Ciberseguridad e infraestructura crítica: los casos de Bélgica, Estonia, Italia y la UE

Autor

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

Nº SUP: 138412

Resumen

La ciberseguridad es “la práctica de proteger sistemas, redes y programas de ataques digitales, que buscan acceder, modificar o destruir información confidencial, extorsionar a las personas o interrumpir un servicio”.

En el paradigma belga, existe desde el 20 de mayo de 2021 una Estrategia de Ciberseguridad Nacional, aprobada por el Consejo de Seguridad Nacional, que constituye el marco para la aproximación de este país en este ámbito. Esta directriz es implementada por el Centro para la Ciberseguridad, autoridad nacional que supervisa, coordina y monitorea su aplicación.

Respecto a 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, al tiempo de velar por el cumplimiento de las metas de la Estrategia de Ciberseguridad 2019-2022. Además, este país ha desarrollado la noción de *Critical Information Infrastructure Protection*, que considera la recolección y administración de datos, el intercambio de información sobre proveedores de servicios y la entrega de análisis de riesgos a los proveedores de servicios.

A su vez, en Italia, la *Agenzia per la Cybersicurezza Nazionale* es la autoridad nacional de carácter autónomo, que busca proteger el ciberespacio del país, previniendo y mitigando incidentes, al tiempo de propender a la restauración de los sistemas atacados, mediante la implementación de la Estrategia Nacional de Ciberseguridad, alianzas internacionales con agencias de terceros estados, la puesta en marcha de iniciativas público-privadas y el desarrollo de cursos de capacitación para formar una fuerza especializada en ciberseguridad.

Finalmente, el 16 de enero de 2023 entró en vigor la Directiva NIS2 de la Unión Europea, cuyo artículo 1 fija un conjunto de obligaciones para los países del bloque, en cuanto a adoptar estrategias de ciberseguridad y designar autoridades especializadas, para hacer frente a distintas crisis en este ámbito; emitir reportes de ciberseguridad; compartir información; y hacer cumplir las obligaciones asumidas como partes integrantes de la alianza europea.

Introducción

A solicitud de la Comisión de Seguridad Ciudadana, de la Cámara de Diputados, el presente informe describe la regulación de la ciberseguridad e infraestructura crítica en países como Bélgica, Estonia e Italia, así como en la Unión Europea (en adelante, UE).

El texto recoge información del informe BCN "Institucionalidad en ciberseguridad e infraestructura crítica a nivel internacional" (julio, 2022), del mismo autor del presente trabajo.

I. Ciberseguridad e infraestructura crítica

1. Conceptos generales

La ciberseguridad puede ser concebida como "la práctica de proteger sistemas, redes y programas de ataques digitales, que buscan acceder, modificar o destruir información confidencial, extorsionar a las personas o interrumpir la continuidad de un servicio" (CISCO, 2022).

Por su parte, en 2004 la Comisión Europea definió la infraestructura crítica como (Comisión Europea, 2004. En Horzella, B., 2019: 2):

"(…) aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información, cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos, o

en el eficaz funcionamiento de los gobiernos de los estados miembros. Las infraestructuras críticas se extienden a través de muchos sectores de la economía, incluyendo la banca y finanzas, el transporte y la distribución, la energía, los servicios públicos, la salud, el suministro de alimentos, y las comunicaciones, así como los servicios gubernamentales claves".

Cuatro años más tarde, el Consejo Europeo, a partir de su Directiva 114, de 2008, la conceptualizó como (Consejo Europeo, 2008. En Horzella, B, 2019: 2):

"(…) el elemento, sistema o parte de este, situado en los estados miembros, que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población, cuya perturbación o destrucción afectaría gravemente a un estado miembro, al no poder mantener esas funciones".

A continuación se describen las principales características de los sistemas ciberespaciales de protección de infraestructura crítica, en países como Bélgica, Estonia e Italia, así como en la UE.

2. Institucionalidad en materia de ciberseguridad e infraestructura crítica

2.1. Bélgica

En el paradigma belga, existe desde el 20 de mayo de 2021 una Estrategia de Ciberseguridad Nacional, aprobada por el Consejo de Seguridad Nacional, que constituye el marco para la aproximación de este país en este ámbito.

