Análisis del marco jurídico y de gobernanza de la ciberseguridad para la protección de las Infraestructuras Críticas en Argentina

Prof. Dr. Carlos Galán
cgalan@atl.es / cgalan@der-pu.uc3m.es

(versión 0) - Junio, 2022

Contenido

0. PREÁMBULO 3

1. SEMBLANZA DEL AUTOR 4

2. LAS INFRAESTRUCTURAS CRÍTICAS Y SU CIBERSEGURIDAD EN EL MUNDO 6

3.1 Concepto y tipología 6

3.2 El Modelo de Gobernanza de la ciberseguridad de las IC 12

3.2.1 Marco regulatorio 12

3.2.2 Marco institucional 12

3. LA ESTRUCTURA ORGANIZATIVA DE LA ADMINISTRACIÓN PÚBLICA NACIONAL CENTRALIZADA DE LA ARGENTINA 16

4. LA REGULACIÓN DE LA CIBERSEGURIDAD DE LAS IC EN LA ARGENTINA 51

4.1 Leyes relacionadas con la ciberseguridad. 52

4.2 Normativa vinculada a las funciones de la Dirección Nacional de Infraestructuras Críticas de la Información y Ciberseguridad 54

5. RESUMEN DE HALLAZGOS, CONCLUSIONES Y PLAN DE ACCIÓN 88

5.1 Resumen de hallazgos: advertencias y/o cuestiones a analizar 88

5.2 Conclusiones generales 91

5.3 Hoja de ruta y acciones subsiguientes 93

ANEXO I: APROXIMACIÓN A LA GOBERNANZA DE LA CIBERSEGURIDAD EN DIFERENTES PAÍSES. 95

AI.1 Estados Unidos 95

AI.2 Reino Unido 107

AI.3 Francia 110

AI.4 España, en el marco regulatorio de la Unión Europea 114

0. PREÁMBULO

El presente Informe se redacta a petición del Banco Interamericano de Desarrollo (BID, en adelante), con el objetivo de:

> **Evaluar la actual situación de la Argentina en lo relativo al ecosistema de ciberseguridad aplicada a la protección de las Infraestructuras Críticas de Información de dicho país.**

Como se contiene en los Términos de Referencia del proyecto, tras exponer brevemente la realidad de la transformación digital de nuestras y los riesgos derivados de operar en el denominado ciberespacio, profusamente analizados por prestigiosas entidades internacionales, concluye señalando que: "La protección de las Infraestructuras Críticas de Información (CIIP por sus siglas en inglés) es uno de los deberes de las naciones. Un incidente de ciberseguridad en estas Infraestructuras podría tener un gran impacto en la calidad de vida de los ciudadanos."

Para abordar estos retos derivados de la digitalización de la sociedad, se crea y desarrolla la **División de Innovación para Servir al Ciudadano (ICS)** del BID que, entre otras, tiene la responsabilidad de atender los temas de gobernanza del sector público y de capacidad institucional del Estado (GA-232-38) en distintos sectores, a todos los niveles de gobierno y con los distintos Poderes del Estado. Parte de su agenda incluye el apoyo a los países miembros del BID en sus esfuerzos en la promoción de un mejor gobierno para la ciudadanía, entendido a partir de tres dimensiones clave alineadas con la Estrategia Sectorial: efectividad en el logro de los resultados gubernamentales previstos; eficiencia en el manejo de los recursos públicos disponibles; y la apertura de las instituciones públicas y de los procesos de formulación e implementación de políticas. Esta agenda se apoya en la generación de capacidades para una gestión pública centrada en la ciudadanía y orientada a mejorar la provisión de servicios públicos de calidad. Todo ello apoyado en los avances que las TIC han contribuido a generar en la administración pública, por medio de nuevas formas de interacción con los ciudadanos, de modernización de los procesos de gestión, y del fortalecimiento de la toma de decisiones. Todo esto considerando cuidadosamente los riesgos de ciberseguridad y la protección de los sistemas críticos.

En base a todo ello, como se ha dicho, el objetivo del proyecto en cuestión es, esencialmente, realizar un diagnóstico de la situación actual de ciberseguridad para la protección de infraestructuras críticas de la información de la Argentina (del punto de vista del marco institucional, regulatorio y gobernanza) y elaborar una hoja de ruta para subsanar los GAP hallados frente a las buenas prácticas internacionales.

1. SEMBLANZA DEL AUTOR

El **Dr. Carlos Galán** es Licenciado y Doctor en Informática, Licenciado en Derecho y Abogado especialista en Derecho de las Tecnologías de la Información, Certified Information Security Manager (CISM) por ISACA, Consultor/Formador Homologado de la EOI y Auditor Técnico de Certificación de Producto (UNE-EN-ISO 17065) por la Entidad Nacional de Acreditación de España (ENAC) para el Esquema Nacional de Seguridad y el Reglamento (UE) de Identidad Electrónica y Servicios de Confianza.

Autor de una decena de libros relacionados con las Tecnologías de la Información, su Derecho y sus aplicaciones, ha escrito asimismo una multiplicidad de artículos y comentarios en prensa y publicaciones especializadas.

Ha desarrollado parte de su carrera profesional en el Grupo Telefónica de España, ocupando diversos cargos y desarrollando significativos proyectos nacionales e internacionales.

Ha sido Vocal Asesor y Director de la Oficina de Modernización del Ministerio del Interior de España, donde, entre otras actividades, diseñó en Plan de Modernización de los Cuerpos y Fuerzas de Seguridad del Estado y presidió la Comisión de Informática y Comunicaciones de la Seguridad de los Juegos Olímpicos de Barcelona ’92.

Ha sido profesor de la Facultad de Informática de la Universidad Politécnica de Madrid, de la Escuela Técnica Superior de Ingenieros Industriales de la UNED, de la licenciatura de Administración y Dirección de Empresas de la Universidad Complutense de Madrid y del Instituto de Postgrado de la Universidad Pontificia de Comillas.

Ha sido Director General de la Agencia de Certificación Electrónica ACE (primera Autoridad de Certificación de España), Vicepresidente de la Asociación de Entidades de Confianza Digital AECODI, Director General de Desarrollo y Tecnología de la Fundación General de la Universidad de Málaga y Presidente del Comité de Nuevas Tecnologías de Hispajuris, la mayor red de despachos de abogados de España.

En el terreno académico, en su calidad de especialista en Administración Electrónica, Seguridad y Firma Electrónica, ha sido profesor de *Calidad, Seguridad y Protección de la Información*, de la Ingeniería de Informática de la Universidad Pontificia de Salamanca.

Actualmente, además de impartir la materia de *Ciberseguridad* en el Máster Universitario en Protección de Datos, Transparencia y Acceso a la Información, de la Universidad San Pablo CEU, es miembro del Área de Derecho Administrativo de la Universidad Carlos III de Madrid, institución en la que imparte *Derecho de las TIC* en el Grado de Derecho de la Facultad de Ciencias Sociales y Jurídicas, *Aspectos Legales de la Ingeniería Informática,* del Máster de Universitario Ingeniería Informática, *Ciberseguridad*, en el Máster de Derecho de las Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información, y en el Máster Universitario en Ciberseguridad y *Aspectos legales del Internet de las Cosas*, en el Máster del mismo nombre, actividades que compagina con la escritura de monografías y artículos y el dictado de conferencias y cursos donde es ponente habitual en las materias relativas al Derecho de las Tecnologías de la Información y las Comunicaciones, la Administración Electrónica, Firma Electrónica, Certificación Digital y la Ciberseguridad IT.

Ha sido asesor parlamentario en la redacción de la Ley 59/2003, de firma electrónica y colaborador del Ministerio de Hacienda y Administraciones Públicas, dónde ha sido miembro del Grupo de Expertos del Plan de Acción de Administración Electrónica.

Desde 2011 es Asesor del Centro Criptológico Nacional (adscrito al Centro Nacional de Inteligencia de España), donde desarrolla su actividad en materias relativas a la normativa nacional, europea e internacional en materia de Ciberseguridad y Esquema Nacional de Seguridad y sus Instrucciones Técnicas derivadas, habiendo formado parte del equipo redactor de las Estrategias de Ciberseguridad Nacionales de 2013 y 2019, varias Guías CCN-STIC.

Ha participado en la adecuación al Esquema Nacional de Seguridad de una multiplicidad de organizaciones públicas y privadas de España.

Asimismo, es miembro del Foro Nacional de Ciberseguridad y miembro del equipo de redacción de Esquema Nacional de Certificación de Responsables de Ciberseguridad, auspiciado por dicho Foro.

Miembro delo equipo docente del Centro Criptológico Nacional, es presidente de la Agencia de Tecnología Legal, vicepresidente de la Comisión de Contratación Electrónica de la Asociación Nacional de Empresas de Internet, miembro del Observatorio Notarial para la Sociedad de la Información y miembro del Observatorio de la Mesa de la Justicia del Ilustre Colegio de Abogados de Madrid.

Ha recibido el primer Premio del Centro Criptológico Nacional por su contribución a lograr del Esquema Nacional de Seguridad un estándar de referencia.

2. LAS INFRAESTRUCTURAS CRÍTICAS Y SU CIBERSEGURIDAD EN EL MUNDO

3.1 Concepto y tipología

Aunque no existe una definición universalmente formalizada del concepto de **Infraestructura Crítica** o de **Infraestructura Crítica de Información**, propiciando con ello que cada país o cada comunidad política pueda acercarse a esta cuestión desde diferentes concepciones, no es menos cierto, sin embargo, que todas las aproximaciones vienen a coincidir en que se trata de infraestructuras (en el sentido más amplio, con componentes físicos y lógicos) que sustentan el desenvolvimiento político, económico y social de las sociedades occidentales y que, en consecuencia, su perturbación supondría una alteración grave para tales sociedades.

Aproximación de la Unión Europea

A nuestro entender, el paradigma que, de forma más completa y rigurosa ha tratado la protección de las Infraestructuras Críticas, especialmente en lo tocante a la ciberseguridad, es el modelo seguido por la Unión Europea (UE), que ha aunado bajo un único marco, aplicable a sus 27 estados miembros, la definición y regulación de la ciberseguridad de tales infraestructuras.

Efectivamente, la **Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas (ICE)**[1] y la evaluación de la necesidad de mejorar su protección, constituyó un primer paso en el proceso de identificación y designación de las ICE y de evaluación de la necesidad de mejorar su protección.

Como hemos señalado, existen en la UE y en el resto de un mundo cada vez más interconectado, una multiplicidad de Infraestructuras Críticas (IC) cuya perturbación o destrucción podrían tener repercusiones importantes, posiblemente con consecuencias transfronterizas intersectoriales derivadas de la interdependencia de las infraestructuras interconectadas, por lo que una de las primeras actividades que han acometido los países (y las comunidades políticas, como la Unión Europea), ha sido la identificación y designación de tales IC atendiendo a un procedimiento común, incluyendo las necesidades de seguridad para estas infraestructuras.

La citada Directiva 2008/114/CE -que, por su amplitud y rigurosidad, tomaremos como referente-, desarrolla los siguientes **conceptos**:

Infraestructura Crítica (IC)	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 y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones;
Información sensible sobre protección de infraestructuras críticas	Datos específicos sobre una infraestructura crítica que, de revelarse, podrían utilizarse para planear y actuar con el objetivo de provocar una perturbación o la destrucción de instalaciones de infraestructuras críticas;
Protección	Todas las actividades destinadas a garantizar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar una amenaza, riesgo o vulnerabilidad;

[1] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32008L0114

Propietarios u operadores de infraestructuras críticas europeas	Las entidades responsables de las inversiones o del funcionamiento diario de un elemento, sistema o parte del mismo, designado como ICE con arreglo a la Directiva.

La Directiva deja a la libre determinación de cada Estado Miembro de la UE la identificación, conforme al procedimiento establecido en su Anexo III, las ICE potenciales que se ajusten a los criterios horizontales y sectoriales y a las definiciones dadas.

Tomando como punto de partida el supuesto impacto de un incidente (como el caso, por ejemplo, de un ciberataque) que ponga en peligro el normal desenvolvimiento de las ICE, la Directiva señala una serie de **criterios horizontales** que deben considerarse para la determinación de las ICE, y que deberán incluir:

a) El número de víctimas (valorado en función del número potencial de víctimas mortales o de heridos);

b) El impacto económico (valorado en función de la magnitud de las pérdidas económicas o el deterioro de productos o servicios, incluido el posible impacto medioambiental);

c) El impacto público (valorado en función de la incidencia en la confianza de la población, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida de servicios esenciales).

Como decimos, los umbrales de tales criterios horizontales atenderán a la gravedad de las repercusiones en relación con la perturbación o destrucción de una infraestructura dada, dejando a cada Estado Miembro de la UE la determinación de estos criterios horizontales en función de la infraestructura crítica considerada, que informará anualmente a la Comisión Europea del número de infraestructuras por sector sobre las que se hayan determinado los umbrales de dichos criterios.

Por su parte, los **criterios sectoriales** tendrán en cuenta las características de los diferentes sectores de las ICE.

En el Anexo I de la Directiva se contiene la relación de sectores concernidos por la norma europea:

Lista de sectores con ICE

Sector	Subsector	
I Energía	1. Electricidad	Infraestructuras e instalaciones de generación y transporte de electricidad, en relación con el suministro de electricidad
	2. Petróleo	Producción de petróleo, refino, tratamiento, almacenamiento y distribución por oleoductos
	3. Gas	Producción de gas, refino, tratamiento, almacenamiento y transporte por gasoductos Terminales de GNL
II Transportes	4. Transporte por carretera 5. Transporte por ferrocarril 6. Transporte aéreo 7. Transporte por vías navegables interiores 8. Transporte marítimo (costero y de altura) y puertos	

En esta misma línea se pronuncia la **Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[2],** publicada en el DOUE el 19 de julio de ese mismo año, y que considera esencial que todos los Estados Miembros de la UE posean unas capacidades mínimas y una estrategia que garanticen un elevado nivel de seguridad de las redes y sistemas de información en su territorio, especialmente en lo tocante a lo que la norma europea definió como ***operadores de servicios esenciales*** y ***proveedores de servicios digitales***, lo que debe traducirse en la adopción de un conjunto de medidas de ciberseguridad exigibles a tales entidades, tendentes a mejorar el funcionamiento del mercado interior.

Los destinatarios últimos de esta Directiva (UE) 2016/1148 se muestran en el cuadro siguiente:

Operadores de servicios esenciales, de los sectores…[3]
Energía: electricidad, crudo y gas.
Transporte: aéreo, ferrocarril, marítimo y fluvial y carretera.
Banca.
Infraestructuras de los mercados financieros.
Sector sanitario: entornos de asistencia sanitaria (entre ellos hospitales y clínicas privadas).
Suministro y distribución de agua potable.
Infraestructura digital: IXP, Proveedores de servicios DNS y Registros de nombres de dominio de primer nivel.
Proveedores de servicios digitales

[2] https://eur-lex.europa.eu/legal-content/ES/LSU/?uri=CELEX:32016L1148

[3] Siempre que sean: a) una entidad presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales; b) la prestación de dicho servicio depende de las redes y sistemas de información, y c) un incidente tendría efectos perturbadores significativos en la prestación de dicho servicio.

Mercados en línea.
Motores de búsqueda en línea.
Servicios de computación en la nube.

Los **criterios para la identificación de los operadores esenciales** fueron:

a) Presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales;

b) La prestación de dicho servicio depende de las redes y sistemas de información, y

c) Un incidente tendría efectos perturbadores significativos en la prestación de dicho servicio.

	Comentario: **Como veremos más adelante, estos criterios han sido recogidos por una regulación argentina posterior. (Resolución 1523/2019. Definición de Infraestructuras Críticas.)**

Como señalamos en el Anexo I del presente documento, en el momento de redactar estos párrafos, las instituciones de la Unión Europea están desarrollando el borrador de lo que será la nueva Directiva, a la que informalmente se ha denominado **Propuesta de Directiva NIS2.0,** que refleja el deseo de la Comisión de extender el ámbito de aplicación de la norma europea a otros actores, tales como los suministradores de servicios o redes públicas de comunicación, los de contenidos o datos, los de plataformas de redes sociales y los dedicados a fomentar la confianza en los anteriores o a las Administraciones Públicas, los servicios postales, la gestión de aguas, el espacio, la alimentación, entre otros, eliminando la clasificación actual de *operadores de servicios esenciales* y *proveedores de servicios digitales*, sustituyéndolos por las denominaciones ***entidades esenciales*** y ***entidades importantes.***

A la fecha de redacción de estas líneas, la adscripción por sectores de las entidades contempladas en la Propuesta de Directiva NIS2.0 es la siguiente:

Entidades Esenciales	Entidades Importantes
- Energía (Electricidad, Calefacción y refrigeración urbana, Crudo, Gas, Hidrógeno) - Transporte (Aire, Ferrocarril, Agua, Carretera). - Banca. - Infraestructuras de los mercados financieros.	- Servicios postales y de mensajería. - Gestión de residuos. - Fabricación, producción y distribución de productos químicos. - Producción, transformación y distribución de alimentos. - Fabricación[5].

