia una gestión pública moderna, eficaz y eficiente.
- Estimular la vinculación entre la ciudadanía y el Estado, mediante un mejor acceso a la tecnología y una política de inclusión digital.
- Fijar metodologías y consagrar buenas prácticas en la seguridad de la información.
- Entablar relaciones con sus pares de otros estados, así como con organismos nacionales e internacionales, tanto públicos como privados.

En la misma línea, el artículo 149 de la Ley 18.719, de 5 de enero de 2011, encomienda a la AGESIC la dirección de las políticas, metodologías y mejores prácticas en materia de ciberseguridad a nivel nacional, así como la fiscalización de las medidas de implementación de estas directrices en las entidades públicas y privadas que se vinculan con los sectores críticos del país, que se efectúan a través de la Dirección de Seguridad de la Información, que alberga al Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy).

Finalmente, el artículo 119 de esta norma crea el Consejo Asesor Honorario de Seguridad de la Información, conformado por el Director de Seguridad de la Información de la AGESIC, un miembro académico y un representante de la Presidencia de la República, el Ministerio de Defensa Nacional, el Ministerio del Interior, el Ministerio de Industria, Energía y Minería, el Banco Central del Uruguay y la Unidad Reguladora de Servicios de Comunicaciones (URSEC) (Presupuesto Nacional 2020-2024, s/i: 35-36).

## III. Información presupuestaria

Respecto al presupuesto asociado a ciberseguridad en Colombia, los proyectos de inversión para 2022, del MINTICS, consideran un monto de 66.051.109.695 pesos colombianos (US$16.237.111) para el ítem "Aprovechamiento y uso de las tecnologías de la información en el sector público nacional".

Además, se destinaron 38.204.449.595 pesos colombianos (US$9.562.161) para el ítem "Servicio de asistencia, capacitación y apoyo para el uso y apropiación de las TIC, con enfoque diferencial y en beneficio de la comunidad para participar en la economía digital nacional" (MINTICS, 2021).

En España, a su vez, el actual gobierno anunció la presentación de un Plan de Ciberseguridad Nacional, con un presupuesto asignado de más de 1.200 millones de Euros, que iría de la mano con la conformación de un Centro de Operaciones de Ciberseguridad de la Administración General del Estado y de sus organismos públicos ("El Español", 2022).

Por su parte, para el año fiscal 2022, el Ejecutivo estadounidense propuso un gasto de US$58.400 millones para las tecnologías de la información, monto destinado a garantizar la seguridad de los sistemas críticos y el resguardo de la información sensible, en el contexto de un gobierno digital.

El presupuesto también apoya la implementación de leyes federales para permitir a las agencias una planificación tecnológica, supervisión y *accountability*, posibilitando una migración segura a "*cloud-solutions*" y servicios compartidos.

Asimismo, los fondos oficiales incluyen unos US$9.800 millones para el ámbito ciudadano, con inversiones para proteger los activos de información del país y estimular la coordinación interagencial (*White House*, s/i: 1, 4).

Por último, la inversión en ciberseguridad en el Reino Unido, fue estimada en 2020 en unos 8.878 millones de libras esterlinas (US$11.213.269.120) (*UK Government*, 2021: 29).

## IV. Dotaciones promedio

Respecto a la cantidad de personal especialista en ciberseguridad, se estima que en Reino Unido, durante 2021, trabajaron en el rubro unas 46.683 personas, insertas en 1.483 firmas, lo cual marca un incremento del 9% en relación al año 2020.

Mientras el 65% de estas personas trabajó en grandes empresas, el tamaño promedio de los equipos de ciberseguridad se redujo ligeramente, con caídas desde las 227 a las 211 personas en las grandes compañías; de las 57 a las 52, en empresas de tamaño medio; y de 18 a 15, en las pequeñas firmas (*UK Government*, 2021: 32-33).

En Uruguay, en tanto, las cifras de 2020 indicaron que un 56% de las empresas contaba con hasta cinco profesionales del área, un 19% registraba hasta diez especialistas, otro tanto exhibía hasta quince expertos, mientras el 6% anotaba más de quince (Presidencia de Uruguay, 2020).

## V. Estructura de los CSIRT nacionales

### 1. Colombia

En el paradigma colombiano, el CSIRT del sector Gobierno busca efectuar una adecuada gestión y reaccionar ante los incidentes cibernéticos de forma centralizada, realizando seguimientos a las principales tipologías de ciberincidentes que lesionan los activos gubernamentales, a la vez que generando alertas y advertencias sobre riesgos y vulnerabilidades, que conduzcan hacia la construcción de una cultura de seguridad digital.

En este sentido, esta entidad apoya a las agencias públicas a "optimizar sus procesos de seguridad de la infraestructura tecnológica, proceder ante incidentes cibernéticos y generar conciencia en seguridad digital".