Esta directriz es implementada por el Centro para la Ciberseguridad (CCB), autoridad nacional que supervisa, coordina y monitorea su aplicación.

Se trata de una entidad establecida a partir del Real Decreto del 10 de octubre de 2014, que opera bajo la autoridad del Primer Ministro, con las misiones de (*Centre for Cybersecurity Belgium*, 2023a):

- Monitorear, coordinar y supervisar la implementación de esta política sectorial.
- Gestionar los diversos proyectos sobre ciberseguridad, utilizando un enfoque integrado y centralizado.
- Lanzar proyectos que robustezcan la ciberseguridad de sectores vitales para el país, tales como energía, transportes, telecomunicaciones, finanzas, servicios sanitarios y salud.
- Asegurar la coordinación entre los departamentos gubernamentales, el sector privado y actores científicos relevantes.
- Formular propuestas adaptables al marco regulatorio vigente.
- Asegurar un buen manejo de crisis, en caso de ciberincidentes, en consonancia con la labor del Centro de Coordinación y Crisis del gobierno.
- Preparar, divulgar y fiscalizar la implementación de estándares y lineamientos de seguridad para los diversos sistemas de información del gobierno y las instituciones públicas del país.
- Coordinar la participación de Bruselas en foros de ciberseguridad internacionales.
- Coordinar la evaluación de seguridad, así como la certificación de sistemas de comunicación e información.

Bélgica cuenta igualmente con un Plan Nacional de Ciberemergencia, aprobado en 2017, con la participación del CCB y del Centro Nacional de Crisis, cuyo objetivo primordial es responder a las crisis del ciberespacio y los incidentes que requieran una coordinación a nivel nacional (*Centre for Cybersecurity Belgium*, 2023a).

A su vez, existe un Departamento de Inteligencia e Investigación de Ciberamenazas, que revisa cualquier incidente, recolectando, analizando y distribuyendo información sobre vulnerabilidades y ataques a los sistemas críticos de la información y comunicación del país.

También es responsable de emitir un Sistema de Alerta Temprana, que incluye el intercambio de información entre el Equipo de Respuesta ante Incidentes de Seguridad Informática belga (CSIRT) y el de otros estados (*Centre for Cybersecurity Belgium*, 2023b).

A nivel normativo, en tanto, el Código Penal sanciona una serie de conductas ilegales en el ciberespacio, como en el caso del sabotaje informático, concebido en el artículo 550 *ter* como la comisión de cualquier acto sin autorización, que modifique o elimine un sistema de información por medios tecnológicos o no tecnológicos, y castigado con penas de entre seis meses y hasta tres años de prisión, o multa de entre 208 y 200.000 Euros. Si la información resulta dañada, la sanción se eleva hasta cinco años de reclusión y multa de 600 mil Euros.

Asimismo, el *phishing* es castigado por el artículo 504 *quater* con entre seis meses de cárcel y multa de hasta 800 mil Euros (*Code Penal*, 2021).

Por otra parte, conforme al artículo 7 de la *Loi relative à la Sécurité et la Protection des Infrastructures Critiques*, de 2011, cada autoridad sectorial debe emitir un listado de infraestructuras críticas potencialmente susceptibles de ser atacadas, acompañado de un plan de seguridad preventivo, una proyección de escenarios y un análisis de vulnerabilidades, tendientes a neutralizar los riesgos de interrupción del servicio o de destrucción de instalaciones sensibles para el Estado (*Loi relative à la sécurité et la protection des infrastructures critiques*, 2011).

La legislación belga sobre ciberseguridad se vio reforzada además con la aprobación, el 3 de mayo de 2019, de la *Belgian Network and Information Systems Law*, dirigida a mejorar los estándares de seguridad de sectores críticos para el Estado, como economía, seguridad pública, energía, transporte, salud, servicios sanitarios e infraestructura digital (KPMG, 2023).

Finalmente, el 15 de febrero de 2023 entró en vigor en este país una nueva normativa, que legalizó, incluso en ausencia de consentimiento, el llamado "*hacking* ético", concebido como el intento por vulnerar la seguridad de un mecanismo informático, a fin de hallar posibles debilidades a corregir, de manera preventiva a cualquier intrusión de parte de ciberdelincuentes (*Ku Leuven*, 2023).