[5] Fabricación de productos sanitarios y productos sanitarios para diagnóstico in vitro; productos informáticos, electrónicos y ópticos; maquinaria y equipos n.c.o.p.; vehículos de motor, remolques y semirremolques y otro material de transporte.

- Salud. - Agua potable. - Aguas residuales. - Infraestructura Digital[4]. - Administraciones públicas. - Espacio.	- Proveedores digitales (Mercados en línea, Motores de búsqueda en línea, Plataformas de servicios de redes sociales.) - Investigación.

Aproximación de los Estados Unidos de Norteamérica

Esta determinación de los sectores que comprenden las IC es similar al realizado por la normativa de los **Estados Unidos de Norteamérica**.

Efectivamente, en los EEUU hay 16 sectores de infraestructuras críticas cuyos activos, sistemas y redes, ya sean físicos o virtuales, se consideran tan vitales para los Estados Unidos que su incapacidad o destrucción tendría un efecto debilitador sobre la seguridad, la seguridad económica nacional, la salud pública nacional o la seguridad, o cualquier combinación de ellas, según dispone la *Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure,* que sustituye a la *Homeland Security Presidential Directive*[6].

Estos sectores son:

1. Sector Químico
2. Sector de las Instalaciones Comerciales.
3. Sector de las Comunicaciones.
4. Sector de la Fabricación Crítica.
5. Sector de Embalses y Presas.
6. Sector de la Industria de la Defensa.
7. Sector de Servicios de Emergencia.
8. Sector de la Energía.
9. Sector de los Servicios Financieros.
10. Sector de Alimentación y Agricultura.
11. Sector de las Instalaciones Gubernamentales.
12. Sector de Sanidad y Salud Pública.
13. Sector de las Tecnologías de la Información.
14. Sector de la Industria Nuclear, Materiales y Residuos.

[4] Entre ellas: - Proveedores de Puntos de Intercambio de Internet - Proveedores de servicios de DNS, excluidos los operadores de servidores de nombres raíz - Registros de nombres de TLD - Proveedores de servicios de computación en la nube - Proveedores de servicios de centros de datos - Proveedores de redes de entrega de contenidos - Proveedores de servicios de confianza a los que se refiere el punto (19) del artículo 3 del Reglamento (UE) n.º 910/2014(1) - Proveedores de redes públicas de comunicaciones electrónicas a los que se refiere el punto (8) del artículo 2 de la Directiva (UE) 2018/1972(2) o proveedores de servicios de comunicaciones electrónicas a los que se refiere el punto (4) del artículo 2 de la Directiva (UE) 2018/1972 cuando sus servicios estén disponibles al público. Gestión de servicios de TIC (B2B); Gestión de servicios de TIC (B2B); Proveedores de servicios gestionados (MSP) - Proveedores de servicios de seguridad gestionados (MSSP).

[6] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

15. Sector de los Sistemas de Transporte.
16. Sector del Agua Potable y Aguas Residuales.

	Comentario: **Como veremos más adelante, estos sectores han sido recogidos por una regulación argentina posterior. (Resolución 1523/2019. Definición de Infraestructuras Críticas.)**

La gobernanza de la ciberseguridad de las IC asignadas a estos sectores ha sido distribuida de la siguiente forma:

- El Department of Homeland Security (Departamento de Seguridad Nacional) ha sido designado como Agencia de Gestión de Riesgos para los sectores 1, 2, 3, 4, 5, 7, 11, 13, 14 y 15.
- El Departamento de Defensa ha sido designado como Agencia de Gestión de Riesgos para el sector 6.
- El Departamento de Energía ha sido designado como Agencia de Gestión de Riesgos para el sector 8.
- El Departamento del Tesoro ha sido designado como Agencia de Gestión de Riesgos para el sector 9.
- El Departamento de Agricultura ha sido designado como Agencia de Gestión de Riesgos para el sector 10.
- El Departamento de Salud y Servicios Humanos ha sido designado como Agencia de Gestión de Riesgos para el sector 12.
- La Agencia de Protección del Medio Ambiente ha sido designada Agencia de Gestión de Riesgos para el sector 16.

De la lista anterior puede observarse claramente la importancia que la legislación norteamericana confiere al Department of Homeland Security (DHS) en las misiones relativas a (ciber)seguridad.

Efectivamente, el DHS es el departamento ejecutivo del gobierno federal de Estados Unidos responsable de la seguridad pública. Entre sus funciones están la lucha contra el terrorismo, la seguridad fronteriza, inmigración y aduanas, la ciberseguridad y la gestión y prevención ante desastres. Comenzó a operar en 2003, creándose a partir de 24 agencias federales ya existentes, como respuesta a los atentados del 11 de septiembre de 2001.

Aproximación del Reino Unido

Una lista similar de IC se encuentra recogida en la regulación del **Reino Unido**, a saber:

En el Reino Unido hay 13 sectores de Infraestructuras Nacionales Críticas:

- Productos químicos
- Civil Nuclear
- Comunicaciones
- Defensa

- Servicios de emergencia
- Energía
- Finanzas
- Alimentación
- Gobierno
- Salud
- Espacio
- Transporte
- Agua

El gobierno británico define las infraestructuras críticas del Reino Unido como: "Aquellos elementos críticos de la Infraestructura (instalaciones, sistemas, sitios, propiedades, información, personas, redes y procesos), cuya pérdida o compromiso tendría un impacto perjudicial importante en la disponibilidad, la prestación o la integridad de los servicios esenciales, provocando graves consecuencias económicas o sociales o la pérdida de vidas".

3.2 El Modelo de Gobernanza de la ciberseguridad de las IC

El modelo de gobernanza de la ciberseguridad de las IC pasa por considerar dos aspectos esenciales: el **marco legal** que regula la ciberseguridad de las IC y las **instituciones** que, al amparo de dicho marco legal, se encargan de ejecutar las acciones correspondientes.

El Anexo I del presente documento desarrolla estos dos elementos, para una serie de países considerados.

En general, todas las estructuras de gobierno de la ciberseguridad de los países occidentales poseen, en mayor o menor medida, con mayor o menor desarrollo, los elementos que se señalan en los epígrafes siguientes:

3.2.1 Marco regulatorio

Que comprende toda legislación aprobada conforme a los principios legislativos del país de que se trate (o de una determinada comunidad política, como es el caso de la Unión Europea), reguladora de la ciberseguridad nacional. Se trata de un elemento indispensable, que debe regular la ciberseguridad desde tres puntos de vista:

- **Nivel Nacional**: con la publicación de una Estrategia de Ciberseguridad Nacional.
- **Nivel Gubernamental o del Sector Público**: con la publicación de la legislación necesaria para garantizar la ciberseguridad de los sistemas de información de las entidades del sector público.
- **Nivel Sectorial**: con la publicación de la legislación necesaria para la garantizar la ciberseguridad de los sistemas de información de los diferentes sectores críticos definidos.

3.2.2 Marco institucional

Desarrollado en tres niveles:

Nivel (I) - Estratégico:

Mediante la constitución de un órgano estratégico, que debe estar situado en dependencia directa de las más altas instancias ejecutivas del país (Jefatura del gobierno), y que estará encargado de fijar la estrategia nacional en materia de ciberseguridad.

	Comentario: **Sobre este particular, en Argentina encontramos el Comité de Ciberseguridad (creado por Decreto 577/2017 del Poder Ejecutivo Nacional), como veremos más adelante.**

En algunos países considerados en el Anexo I del presente documento (por ejemplo, España), este órgano ha tomado la forma de **Consejo Nacional de Ciberseguridad**, como órgano colegiado dependiente de un órgano superior (Consejo de Seguridad Nacional) y de asistencia al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional en el ámbito de la ciberseguridad.

Este órgano tendrá la misión esencial de materializar la antedicha Estrategia de Ciberseguridad Nacional, desarrollando los correspondientes planes y líneas de acción derivados. Estos planes derivados deberán abordar distintos aspectos de la ciberseguridad como incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en la Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional, la investigación y persecución del ciberterrorismo, el ciberspionaje y la ciberdelicuencia, así como la ciberseguridad en el sector privado o la cultura de ciberseguridad.

Nivel (II) - Ejecutivo:

Mediante la constitución de un órgano encargado de materializar las instrucciones emanadas del órgano superior.

En algunos países, esta responsabilidad está compartimentada en varias instituciones, cada una de ellas responsable de un sector específico. Así, por ejemplo, en algunos países de los considerados en el Anexo I del presente documento (por ejemplo, Reino Unido, Francia o España), este órgano ha tomado la forma de un **Centro Nacional de Ciberseguridad**, al objeto de identificar, analizar y tratar las ciberamenazas nacionales[7].

Este, así llamado, Centro Nacional de Ciberseguridad -cuyas responsabilidades deben establecerse en la respectiva Estrategia de (Ciber)Seguridad Nacional y en las decisiones del Consejo de Seguridad Nacional, que preside el Presidente del Gobierno o Primer Ministro-, ayuda a proteger los servicios críticos del Estado frente a los ciberataques, gestiona los incidentes importantes y mejora la seguridad subyacente de la Internet del país de que se trate, mediante la mejora tecnológica y el asesoramiento a los ciudadanos y las organizaciones, apoyando a las organizaciones más críticas del país, al sector público en general, a la industria y a las pequeñas y medianas empresas (PYMES).

[7] Por ejemplo, la misión de ciberseguridad del Reino Unido está dirigida por el National Cyber Security Centre (NCSC, https://www.ncsc.gov.uk/), que forma parte del Government Communications Headquarters (GCHQ, https://www.gchq.gov.uk/)

	Comentario: **Sobre este particular, en Argentina encontramos la Dirección Nacional de Ciberseguridad, como veremos más adelante.**

En algunos países (Reino Unido, por ejemplo) se ha habilitado dentro de este Centro Nacional de Ciberseguridad una unidad específica en materia de Protección de Infraestructuras Críticas (el **CNI hub-*Critical National Infraestructure***[8]), cuyo ámbito de aplicación se extiende tanto a las IC públicas como privadas.

Una vez constituida, la unidad específica para la Protección de las IC en materia de ciberseguridad, suele tener las siguientes **atribuciones**:

1. Asesoramiento, apoyo y orientación: proporcionando asesoramiento técnico en todos los sectores de las IC, desarrollando y compartiendo consejos y orientaciones autorizados en respuesta a los desafíos únicos de las organizaciones IC. Esto puede abarcar desde el suministro de orientación sobre las mejores prácticas hasta la dedicación de apoyo para trabajar mano a mano con los socios en sus problemas más difíciles.
2. Grupos y eventos de confianza: creando y participando en grupos de trabajo y eventos de confianza en todos los sectores de las IC. Estos foros proporcionan un espacio único y comercialmente seguro para reunir a los organismos gubernamentales e industriales junto con el mundo académico y los reguladores dentro de los sectores IC del país de que se trate para apoyar y desarrollar las mejores prácticas de ciberseguridad.
3. Servicios de apoyo: garantizando que los proveedores de ciberseguridad de las organizaciones IC cumplen las normas aprobadas a través de nuestros esquemas oficiales de garantía. Apoyando también directamente las respuestas de las organizaciones a incidentes cibernéticos significativos.
4. Colaboración con la industria: trabajando estrechamente con las organizaciones IC para compartir conocimientos a través de los programas nacionales que puedan desarrollarse al efecto, acogiendo a la industria para que trabaje en el Centro Nacional de Ciberseguridad y colocando recursos del centro Nacional de Ciberseguridad en las organizaciones IC, como parte de los planes de desarrollo de habilidades.
5. Apoyo a la política y la regulación: proporcionando asesoramiento y asistencia a aquellos reguladores nacionales que supervisan la ciberseguridad en los sectores de las IC. Para ello pueden usarse un **Esquema de Evaluación y Certificación de la Ciberseguridad** (como el Esquema Nacional de Seguridad, en el caso de España[9]), como ayuda a las organizaciones a evaluar su ciberseguridad, pudiendo utilizarse por los reguladores para verificar que se cumplen los requisitos legales y reglamentarios. Además, este Centro Nacional de Ciberseguridad debe colaborar con los departamentos gubernamentales del país de que se trate para ayudarles a desarrollar la ciberpolítica relacionada con las IC nacionales.
6. Inteligencia sobre amenazas: proporcionando una fuente única de información sobre amenazas, tanto táctica como estratégica, que va desde informes técnicos de duración

[8] https://www.cni-hub.com/
[9] https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191

crítica hasta análisis estratégicos de la amenaza cambiante a las IC, compartiéndolos a través de múltiples canales, públicos o a través de compromisos individuales.

7. Seguridad en las nuevas tecnologías: prestando apoyo a las tecnologías nuevas y emergentes, teniendo como objetivo aumentar la comprensión de los proyectos actuales nacionales, aumentar la concienciación de las ciberamenazas para estas tecnologías y crear normas mínimas de seguridad para tales tecnologías.
8. Seguridad de los proveedores clave de las IC: apoyando a los proveedores clave, como los proveedores de servicios gestionados (MSP), que albergan y gestionan los datos informáticos de sus clientes o prestan servicios empresariales y de gestión a las IC nacionales.

	Comentario: **Sobre este particular, en Argentina encontramos la Dirección Nacional de Infraestructuras Críticas de la Información y Ciberseguridad, como veremos más adelante.**

En ocasiones, este Centro Nacional de Ciberseguridad suele ser asimismo responsable del CSIRT Nacional, como elemento para garantizar una respuesta eficaz a los incidentes y ciberataques para minimizar los daños, ayudando a la recuperación y aprendiendo lecciones para el futuro.

Nivel (III) – Táctico - Respuesta a Incidentes de Seguridad (CSIRT):

Mediante la constitución de un órgano encargado de atender de forma armonizada los incidentes de seguridad que le sean reportados.

Pueden existir varias de estas entidades, atendiendo a los sectores implicados o a los diferentes tipos de administración pública (estatal o regional, habitualmente).

	Comentario: **Sobre este particular, en Argentina encontramos el CERT.AR, como veremos más adelante.**

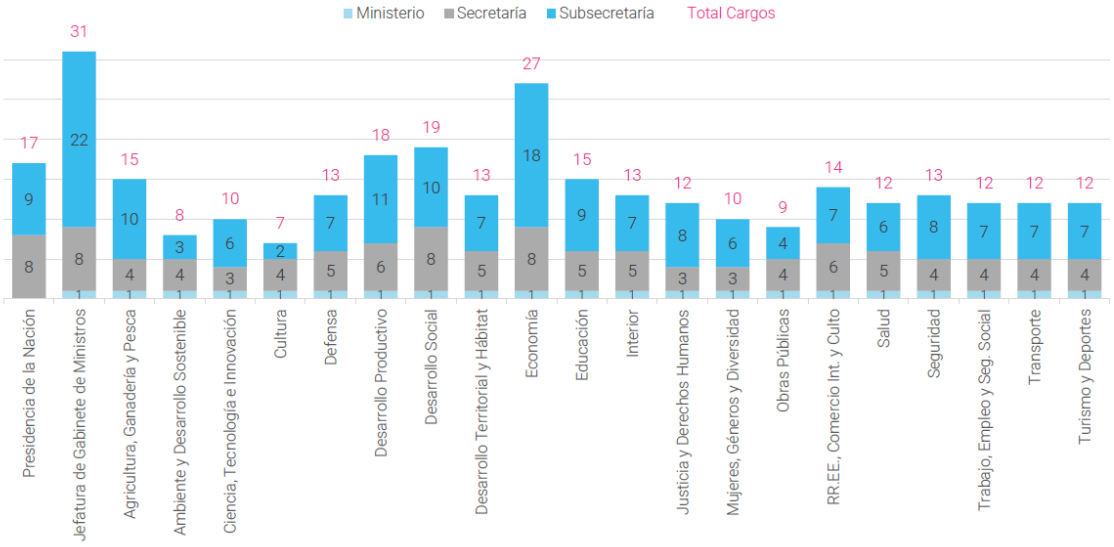
3. LA ESTRUCTURA ORGANIZATIVA DE LA ADMINISTRACIÓN PÚBLICA NACIONAL CENTRALIZADA DE LA ARGENTINA

Las normas esenciales que regulan la estructura de la Administración Pública de la Argentina son:

- El Decreto Nacional 7/2019, de 10 de diciembre de 2019, del Poder Ejecutivo Nacional, regula la Ley de Ministerios.
- El Decreto Nacional 50/2019, de 19 de Diciembre de 2019, del Poder Ejecutivo Nacional, aprueba el organigrama de aplicación de la Administración Nacional Centralizada hasta el nivel de Subsecretaría.

En su *Informe sobre la Estructura Organizativa de la Administración Pública Nacional Centralizada (APN Central) – Autoridades Superiores (AS)*[10], de la Dirección Nacional de Diseño Organizacional de la Jefatura de Gabinete de Ministros, las unidades según su jerarquía organizacional son las mostradas seguidamente.

[10] Enero, 2022.