Los servicios ofrecidos por el CSIRT colombiano son tanto proactivos como reactivos. Entre los primeros, cabe mencionar la generación de alertas y advertencias, que posibiliten ajustes a la infraestructura tecnológica ante los riesgos; un análisis de vulnerabilidades *web*, con acciones de mitigación y prevención; y un monitoreo de eventos de seguridad, basado en la infraestructura de las tecnologías de la información.

Los servicios reactivos, en tanto, incluyen la gestión de incidentes a todo nivel, vale decir, en las etapas de detección, evaluación, análisis, notificación, contención, erradicación y recuperación; y el análisis de *malware* (Gobierno Digital de Colombia, 2022).

También existe un Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional (CSIRT-PONAL), grupo conformado para hacer frente a las necesidades de prevención, atención e investigación de incidentes informáticos, a objeto de cautelar la infraestructura tecnológica y los activos de información de la Policía Nacional, como respaldo a la Estrategia de Ciberseguridad y Ciberdefensa de la Nación.

Esta instancia igualmente establece alianzas estratégicas con entidades nacionales e internacionales, tanto del ámbito público como privado, a fin de potenciar la asistencia recíproca en materia de seguridad de la información (Ministerio de Defensa Nacional de Colombia, 2022b).

### 2. España

En España, el INCIBE-CERT es el centro de respuesta a incidentes de seguridad, cuya acción se enfoca en los ciudadanos y los organismos de derecho privado.

Se trata de un ente subordinado a la Secretaría de Estado de Digitalización e Inteligencia Artificial, y operado en conjunto con INCIBE y la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior.

Este organismo actúa en coordinación con el resto de los equipos nacionales e internacionales, en pos de mejorar los resultados en el combate a los delitos que involucran redes de información (INCIBE-CERT, 2022a).

En suma, el INCIBE-CERT tiene atribuciones para (INCIBE-CERT, 2022b):

- Entregar soporte técnico para resolver incidentes de ciberseguridad.
- Utilizar técnicas de detección temprana de incidentes, notificando a los afectados.
- Mantener el contacto con los proveedores de *Internet* y otros CERT nacionales e internacionales.

### 3. EE.UU.

El *CISA Incident Reporting System* provee los medios informáticos para reportar incidentes de ciberseguridad a la CISA.

El sistema cuenta con analistas que entregan información en tiempo real de los ciberincidentes, teniendo la capacidad de conducir análisis caso a caso (CISA, 2022b).

## 4. Estonia

El CERT-EE es una organización establecida en 2006, que gestiona los incidentes de ciberseguridad que afectan a las redes del país, o que son notificados por ciudadanos e instituciones locales o extranjeras.

Entre sus competencias, esta unidad se encarga de (*Information System Authority*, 2021):

- Compartir información y entregar notificaciones acerca de riesgos y brechas de seguridad, o de eventos que puedan alterar la confidencialidad, integridad y procesabilidad de los sistemas de información.
- Ayudar a las instituciones públicas y privadas a responder ante ciberincidentes, otorgándoles también apoyo legal, en caso de ser necesaria una investigación.
- Impulsar campañas periódicas en los medios de comunicación, respecto a la importancia de tomar conciencia acerca de la seguridad informática.

Esta organización proriza los ciberincidentes según su potencial severidad y ámbito, teniendo en cuenta factores como el número de usuarios afectados, el tipo de incidente, el blanco de un ataque, el origen del mismo y los recursos requeridos para manejar el incidente. Así, por ejemplo, los ciberataques graves son aquellos que amenazan la vida de las personas o dañan la infraestructura crítica del país.

## 5. Reino Unido

En la experiencia británica, en tanto, el *Cybersecurity Incident Response Team* se ocupa de minimizar el impacto de los ciberataques, a partir de un rápido despliegue de expertos en ciberseguridad; de investigar la respuesta a ciberincidentes, dirigir investigaciones forenses, implementar medidas para incrementar los niveles de ciberseguridad del sector afectado, emitir un informe final sobre el ciberincidente, con hallazgos y recomendaciones; y elaborar un Análisis de Preparación ante Incidentes, entre otros.

A partir de este enfoque, el organismo busca reducir los ciber-riesgos organizacionales; minimizar la disrupción de incidentes ciberespaciales; analizar las causas de origen y la efectividad de la respuesta; entregar análisis técnico, contención y recuperación post-incidente; y reducir el impacto y los tiempos de respuesta ante ciberincidentes (Gov.uk, 2022).