2.2. Estonia

La infraestructura crítica es concebida en Estonia como los sistemas de información y comunicaciones, cuyo mantenimiento, confiabilidad y seguridad son esenciales para el apropiado funcionamiento del país (*Republic of Estonia*, 2022a).

En cuanto a la institucionalidad, 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, al tiempo de velar por el cumplimiento de las metas de la Estrategia de Ciberseguridad 2019-2022, 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):

- 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 aquellos de carácter transfronterizo.

Asimismo, esta hoja de ruta prevé la realización de ejercicios conjuntos regulares con los proveedores de servicios vitales, autoridades políticas y organizaciones militares, a la vez que desarrolla 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).

Por otra parte, 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*, 2022b):

- La disponibilidad y funcionamiento seguro de los servicios esenciales.
- La continuidad digital de los procesos gubernamentales.
- 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), que apunta a recolectar y administrar datos, compilar informes sectoriales sobre riesgos asociados, intercambiar información sobre proveedores de servicios, desarrollar medidas de seguridad, entregar análisis de riesgos a los proveedores de servicios y elevar los niveles de conciencia en torno a la ciberseguridad entre la población (*Republic of Estonia*, 2022a).

Bajo esta lógica, la *Information System Authority* (RIA) es la entidad 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.

Asimismo, cabe mencionar el rol del Centro de Coordinación Nacional de Estonia, adscrito a la red europea de centros de ciberseguridad, que es administrado por el Departamento de Coordinación e Investigación de la RIA, con el objetivo de promover el desarrollo de la industria de la ciberseguridad, tecnología e investigación, incrementando la competitividad del sector, tanto a nivel nacional como internacional.

Esta entidad también apoya la participación de compañías de ciberseguridad en proyectos internacionales, promoviendo una sociedad más resiliente; asegurando un mayor número de especialistas en la materia; monitoreando el desarrollo del ecosistema de ciberseguridad en el país; y estimulando la comunicación entre proveedores, consumidores, investigadores y otras partes interesadas en el ciberespacio (*Republic of Estonia*, 2022b).

En el ámbito normativo, en tanto, 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 los servicios.

En tal sentido, cada proveedor tiene que preparar un sistema de análisis de riesgos, que contemple un listado de amenazas a la seguridad de los activos críticos, determinando la severidad de las consecuencias de ciberincidentes asociados, y 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 RIA, 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 previstos por el artículo 16 de la Directiva 1148, de 2016, del Parlamento Europeo, de manera que ante un problema que llegue a tener un impacto significativo sobre la continuidad de un servicio digital en un tercer estado, la RIA avise de inmediato 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 sección siguiente, en tanto, dispone la existencia de un Registro de Incidentes Ciberespaciales, entendido como una base de datos mantenida por la propia RIA, con el fin de grabar y analizar los ciberataques, para luego resolverlos.

De igual forma, la Sección 16 de la ley establece que la autoridad puede restringir 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 problema (*Cybersecurity Act*, 2018).

2.3. Italia

La *Agenzia per la Cybersicurezza Nazionale* (ACN) es una autoridad nacional de carácter autónomo, establecida en función del Decreto Ley 82, del 14 de junio de 2021, que busca proteger el ciberespacio italiano, previniendo y mitigando incidentes, al tiempo de propender a la restauración de los sistemas atacados, mediante (ACN, 2023):

- La implementación de la Estrategia Nacional de Ciberseguridad.
- La promoción de un marco regulatorio coherente, con inspecciones periódicas y un régimen de sanciones.
- La consolidación de alianzas internacionales con agencias de terceros estados.
- La coordinación entre actores públicos y la puesta en marcha de iniciativas público-privadas, para fortalecer la autonomía digital del país.
- El desarrollo de cursos de capacitación para formar una fuerza especializada en ciberseguridad, junto a la promoción de campañas que hagan consciente entre la población una cultura de la ciberseguridad.