** A fines analíticos se contabiliza como Ministro al Jefe de Gabinete de Ministros, si bien el Art. 1º del Decreto DNU Nº 7/2019 establece la conformación de 20 ministerios.*
** Incluye Ministros, Secretarios y Subsecretarios. No se contabilizan al Presidente ni a la Vicepresidenta de la Nación.*

El art. 1 del Decreto 7/2019 (Ley de Ministerios) señala que -tras el Presidente de la Nación Argentina-, la estructura orgánica se configura con "El Jefe de Gabinete de Ministros y VEINTE (20) Ministros Secretarios o Ministras Secretarias tendrán a su cargo el despacho de los negocios de la Nación."[11]

Cada Ministerio podrá proponer al Poder Ejecutivo Nacional la creación de las Secretarías o Subsecretarías que estime necesario de conformidad con las exigencias de sus respectivas áreas de competencia. Las funciones de dichas Secretarías o Subsecretarías serán determinadas por decreto. (art. 8).

Por su importancia para el propósito del presente Informe, el art. 16 de la Ley de Ministerios señala las **atribuciones del Jefe de Gabinete de Ministros. Se subrayan aquellas que pueden tener relación, directa o indirecta, con la gestión de la ciberseguridad pública**:

1. Cumplir y hacer cumplir la Constitución Nacional y la legislación vigente.
2. <u>Ejercer la administración general del país y asistir al Presidente de la Nación</u> en la conducción política de dicha administración.
3. <u>Ejercer las atribuciones de administración que le delegue el Presidente de la Nación</u>, respecto de los poderes propios de éste.
4. Entender en la organización y convocatoria de las reuniones y acuerdos de gabinete, coordinando los asuntos a tratar.
5. <u>Coordinar y controlar las actividades de los Ministerios</u> y, de las distintas áreas a su cargo realizando su programación y control estratégico, a fin de obtener coherencia en el accionar de la administración e incrementar su eficacia.
6. <u>Coordinar las relaciones del Poder Ejecutivo Nacional con ambas Cámaras del Honorable Congreso de la Nación</u>, sus Comisiones e integrantes, en cumplimiento de las atribuciones

[11] Los Ministerios recogidos en la norma son: Del Interior, De Relaciones Exteriores, Comercio Internacional y Culto, De Defensa, De Economía, De Desarrollo Productivo, De Agricultura, Ganadería y Pesca, De Transporte, De Obras Públicas, De Justicia y Derechos Humanos, De Seguridad, De Salud, - De Desarrollo Social, De las Mujeres, Géneros y Diversidad, De Educación, De Cultura, De Ciencia, Tecnología e Innovación, De Trabajo, Empleo y Seguridad Social, De Ambiente y Desarrollo Sostenible, - De Turismo y Deportes y De Desarrollo Territorial y Hábitat.

que le asigna la Constitución Nacional procurando la mayor fluidez en dichas relaciones y el más pronto trámite de los mensajes del Presidente de la Nación que promuevan la iniciativa legislativa.
7. Producir los informes mensuales que establece el artículo 101 de la Constitución Nacional, relativos a la marcha del Gobierno, y los demás que le fueren requeridos por las Cámaras del Congreso.
8. Dictar Decisiones Administrativas, referidas a los actos y reglamentos que sean necesarios para ejercer las facultades que le atribuye la Constitución Nacional y aquellas que le delegue el Presidente de la Nación, con el refrendo del Ministro Secretario que corresponda en razón de la materia.
9. Presentar al Honorable Congreso de la Nación, junto con los Ministros Secretarios, la memoria anual detallada del estado de la Nación en lo relativo a los negocios de los Ministerios.
10. Hacer recaudar las rentas de la Nación.
11. Intervenir en la elaboración y control de ejecución de la Ley de Presupuesto, como así también en los niveles del gasto y de los ingresos públicos, sin perjuicio de la responsabilidad primaria del Ministro Secretario del área y de la supervisión que al Presidente de la Nación compete en la materia.
12. Requerir de los Ministros Secretarios, Secretarios y demás funcionarios de la Administración Pública Nacional la información necesaria para el cumplimiento de su función específica y de las responsabilidades emergentes de los artículos 100, incisos 10 y 11, y 101 de la Constitución Nacional, la que deberá producirse dentro del plazo que a tal efecto establezca.
13. Asistir al Presidente de la Nación en el análisis de los mensajes que promueven la iniciativa legislativa, en particular los proyectos de Ley de Ministerios y de Presupuesto que deberán ser tratados en Acuerdo de Gabinete, y de los proyectos de ley sancionados por el Congreso Nacional.
14. Asistir al Presidente de la Nación en el dictado de instrucciones y reglamentos que sean necesarios para la ejecución de las leyes de la Nación y de los decretos que dispongan la prórroga de las sesiones ordinarias o la convocatoria a extraordinarias del Congreso de la Nación.
15. Coordinar y controlar la ejecución de las delegaciones autorizadas a los Ministros Secretarios.
16. Velar por el cumplimiento de las decisiones que emanen del Poder Judicial en uso de sus atribuciones.
17. Participar en la definición de prioridades vinculadas con el financiamiento proveniente de organismos internacionales, multilaterales y bilaterales de desarrollo.
18. Coordinar el seguimiento de la relación fiscal entre la Nación, las provincias y la Ciudad Autónoma de Buenos Aires.
19. Entender en la evaluación y priorización del gasto, efectuando el diagnóstico y seguimiento permanente de sus efectos sobre las condiciones de vida de la población.
20. Entender en la distribución de las rentas nacionales, según la asignación de Presupuesto aprobada por el Congreso, y en su ejecución.
21. Intervenir en los planes de acción y los presupuestos de las sociedades del Estado, entidades autárquicas, organismos descentralizados o desconcentrados y cuentas y fondos especiales, cualquiera sea su denominación o naturaleza jurídica en su área; así como en su intervención, liquidación, cierre, privatización, fusión, disolución o centralización.
22. Entender en la formulación, ejecución y control de las políticas de comunicación social y de medios de comunicación social, en particular a la difusión de opciones educativas.

23. Entender en la difusión de la actividad del Poder Ejecutivo Nacional, como así también la difusión de los actos del Estado Nacional a fin de proyectar la imagen del país en el ámbito interno y externo.
24. Administrar y controlar los medios de difusión que se encuentran bajo la responsabilidad del Poder Ejecutivo Nacional y aquellas empresas del sector en las que la jurisdicción sea accionista.
25. Entender en la administración y operación del "PARQUE TECNÓPOLIS DEL BICENTENARIO, CIENCIA, TECNOLOGÍA, CULTURA Y ARTE".
26. Entender en la administración y operación del "CENTRO CULTURAL KIRCHNER" y "CASAS DE CONTENIDOS FEDERALES".
27. Entender en la aplicación de los tratados internacionales relacionados con los temas de su competencia, e intervenir en la formulación de convenios internacionales en los asuntos propios de su área.
28. Entender en el lineamiento de las políticas referentes a Medios Públicos Nacionales y su instrumentación.
29. Participar en la aplicación de la política salarial del sector público, con participación de los Ministerios y organismos que correspondan.
30. Entender en la elaboración, registro, seguimiento, evaluación y planificación de los proyectos de inversión pública y en el control de la formulación, registro, seguimiento y evaluación de esos proyectos cuando sean ejecutados a través de contratos de participación público-privada en los términos de la Ley N° 27.328
31. Entender en el análisis y propuesta del diseño de la estructura de la Administración Nacional Centralizada y Descentralizada y aprobar las modificaciones propuestas.
32. Garantizar el efectivo ejercicio del derecho de acceso a la información pública y controlar la aplicación de la Ley N° 25.326 de Protección de los Datos Personales.
33. Entender en el diseño y ejecución de políticas relativas al empleo público, a la innovación de gestión, a la modernización de la Administración Pública Nacional, al régimen de compras y contrataciones, a las tecnologías de la información, las telecomunicaciones, los servicios de comunicación audiovisual y los servicios postales.
34. Entender en la organización, dirección y fiscalización del registro de empresas contratistas de obras públicas y de consultorías.
35. Entender en el diseño y ejecución de políticas públicas para la prevención y tratamiento relacionadas con el consumo de sustancias psicoactivas.

Comentario:
De lo anterior (atribución 5) se desprende que el Jefe de Gabinete de Ministros se configura como una suerte de "primer ministro" o, mejor aún, de un *primus inter pares.*
No obstante, se hace notar que (atribución 8) el dictado de Decisiones Administrativas, referidas a los actos y reglamentos que sean necesarios para ejercer las facultades que le atribuye la Constitución Nacional y aquellas que le delegue el Presidente de la Nación, requieren el refrendo del Ministro Secretario que corresponda en razón de la materia.

Como decimos, el citado Decreto Nacional 50/2019 (y sus posteriores modificaciones) recoge la estructura de la Administración Pública Nacional.

Destacamos el art. 4 de este Decreto, que establece que el/la Jefe/a de Gabinete de Ministros y los Secretarios y las Secretarias de la Presidencia de la Nación podrán solicitar al Presidente de la Nación la creación de los cargos extraescalafonarios que resulten necesarios para el cumplimiento de las funciones asignadas a sus Jurisdicciones y a las Entidades actuantes en su órbita.

Por su importancia para el presente Informe, recogemos lo que este Decreto Nacional prescribe en relación con la Jefatura de Gabinete de Ministros[12], a saber: la Jefatura de Gabinete de Ministros está compuesta por las siguientes Secretarías y Subsecretarías, incluyendo los objetivos que la ley confiere a tales unidades.

Por su importancia para el presente Informe, se resaltan en gris las unidades y objetivos de la Secretaría de Innovación Pública. (Los subrayados son nuestros y pretenden resaltar objetivos concretos que podrían tener una repercusión significativa en materia de ciberseguridad pública):

Secretarías	Subsecretarías	Objetivos
UNIDAD GABINETE DE ASESORES		1. Coordinar el Gabinete de Asesores del Jefe de Gabinete de Ministros. 2. Entender en la coordinación integral de los circuitos destinados a dar adecuada y rápida respuesta a las cuestiones priorizadas por el Jefe de Gabinete de Ministros. 3. Entender y asistir al Jefe de Gabinete de Ministros en todas las cuestiones vinculadas a los aspectos logísticos y administrativos propios del desarrollo de sus funciones institucionales. 4. Asistir al Jefe de Gabinete de Ministros en materia de relaciones institucionales, comunicación y prensa. 5. Entender en la definición de los procedimientos de evaluación y seguimiento de los planes, programas y proyectos de la Jefatura de Gabinete de Ministros, la optimización de la gestión de los mismos, el intercambio y evaluación de impacto en la implementación de las políticas. 6. Entender en el diseño, elaboración, definición de ajustes y actualizaciones de instrumentos, herramientas y procedimientos tendientes a posibilitar la disponibilidad de insumos de información en coordinación con las áreas competentes
SECRETARÍA DE COORDINACIÓN ADMINISTRATIVA	Subsecretaría legal	1. Asistir al Jefe de Gabinete de Ministros en el diseño de la política presupuestaria de la Jurisdicción y en la evaluación de su cumplimiento. 2. Asistir al Jefe de Gabinete de Ministros en la formulación y programación de la ejecución

[12] Recogiendo las modificaciones operadas por el Decreto N° 139/2021 B.O. 5/3/2021.

		presupuestaria de las unidades ejecutoras de las distintas categorías programáticas, y en las modificaciones que se proyecten durante el ejercicio financiero. 3. Dirigir y coordinar el desarrollo de las actividades de apoyo legal, técnico y administrativo del Ministerio. 4. Asistir al Jefe de Gabinete de Ministros en la realización de los trámites administrativos relacionados con la gestión de los recursos humanos y la obtención de materiales, equipamientos tecnológicos y de todo otro insumo necesario para las unidades ejecutoras de las distintas categorías programáticas. 5. Coordinar, monitorear y supervisar las acciones que hacen al desarrollo de las tareas relacionadas con los aspectos económicos, financieros, contables, patrimoniales, de sistemas informáticos y de control de gestión de la Jurisdicción. 6. Entender en la administración y desarrollo de los recursos humanos de la Jurisdicción, y en la instrucción de los sumarios administrativos y disciplinarios de la Jurisdicción. 7. Entender en la gestión documental de la Jurisdicción y en el seguimiento y archivo de todos los actos administrativos dictados por el Jefe de Gabinete de Ministros y por los titulares de las distintas dependencias de la Jurisdicción, como así también de toda la documentación administrativa vinculada con la actividad sustantiva de la misma. 8. Entender en la ejecución operativa y de los procesos de gestión administrativa, presupuestaria y financiera-contable de programas, proyectos, cooperaciones técnicas, donaciones y asistencias técnicas con financiamiento externo.
SECRETARÍA DE GESTIÓN Y EMPLEO PÚBLICO	• Subsecretaría de Empleo Público • Subsecretaría de Fortalecimiento Institucional • Instituto nacional de la administración pública (INAP)	**SECRETARÍA DE GESTIÓN Y EMPLEO PÚBLICO** 1. Asistir al Jefe de Gabinete de Ministros en la implementación de las políticas relativas a la mejora estratégica de los recursos humanos y su capacitación, la política salarial, la promoción y en el desarrollo de carrera de los agentes de la Administración Pública Nacional, y en la propuesta de las normas reglamentarias en la materia. 2. Entender en la formulación de las políticas nacionales en materia de recursos humanos, gestión del empleo público, evaluaciones de desempeño, compensaciones y monitoreos, en el ámbito de su competencia. 3. Asistir al Jefe de Gabinete de Ministros en la aplicación de la política salarial en el marco de los límites presupuestarios establecidos por la ley.

		4. Intervenir en el análisis y aprobación de las medidas relativas a la política salarial de la Administración Pública Nacional y de los sistemas de incentivos del empleo público. 5. Desarrollar programas de asistencia a los organismos del Sector Público Nacional y a las provincias que así lo requieran, que tengan por objeto la optimización de la gestión del empleo público, en coordinación con los organismos competentes en la materia. 6. Entender en la interpretación de la normativa de empleo público, en el ámbito de su competencia. 7. Entender en la sistematización de los procesos de administración de los recursos humanos: liquidación de salarios, justificación de inasistencias, otorgamiento y convalidación de licencias y protección de la salud en el trabajo en coordinación con la Subsecretaría de Innovación Administrativa de la Secretaría de Innovación Pública. 8. Asistir al Jefe de Gabinete de Ministros en la temática de gestión y empleo público concerniente al Consejo Federal de la Función Pública (COFEFUP). (Objetivo sustituido por art. 4º del Decreto Nº 606/2020 B.O. 21/7/2020) 9. Asistir al Jefe de Gabinete de Ministros en el diseño, desarrollo e implementación de las políticas de capacitación y carrera administrativa para el personal de la Administración Pública Nacional. 10. Entender en la elaboración de planes y programas tendientes a la vinculación y la cooperación técnico-académica en el ámbito de su competencia, con universidades nacionales e internacionales, Entidades y/o centros académicos, de formación y/o investigación, organismos internacionales y organizaciones de la sociedad civil. 11. Asistir al Jefe de Gabinete de Ministros en la formulación e implementación de políticas de fortalecimiento del empleo público en el Sector Público Nacional y de la normativa aplicable en materia de relaciones laborales. 12. Representar al Estado Nacional en las negociaciones colectivas en las cuales el Estado Nacional sea parte, en coordinación con otras Jurisdicciones competentes. 13. Integrar las Comisiones Negociadoras que se constituyan en el marco de la Ley N° 14.250, en las que intervengan organismos descentralizados,

		comprendiendo en estos últimos a las instituciones de seguridad social y entes estatales o empresas y Sociedades del Estado, como parte del sector empleador. 14. Asesorar y/o intervenir frente a requerimientos, consultas o presentaciones efectuadas por parte de Entidades gremiales, estableciendo un criterio uniforme para toda la Administración Pública Nacional. 15. Asistir al Jefe de Gabinete de Ministros en los procesos de resolución de conflictos individuales o colectivos del personal del Sector Público Nacional en materia de relaciones laborales. 16. Ejercer la representación del Estado empleador en el Consejo de Administración del Fondo Permanente de Capacitación y Recalificación Laboral (FOPECAP) y asistir técnicamente en la formulación y evaluación de los programas académicos a financiar por el Fondo Permanente de Capacitación y Recalificación Laboral (FOPECAP). 17. Asistir al Jefe de Gabinete de Ministros en el diseño, desarrollo e implementación de políticas públicas que fortalezcan la integridad en la función pública y prevengan la corrupción, en coordinación con los organismos del Estado Nacional con competencias en la materia. 18. Asistir al Jefe de Gabinete de Ministros en la definición de lineamientos estratégicos para la realización de programas dirigidos a mejorar la gestión sobre la base de la implementación de la gestión por resultados y la planificación estratégica en las Jurisdicciones y Entidades del Sector Público Nacional. 19. Asistir al Jefe de Gabinete de Ministros en el diseño e implementación de programas que propendan a la mejora de los servicios al ciudadano, propiciando la mejora de la calidad en la gestión de los organismos públicos. 20. Asistir al Jefe de Gabinete de Ministros en el diseño, desarrollo e implementación de programas de optimización de procesos y procedimientos en las Jurisdicciones y Entidades del Sector Público Nacional. **SUBSECRETARÍA DE EMPLEO PÚBLICO** 1. Asistir a la Secretaría en la planificación y formulación de políticas nacionales en materia de recursos humanos y gestión de la política salarial. 2. Promover la realización de programas dirigidos a mejorar la gestión del empleo público en los organismos

		del Sector Público Nacional, brindando asistencia técnica en la materia. 3. Implementar las políticas de evaluación de desempeño de los recursos humanos del Estado, y controlar la correcta ejecución de las políticas de selección y reclutamiento de personal. 4. Supervisar el análisis de la información vinculada a la evolución del empleo público, el diseño y la administración de la política salarial del personal de la Administración Pública Nacional. 5. Asistir en la sistematización de los procesos de administración de los recursos humanos tales como, liquidación de salarios, justificación de inasistencias, otorgamiento y convalidación de licencias y protección de la salud en el trabajo. 6. Colaborar con los gobiernos provinciales y municipales en el desarrollo de capacidades de gestión de empleo público. 7. Asesorar a la Secretaría sobre las normas, doctrina y criterios jurisprudenciales relativos a la gestión de las relaciones laborales en el ámbito del Sector Público Nacional. 8. Asistir a la Secretaría en la interpretación y el control en la aplicación de la normativa que rige las relaciones laborales de empleo público, realizando estudios y propuestas normativas, proponiendo acciones para revisar y consolidar la legislación referida. 9. Coordinar la implementación de mecanismos de interacción con las áreas vinculadas a la gestión de las relaciones laborales y de recursos humanos de las Jurisdicciones y Entidades del Sector Público Nacional. 10. Asistir a la Secretaría en las Comisiones Negociadoras que se constituyan en el marco de la Ley N° 14.250, en las que intervengan organismos descentralizados, comprendiendo en estos últimos a las instituciones de seguridad social y entes estatales o empresas y Sociedades del Estado, como parte del sector empleador. (Objetivo incorporado por art. 5º del Decreto Nº 606/2020 B.O. 21/7/2020) **SUBSECRETARÍA DE FORTALECIMIENTO INSTITUCIONAL** 1. Asistir a la Secretaría en el diseño, desarrollo e implementación de políticas públicas que fortalezcan la integridad en la función pública y prevengan la corrupción, en coordinación con los organismos del Estado Nacional con competencias en la materia.