## 6. Uruguay

Respecto a Uruguay, el D-CSIRT es un Equipo de Respuesta a Incidentes de Seguridad Informática de Defensa, creado por el Decreto 36, de 27 de enero de 2015, cuya tarea es “participar de forma eficaz y eficiente en la

respuesta a incidentes cibernéticos sobre infraestructuras críticas y servicios esenciales de la comunidad objetivo, así como desarrollar capacidades de prevención y detección temprana de incidentes de seguridad informática" (Centro Nacional de Respuesta a Incidentes de Seguridad Informática, 2022).

Los objetivos generales de esta instancia, son hacer las veces de punto de contacto para su comunidad, ante la ocurrencia de incidentes cibernéticos; ser enlace del Ministerio de Defensa, en la respuesta a incidentes informáticos internos y externos; concientizar y capacitar a la comunidad nacional en materia de ciberseguridad; impulsar investigaciones en el ámbito de la seguridad informática; y colaborar activamente con el CERTuy.

A su vez, entre sus objetivos específicos, se encuentran (Ministerio de Defensa Nacional de Uruguay, 2022):

- La coordinación de respuestas ante ciberincidentes, con la emisión de alertas y avisos.
- La implementción de una Política de Gestión de Riesgos de Activos de Información, así como de una metodología para detectar amenazas, en coordinación con las directrices establecidas por el CERTuy.
- La identificación, planificación y coordinación de actividades de protección de activos críticos.

## VI. Vínculos con la academia y el mundo privado

### 1. Colombia

En Colombia, el Centro de Ciberseguridad Industrial conforma el principal ecosistema de organizaciones industriales, proveedores de servicios y soluciones de ciberseguridad industrial, del ámbito público o privado, teniendo por norte el impulso a un mejor ambiente ciberespacial, desde una perspectiva de personas, procesos y tecnologías (Centro de Ciberseguridad Industrial, 2022b).

A su vez, el Ministerio de Tecnologías de la Información y las Comunicaciones dio a conocer recientemente el Proyecto de Decreto que crea un modelo de gobernanza dirigido a la seguridad digital y cibernética, el cual enfatiza en la necesidad de mayores capacidades de análisis, prevención y respuesta entre el sector público y privado.

Esta iniciativa tiene como fin establecer un esquema de coordinación y fortalecimiento de capacidades de los actores involucrados en la seguridad digital, a fin de establecer respuestas más oportunas y poder resguardar los activos del entorno digital del país.

En esta línea, el Ministerio de Defensa sería responsable de diseñar un catastro de la infraestructura cibernética nacional y de los servicios esenciales, mientras los proveedores de servicios de telecomunicaciones colombianos, tendrían que "implementar medidas humanas, técnicas y administrativas para garantizar la seguridad digital, la gestión de riesgos de ciberseguridad, lo mismo que la identificación y reporte de ciberinfraestructuras críticas y de servicios esenciales" (Brigard Urrutia, 2022).

De igual modo, esta propuesta tiene como meta la creación de nuevos entes administrativos, incluido un CSIRT para regular, implementar y hacer cumplir las obligaciones en materia de seguridad digital y cibernética.

Por último, es posible mencionar el rol de la Mesa colombiana de Gobernanza de Internet, entre cuyas preocupaciones se encuentra la seguridad digital, con aportes desde el gobierno, la empresa privada, la sociedad civil, la academia y la comunidad técnica (Foro Colombiano de Gobernanza de *Internet*, 2022).

## 2. España

La cooperación público-privada en materia de ciberseguridad en España, ha sido liderada por INCIBE, organismo que, en el marco del Plan de Confianza en el Ámbito Digital, condujo el proceso de conformación de la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), que quedó constituida el 1 de julio de 2016, para seis días más tarde adscribirse como miembro pleno de la *European Cyber Security Organistion* (ECSO).

Se trata de un conglomerado que considera centros de investigación, universidades y otros actores del ecosistema de ciberseguridad, cuyos objetivos buscan alinearse con una estrategia de alcance europeo, además de configurarse en función de las necesidades de la industria y los usuarios finales.

La Red pretende conseguir (INCIBE, 2022):

- La colaboración de los agentes expertos en ciberseguridad.
- La reunión y centralización de una masa crítica de recursos investigadores.
- La difusión de las conclusiones de trabajos investigativos, que posibiliten la transferencia de conocimiento.
- La promoción de una capacitación y desarrollo de talentos, a partir de una política de incentivos.

En cuanto a planes específicos, este organismo ha propuesto la definición de un mapa de conocimiento de investigación y desarrollo en ciberseguridad, la organización de las Jornadas Nacionales de Investigación en Ciberseguridad y el estímulo a un plan director, que busque sentar las bases de una Estrategia de Ciberseguridad.