La estructura de la ACN contempla un Equipo de Respuesta ante Incidentes de Ciberseguridad (“CSIRT Italia”), un Centro Nacional de Coordinación, y un Centro de Certificación y Evaluación Nacional, para el escrutinio tecnológico de los activos digitales estratégicos del país.

Asimismo, en el plano normativo, el artículo 4 del *Decreto-Legge 14, per disposizioni urgenti in materia di Cybersicurezza, Definizione dell'Architettura Nazionale di Cybersicurezza e Istituzione dell'Agenzia per la Cybersicurezza Nazionale*, establece la existencia del *Comitato Interministeriale per la Cybersicurezza*, encargado de asesorar a la Presidencia del Consejo de Ministros en materias de ciberseguridad, proponiendo al titular de este órgano indicaciones generales para proceder en este ámbito (*Decreto-legge 14*, 2021).

En cuanto a la Estrategia Nacional de Ciberseguridad, esta directiva prescribe tres grandes ámbitos de desarrollo en el ciberespacio, como son (*Strategia Nazionale di Cybersicurezza*, 2022-2026):

- La protección de los activos esenciales del Estado, con el objetivo de minimizar riesgos y facilitar la transición digital.
- La respuesta ante vulnerabilidades digitales, apoyando la aplicación de configuraciones de ciberseguridad y favoreciendo el desarrollo criptográfico en el ámbito financiero, en el afán de contribuir a la consolidación de un ecosistema nacional en materia de ciberseguridad. Esta función va en línea con el desarrollo de un sistema de gestión de crisis cibernéticas de alcance nacional y transnacional, denominado *Nucleo per la Cybersicurezza* (NCS), que busca asegurar el despliegue de un mecanismo sinérgico, de coordinación continua entre todos los departamentos del Estado, con una actualización permanente de los procedimientos previstos ante ciberincidentes.
- El desarrollo de las tecnologías digitales y de la competitividad de la industria afín, con el objetivo de estar en sintonía con las necesidades del país en materia de ciberseguridad.

2.4. UE

El 27 de diciembre de 2022 fue publicada y el 16 de enero del presente año entró en vigor la Directiva NIS2 de la UE (*European Parliament*, 2023: 12), cuyo artículo 1 fija un conjunto de obligaciones para los Estados Miembros del bloque, en cuanto a adoptar estrategias de ciberseguridad y designar autoridades especializadas en la materia, para hacer frente a distintas crisis en este ámbito; emitir reportes de ciberseguridad; compartir información; y supervisar y hacer cumplir las obligaciones asumidas como partes integrantes de la alianza europea.

El siguiente artículo, en tanto, dispone la aplicación de esta Directiva para organismos públicos y privados, sin consideración del tamaño de cada entidad.

Bajo esta lógica, el artículo 7 del texto legal precisa que las antes mencionadas estrategias de ciberseguridad diseñadas por cada país, tienen que incluir (*Directive (EU) 2.555*, 2022):

- Objetivos y prioridades en la cobertura de sectores vitales.
- Un marco de gobernanza para alcanzar las metas trazadas en el punto anterior.
- El establecimiento de roles y responsabilidades claros para el caso de los agentes relevantes del sistema a nivel nacional.
- La coordinación y cooperación entre autoridades gubernamentales y equipos de respuesta ante crisis.
- Los mecanismos que permitan identificar los activos críticos, junto a una evaluación de riesgos.
- La disposición de medidas para responder ante ciberincidentes, así como para recuperar las capacidades afectadas, con un foco en la colaboración público-privada.
- El diseño de un plan para incrementar la conciencia ciudadana en torno a materias de ciberseguridad.
- La puesta en marcha de directrices que promuevan el desarrollo e integración de tecnologías avanzadas para la implementación de medidas de gestión de riesgos en el ciberespacio.

Junto a lo anterior, la norma dispone que la Agencia para la Ciberseguridad de la UE (ENISA) debe asesorar a los decisores de gobierno en la revisión, al menos quinquenal, de las estrategias de seguridad de cada país.

Este organismo, conforme al artículo 18 del texto, también debe remitir al Parlamento Europeo un reporte bienal sobre el estado de la ciberseguridad en el bloque, incluyendo aspectos como el nivel de riesgo en el ciberespacio y un análisis del desarrollo de cibercapacidades, tanto a nivel público como privado.