		2. Diseñar y proponer lineamientos relacionados con el fortalecimiento institucional y la promoción de políticas de integridad en la función pública, en coordinación con las áreas con competencia del Estado Nacional. 3. Asistir a la Secretaría en el seguimiento de la implementación de las políticas de integridad y fortalecimiento institucional, y en la coordinación de su ejecución, en relación con los organismos del Estado Nacional con competencia en la materia. 4. Evaluar y consolidar la información originada en las Jurisdicciones cuyas competencias se encuentran vinculadas con los sistemas de control del sector público nacional, las políticas públicas de integridad y fortalecimiento institucional del Estado Nacional. 5. Desarrollar y administrar instrumentos de seguimiento y análisis referidos a las políticas públicas de integridad y fortalecimiento institucional en el ámbito de la Administración Pública Nacional. 6. Formular y desarrollar programas de fortalecimiento de las capacidades institucionales para la Administración Pública Nacional, con foco prioritario en la mejora de la calidad en la gestión y del servicio público. 7. Establecer pautas y criterios metodológicos para la implementación de un modelo de gestión por resultados en los organismos de la Administración Pública Nacional. 8. Formular y desarrollar las pautas e instrumentos metodológicos para la implementación de planes de reingeniería de procesos sustantivos y de apoyo administrativo para la Administración Pública Nacional. 9. Desarrollar y establecer las pautas e instrumentos metodológicos para la implementación de planes estratégicos y operativos en las organizaciones públicas. 10. Desarrollar pautas y lineamientos metodológicos para el seguimiento, monitoreo y evaluación de planes, programas y proyectos establecidos por las organizaciones públicas. 11. Diseñar programas de desarrollo y fortalecimiento de la cultura organizacional en las Jurisdicciones y Entidades de la Administración Pública Nacional. 12. Asistir técnicamente al Secretario, en su carácter de Autoridad de aplicación de la Ley N° 24.127 que instituye el Premio Nacional a la Calidad, en lo referido al sector público.

		INSTITUTO NACIONAL DE LA ADMINISTRACIÓN PÚBLICA (INAP) 1. Ejercer las funciones fijadas por la Ley N° 20.173 y sus normas modificatorias. 2. Aprobar, en su carácter de órgano rector del Sistema Nacional de Capacitación, los planes de capacitación y de formación propuestos por los Ministerios y organismos descentralizados, así como los créditos aplicables a la carrera administrativa. 3. Entender en la ejecución de la política de capacitación y formación para el personal de las distintas Jurisdicciones y Entidades del Sector Público Nacional, estableciendo pautas metodológicas y didácticas y brindar asistencia técnica a requerimiento de los gobiernos provinciales y municipales en el ámbito de su competencia. 4. Supervisar la operación y funcionamiento del Sistema Nacional de Capacitación, estableciendo normas de calidad de las acciones de formación, evaluando su impacto en el desempeño del personal y en las unidades organizativas en las que trabajen, en cumplimiento de los objetivos y metas de las distintas Jurisdicciones y Entidades. 5. Entender en el diseño y ejecución de programas de capacitación y de formación destinados a los funcionarios de nivel gerencial, en el ámbito de su competencia. 6. Entender en la acreditación, supervisión y evaluación de los planes, programas y acciones de formación y capacitación del Sector Público Nacional, en línea con la carrera administrativa. 7. Administrar los datos del registro de prestadores de servicios formativos. 8. Asistir técnicamente en la elaboración y/o desarrollo de programas de capacitación específicos e investigación a requerimiento de los gobiernos provinciales y municipales. 9. Promover y realizar estudios e investigaciones que releven buenas prácticas de administración pública y contribuyan a la mejora de la gestión y la innovación del Estado Nacional. 10. Coordinar la red nacional de documentación e información sobre Administración Pública, manteniendo un centro de referencia en materia de Administración Pública, resguardando en forma sistematizada la información y documentación correspondiente.

		11. (Objetivo derogado por art. 3° del Decreto N° 139/2021 B.O. 5/3/2021. Vigencia: a partir del día siguiente al de su publicación en el BOLETÍN OFICIAL.)
SECRETARÍA DE INNOVACIÓN PÚBLICA	• Subsecretaría de Gestión Administrativa de Innovación Pública • Subsecretaría de Gobierno Abierto y País Digital • Subsecretaría de Innovación Administrativa • Oficina Nacional de Contrataciones • Subsecretaría de Tecnologías de la Información y las Comunicaciones	**SECRETARÍA DE INNOVACIÓN PÚBLICA** 1. Diseñar, proponer y coordinar las políticas de innovación administrativa y tecnológica del Estado Nacional en sus distintas áreas, su Administración central y descentralizada, y determinar los lineamientos estratégicos y la propuesta de las normas reglamentarias en la materia. 2. Entender en el diseño de las políticas que promuevan la apertura e innovación y el gobierno digital, como principios de diseño aplicables al ciclo de políticas públicas en el Sector Público Nacional. 3. Intervenir en la definición de estrategias y estándares sobre tecnologías de la información, comunicaciones asociadas y otros sistemas electrónicos de tratamiento de información de la Administración Nacional. 4. Colaborar con las provincias y municipios en sus procesos de innovación administrativa y tecnológica, coordinando las acciones específicas de las Entidades del Poder Ejecutivo Nacional. 5. Diseñar, coordinar e implementar la incorporación y mejoramiento de los procesos, tecnologías, infraestructura informática y sistemas y tecnologías de gestión de la Administración Pública Nacional. 6. Proponer diseños en los procedimientos administrativos que propicien su simplificación, transparencia y control social, y elaborar los desarrollos informáticos correspondientes. 7. Actuar como Autoridad de Aplicación del régimen normativo que establece la infraestructura de firma digital estipulada por la Ley N° 25.506. 8. Intervenir en el desarrollo de sistemas tecnológicos con alcance transversal, o comunes a los organismos y entes de la Administración Pública Nacional, centralizada y descentralizada. 9. Entender en lo relativo a las políticas, normas y sistemas de compras del sector público nacional y supervisar las acciones desempeñadas por la Oficina Nacional de Contrataciones. 10. Intervenir en la formulación e implementación de las políticas en materia de inscripción y calificación de constructores y firmas consultoras de obras públicas y ejercer el contralor en todo lo relacionado con el accionar

		del Registro Nacional de Constructores y Firmas Consultoras de Obras Públicas. 11. Entender en la elaboración y en la ejecución de la política en materia de telecomunicaciones e intervenir en la elaboración de las estructuras arancelarias en materia de comunicaciones. 12. Entender en la elaboración de las políticas, leyes y tratados, y supervisar a los organismos y entes de control de los prestadores de los servicios en materia de comunicaciones y de las normas de regulación de las licencias, autorizaciones, permisos o registros de servicios de comunicaciones, o de otros títulos habilitantes pertinentes otorgados por el Estado Nacional o las provincias acogidas por convenios a los regímenes federales en la materia. 13. Entender en la elaboración, ejecución, fiscalización y reglamentación del régimen del servicio postal. 14. Entender en la promoción del acceso universal a las nuevas tecnologías como herramientas de información y conocimiento, como asimismo en la coordinación con las Provincias, las empresas y los organismos de su dependencia, en relación a la optimización del uso de las facilidades y redes existentes. 15. Administrar las participaciones del Estado en ARSAT S.A. y Correo Oficial de la República Argentina S.A. 16. Ejercer el control tutelar del Ente Nacional de Comunicaciones (ENACOM). 17.- Entender en la **ciberseguridad y protección de infraestructuras críticas de información y comunicaciones** asociadas del Sector Público Nacional y de los servicios de información y comunicaciones definidos en el artículo primero de la Ley Nº 27.078. (Objetivo incorporado por art. 4° del Decreto N° 139/2021 B.O. 5/3/2021. Vigencia: a partir del día siguiente al de su publicación en el BOLETÍN OFICIAL.) 18. Dirigir y supervisar el accionar de la Oficina Nacional de Tecnologías de Información (ONTI), promoviendo la integración de nuevas tecnologías, su compatibilidad e interoperabilidad de acuerdo con los objetivos y estrategias definidas en el Plan de Modernización del Estado. (Objetivo incorporado por art. 4° del Decreto N° 139/2021 B.O. 5/3/2021. Vigencia: a partir del día siguiente al de su publicación en el BOLETÍN OFICIAL.) 19.- Entender en la elaboración y ejecución de políticas vinculadas al desarrollo, uso y fomento del software público, su interoperabilidad, estandarización y

		reutilización por parte del Estado Nacional. (Objetivo incorporado por art. 4° del Decreto N° 139/2021 B.O. 5/3/2021. Vigencia: a partir del día siguiente al de su publicación en el BOLETÍN OFICIAL.) **SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA DE INNOVACIÓN PÚBLICA** 1. Atender las cuestiones vinculadas con la gestión económica, financiera, patrimonial, de infraestructura, de mantenimiento, administración de bienes muebles e inmuebles y de servicios de la Secretaría, en coordinación con las áreas pertinentes de la Secretaría de Coordinación Administrativa. 2. Entender en materia de administración y gestión de recursos humanos de la Secretaría, en coordinación con las áreas pertinentes de la Secretaría de Coordinación Administrativa. 3. Entender y planificar las acciones relativas a la gestión y administración de las tecnologías de la información de la Secretaría, en coordinación con las áreas pertinentes de la Secretaría de Coordinación Administrativa. 4. Entender en la gestión documental de la Secretaría. 5. Coordinar el asesoramiento jurídico permanente sobre aspectos específicos y funcionales de la Secretaría. 6. Coordinar los aspectos que guardan relación con cuestiones sumariales. 7. Entender en la ejecución operativa y en los procesos de gestión administrativa, presupuestaria y financiera-contable de programas, proyectos, cooperaciones técnicas, donaciones y asistencias técnicas con financiamiento externo, como así también en los proyectos de participación público-privada, en coordinación con las áreas pertinentes de la Secretaría de Coordinación Administrativa. 8. Coordinar la ejecución de los procedimientos de adquisiciones y contrataciones y de las actividades de auditoría y monitoreo de programas, proyectos, cooperaciones técnicas, donaciones y asistencias técnicas con financiamiento externo y/o proyectos de participación público-privada, en coordinación con las áreas pertinentes de la Secretaría de Coordinación Administrativa. **SUBSECRETARÍA DE GOBIERNO ABIERTO Y PAÍS DIGITAL** 1. Asistir en el desarrollo y coordinación de las políticas que promuevan la apertura e innovación y el gobierno

		digital como principios de diseño aplicables al ciclo de políticas públicas en el Sector Público Nacional. 2. Asistir a la Secretaría en el desarrollo de una estrategia nacional de gobierno abierto, en el marco de la agenda de innovación del Sector Público Nacional. 3. Desarrollar y coordinar las políticas, marcos normativos y plataformas tecnológicas necesarias para el gerenciamiento de la información pública. 4. Entender en el diseño, planificación y ejecución de la estrategia de apertura de datos e información pública del Sector Público Nacional. 5. Entender en la formulación y seguimiento del Plan de Acción Nacional de Gobierno Abierto, en el marco de la participación en la Alianza para el Gobierno Abierto. 6. Promover la realización de acuerdos bilaterales, multilaterales e interjurisdiccionales que favorezcan la apertura en el Sector Público Nacional, Provincial y Municipal, en coordinación con los organismos competentes. 7. Desarrollar y coordinar las políticas, marcos normativos y plataformas tecnológicas necesarias para promover la participación e innovación ciudadana en el proceso de formulación de políticas públicas. 8. Promover la creación de una red de innovación pública y gobierno abierto a nivel nacional generando espacios de trabajo colaborativo, intercambio y capacitación con el Sector Público Nacional, Provincial, de la Ciudad Autónoma de Buenos Aires y Municipal, el sector privado, académico y organizaciones de la sociedad civil. 9. Asistir a la Secretaría en la promoción de políticas, programas y acuerdos de innovación pública en el territorio nacional, en particular en las Jurisdicciones provinciales, municipales y en la Ciudad Autónoma de Buenos Aires. 10. Asistir a la Secretaría en la promoción de acuerdos federales y en el desarrollo de programas de asistencia técnica a los gobiernos provinciales, municipales, la Ciudad Autónoma de Buenos Aires y a otros poderes del Estado Nacional, en la implementación de los productos y programas que la Secretaría diseñe. 11. Simplificar, mejorar y digitalizar los principales trámites a nivel provincial, de la Ciudad Autónoma de Buenos Aires y municipal, gestionando una plataforma digital única, diseñada de forma personalizada y de acuerdo a los perfiles de los diferentes usuarios.

		12. Asistir a los gobiernos provinciales, municipales y a la Ciudad Autónoma de Buenos Aires en materia de estándares, normativas y procesos de innovación pública definidos por la Secretaría. 13. Supervisar el funcionamiento del Programa Punto Digital en todo el territorio nacional. 14. Coordinar la Mesa Ejecutiva responsable de la elaboración y ejecución del Plan de Acción anual de la AGENDA DIGITAL ARGENTINA, creada por el artículo 4° del Decreto N° 996/18. **SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA** 1. Promover y coordinar la aplicación de las nuevas tecnologías de Gestión Documental para la paulatina supresión del soporte papel como medio de almacenamiento y legalidad de los actos administrativos, en el ámbito del Sector Público Nacional, Municipal, Provincial y de otros poderes. 2. Coordinar el accionar de los referentes de tecnología y procesos de los organismos del Estado Nacional para la implementación de los Sistemas de Gestión Documental y su integración con sus sistemas verticales. 3. Supervisar la implementación de las iniciativas de innovación relativas a la gestión documental, procesos, servicios de tramitación a distancia y sistemas de autenticación electrónica de personas, en relación con los sistemas transversales centrales. 4. Asistir a los organismos del Sector Público Nacional en el diseño de políticas de innovación que tiendan a la mejora de los procesos, y coordinar acciones para lograr la ejecución de las mismas. 5. Intervenir en el marco regulatorio del régimen relativo a la validez legal del documento y firma digital, así como intervenir en aquellos aspectos vinculados con la incorporación de estos últimos a los circuitos de información del Sector Público Nacional y con su archivo en medios alternativos al papel. 6. Monitorear el cumplimiento de los estándares y normativas definidas por la Secretaría en las soluciones transversales que se propongan o implementen desde la Secretaría. 7. Entender en el desarrollo de tableros de reportes de sistemas transversales que se implementen en el ámbito de su competencia y proveer información a los organismos gubernamentales.