## 3. EE.UU.

La CISA ha instado a avanzar en una cooperación permanente entre los sectores público y privado de este país, a partir de una evaluación de riesgos y falencias en los dos ámbitos, y considerando que ambos comparten las mismas redes de proveedores de *software* (*US Chamber of Commerce*, 2020).

Al respecto, uno de los pasos más importantes fue la *Cybersecurity Information Sharing Act*, de 2015, normativa que estableció canales para compartir información entre el sector comercial, el gobierno y los órganos civiles, de manera de tender hacia un sistema que identifique y establezca defensas ante los ciberataques.

Luego, en julio del año pasado, el gobierno estadounidense publicó un Memorando de Seguridad Nacional, estableciendo metas voluntarias en materia de ciberseguridad, tanto para propietarios como operadores de infraestructura crítica.

En el plano internacional, en tanto, la administración Biden instó a los países del “G-7” a denunciar a los estados que encubren actividad criminal en materia de ciberdatos, así como a actualizar la política de ciberseguridad de la OTAN (*White House*, 2021).

En agosto del año pasado, a su vez, el gobierno estadounidense organizó una cumbre de ciberseguridad con los principales CEO de las industrias del país, para comprometer recursos que refuercen los planes de ciberseguridad.

Dos meses después, Chris Inglis, el "Ciber-zar" de la administración Biden, anunció un nuevo esfuerzo para proteger los sectores público y privado, introduciendo regulaciones en los sectores industriales claves, como los de energía y transporte, al tiempo de propiciar el paso de las agencias gubernamentales hacia un modelo "*Zero Trust*", que asume que toda la actividad de las redes computacionales es maliciosa, hasta que los usuarios prueban lo contrario (RSA *Conference*, 2021).

En cuanto a los vínculos con la academia, la CISA ha incentivado la adopción de buenas prácticas y de un sentido de responsabilidad compartida en este ámbito (CISA, 2022c).

En esta línea, el Departamento de Seguridad Interior (DHS, por sus iniciales en inglés) y la Agencia de Seguridad Nacional, auspiciaron el programa "*National Centers of Academic Excellence in Cybersecurity*" (NCAE-C), cuya meta es reducir la vulnerabilidad de la infraestructura de información nacional, promoviendo una mayor experiencia en la materia (NICCS, 2021).

## 4. Estonia

La Estrategia de Ciberseguridad de Estonia, de 2008, incluye un programa de educación comprehensiva, que considera actividades como (BSA, 2022):

- La promoción de una mayor conciencia en la opinión pública, en materia de seguridad de la información, en consonancia con el sector privado, con particular foco en usuarios básicos, pequeñas y medianas empresas, empleados de gobiernos locales, agencias del estado, profesores y estudiantes.

- La conducción de campañas de ciberseguridad en los medios de comunicación.

A su vez, la Ciberunidad de la Liga de la Defensa de Estonia es una organización voluntaria, que busca proteger el ciberespacio de este país báltico.

Sus principales objetivos son (KAITSELIIT, 2022):

- El desarrollo de un esquema de cooperación entre especialistas en tecnologías de la información.

- El incremento en el nivel de ciberseguridad de la infraestructura crítica, a través de la divulgación de conocimiento.

- La creación de una red para facilitar la alianza público-privada, lo mismo que la preparación para hacer frente a situaciones de crisis.

- La capacitación en seguridad informática, de cara a eventos internacionales de ciberseguridad.

Por su parte, CYBERS es una firma instituida en 2010, que entrega soluciones de ciberseguridad a los sectores público y privado, en una modalidad de monitoreo 24/7, bajo los estándares ISO27001, PCI/DSS y GDPR (CYBERS, 2022).

Finalmente, "VAATA" es una alianza público-privada fundada en 2001, que se dedica a promover servicios tecnológicos y de *Internet*, involucrando a proveedores internacionales del mercado de las telecomunicaciones.

## 5. Reino Unido

En el Reino Unido, el NCSC cuenta con un equipo dedicado a apoyar la ciberseguridad y proteger los activos críticos del Estado, promoviendo buenas prácticas y estimulando foros de trabajo que provean un espacio seguro entre el gobierno, la industria y la academia.

Este organismo apoya a las entidades públicas y privadas, para responder de forma efectiva ante ciberincidentes, mediante el programa "*Industry* 100", el desarrollo del *Cyber Assessment Framework*, la provisión de una fuente única de información de ciberamenazas tácticas y estratégicas, y la implementación de tecnologías emergentes, como en el caso del programa "*Smart Cities*", que consiste en áreas urbanas que integran tecnologías de la información, con soluciones inteligentes para optimizar la gobernanza en ciberseguridad (NCSC, 2022b).