De igual modo, el artículo 9 puntualiza que los Estados Miembros deben adoptar un plan nacional a gran escala, para hacer frente a crisis e incidentes en el ciberespacio, considerando tareas, procedimientos de gestión, ejercicios de entrenamiento y alianzas público-privadas.

Respecto a los equipos de respuesta ante incidentes, el artículo 11 les encomienda las misiones de (*Directive (EU) 2.555*, 2022):

- Monitorear y analizar en tiempo real las redes y sistemas de información.
- Entregar alertas tempranas y divulgar información que sea relevante para las autoridades, en materia de ciberamenazas, vulnerabilidades e incidentes.
- Responder ante eventos críticos, con asistencia a las entidades afectadas.
- Recoger y analizar información sensible, realizando análisis de riegos situacionales.

Finalmente, el artículo 23 de la norma obliga a las entidades especializadas de cada Estado Parte a notificar a la brevedad cualquier ciberincidente en sus servicios esenciales, teniendo presente que un ciberataque será considerado significativo cuando sea capaz de causar una severa disrupción operacional en los servicios; una pérdida financiera estimable; o un perjuicio material o inmaterial sobre personas naturales o jurídicas.

Referencias

ACN. (2023). *About Us*. Disponible en: https://www.acn.gov.it/en/agenzia/chi-siamo.

Centre for Cybersecurity Belgium. (2023). *Organisation*. Disponible en: https://ccb.belgium.be/en/organisation.

Centre for Cybersecurity Belgium. (2023). *Vital sectors*. Disponible en: https://ccb.belgium.be/en/vital-sectors.

CISCO. (2022, julio 8). ¿Qué es la ciberseguridad? Disponible en: http://bcn.cl/33jwp.

Code Penal. (2021, febrero 24). Disponible en: https://legislationline.org/sites/default/files/documents/6e/BELG_CC_fr.pdf.

Comisión Europea. (2004). En Horzella, Bárbara. [2019, diciembre]. Protección de Infraestructura Crítica y Fuerzas Armadas. Conceptualización y experiencia comparada. BCN. Disponible en: http://bcn.cl/2lf8z.

Consejo Europeo. (2008). En Horzella, Bárbara. [2019, diciembre]. Protección de Infraestructura Crítica y Fuerzas Armadas. Conceptualización y experiencia comparada. BCN. Disponible en: http://bcn.cl/2lf8z.

Cybersecurity Act. (2018, mayo 9). Disponible en: http://bcn.cl/33h69.

Cybersecurity Strategy (2019-2022). Disponible en: file:///C:/Users/jjarufe/Downloads/kuberturvalisuse_strateegia_2019-2022_0-2.pdf.

Decreto-legge 14, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale. (2021, junio 15). Disponible en: https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/SG.

Directive (EU) 2022/2.555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). (2022, diciembre 27). Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.

European Parliament. (2023). *The NIS2 Directive. A high common level of cybersecurity in the EU*. Disponible en: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.

KPMG. (2023). *NIS – Belgium's first complete cyber security...* Disponible en: https://kpmg.com/be/en/home/insights/2020/04/ta-nis-belgium-first-complete-cyber-security-legislation.html.

Ku Leuven. (2023, mayo 3). *Belgium legalises ethical hacking: a threat or an opportunity for cybersecurity?* Disponible en: https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/.

Loi relative à la sécurité et la protection des infrastructures critiques. (2011, julio 1). Disponible en: https://centredecrise.be/sites/default/files/documents/files/2021-03/PDFsam_15_2.pdf.

Republic of Estonia. (2022, noviembre 17). *Cyber defence of critical infrastructure*. Disponible en: https://www.ria.ee/en/cyber-security/cyber-defence-critical-infrastructure/cyber-defence-critical-infrastructure.

Republic of Estonia. (2022, noviembre 21). *National Coordination Center (NCC-EE)*. Disponible en: https://www.ria.ee/en/cyber-security/national-coordination-center-ncc-ee/national-coordination-center-ncc-ee.

Strategia Nazionale di Cybersicurezza. (2022-2026). Disponible en: https://www.acn.gov.it/ACN_Strategia.pdf.