		OFICINA NACIONAL DE CONTRATACIONES 1. Proponer políticas de contrataciones y de organización del sistema, especialmente a fin de promover el estricto cumplimiento de los principios generales a los que debe ajustarse la gestión de las contrataciones públicas. 2. Desarrollar mecanismos que promuevan la adecuada y efectiva instrumentación de criterios de sustentabilidad ambientales, éticos, sociales y económicos en las contrataciones públicas. 3. Promover el perfeccionamiento permanente del Sistema de Contrataciones de la Administración Pública Nacional. 4. Diseñar, implementar y administrar los sistemas que sirvan de apoyo a la gestión de las contrataciones, los que serán de utilización obligatoria por parte de las Jurisdicciones y Entidades contratantes. 5. Diseñar, implementar y administrar un sistema de información en el que se difundirán las políticas, normas, sistemas, procedimientos, instrumentos y demás componentes del sistema de contrataciones de la Administración Nacional. 6. Administrar la información que remitan las Jurisdicciones y Entidades contratantes en cumplimiento de las disposiciones legales vigentes. 7. Administrar el sitio web en el que se difundan las políticas, normas, sistemas, procedimientos, instrumentos y demás componentes del Sistema de Contrataciones de la Administración Nacional. 8. Administrar y reglamentar el funcionamiento del Registro Nacional de Constructores de Obras Públicas creado por el artículo 13 de la Ley N° 13.064 y sus modificatorias, debiendo intervenir en la formulación e implementación de las políticas de inscripción y calificación de constructores y firmas consultoras de obras públicas y ejercer el contralor en todo lo relacionado con el accionar del citado Registro. 9. Administrar el Sistema Electrónico de Contrataciones. 10. Proyectar las normas legales y reglamentarias en la materia de su competencia. 11. Intervenir en forma previa y obligatoria en la elaboración de los proyectos de normas vinculados con el ámbito de su competencia producidos por otros organismos cuando las mismas resulten aplicables a todas

		o algunas de las Jurisdicciones y Entidades comprendidas en el artículo 8°, inciso a) de la Ley N° 24.156. 12. Asesorar y dictaminar en las cuestiones particulares, que, en materia de contrataciones públicas, sometan las Jurisdicciones y Entidades a su consideración y dictar las normas aclaratorias, interpretativas y complementarias en el ámbito de su competencia. 13. Elaborar el Pliego Único de Bases y Condiciones Generales para las contrataciones de obras públicas y concesiones de obras públicas, establecer su régimen de penalidades y la forma, plazo y demás condiciones para confeccionar e informar el Plan Anual de Contrataciones. 14. Aplicar las sanciones fijadas en el Pliego Único de Bases y Condiciones Generales para las contrataciones de obras públicas y concesiones de obras públicas. **SUBSECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES** 1. Asistir a la Secretaría en el diseño de políticas y regulaciones tendientes al desarrollo e inclusión de las comunicaciones y de los servicios postales, y elaborar estudios y propuestas de regulaciones, en el ámbito de su competencia. 2. Diseñar y proponer a la Secretaría la actualización de los marcos regulatorios de telecomunicaciones, tecnologías de la información y postal, y actualizaciones normativas en el ámbito de su competencia. 3. Asesorar a la Secretaría en el otorgamiento o caducidad de licencias, permisos o autorizaciones cuyo dictado corresponda el Poder Ejecutivo Nacional. 4. Recomendar alternativas para la adecuada utilización de la infraestructura de Red de ARSAT y el desarrollo satelital. 5. Analizar el desarrollo de los servicios postales, y promover el desarrollo de la distribución de logística liviana. 6. Promover la actualización y coordinación internacional del Cuadro Nacional de Atribución de Bandas del Espectro Radioeléctrico, tendientes a la universalización de internet y los servicios móviles. 7. Elaborar recomendaciones a la Secretaría para un mejor ejercicio de los derechos societarios de las participaciones accionarias o de capital del Estado Nacional en Argentina Soluciones Satelitales S.A. (ARSAT) y en el Correo Oficial de la República Argentina S.A.

		8. Elaborar las propuestas que presente la Secretaría en las reuniones de consultas, técnicas o negociaciones con autoridades de comunicaciones y postales de los demás países, como insumo para la elaboración de los instrumentos de regulación, estandarización y coordinación del sector. 9. Asistir a la Secretaría en la interpretación de las Leyes Nros. 19.798, 20.216, 26.522 y 27.078. 10. Elaborar propuestas para el dictado de los Planes Técnicos Fundamentales de Numeración, Señalización, y Portabilidad Numérica. 11. Proponer a la Secretaría planes y programas para la aplicación del fondo fiduciario de servicio universal. 12. Proponer a la Secretaría estrategias, estándares y **regulaciones para la ciberseguridad y protección de infraestructuras críticas de la información y las comunicaciones** asociadas del Sector Público Nacional y de los servicios de información y comunicaciones definidos en el artículo primero de la Ley Nº 27.078. (Objetivo sustituido por art. 5° del Decreto N° 139/2021 B.O. 5/3/2021. Vigencia: a partir del día siguiente al de su publicación en el BOLETÍN OFICIAL.)
SECRETARÍA DE RELACIONES PARLAMENTARIAS, INSTITUCIONALES Y CON LA SOCIEDAD CIVIL	• Subsecretaría de Asuntos Parlamentarios • Subsecretaría de relaciones Institucionales y de Gobierno • Subsecretaría de relaciones con la Sociedad Civil	**SECRETARÍA DE RELACIONES PARLAMENTARIAS, INSTITUCIONALES Y CON LA SOCIEDAD CIVIL** 1. Diseñar e implementar las relaciones parlamentarias del Poder Ejecutivo Nacional, cumpliendo las obligaciones y prerrogativas constitucionales inherentes a su vínculo con el Honorable Congreso de la Nación. 2. Asistir al Jefe de Gabinete de Ministros en materia política e institucional y coordinar la sistematización de la información de gestión para la confección de insumos para la toma de decisiones. 3. Asistir al Jefe de Gabinete de Ministros en la evaluación de la oportunidad, mérito y conveniencia de los Proyectos de Ley, de mensajes al Honorable Congreso de la Nación y del decreto que disponga la prórroga de sesiones ordinarias o de la convocatoria a sesiones extraordinarias. 4. Coordinar las acciones necesarias para la concurrencia del Jefe de Gabinete de Ministros al Honorable Congreso de la Nación, en el cumplimiento de lo dispuesto en el artículo 101 de la Constitución Nacional y confeccionar y supervisar la elaboración de la memoria detallada de la marcha del Gobierno de la Nación. 5. Entender en la elaboración de los informes solicitados por ambas Cámaras y la Comisión Bicameral Permanente

		del Honorable Congreso de la Nación, en cumplimiento de lo dispuesto por el artículo 100, incisos 9 y 11, de la Constitución Nacional. 6. Entender en las relaciones del Poder Ejecutivo Nacional con ambas Cámaras del Honorable Congreso de la Nación, sus comisiones e integrantes y en lo relativo a la tramitación de los actos que deban ser remitidos a ese Poder en cumplimiento de lo establecido en el artículo 100, inciso 6, de la Constitución Nacional y de otras Leyes. 7. Entender en la coordinación de las relaciones institucionales con Organismos y Autoridades en el ámbito Nacional, Provincial, Ciudad Autónoma de Buenos Aires o Municipal, así como con los distintos sectores del ámbito público y privado, en el marco de las competencias asignadas a la Jefatura de Gabinete de Ministros. 8. Asesorar y confeccionar informes al Jefe de Gabinete de Ministros sobre el contexto sociopolítico e impacto de las políticas públicas en el territorio nacional. 9. Asesorar al Jefe de Gabinete de Ministros en las relaciones con organizaciones y sectores representativos de la comunidad. **SUBSECRETARÍA DE ASUNTOS PARLAMENTARIOS** 1. Organizar y coordinar la vinculación con ambas Cámaras del Honorable Congreso de la Nación, en lo atinente a la confección y presentación del Informe del Jefe de Gabinete de Ministros en el Honorable Congreso de la Nación y la Memoria detallada del estado de la Nación, y asistir en el tratamiento de las materias y proyectos específicos del área. 2. Diseñar los mecanismos institucionales tendientes a la elaboración de los Informes del Jefe de Gabinete de Ministros al Honorable Congreso de la Nación. 3. Entender en la elaboración del Informe Mensual y la Memoria Anual, y su publicación. 4. Asistir a la Secretaría en la coordinación de las acciones necesarias para la concurrencia del Jefe de Gabinete de Ministros al Honorable Congreso de la Nación y confeccionar y supervisar la elaboración de la memoria detallada de la marcha del Gobierno de la Nación asistiendo al Jefe de Gabinete de Ministros en el cumplimiento de lo dispuesto en el artículo 101 de la Constitución Nacional. 5. Coordinar las relaciones del Poder Ejecutivo Nacional con ambas Cámaras del Honorable Congreso de la Nación,

		sus Comisiones e integrantes y , en especial, en lo relativo a la tramitación de los actos que deban ser remitidos a ese Poder en cumplimiento de lo establecido en el artículo 100, inciso 6, de la Constitución Nacional y otras leyes. 6. Asistir a la Secretaría en la elaboración de los informes que cualquiera de las Cámaras le solicite y los que deba brindar a la Comisión Bicameral Permanente, atento a lo normado por el artículo 100, incisos 9 y 11 de la Constitución Nacional. 7. Gestionar a requerimiento del Honorable Congreso de la Nación, el suministro de información y documentación requerida ante los organismos competentes y la asistencia de funcionarios cuando sea debidamente requerida. 8. Coordinar el seguimiento de los proyectos legislativos considerados prioritarios por la Secretaría, produciendo los informes correspondientes. 9. Asistir a la Secretaría en la coordinación de las relaciones institucionales y políticas con los representantes de ambas Cámaras del Honorable Congreso de la Nación y sus autoridades. **SUBSECRETARÍA DE RELACIONES INSTITUCIONALES Y DE GOBIERNO** 1. Asistir a la Secretaría en el diagnóstico del contexto sociopolítico nacional y confeccionar informes al Jefe de Gabinete de Ministros en la materia. 2. Diseñar y ejecutar una agenda política tendiente a la gestión de demandas y necesidades de naturaleza nacional y local. 3. Entender en la coordinación interinstitucional de los temas que requieran intervención de las distintas áreas de gobierno. 4. Desarrollar e instrumentar mecanismos de coordinación interinstitucional con otros organismos del Estado Nacional, Poderes y Jurisdicciones. 5. Asistir a la Secretaría en las relaciones con los Ministros y Secretarios para el cumplimiento de los objetivos de gobierno. 6. Generar información para la Secretaría como insumo de la toma de decisiones. **SUBSECRETARÍA DE RELACIONES CON LA SOCIEDAD CIVIL**

		1. Asistir a la Secretaría en la relación con las organizaciones y sectores políticos, sociales, económicos y representativos de la comunidad. 2. Gestionar canales de comunicación relativos a las relaciones de la Jefatura de Gabinete de Ministros con las organizaciones y sectores políticos, sociales, económicos y representativos de la comunidad, y en la centralización de las gestiones que sus integrantes realicen ante las autoridades. 3. Elaborar diagnósticos en el área de su competencia y realizar la planificación estratégica de la integración entre el Estado y la Sociedad Civil. 4. Formular estrategias de negociación tendientes a la pacificación y resolución de los conflictos planteados por las distintas organizaciones de la Sociedad Civil. 5. Proponer los cursos de acción a seguir en materia de cooperación y diálogo entre los sectores representativos de la comunidad. 6. Elaborar e implementar estudios, programas y proyectos que fortalezcan la participación de la sociedad civil en las políticas públicas del Poder Ejecutivo Nacional. 7. Promover el debate en la sociedad civil con gobiernos municipales y provinciales y con gobiernos, parlamentos y organizaciones sociales de otros países de la región, en coordinación con las áreas con competencia en la materia.
SECRETARÍA DE MEDIOS Y COMUNICACIÓN PÚBLICA	• Subsecretaría de Comunicación Pública • Subsecretaría de Comunicación y Contenidos de Difusión • Subsecretaría de Medios Públicos • Subsecretaría de Contenidos Públicos • Subsecretaría de Gestión Operativa de Medios Públicos	**SECRETARÍA DE MEDIOS Y COMUNICACIÓN PÚBLICA** (Objetivos sustituidos por art. 4° del Decreto N° 335/2020 B.O. 5/4/2020) 1. Intervenir en la formulación, ejecución y supervisión de la política de la comunicación pública del Estado Nacional. 2. Intervenir en la comunicación de las actividades del Sector Público Nacional, de los actos del Estado Nacional y en su relación institucional con los medios de comunicación. 3. Coordinar el diseño, planificación e implementación de las campañas de comunicación del Estado Nacional. 4. Coordinar mecanismos para el seguimiento y la circulación de la información de gestión de los organismos y las acciones de gobierno. 5. Intervenir en acciones de vinculación del Estado Nacional con la ciudadanía, en el ámbito de su competencia.

		6. Fortalecer la libertad de expresión y la pluralidad cultural e informativa. 7. Efectuar la planificación, y ejecución de la publicidad oficial de gestión centralizada y coordinar y ejecutar la publicidad oficial de gestión descentralizada. 8. Intervenir en la planificación y elaboración de contenidos audiovisuales y digitales, e impulsar el uso de herramientas tecnológicas. 9. Intervenir en la administración de los activos digitales del Poder Ejecutivo Nacional. 10. Desarrollar la imagen institucional del Estado Nacional. 11. Entender en la aplicación de los tratados y convenios nacionales e internacionales, leyes y reglamentos generales relativos a la materia. 12. Asistir al Jefe de Gabinete de Ministros en todo lo inherente a las expresiones tecnológicas, artísticas, educativas, culturales, informativas y formativas y aquellas vinculadas a la divulgación del conocimiento que el Estado Nacional propicie difundir a través de medios audiovisuales, redes digitales, parques temáticos y otros. 13. Entender en la administración, operación, desarrollo y explotación de los servicios de radiodifusión sonora y televisiva del Estado Nacional, a nivel local e internacional. 14. Organizar la producción y distribución de contenido en todo el espectro de medios que forman parte de las licencias del Estado Nacional, con criterio federal. 15. Intervenir en la administración y funcionamiento de Radio y Televisión Argentina S.E., integrada por LS82 Canal 7, LRA Radio Nacional y Radiodifusión Argentina al Exterior (RAE). 16. Intervenir en la administración y el funcionamiento de TELAM S.E. y de Contenidos Públicos S.E., así como en la operación, desarrollo y explotación del contenido y funcionamiento del Polo de Producción Audiovisual y de las señales integrantes de dicha sociedad. 17. Entender en la participación del Estado Nacional en TELESUR. 18. Ejercer la presidencia del Consejo Asesor del sistema Argentino de Televisión Digital Terrestre, pudiendo

		delegar dicha función en un funcionario de la Secretaría con rango no inferior a Subsecretario. 19. Entender en la administración, operación y desarrollo del Banco Audiovisual de Contenidos Universales Argentino (BACUA), sus señales, medios relacionales y conexos. 20. Intervenir, en coordinación con las restantes áreas con competencia en la materia, en todo lo relativo a las transmisiones presidenciales, incluyendo todas las tareas relativas a producción, edición y fotografía. **SUBSECRETARÍA DE COMUNICACIÓN PÚBLICA** 1. Asistir a la Secretaría en todo lo relativo a la organización y difusión de las actividades del Sector Público Nacional y de los actos del Estado Nacional. 2. Asistir a la Secretaría en la comunicación del Estado Nacional con los medios de comunicación, nacionales y provinciales. 3. Asistir a la Secretaría en las relaciones internacionales vinculadas con la prensa en el exterior. 4. Asistir a la Secretaría en la planificación, contratación y ejecución de la publicidad oficial de gestión centralizada y la coordinación y ejecución de la publicidad oficial de gestión descentralizada. **SUBSECRETARÍA DE COMUNICACIÓN Y CONTENIDOS DE DIFUSIÓN** 1. Asistir a la Secretaría en la ejecución y supervisión de la política de la comunicación pública. 2. Asistir a la Secretaría en los temas relacionados con la información pública del Gobierno Nacional. 3. Asistir a la Secretaría en las relaciones instituciones, organismos privados, estatales o de la sociedad civil que requieran información sobre los objetivos gubernamentales. 4. Intervenir en la difusión de los objetivos de gestión del Estado Nacional, a fin de proyectar la imagen del país en el ámbito interno y externo. 5. Asistir a la Secretaría en la definición de los lineamientos para el asesoramiento a los titulares de las Jurisdicciones y Entidades de la Administración Pública Nacional, en temas vinculados con la información de gobierno.