Asimismo, el NCSC y el *Physical Sciences Research Council* entregan un reconocimiento a los centros académicos de excelencia en investigación de ciberseguridad, por su compromiso a invertir en capacidades investigativas en ciberseguridad, y destinar una masa crítica de académicos a liderar proyectos investigativos asociados, publicar investigaciones y financiar nuevas iniciativas en este ámbito.

Adicionalmente, el NCSC apoya el desarrollo de tesis doctorales sobre la materia, para lo cual existen en el país tres centros de capacitación doctoral en ciberseguridad (NCSC, 2022c).

### 6. Uruguay

El Plan Nacional de Ciudadanía Digital, presente en Uruguay, se sustenta en la Estrategia de Ciudadanía Digital para una Sociedad de la Información y el Conocimiento", que apunta a la adopción de acciones para alcanzar la accesibilidad digital de los servicios e información para ciudadanos y empresas públicas, por medio de normas, requisitos y exigencias técnicas, así como de un plan de generación de capacidades estatales.

De igual modo, Uruguay ha implementado nuevos modelos de procesos tecnológicos, "en aras de una mayor transparencia de las políticas públicas, la apertura de datos, la colaboración y la participación ciudadana digital" (Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento, 2022b). En tal sentido, este país ha avanzado en la disposición de una Plataforma de Participación Ciudadana Digital, con soluciones para la rendición de cuentas y el monitoreo ciudadano; la puesta en marcha de políticas de datos abiertos en todas las instituciones públicas; y la creación de procesos de colaboración ciudadana, en el contexto de la entrada en vigor del 5° y 6° Plan de Acción Nacional de Gobierno Abierto, durante el período 2021-2025.

Por último, cabe mencionar la existencia del Observatorio de Sociedad de la Información, que articula fuentes, indicadores y herramientas de análisis, para estandarizar información para conocer el nexo de los individuos con el ecosistema digital, coordinando investigaciones aplicadas y difundiendo datos, en consonancia con las buenas prácticas internacionales.

## VII. Gobernanza en ciberseguridad y labor policial ante el cibercrimen

### 1. Colombia

En Colombia, el Centro Cibernético Policial es el ente a cargo de investigar judicialmente y gestionar los datos criminales relacionados con las conductas delictivas que afectan a menores de edad en la red, así como de aminorar el impacto de las nuevas tecnologías en la comisión de delitos.

Esta organización se encarga de (Centro Cibernético Policial, 2022):

- Investigar las conductas que lesionen a menores de edad en materia sexual.
- Identificar nuevos delitos que emerjan a partir del empleo inapropiado de las nuevas tecnologías.
- Encabezar campañas de prevención y difusión, referidas a riesgos para niños, niñas y adolescentes, como consecuencia de la utilización de las tecnologías de la información y las comunicaciones.
- Tomar parte en grupos interinstitucionales, concentrados en la protección de los derechos de los menores de edad, frente al uso de las nuevas tecnologías.
- Utilizar las herramientas tecnológicas necesarias para la persecución de causas transnacionales de delitos en *Internet* contra niños, niñas y adolescentes.
- Coordinar medidas ante la Unidad Nacional de Delitos Sexuales, de la Fiscalía General de la Nación, en orden a robustecer la indagatoria judicial contra la pornografía infantil en la red.

### 2. España

La Brigada Central de Investigación Tecnológica, es la unidad policial que se dedica en España a la respuesta a los desafíos de las nuevas formas de delincuencia, como estafas por *Internet* y ciberataques.

Este departamento se inscribe en la Unidad de Investigación Tecnológica, órgano de la Dirección General de la Policía, que se aboca a la investigación y persecución de los ciberdelitos nacionales y transnacionales, actuando como Centro de Prevención y Respuesta "*E- Crime*" de la Policía Nacional, ante ilícitos como (Policía Nacional de España, 2022):

- Amenazas, injurias o calumnias por correo electrónico, mensajes sms, foros o *newsgroups*.
- Pornografía infantil.
- Fraudes y estafas por *Internet*.
- Ataques de denegación de servicio, sustracción de datos, *hackeos* y sustracción de cuentas.

### 3. EE.UU.

En el país norteamericano, la Ley Federal prohíbe el uso de *Internet* para actividades de explotación sexual infantil, delito perseguido por la *Attorney's Office*, bajo la *Child Pornography Prevention Act* y la *Mann Act*.

La misma agencia persigue el *hackeo* de cuentas y sistemas computacionales, de acuerdo al Título 18, Sección 1030, del *United States Code*, que prohíbe el acceso no autorizado a equipos protegidos, que ocasione un daño en la integridad de la información, superior a los US$5.000 (*US Department of Justice*, 2022).

Por su parte, el *Bureau of International Narcotics and Law Enforcement Affairs* (INL) es un órgano que busca reforzar las capacidades de la policía en materia de cibercrimen, identificando vulnerabilidades que puedan ser explotadas por grupos criminales organizados.

En dicho afán, el INL estimula la búsqueda de vínculos bilaterales con terceros países; el fortalecimiento de alianzas multilaterales y regionales, incluyendo al "G-7", Naciones Unidas, la Organización de Estados Americanos (OEA), la Unión Africana y la Asociación de Naciones del Sudeste Asiático; y la ratificación de tratados internacionales, tales como la Convención sobre Cibercrimen, del Consejo de Europa.

Además, esta entidad comparte información con agencias de otros países, respecto a las mejores formas de identificar, perseguir y castigar el cibercrimen. Al respecto, un instrumento clave es la *U.S. Transnational and*

*High Tech Crime Global Law Enforcement Network* (GLEN), que despliega en el exterior la experiencia de especialistas norteamericanos, para capacitar a sus contrapartes foráneas.

El INL también opera la Red Global de Academias de Derecho Internacional, que provee asistencia a los legisladores de terceros países, en materia de marcos legales para el cibercrimen y protección informática, a la vez que capacita a jueces, clientes y agentes fronterizos, que buscan fortalecer el control de su territorio (*US Department of State*, 2022).

A su vez, el Servicio Secreto se encarga de detectar, investigar y arrestar a personas que violen ciertas normas sobre sistemas financieros. Esta entidad actúa en alianza con las Fuerzas de Tarea de Ciberfraude, que incluye en el monitoreo a las agencias de aplicación de la ley, la industria privada y la academia, con labores de prevención, detección, mitigación e investigación.

Por último, el *Global Investigative Operations Center* (GIOC) conduce análisis de fuentes de datos no tradicionales, trabajando en el combate a las organizaciones criminales transnacionales (*US Secret Service*, 2022).

## 4. Estonia

En Estonia opera la *Cyber Defence League* y el Centro de Ciberdefensa Operativa de la OTAN, con sede en Tallin, la capital del país (*Ministry of Foreign Affairs*, 2015).

Respecto al plano policial, hay que destacar la labor de la Policía de Seguridad del país, que se encarga de reducir las amenazas a la seguridad nacional provenientes del ciberespacio, sin confinarlas solo al ámbito local, sino también compartiendo un área de seguridad común con la OTAN y la Unión Europea (OSCE POLIS, 2022).

## 5. Reino Unido

La experiencia británica se sustenta en un modelo de respuesta integrada contra el cibercrimen, liderado por la *National Crime Agency*, que considera la participación de la policía británica, la industria privada y algunos socios internacionales, como EUROPOL, el *Federal Bureau of Investigation* (FBI) y el Servicio Secreto estadounidense, todos quienes comparten inteligencia y coordinan acciones conjuntas contra esta problemática (*National Crime Agency*, 2022).

Esta aproximación también incluye la labor de ciberequipos al interior de las unidades policiales de alcance regional y local, con una creciente puesta en marcha de soluciones de identidad digital frente al cibercrimen.

De igual modo, la inversión en cibercapacidades se ha incrementado, a través del *National Offensive Cyber Programme* y del establecimiento de la *National Cyber Force*, que congrega bajo un mando unificado a especialistas de los *Government Communications Headquarters*, el Ministerio de Defensa, el Servicio Secreto de Inteligencia, y el Laboratorio de Ciencia y Tecnología para la Defensa (*National Cyber Strategy*, 2022).

## 6. Uruguay

En el modelo uruguayo, el Departamento de Delitos Tecnológicos, de la Dirección General de Lucha Contra el Crimen Organizado e INTERPOL, se encargan de combatir la ciberdelincuencia, indagando diversas modalidades de fraude en *Internet* y las redes sociales.

Tras recibir cualquier denuncia de esta índole, este organismo comprueba la veracidad de los hechos, para luego diseñar un perfil del ciberdelincuente y entregar los antecedentes a la justicia (Ministerio del Interior de Uruguay, 2016).

Asimismo, en agosto del año pasado se creó la Unidad de Cibercrimen, de la Dirección de Investigaciones de la Policía Nacional, para enfocarse específicamente en *hackeos* que atenten contra la seguridad, confidencialidad e integridad de los sistemas informáticos" ("El País", 2021).

## Referencias

Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento. (2020, septiembre 15). Cometidos. Disponible en: http://bcn.cl/2l030.

Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento. (2020, septiembre 15). Creación y evolución histórica. Disponible en: http://bcn.cl/2l02w.

Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento. (2020, marzo 23).Marco de Ciberseguridad: nueva versión disponible. Disponible en: http://bcn.cl/2l036.

Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento. (2020, septiembre 15). Planes. Disponible en: http://bcn.cl/2l033.

Agencia de Gobierno Electrónico, y Sociedad de la Información y del Conocimiento. (2022, abril 27). CERTuy. Disponible en: http://bcn.cl/30e48.

Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento. (2022, abril 27). Fortalecimiento de la Sociedad de la Información. Disponible en: http://bcn.cl/30e43.

Brigard Urrutia. (2022, marzo 25). MINTICS propone mayor regulación a la ciberseguridad en Colombia. Disponible en: http://bcn.cl/30d4v.

BSA. (2022, abril 26). *Country: Estonia*. Disponible en: http://bcn.cl/30d4r.

Centro Cibernético Policial. (2022, abril 28). Funciones. Disponible en: http://bcn.cl/30gfn.

Centro de Ciberseguridad Industrial. (2022, abril 26). El mayor ecosistema de sus características… Disponible en: http://bcn.cl/30ggk.

Centro de Ciberseguridad Industrial. (2022, abril 28). La ciberseguridad industrial en Colombia. Disponible en: http://bcn.cl/30ghd.

Centro Nacional de Respuesta a Incidentes de Seguridad Informática. (2022, abril 26). Cometidos. Disponible en: http://bcn.cl/30d2g.

CISA. (2022, abril 26). *About* CISA. Disponible en: http://bcn.cl/30ggw.

CISA. (2022, abril 26). CISA *Incident Reporting System*. Disponible en: http://bcn.cl/30d29.

CISA. (2022, abril 26). *Resources for Academia*. Disponible en: http://bcn.cl/30d4e.

CONPES. (2016, enero 22). Política Nacional de Seguridad Digital. Disponible en: http://bcn.cl/2l22x.

CYBERS. (2022, abril 26). *Our Story*. Disponible en: http://bcn.cl/30d3w.

*Cybersecurity & Infrastructure Security Agency*. (2020, marzo 24). *Critical Infrastructure Sectors*. Disponible en: http://bcn.cl/2lhp6.

*Cybersecurity & Infrastructure Security Agency*. (2020, octubre 9). *National Infrastructure Coordinating Center*. Disponible en: http://bcn.cl/2lkqx.

*Cybersecurity Strategy*. (2019-2022). Disponible en: http://bcn.cl/2an8g.

*Defence Forces*. (2022, abril 26). *Cyber Command*. Disponible en: http://bcn.cl/30d1z.

*Department of the Prime Minister and Cabinet*. (2020, septiembre 16). *National Cyber Policy Office*. Disponible en: http://bcn.cl/2mw3h.

"Eje 21". (2022, abril 28). Gobierno Nacional crea Modelo de Gobernanza, para liderar coordinación entre actores del entorno digital. "*Eje 21*". Disponible en: http://bcn.cl/30ghg.

"El Español". (2022, marzo 28). El Gobierno destina 1.200 millones de Euros a la puesta en marcha de un nuevo Plan de Ciberseguridad. "*El Español*". Disponible en: http://bcn.cl/30d3i.

"El País". (2021, septiembre 20). Ministerio del Interior creó una unidad para combatir *hackers*. "*El País*". Disponible en: http://bcn.cl/30gec.

Estrategia Nacional de Ciberseguridad de España. (2019). Disponible en: http://bcn.cl/30d3o.

Foro Colombiano de Gobernanza de *Internet*. (2022, abril 26). Sobre la Mesa de Gobernanza. Disponible en: http://bcn.cl/30d50.

Gobierno Digital de Colombia. (2022, abril 26). CSIRT Gobierno. Disponible en: http://bcn.cl/30d0w.

Gov.uk. (2022, abril 26). *Cyber Security Incident Response Team* (CSIRT) *Service*. Disponible en: http://bcn.cl/30d2l.

*Homeland Security*. (2020, julio 14). *Critical Infrastructure Security*. Disponible en: http://bcn.cl/2lkrs.

INCIBE. (2019, julio 5). Qué es INCIBE. Disponible en: http://bcn.cl/2an71.

INCIBE. (2019, julio 5). Qué hacemos. Disponible en: http://bcn.cl/2an7f.

INCIBE. (2022, abril 28). Red de Excelencia Nacional de Investigación en Ciberseguridad. Disponible en: http://bcn.cl/30gg5.

INCIBE-CERT. (2022, abril 26). Qué es INCIBE-CERT. Disponible en: http://bcn.cl/30czu.

INCIBE-CERT. (2022, abril 26). Respuesta a incidentes. Disponible en: http://bcn.cl/30d01.

*Information System Authority*. (2021, julio 26). CERT-EE. Disponible en: http://bcn.cl/30d1e.

KAITSELIIT. (2022, abril 26). *Estonian Defence League's Cyber Unit*. Disponible en: http://bcn.cl/30d4p.

Ministerio de Defensa Nacional de Colombia. (2022, abril 26). Ciberdefensa. Disponible en: http://bcn.cl/30d2q.