		6. Asistir a la Secretaría en lo relativo a la planificación y proyección de opinión pública y pedidos de información de gestión. 7. Asistir a la Secretaría en la supervisión y seguimiento de la producción de contenidos de comunicación. **SUBSECRETARÍA DE MEDIOS PÚBLICOS** 1. Asistir en la administración, operación, desarrollo y explotación de los servicios de radiodifusión sonora y televisiva del Estado Nacional a nivel local e internacional. 2. Asistir a la Secretaría en la administración y el funcionamiento de Radio y Televisión Argentina Sociedad del Estado (RTA SE) integrada por LS82 Canal 7, LRA Radio Nacional, Radiodifusión Argentina al Exterior (RAE) y de TELAM Sociedad del Estado. 3. Asistir en la producción y distribución de contenido en todo el espectro de medios que formen parte de las licencias del Estado Nacional, con criterio federal. 4. Asistir en la administración y funcionamiento de Radio y Televisión Argentina Sociedad del Estado (RTA SE). 5. Asistir en la administración y funcionamiento de TELAM Sociedad del Estado. 6. Asistir a la Secretaría en la planificación y administración de la ejecución de la publicidad oficial de los actos de gobierno. 7. Participar en la definición, planificación, dirección y ejecución de las políticas y actividades productivas que integran el sistema nacional de medios públicos. 8. Impulsar estudios, asistencias técnicas y actividades de capacitación en lo que hace específicamente al sistema nacional de medios públicos. 9. Participar en la formulación de convenios nacionales e internacionales, en el ámbito de su competencia. 10. Intervenir en la aplicación de los tratados y convenios nacionales e internacionales, leyes y reglamentos generales relativos a la materia, en el ámbito de su competencia. 11. Intervenir en la coordinación de la cooperación internacional en el ámbito de su competencia. 12. Asistir a la Secretaría en la participación del Estado Nacional en TELESUR.

		SUBSECRETARÍA DE CONTENIDOS PÚBLICOS (Objetivos sustituidos por art. 4° del Decreto N° 335/2020 B.O. 5/4/2020) 1. Organizar la producción y distribución de contenido en todo el espectro de medios que forman parte de las licencias del Estado Nacional, con criterio federal. 2. Colaborar en la realización de actividades de producción y emisión de programas de televisión educativa y multimedial, destinados a fortalecer y complementar las estrategias nacionales de equidad y mejoramiento de la calidad de la educación. 3. Asistir a la Secretaría en la administración y el funcionamiento de Contenidos Públicos Sociedad del Estado, así como en la operación, desarrollo y explotación del contenido y funcionamiento del Polo de Producción Audiovisual y de las señales integrantes de dicha Sociedad. 4. Dirigir la generación de contenidos del Polo de Producción Audiovisual y en las señales Encuentro, PakaPaka y Depor TV. 5. Participar en la administración y funcionamiento de la formulación y ejecución de políticas de inclusión digital, con criterio federal, en el ámbito de su competencia. 6. Participar en la integración digital de espacios culturales a través de una red federal de cultura digital. 7. Gestionar políticas públicas de promoción de contenidos para actores locales. 8. Formular y propiciar la celebración de convenios nacionales e internacionales, en el ámbito de su competencia. 9. Intervenir en la aplicación de los tratados y convenios nacionales e internacionales, leyes y reglamentos generales relativos a la materia de su competencia. 10. Intervenir en el ámbito de su competencia en la promoción, organización y participación de exposiciones, ferias, concursos, espectáculos y muestras donde se difundan producciones nacionales e internacionales de orden artístico, tecnológico, científico, educativo y cultural, con criterio federal y en coordinación con los organismos competentes. 11. Intervenir, en el ámbito de su competencia, en la promoción, organización y participación en exposiciones, ferias, concursos, espectáculos, muestras y misiones en el

		exterior, en coordinación con los organismos competentes. **SUBSECRETARÍA DE GESTIÓN OPERATIVA DE MEDIOS PÚBLICOS** 1. Coordinar la relación administrativa entre las distintas áreas de la Secretaría de Medios y Comunicación Pública. 2. Proponer y coordinar con las distintas dependencias del Sistema, la elaboración y ejecución de los planes, programas y proyectos relativos a la gestión de los medios públicos de competencia de la Secretaría. 3. Propiciar los instrumentos legales que permitan el eficiente funcionamiento los medios públicos competencia de la Secretaría. 4. Asistir al Secretario en la articulación de las relaciones que se establezcan con otras Jurisdicciones del Estado Nacional o con los gobiernos provinciales, municipales y de la Ciudad Autónoma de Buenos Aires. 5. Coordinar los servicios de apoyo técnico, administrativo, jurídico, de recursos humanos, de administración financiera, de organización, de sistemas administrativos e informáticos y la gestión documental de las áreas con competencia en medios públicos de la Secretaría, en coordinación con la Secretaría de Coordinación Administrativa. 6. Intervenir en los proyectos de leyes y actos administrativos que introduzcan o modifiquen normas vinculadas con las áreas con competencia en medios públicos de la Secretaría, en coordinación con las áreas pertinentes de la Secretaría de Coordinación Administrativa.
SECRETARÍA DE EVALUACIÓN PRESUPUESTARIA, INVERSIÓN PÚBLICA Y PARTICIPACIÓN PÚBLICO PRIVADA	• Subsecretaría de Coordinación Presupuestaria • Subsecretaría de Participación Público Privada	**SECRETARÍA DE EVALUACIÓN PRESUPUESTARIA, INVERSIÓN PÚBLICA Y PARTICIPACIÓN PÚBLICO PRIVADA** 1. Asistir al Jefe de Gabinete de Ministros en la coordinación y supervisión del análisis, la formulación y la evaluación de la estrategia presupuestaria, como así también en la elaboración del Proyecto de la Ley de Presupuesto Nacional y en el seguimiento de su ejecución. 2. Asistir al Jefe de Gabinete de Ministros en la determinación de los lineamientos estratégicos que permitan la evaluación y toma de decisiones con relación a los programas y proyectos de inversión, cualquiera sea su fuente de financiamiento, en coordinación con las áreas competentes.

		3. Coordinar la evaluación del gasto, colaborando en el diagnóstico y seguimiento de la producción pública contemplada en el Presupuesto Nacional. 4. Colaborar en el seguimiento y análisis de la relación fiscal entre la Nación y las Provincias y monitorear el grado de cumplimiento de las metas fiscales contenidas en la Ley de Presupuesto Nacional. 5. Intervenir en la elaboración de los informes que, en materia presupuestaria, le sean requeridos por el Jefe de Gabinete de Ministros en oportunidad de su concurrencia al Honorable Congreso de la Nación, como así también en aquellos informes que cualquiera de las Cámaras le solicite y los que deba brindar a la Comisión Bicameral Permanente. 6. Dictar, en su carácter de Autoridad de Aplicación del Sistema Nacional de Inversiones Públicas, creado por la Ley N° 24.354, las normas de instrumentación, complementarias y/o aclaratorias y celebrar todos los actos que se requieran para la debida implementación del mismo. 7. Intervenir en el estudio y ejecución de los proyectos de inversión, así como en el seguimiento promoción asistencia y toda otra actividad tendiente a lograr la concreción de los proyectos de inversión que surjan a partir de los mismos, en coordinación con las áreas competentes. 8. Entender en la centralización normativa de los contratos regidos por la Ley N° 27.328. 9. Coordinar, en el marco de los proyectos regidos por la Ley N° 27.328, el apoyo consultivo, operativo y técnico a los órganos o entes licitantes, en las etapas de formulación del proyecto, elaboración de la documentación licitatoria y ejecución del contrato. **SUBSECRETARÍA DE COORDINACIÓN PRESUPUESTARIA** 1. Asistir a la Secretaría en la coordinación y supervisión del análisis, la formulación y la evaluación de la estrategia presupuestaria. 2. Asistir a la Secretaría en la elaboración del Proyecto de la Ley de Presupuesto Nacional y en el seguimiento de su ejecución. 3. Participar en la evaluación del gasto contemplado en el Presupuesto Nacional y en el seguimiento y análisis de la relación fiscal entre la Nación y las provincias.

		4. Participar en el monitoreo del grado de cumplimiento de las metas fiscales contenidas en la Ley de Presupuesto Nacional. 5. Asistir a la Secretaría en la elaboración de los informes que, en materia presupuestaria, le sean requeridos por el Jefe de Gabinete de Ministros. 6. Entender en el control de la formulación y evaluación de los proyectos de inversión realizadas por las Jurisdicciones, en cuanto al cumplimiento de las metodologías y procedimientos establecidos. 7. Participar en la elaboración del Plan Nacional de Inversiones Públicas (PINP). 8. Gestionar el Banco de Proyectos de Inversión (BAPIN). 9. Asistir a la Secretaría en la determinación de los lineamientos estratégicos que permitan la evaluación y toma de decisiones con relación a los programas y proyectos de inversión, elaborando una propuesta de priorización. 10. Participar en el Fondo de Convergencia Estructural del MERCOSUR (FOCEM). **SUBSECRETARÍA DE PARTICIPACIÓN PÚBLICO PRIVADA** 1. Intervenir en la centralización normativa de los contratos regidos por la Ley N° 27.328. 2. Prestar, en los términos de la Ley N° 27.328, apoyo consultivo, operativo y técnico, a solicitud de los órganos o entes licitantes, en las etapas de formulación del proyecto, elaboración de la documentación licitatoria y ejecución del contrato. 3. Participar en la elaboración de programas y planes de desarrollo de proyectos de participación público-privada y promover propuestas tendientes a optimizar el funcionamiento general del régimen de participación público privada. 4. Entender, en los casos previstos en la Ley N° 27.328 y su reglamentación, en el establecimiento de criterios y parámetros para evaluar la satisfacción del interés público, mediante el recurso a la modalidad de participación público-privada frente a otras alternativas contractuales disponibles. 5. Intervenir, en los casos previstos en la Ley N° 27.328 y su reglamentación, con relación a la factibilidad y evaluación de cada contratación, mediante el régimen de participación público-privada.

		6. Coordinar las intervenciones de los distintos integrantes del Sector Público Nacional que se requieran en las diferentes etapas del desarrollo de un proyecto de participación público-privada. 7. Entender en la implementación y administración de un registro que centralice toda la documentación relativa a cada uno de los proyectos de participación público-privada. 8. Intervenir en forma previa a la cesión, total o parcial, de un contrato de participación público-privada. 9. Elaborar, en los casos previstos en la Ley N° 27.328 y en su reglamentación, informes sobre el estado de ejecución y cumplimiento de los contratos de participación público-privada en curso y de los proyectos que se considere conveniente desarrollar bajo dicha modalidad. 10. Entender en la selección de profesionales habilitados para integrar los Paneles Técnicos y efectuar el listado respectivo. 11. Intervenir en la identificación de las mejores prácticas de ética y transparencia para el desarrollo de proyectos de participación público-privada en coordinación con la Oficina Anticorrupción, dependiente del Ministerio de Justicia y Derechos Humanos. 12. Entender en el control de la formulación y evaluación de los proyectos de inversión realizados en las Jurisdicciones, en cumplimiento de lo establecido en el inciso b) del artículo 5° de la Ley N° 24.354, cuando se trate de proyectos de inversión pública ejecutados a través de contratos de participación público privada en los términos de la Ley N° 27.328.
SECRETARÍA DE POLÍTICAS INTEGRALES SOBRE DROGAS DE LA NACIÓN ARGENTINA	• Subsecretaría de Gestión Administrativa • Subsecretaría de Atención y Acompañamiento en materia de Drogas • Subsecretaría de Prevención, Investigación y Estadísticas en materia de Drogas	**SECRETARÍA DE POLÍTICAS INTEGRALES SOBRE DROGAS DE LA NACIÓN ARGENTINA** (Objetivo sustituidos por art. 7º del Decreto Nº 606/2020 B.O. 21/7/2020) 1. Elaborar políticas y planificar estrategias nacionales que tengan como eje principal el cuidado de las personas, a través de la atención, la prevención y la capacitación en materia de consumo problemático de estupefacientes y sustancias psicoactivas. 2. Supervisar el cumplimiento de la legislación nacional e internacional en lo que esmateria de su competencia. 3. Coordinar acciones relativas al diseño y ejecución de políticas y estrategias para la prevención, capacitación y tratamiento en materia de consumo problemático de

		estupefacientes y sustancias psicoactivas con las Jurisdicciones y Entidades de la Administración Pública Nacional con competencia en la materia. 4. Coordinar la aplicación de las políticas y estrategias para la prevención, capacitación, tratamiento del consumo problemático de estupefacientes y sustancias psicoactivas con los gobiernos provinciales y de la Ciudad Autónoma de Buenos Aires. 5. Brindar asistencia técnica a los gobiernos provinciales y de la Ciudad Autónoma de Buenos Aires, a fin de homogeneizar las actividades, maximizar los recursos y generar espacios de discusión, trabajo conjunto e intercambio de información. 6. Coordinar con el Poder Judicial de la Nación y el Ministerio Público acciones para la atención y prevención del consumo problemático de estupefacientes y sustancias psicoactivas, brindando asistencia técnica en causas penales. 7. Coordinar con el Poder Legislativo Nacional acciones para la prevención y atención del consumo problemático de estupefacientes y sustancias psicoactivas, promoviendo y brindando asistencia técnica en el análisis y la elaboración de proyectos legislativos. 8. Realizar asistencias técnicas para el diseño de capacitaciones de los recursos humanos de las fuerzas de seguridad y otras instituciones nacionales sobre prevención, atención y cuidado en materia de consumo problemático de estupefacientes y sustancias psicoactivas. 9. Representar al Gobierno Nacional en las reuniones de los organismos especializados en la materia, implementando el cumplimiento de los tratados internacionales suscritos por la República Argentina, en coordinación con el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto, así como también coordinar la producción de la información específica y la documentación técnica respectiva. 10. Centralizar la recopilación general de datos y de información especializada acerca de los aspectos involucrados en el consumo problemático de estupefacientes y sustancias psicoactivas y problemas relacionados, analizando su evolución y tendencias, a nivel nacional, provincial, de la Ciudad Autónoma de Buenos Aires, regional e internacional como insumo para la implementación de un sistema de información y de alerta temprana nacional y federal, que provea información para la elaboración de políticas públicas.

		11. Coordinar el diseño y desarrollo de actividades de investigación técnico-científica, normativa y social, a nivel nacional, provincial, de la Ciudad Autónoma de Buenos Aires y municipal, identificando los modelos y metodologías para los procesos de intervención en consumo problemático de estupefacientes y sustancias psicoactivas y problemas relacionados. 12. Presidir el Consejo Federal de Drogas (COFEDRO). 13. Designar oficiales de enlace, a propuesta de los titulares de las diferentes Jurisdicciones de la Administración Pública Nacional o Provincial, destinados a cumplir funciones de consulta o coordinación con los respectivos organismos de origen en materia de drogas o afines. **SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA** (Objetivo sustituidos por art. 7º del Decreto Nº 606/2020 B.O. 21/7/2020) 1. Intervenir en las cuestiones vinculadas con la gestión económica, financiera, patrimonial, de infraestructura, de mantenimiento, administración de bienes muebles e inmuebles y de servicios de la Secretaría, en coordinación con las áreas pertinentes de la Secretaría de Coordinación Administrativa de la Jefatura de Gabinete de Ministros. 2. Entender en materia de administración y gestión de recursos humanos de la Secretaría, en coordinación con las áreas pertinentes de la Secretaría de Coordinación Administrativa de la Jefatura de Gabinete de Ministros. 3. Entender y planificar las acciones relativas a la gestión y administración de las tecnologías de la información de la Secretaría, en coordinación con las áreas pertinentes de la Secretaría de Coordinación Administrativa de la Jefatura de Gabinete de Ministros. 4. Entender en la gestión documental de la Secretaría. 5. Coordinar el asesoramiento jurídico permanente sobre aspectos específicos y funcionales de la Secretaría. 6. Asistir a la Secretaría en la apoyatura administrativa, técnica y legal del Consejo Federal de Drogas (COFEDRO). 7. Coordinar los aspectos relativos a cuestiones sumariales. 8. Entender en la ejecución operativa y en los procesos de gestión administrativa, presupuestaria y financiera-contable de programas, proyectos, cooperaciones

		técnicas, donaciones y asistencias técnicas con financiamiento externo, como así también en los proyectos de participación público-privada, en coordinación con las áreas pertinentes de la Secretaría de Coordinación Administrativa de la Jefatura de Gabinete de Ministros. 9. Coordinar la ejecución de los procedimientos de adquisiciones y contrataciones y de las actividades de auditoría y monitoreo de programas, proyectos, cooperaciones técnicas, donaciones y asistencias técnicas con financiamiento externo y/o proyectos de participación público-privada, en coordinación con las áreas pertinentes de la Secretaría de Coordinación Administrativa de la Jefatura de Gabinete de Ministros. 10. Asistir a la Secretaría en la administración de los beneficios económicos a que refieren la Ley N° 23.737 y su decreto reglamentario Nº 1148/91, los bienes decomisados mediante sentencia condenatoria (en el marco de la Comisión Mixta de Registro, Administración y Disposición Ley N° 23.737) y los respectivos producidos por sus ventas, así como las multas que se recauden por la aplicación de la ley mencionada. **SUBSECRETARÍA DE ATENCIÓN Y ACOMPAÑAMIENTO EN MATERIA DE DROGAS** (Objetivo sustituidos por art. 7º del Decreto Nº 606/2020 B.O. 21/7/2020) 1. Asistir a la Secretaría en la elaboración de políticas nacionales y en la planificación de estrategias de desarrollo y abordaje territorial en materia de drogas. 2. Coordinar, generar y promover dispositivos de atención y acompañamiento que aborden la complejidad del consumo problemático de sustancias psicoactivas en el territorio nacional según los lineamientos y la normativa vigente, la Ley de Salud Mental Nº 26.657, los Tratados Internacionales de Derechos Humanos y la Ley Nº 26.934 de Plan IACOP. 3. Planificar y coordinar la red de atención y acompañamiento en materia de consumo problemático de estupefacientes y sustancias psicoactivas desde una perspectiva amplia y federal. 4. Realizar el seguimiento y control de avance de los convenios nacionales suscritos por la Secretaría. 5. Asistir a la Secretaría en la articulación de la relación con el Honorable Congreso de la Nación, brindando asistencia técnica en el análisis y la elaboración de