Ministerio de Defensa Nacional de Colombia. (2022, abril 27). Quiénes somos. Disponible en: http://bcn.cl/310no.

Ministerio de Defensa Nacional de Uruguay. (2022, abril 26). Equipo de Respuesta a Incidentes de Seguridad Informática de Defensa (D-CSIRT). Disponible en: http://bcn.cl/30d2j.

Ministerio del Interior de Uruguay. (2016, enero 26). Delitos en las redes. Disponible en: http://bcn.cl/30ge8.

*Ministry of Economic Affairs and Communications*. (2020, abril 15). *Cyber security*. Disponible en: http://bcn.cl/2lkt6.

*Ministry of Foreign Affairs*. (2015, julio 28). *Estonian police to set up cyber crime unit*. Disponible en: http://bcn.cl/30e0o.

MINTICS. (2014, marzo). Agenda Estratégica de Innovación: ciberseguridad. Disponible en: http://bcn.cl/2l22o.

MINTICS. (2021, noviembre 12). Proyectos de inversión 2022. Disponible en: http://bcn.cl/30d2p.

*National Crime Agency*. (2022, abril 27). *Cyber crime*. Disponible en: http://bcn.cl/30dyn.

*National Cyber Strategy*. (2022, febrero 7). Disponible en: http://bcn.cl/30ghu.

NCSC. (2020, septiembre 22). *National Cyber Security Centre*(NCSC). Disponible en: http://bcn.cl/2mw3l.

NCSC. (2022, abril 26). *Academic Centres of Excellence in Cyber Security Research*. Disponible en: http://bcn.cl/30d4n.

NCSC. (2022, abril 26). *CNI Hub*. Disponible en: http://bcn.cl/30d4o.

NCSC. (2022, abril 28*). What we do*. Disponible en: http://bcn.cl/30ghn.

NICCS. (2021, diciembre 13). *National Centers of Academic Excellence in Cybersecurity* (NCAE–C). Disponible en: http://bcn.cl/30d4h.

OSCE POLIS. (2022, abril 27). Estonia. Disponible en: http://bcn.cl/30e15.

Plan de la Sociedad de la Información y del Conocimiento. (2020, septiembre 20). Estrategia Nacional de Ciberseguridad (Programa 1). Disponible en: http://bcn.cl/2l3dj.

Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia. (2017). Disponible en: http://bcn.cl/2lh78.

Policía Nacional de España. (2022, abril 27). Brigada Central de Investigación Tecnológica. Disponible en: http://bcn.cl/30e4e.

Presidencia de Uruguay. (2020, junio). Ecosistema de Ciberseguridad en Uruguay. Un análisis cualitativo. Disponible en: http://bcn.cl/30ehy.

Presupuesto Nacional 2020-2024. (s/i). Disponible en: http://bcn.cl/304re.

*Republic of Estonia*. (2018, septiembre 9). *Critical Information Infrastructure Protection* CIIP. Disponible en: http://bcn.cl/2lkso.

RSA Conference. (2021, noviembre 30). *Government and Private Sector Cybersecurity Collaboration Finally Showing Signs of Life*. Disponible en: http://bcn.cl/30d43.

*UK Cabinet Office*. (2018). *Public Summary of Sector Security and Resilience Plans*. Disponible en: http://bcn.cl/2c9ye.

*UK Government*. (2021). *UK Cyber Security. Sectoral Analysis* 2021. Disponible en: http://bcn.cl/30d37.

*US Chamber of Commerce*. (2020, octubre 7). *CISA's Current Capabilities Being Put to the Test in Private Sectors*. Disponible en: http://bcn.cl/30d40.

*US Department of Justice*. (2022, abril 26). *Cybercrime*. Disponible en: http://bcn.cl/30d5a.

*US Department of State*. (2022, abril 26). *Cybercrime and Intellectual Property Crime*. Disponible en: http://bcn.cl/30d5b.

*US Secret Service*. (2022, abril 27). *Cyber Investigations*. Disponible en: http://bcn.cl/30dy2.

*White House*. (2021, agosto 25). *Fact sheet: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity*. Disponible en: http://bcn.cl/30d4a.

*White House*. (s/i). *Information Technology and Cybersecurity Funding*. Disponible en: http://bcn.cl/30d31.

**Textos normativos**

*Cybersecurity Act*. (2018, mayo 9). Disponible en: http://bcn.cl/2lkss.

*Cybersecurity and Infrastructure Agency Act*. (2018, noviembre 16). Disponible en: http://bcn.cl/2lkrv.

Ley 8, por la que se establecen medidas para la protección de las infraestructuras críticas. (2011, abril 28). Disponible en: http://bcn.cl/2caft.