		proyectos legislativos, vinculados a la temática de competencia de la Secretaría. 6. Diseñar líneas de acción para construir una articulación entre el Estado Nacional y las organizaciones de la sociedad civil con despliegue territorial. 7. Proponer y elaborar lineamientos y protocolos de intervención para los dispositivos ambulatorios, centros comunitarios de residencia y centros de internación. en coordinación con las áreas competentes de la Administración Pública Nacional. 8. Implementar herramientas de seguimiento de las acciones desarrolladas por las diversas áreas de la Secretaría. 9. Diseñar planes y programas de carácter nacional referentes a la capacitación y asistencia técnica dirigidos a los equipos de los dispositivos ambulatorios, centros comunitarios y centros de residencia en materia de asistencia y abordaje territorial en adicciones, adaptándose a las necesidades y características locales, en coordinación con las áreas competentes de la Administración Pública Nacional. 10. Intervenir en lo relativo a la red de articulación de dispositivos de atención y atención crítica en articulación con el Sistema de Salud, centros comunitarios de residencia y centros de internación. **SUBSECRETARÍA DE PREVENCIÓN, INVESTIGACIÓN Y ESTADÍSTICAS EN MATERIA DE DROGAS** (Objetivo sustituidos por art. 7º del Decreto Nº 606/2020 B.O. 21/7/2020) 1. Asistir a la Secretaría en la elaboración de las políticas nacionales y en la planificación de estrategias para la prevención y tratamiento relacionadas con el consumo de sustancias psicoactivas. 2. Supervisar la aplicación de las políticas y estrategias para la prevención y tratamiento del consumo de sustancias psicoactivas, en coordinación con el Ministerio de Salud, el Ministerio de Desarrollo Social, el Ministerio de Educación, el Ministerio de Trabajo, Empleo y Seguridad Social y el Ministerio de Turismo y Deportes, entre otros organismos nacionales. 3. Impulsar, coordinar y evaluar el desarrollo de investigaciones, estudios y estadísticas relevantes en materia de cuidado y prevención del consumo de sustancias con base en la Ley Nº 26.934 de Plan Integral para el Abordaje de los Consumos Problemáticos (Plan

		IACOP), Ley Nacional de Salud Mental Nº 26.657 y tratados internacionales de derechos humanos, como así también marcos de referencia y planes de acción en la temática. 4. Elaborar un modelo de referencia que -mediante acciones interdisciplinarias y de complementariedad entre las diferentes áreas del conocimiento- permita elaborar un marco interpretativo de las situaciones de consumo desde una perspectiva de derechos humanos que contemple todas las dimensiones de la problemática. 5. Impulsar acuerdos con la Mesa Federal en materia de Drogas y organismos competentes en la toma de decisiones, la coordinación y colaboración para la implementación de las diversas líneas de acción objeto de su competencia. 6. Desarrollar, en articulación con la Mesa en materia de Federal, una red de investigación e información con alcance nacional e internacional sobre las modalidades y representaciones de consumo de alcohol y otras drogas y de las adicciones en general. 7. Coordinar la elaboración de los insumos necesarios para lograr los objetivos estratégicos planteados por la Secretaría. 8. Supervisar el desarrollo de las actividades del Observatorio Argentino de Drogas.

	Comentario: **Como puede observarse, el papel que la legislación nacional confiere a la Jefatura de Gabinete de Ministros, a través de la Secretaría de Innovación Pública, es fundamental para articular la ciberseguridad pública de la nación Argentina.** **Estas funciones, situadas así en un nivel de dependencia jerárquica muy elevado asegura un desenvolvimiento adecuado de las competencias den materia de ciberseguridad pública.**

4. LA REGULACIÓN DE LA CIBERSEGURIDAD DE LAS IC EN LA ARGENTINA

Al tiempo de redacción del presente Informe, el vigente marco jurídico regulador de la ciberseguridad pública o de interés público en la Argentina está compuesto por las siguientes normas, así definidas y agrupadas por el Estado[13]:

Leyes relacionadas a la ciberseguridad:

- Ley 26.388 de Delito informático
- Ley 25.326 de Protección de Datos Personales
- Decreto Reglamentario N° 1558/2001
- Ley 25.506 de Firma Digital
- Decreto Reglamentario N° 2628/2002
- Ley 26.904 de Grooming

Normativa vinculada a las funciones de la Dirección Nacional de Infraestructuras críticas de la información y ciberseguridad:

- Decisión Administrativa 641/2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos
- Disposición 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras.
- Disposición 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad.
- Resolución 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.
- Disposición ONTI 3/2013. Aprobación de la Política Modelo de Seguridad de la Información.
- Resolución 1523/2019. Definición de Infraestructuras Críticas.

Otras normativas relacionadas a la ciberseguridad:

- Decreto 577/2017. Creación del Comité de Ciberseguridad.
- Decreto 480/2019. Modificación del Decreto 577/2017.
- Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad.
- Resolución 141/2019. Presidencia del Comité de Ciberseguridad.

[13] https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa

Seguidamente se analizan cada una de tales normativas, señalando sus aspectos más significativos para el propósito del presente Informe.

4.1 Leyes relacionadas con la ciberseguridad.

- **Ley 26.388 de Delito informático (Código Penal)[14]**

Por el Honorable Congreso de la Nación Argentina (2008-06-25).

La Ley 26.388 (de modificación del Código Penal) fue sancionada por el Senado y la Cámara de Diputados de la Nación Argentina reunidos en Congreso, con fuerza de Ley, el 4 de Junio de 2008 y promulgada de hecho el 24 de Junio 2008, y publicada un día después.

Se trata de una regulación que incorpora al Código Penal de la Nación Argentina determinados comportamientos en los que, de una forma u otra, se ven involucradas las TIC, que pasan a estar tipificados como delitos, entre ellos: la pornografía infantil, interceptación ilegítima de comunicaciones, violación del secretos o acceso ilegítimo a información restringida, publicación ilegítima de datos o su revelación, violación de la confidencialidad de datos personales, manipulación de sistemas informáticos o de telecomunicaciones o la destrucción o inutilización de su contenido o introducción de programas dañinos (malware), obstrucción al ejercicio de la autoridad, interrupción de comunicaciones y destrucción de pruebas.

- **Ley 25.326 de Protección de Datos Personales (Habeas Data)[15]**

Por el Honorable Congreso de la Nación Argentina (2000-11-02).

La Ley 25.326 (Habeas Data) fue sancionada el 4 de octubre de 2000 y publicada en el Boletín Nacional el 2 de Noviembre de 2000.

Se trata de una norma jurídica que regula la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

Tras el articulado relativo a definir los conceptos esenciales, la norma desarrolla los principios de la protección de datos (Licitud, Calidad de los datos, Consentimiento, Información, Categoría de datos, Datos relativos a la salud, Seguridad de los datos, Deber de confidencialidad, Cesión, Transferencia internacional), los derechos de los titulares de datos (Derecho de Información, Derecho de acceso, Contenido de la información, Derecho de rectificación, actualización o supresión, Excepciones, Comisiones legislativas, Gratuidad, Impugnación de valoraciones personales), las cautelas debidas a usuarios y responsables de archivos, registros y bancos de datos (Registro de archivos de datos. Inscripción, Archivos, registros o bancos de datos públicos, Supuestos especiales, Archivos, registros o bancos de datos privados, Prestación de servicios informatizados de datos personales, Prestación de servicios de información crediticia, Archivos, registros o bancos de datos con fines de publicidad, Archivos, registros o bancos de datos

[14] https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto
[15] https://www.argentina.gob.ar/normativa/nacional/decreto-1558-2001-70368/texto

relativos a encuestas), medidas de control (Órgano de Control, Códigos de conducta), sanciones (Sanciones administrativas, Sanciones penales), acciones de protección de los datos personales (Procedencia, Legitimación activa, Legitimación pasiva, Competencia, Procedimiento aplicable, Requisitos de la demanda, Trámite, Confidencialidad de la información, Contestación del informe, Ampliación de la demanda, Sentencia, Ámbito de aplicación, Disposiciones transitorias).

- **Decreto Reglamentario N° 1558/2001 (Protección de los Datos Personales)[16]**

Por el Poder Ejecutivo Nacional (P.E.N.) (2001-12-03).

Se trata del desarrollo reglamentario de la norma anterior, sancionado por el Poder Ejecutivo con fecha 3 de diciembre de 2001.

Incluye preceptos de detalle de regulación de los principios generales relativos a la protección de datos, los derechos de los titulares de los datos, los relativos a los usuarios y responsables de archivos, registros y bancos de datos, medidas de control (que crea la Dirección Nacional de Protección de Datos Personales, en el ámbito de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos, como órgano de control de la Ley Nº 25.326) y detalle de las sanciones.

- **Ley 25.506 de Firma Digital[17]**

Por el Honorable Congreso de la Nación Argentina.

La Ley 25.506 fue sancionada el 14 de Noviembre de 2001 y publicada en el Boletín Nacional del 14 de Diciembre de 2001.

Esta ley, tras realizar unas consideraciones generales previas, tendentes a reconocer el empleo de la firma electrónica y de la firma digital y su eficacia jurídica (firma digital, firma electrónica, documento digital, validez, remitente, original y conservación), regula los certificados digitales, los certificadores licenciados, los titulares de certificados digitales, la organización institucional, la autoridad de aplicación, el sistema de auditoría, la Comisión Asesora para la Infraestructura de Firma Digital, la responsabilidad, las sanciones y ciertas disposiciones complementarias.

La Ley concluye con un Anexo de definiciones.

- **Decreto Reglamentario N° 2628/2002 (Firma Digital)[18]**

Por el Poder Ejecutivo Nacional (P.E.N.)

Este Decreto fue sancionado el 19 de diciembre de 2002 y publicado en el Boletín Nacional del 20 de Diciembre de 2002.

Se trata del desarrollo reglamentario de la norma anterior que, tras unas consideraciones generales previas, regula aspectos concretos de la Ley, tales como la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital, el Ente Administrador de Firma Digital, el Sistema de Auditoría, los Estándares Tecnológicos, la Revocación de Certificados Digitales, los

[16] https://www.argentina.gob.ar/normativa/nacional/decreto-1558-2001-70368/texto
[17] https://www.argentina.gob.ar/normativa/nacional/ley-25506-70749
[18] https://www.argentina.gob.ar/normativa/nacional/decreto-2628-2002-80733

Certificadores Licenciados, las Autoridades de Registro y ciertas Disposiciones para la Administración Pública Nacional.

- **Ley 26.904 de Grooming (Código Penal)**[19]

Por el Honorable Congreso de la Nación Argentina.

La Ley 26.904 fue sancionada el 13 de Noviembre de 2013 y publicada en el Boletín Nacional del 11 de Diciembre de 2013.

Se trata de una norma que incorpora al Código Penal, con carácter de delito, aquella conducta que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

4.2 Normativa vinculada a las funciones de la Dirección Nacional de Infraestructuras Críticas de la Información y Ciberseguridad.

Se presentan en orden cronológico de publicación inicial.

- **Resolución 580/2011 (Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad – Creación)**[20]

Por la Jefatura del Gabinete de Ministros.

Esta Resolución fue sancionada el 28 de Julio de 2011 y publicada en el Boletín Nacional del 2 de Agosto de 2011.

Esta Resolución crea el **Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad**, señalando sus objetivos y derogando la Resolución de la ex Secretaria de la Función Pública nº 81 del 14 de julio de 1999, sus modificatorias y complementarias.

La Resolución arranca poniendo de manifiesto el creciente uso las tecnologías de la información y la comunicación en la sociedad, y cómo se encuentran sustentadas en gran medida en el ciberespacio, añadiendo que la utilización de las comunicaciones virtuales constituye un recurso que depende de la infraestructura digital, la cual es considerada como infraestructura crítica, entendiéndose ésta como imprescindible para el funcionamiento de los sistemas de información y comunicaciones, de los que a su vez dependen de modo inexorable, tanto el Sector Público Nacional como el sector privado, para cumplir sus funciones y alcanzar sus objetivos.

Sigue el preámbulo de la Resolución recordando que la infraestructura digital se encuentra expuesta a constantes amenazas, que en caso de materializarse pueden ocasionar graves incidentes en los sistemas de información y comunicaciones, por lo que resulta imprescindible adoptar las medidas necesarias para garantizar el adecuado funcionamiento de las infraestructuras críticas.

[19] https://www.argentina.gob.ar/normativa/nacional/ley-26904-223586
[20] https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-580-2011-185055

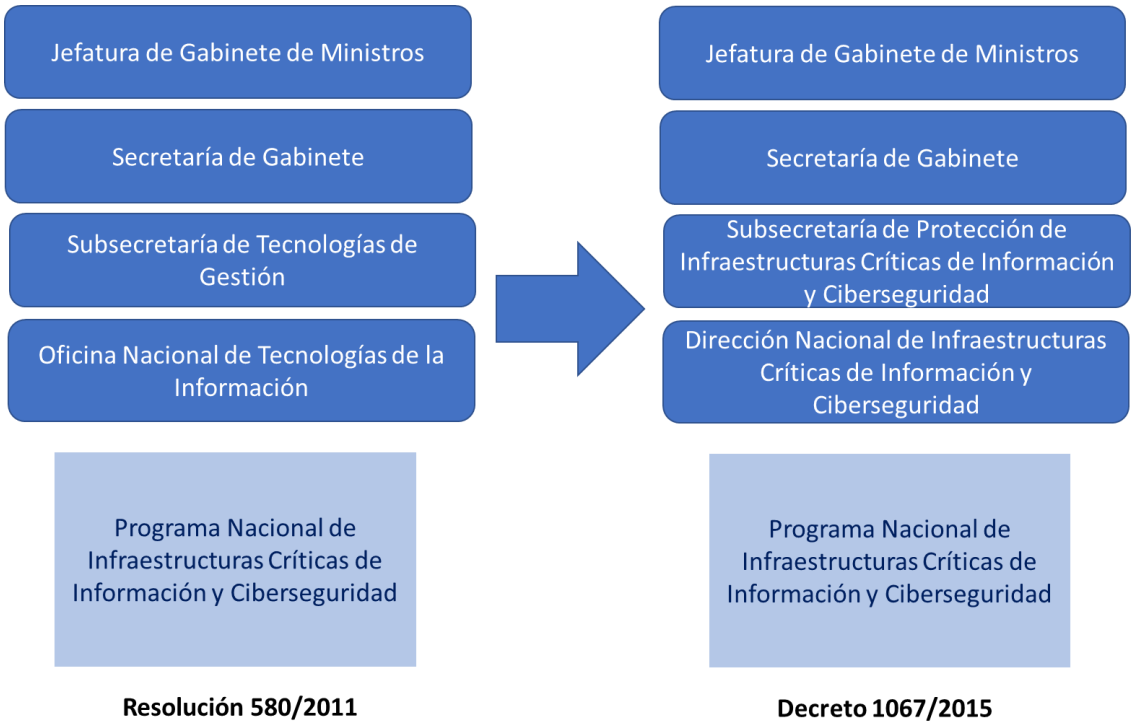
A los efectos de tratar adecuadamente tales riesgos, señala la norma que, mediante Resolución ex SFP Nº 81/99 (que con la presente Resolución se deroga) se creó en su momento la **Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina (ARCERT)**, en el ámbito de la ex Subsecretaria de Tecnologías Informáticas de la ex Secretaria de la Función Pública de la Jefatura de Gabinete de Ministros.

Insistiendo en la necesidad de tratar adecuadamente los riesgos del ciberespacio, sigue la norma señalando la conveniencia de crear el **Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad,** en el ámbito de la Oficina Nacional de Tecnologías de Información de la Subsecretaria de Tecnologías de Gestión de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros, a fin de:

> *Impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran, y la colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías, entre otras acciones.*

	Comentario: Con posterioridad a esta Resolución, el art. 5° del Decreto 1067/2015 (B.O. 12/06/2015), del Poder Ejecutivo Nacional, transfirió la competencia sobre dicho Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad a la órbita de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad dependiente de la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad dependiente de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros. **Esta adscripción parece adecuada y sitúa la gestión de la ciberseguridad pública en el nivel de decisión adecuado.**

La figura siguiente muestra dicho cambio de dependencia.



Los **objetivos generales** del Plan Nacional de Infraestructuras Críticas de Información y Ciberseguridad eran los siguientes:

1. Elaboración de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas de las entidades y jurisdicciones definidas en el artículo 8º de la Ley Nº 24.156[21] y sus modificatorios,
2. Los organismos interjurisdiccionales[22],

[21] Ley 24.156. Honorable Congreso de la Nación Argentina. ADMINISTRACION FINANCIERA Y SISTEMAS DE CONTROL DISPOSICIONES GENERALES. Fecha de sanción 30-09-1992. Publicada en el Boletín Nacional del 29-Oct-1992. Las entidades jurisdiccionales que se mencionan son: a) Administración Nacional, conformada por la Administración Central y los Organismos Descentralizados, comprendiendo en estos últimos a las Instituciones de Seguridad Social. b) Empresas y Sociedades del Estado que abarca a las Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias. c) Entes Públicos excluidos expresamente de la Administración Nacional, que abarca a cualquier organización estatal no empresarial, con autarquía financiera, personalidad jurídica y patrimonio propio, donde el Estado nacional tenga el control mayoritario del patrimonio o de la formación de las decisiones, incluyendo aquellas entidades públicas no estatales donde el Estado nacional tenga el control de las decisiones. d) Fondos Fiduciarios integrados total o mayoritariamente con bienes y/o fondos del Estado nacional. Serán aplicables las normas de esta ley, en lo relativo a la rendición de cuentas de las organizaciones privadas a las que se hayan acordado subsidios o aportes y a las instituciones o fondos cuya administración, guarda o conservación está a cargo del Estado nacional a través de sus Jurisdicciones o Entidades.

[22] La citada Ley 24.156 señala como "jurisdicción" cada una de las siguientes unidades: a) Institucionales (Poder Legislativo, Poder Judicial, Ministerio Público, Presidencia de la Nación, Jefatura de Gabinete de Ministros, los Ministerios y Secretarías del Poder Ejecutivo Nacional); b) Administrativo-Financieras (Servicio de la Deuda Pública, Obligaciones a cargo del Tesoro).

3. Las organizaciones civiles y del sector privado que así lo requieran, y
4. El fomento de la cooperación y colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías.

Estos objetivos generales se concretan en los siguientes **objetivos específicos**:

a) Elaborar y proponer normas destinadas a incrementar los esfuerzos orientados a elevar los umbrales de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas en el ámbito del Sector Publico Nacional.
b) Colaborar con el sector privado para elaborar en conjunto políticas de resguardo de la seguridad digital con actualización constante, fortaleciendo lazos entre los sectores público y privado; haciendo especial hincapié en las infraestructuras críticas.
c) Administrar toda la información sobre reportes de incidentes de seguridad en el Sector Público Nacional que hubieren adherido al Programa y encausar sus posibles soluciones de forma organizada y unificada.
d) Establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad, asegurando la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas.
e) Investigar nuevas tecnologías y herramientas en materia de seguridad informática.
f) Incorporar tecnología de última generación para minimizar todas las posibles vulnerabilidades de la infraestructura digital del Sector Público Nacional.
g) Asesorar a los organismos sobre herramientas y técnicas de protección y defensa de sus sistemas de información.
h) Alertar a los organismos que se adhieran al presente Programa sobre casos de detección de intentos de vulneración de infraestructuras críticas, sean estos reales o no.
i) Coordinar la implementación de ejercicios de respuesta ante la eventualidad de un intento de vulneración de las infraestructuras críticas del Sector Público Nacional.
j) Asesorar técnicamente ante incidentes de seguridad en sistemas informáticos que reporten los organismos del Sector Público Nacional que hubieren adherido.
k) Centralizar los reportes sobre incidentes de seguridad ocurridos en redes teleinformáticas del Sector Público Nacional que hubieren adherido al Programa y facilitar el intercambio de información para afrontarlos.
l) Actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa.
m) Promover la coordinación entre las unidades de administración de redes informáticas del Sector Público Nacional, para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad.
n) Elaborar un informe anual de la situación en materia de ciberseguridad, a efectos de su publicación abierta y transparente.
o) Monitorear los servicios que el Sector Público Nacional brinda a través de la red de Internet y aquellos que se identifiquen como Infraestructura Crítica para la prevención de posibles fallas de Seguridad.
p) Promover la concientización en relación a los riesgos que acarrea el uso de medios digitales en el Sector Público Nacional, las Organizaciones de Gobierno, al público en general, como así también del rol compartido entre el Sector Público y Privado para el resguardo de la Infraestructura Crítica.

q) Difundir información útil para incrementar los niveles de seguridad de las redes teleinformáticas del Sector Público Nacional.
r) Interactuar con equipos de similar naturaleza.

⚠	**Advertencia / Cuestión a analizar:** **¿Hasta qué punto de se han desarrollado estos objetivos específicos en las posteriores actuaciones -de naturaleza jurídica u operativa- en la Argentina?**

La instrumentalización de los objetivos anteriores, originariamente encomendada a la Oficina Nacional de Tecnologías de Información, se materializa en la actualidad por la **Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad**, cuyas **funciones** son:

a) Dictar las normas que resulten necesarias para su implementación.
b) Crear una página web para ejecutar las acciones tendientes a cumplir con los objetivos establecidos.
c) Coordinar las actividades con las entidades y jurisdicciones del Sector Público Nacional, los entes interjurisdiccionales y las organizaciones civiles y del sector privado que adhieran al 'Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad'.

⚠	**Advertencia / Cuestión a analizar:** **¿Se han desarrollado estas funciones posteriormente en Argentina?** **De la redacción de la letra c) anterior cabe deducir que la adhesión al Programa Nacional de Infraestructuras Críticas es opcional y voluntario para las organizaciones. Si esto es así, la ausencia de un marco regulatorio común y obligatorio para todas las Infraestructuras Críticas de Información, ya se encuentren en manos públicas o privadas, dificulta una protección armonizada de dichas infraestructuras, pudiendo poner en riesgo el mantenimiento de la ciberseguridad nacional.** **Las funciones encomendadas a la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad citadas no contemplan la implementación de todos los objetivos específicos del Plan Nacional de Infraestructuras Críticas de Información y Ciberseguridad, señalados anteriormente.**

- **Disposición ONTI 3/2013. Aprobación de la Política Modelo de Seguridad de la Información**

Por la Oficina Nacional de Tecnologías de Información.

Esta Disposición fue sancionada el 27 de Agosto de 2013 y publicada en el Boletín Nacional del 02 de Septiembre de 2013.

Esta Disposición reemplaza a la Disposición ONTI Nº6/2005 de la Oficina Nacional de Tecnologías de Información de la Subsecretaría de Tecnologías de Gestión de la Secretaría de Gabinete y Coordinación Administrativa de la Jefatura de Gabinete de Ministros que, en su artículo 1º, aprobó la "**Política de Seguridad de la Información Modelo**" ordenada por la Decisión Administrativa JGM Nº 669/2004.

⚠	**Advertencia / Cuestión a analizar:** **Llama la atención que una norma de la importancia de esta, que supone sentar las bases para disponer de una "Política de Seguridad de la Información", de alcance público, haya sido dictada por un instrumento de rango jurídico menor, como es el caso de las Decisiones Administrativas[23].**

Esta Política Modelo de seguridad de la Información deberá servir como base para la elaboración de las respectivas políticas a dictarse por cada organismo alcanzado por la Decisión Administrativa Nº 669/2004, debiendo ser interpretada como un compendio de mejores prácticas en materia de seguridad de la información para las entidades, públicas y adaptada a la realidad y recursos de cada organismo.

Por otra parte, las funciones a las que hace alusión dicha Política deberán ser asignadas de acuerdo a las particularidades y operatoria de cada organismo, evitando la duplicación de tareas y asegurando la segregación de funciones incompatibles siempre que sea posible, o bien mediante la implementación de controles para mitigar dicho riesgo.

El **contenido** de la Política es el siguiente:

[23] Por ejemplo, en el caso de España, la obligación de que todos los organismos del sector público deban disponer de una Política de Seguridad de la Información, y que incluye las directrices generales a las que deben acomodarse las Políticas de Seguridad específicas de cada organismo, está regulado en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, una norma cuyo rango normativo se corresponde con la potestad reglamentaria del Gobierno, a un nivel inmediatamente inferior a las leyes, aprobadas por el Parlamento.

1 Introducción
1.1 Alcance
1.2 Qué es seguridad de la información
1.3 ¿Por qué es necesario
1.4 Requerimientos de seguridad
1.5 Evaluación de los riesgos de seguridad
1.6 Selección de controles
1.7 ¿Cómo empezar
1.8 Factores críticos de éxito

2 Términos y Definiciones
2.1 Seguridad de la Información
2.2 Evaluación de Riesgos
2.2 Tratamiento de Riesgos
2.3 Gestión de Riesgos
2.4 Comité de Seguridad de la Información
2.5 Responsable de Seguridad de la Información
2.6 Incidente de Seguridad
2.8 Riesgo
2.9 Amenaza
2.10 Vulnerabilidad
2.11 Control

3. Estructura de la política Modelo

4. Evaluación y tratamiento de riesgos
4.1 Evaluación de los riesgos de seguridad
4.2 Tratamiento de riesgos de seguridad

5. Cláusula: Política de Seguridad de la Información
5.1 Categoría: Política de Seguridad de la información
5.1.1 Control: Documento de la política de seguridad de la información
5-1-2 Control: Revisión de la política de seguridad de la información

6. Cláusula: Organización
6.1 Categoría: Organización interna
6.1.1 Control: Compromiso de la dirección con la seguridad de la información
6-1-2 Control: Coordinación de la seguridad de la información
6-1-3 Control: Asignación de responsabilidades de la seguridad de la información
6-1-4 Control: Autorización para Instalaciones de Procesamiento de Información
6-1-5 Control: Acuerdos de confidencialidad
6-1-6 Control: Contacto con otros organismos
6-1-7 Control: Contacto con grupos de interés especial
6-1-8 Control: Revisión independiente de la seguridad de la información
6.2 Categoría: Grupos o personas externas
6.2.1 Control: Identificación de los riesgos relacionados con grupos externos
6-2-2 Control: Puntos de seguridad de la información a considerar en Contratos o Acuerdos con terceros
6-2-3 Control: Puntos de Seguridad de la Información a ser considerados en acuerdos con terceros

7. Cláusula: Gestión de Activos
7.1 Categoría: Responsabilidad sobre los activos
7.1.1 Control: Inventario de activos
7.1.2 Control: Propiedad de los activos
7.1.3 Control: Uso aceptable de los activos
7.2 Categoría: Clasificación de la información
7.2.1 Control: Directrices de clasificación
7.2.2 Control: Etiquetado y manipulado de la información

8. Cláusula: Recursos Humanos
8.1 Categoría: Antes del empleo
8.1.1 Control: Funciones y responsabilidades
8.1.2 Control: Investigación de antecedentes
8.1.3 Control: Términos y condiciones de contratación
8.2 Categoría: Durante el empleo

8.2.1 Control: Responsabilidad de la dirección
8.2.2 Control: Concientización, formación y capacitación en seguridad de la información
8.2.3 Control: Proceso disciplinario
8.3 Categoría: Cese del empleo o cambio de puesto de trabajo
8.3.1 Control: Responsabilidad del cese o cambio
8.3.2 Control: Devolución de activos
8.3.3 Control: Retiro de los derechos de acceso

9. Cláusula: Física y Ambiental
9.1 Categoría: Areas Seguras
9.1.1 Control: Perímetro de seguridad física
9.1.2 Control: Controles físicos de entrada
9.1.3 Control: Seguridad de oficinas, despachos, instalaciones
9.1.4 Control: Protección contra amenazas externas y de origen ambiental
9.1.5 Control: Trabajo en áreas seguras
9.1.6 Control: Areas de acceso público, de carga y descarga
9.2 Categoría: Seguridad de los equipos
9.2.1 Control: emplazamiento y protección de equipos
9.2.2 Control: Instalaciones de suministro
9.2.3 Control: Seguridad del cableado
9.2.4 Control: Mantenimiento de los equipos
9.2.5 Control: Seguridad de los equipos fuera de las instalaciones
9.2.6 Control: Reutilización o retiro seguro de equipos
9.2.7 Control: Retirada de materiales propiedad de la empresa
9.2.8 Políticas de Escritorios y Pantallas Limpias

10. Cláusula: Gestión de Comunicaciones y Operaciones
10.1 Categoría: Procedimientos y Responsabilidades Operativas
10.1.1 Control: Documentación de los Procedimientos Operativos
10.1.2 Control: Cambios en las Operaciones
10.1.3 Control: Separación de Funciones
10.1.4 Control: Separación entre Instalaciones de Desarrollo e Instalaciones Operativas
10.2 Categoría: Gestión de Provisión de Servicios
10.2.1 Control: Provisión de servicio
10.2.2 Control: Seguimiento y revisión de los servicios de las terceras partes
10.2.3 Control: Gestión del cambio de los servicios de terceras partes
10.3 Categoría: Planificación y Aprobación de Sistemas
10.3.1 Control: Planificación de la Capacidad
10.3.2 Control: Aprobación del Sistema
10.4 Categoría: Protección Contra Código Malicioso
10.4.1 Control: Código Malicioso
10.4.2 Control: Código Móvil
10.5 Categoría: Respaldo o Back-up
10.5.1 Control: Resguardo de la Información
10.5.2 Control: Registro de Actividades del Personal Operativo
10.5.3 Control: Registro de Fallas
10.6 Categoría: Gestión de la Red
10.6.1 Control: Redes
10.7 Categoría: Administración y Seguridad de los medios de almacenamiento
10.7.1 Control: Administración de Medios Informáticos Removibles
10.7.2 Control: Eliminación de Medios de Información
10.7.3 Control: Procedimientos de Manejo de la Información
10.7.4 Control: Seguridad de la Documentación del Sistema
10.8 Categoría: Intercambios de Información y Software
10.8.1 Control: Procedimientos y controles de intercambio de la información

10.8.2 Control: Acuerdos de Intercambio de Información y Software
10.8.3 Control: Seguridad de los Medios en Tránsito
10.8.4 Control: Seguridad de los la Mensajería
10.8.5 Control: Seguridad del Gobierno Electrónico
10.9 Categoría: Seguridad del Correo Electrónico
10.9.1 Control: Riesgos de Seguridad
10.9.2 Control: Política de Correo Electrónico
10.9.3 Control: Seguridad de los Sistemas Electrónicos de Oficina
10.9.4 Control: Sistemas de Acceso Público
10.9.5 Control: Otras Formas de Intercambio de Información
10.10 Categoría: Seguimiento y control
10.10.1 Control: Registro de auditoría
10.10.2 Control: Protección de los registros
10.10.3 Control: Registro de actividad de administrador y operador
10.10.4 Control: Sincronización de Relojes

11. Cláusula: Gestión de Accesos
11.1 Categoría: Requerimientos para el Control de Acceso
11.1.1 Control: Política de Control de Accesos
11.1.2 Control: Reglas de Control de Acceso
11.2 Categoría: Administración de Accesos de Usuarios
11.2.1 Control: Registración de Usuarios
11.2.2 Control: Gestión de Privilegios
11.2.3 Control: Gestión de Contraseñas de Usuario
11.2.4 Control: Administración de Contraseñas Críticas
11.2.5 Revisión de Derechos de Acceso de Usuarios
11.3 Categoría: Responsabilidades del Usuario
11.3.1 Control: Uso de Contraseñas
11.3.2 Control: Equipos Desatendidos en Areas de Usuarios
11.4 Categoría: Control de Acceso a la Red
11.4.1 Control: Política de Utilización de los Servicios de Red
11.4.2 Control: Camino Forzado
11.4.3 Control: Autenticación de Usuarios para Conexiones Externas
11.4.4 Control: Autenticación de Nodos
11.4.5 Control: Protección de los Puertos (Ports) de Diagnóstico Remoto
11.4.6 Control: Subdivisión de Redes
11.4.7 Control: Acceso a Internet
11.4.8 Control: Conexión a la Red
11.4.9 Control: Ruteo de Red
11.4.10 Control: Seguridad de los Servicios de Red
11.5 Categoría: Control de Acceso al Sistema Operativo
11.5.1 Control: Identificación Automática de Terminales
11.5.2 Control: Procedimientos de Conexión de Terminales
11.5.3 Control: Identificación y Autenticación de los Usuarios
11.5.4 Control: Sistema de Administración de Contraseñas
11.5.5 Control: Uso de Utilitarios de Sistema
11.5.6 Control: Alarmas Silenciosas para la Protección de los Usuarios
11.5.7 Control: Desconexión de Terminales por Tiempo Muerto
11.5.8 Control: Limitación del Horario de Conexión
11.6 Categoría: Control de Acceso a las Aplicaciones
11.6.1 Control: Restricción del Acceso a la Información
11.6.2 Control: Aislamiento de los Sistemas Sensibles
11.7 Categoría: Monitoreo del Acceso y Uso de los Sistemas
11.7.1 Control: Registro de Eventos
11.7.2 Control: Procedimientos y Areas de Riesgo
11.8 Categoría: Dispositivos Móviles y Trabajo Remoto

11.8.1 Control: Computación Móvil
11.8.2 Control: Trabajo Remoto

12. Cláusula: Adquisición, desarrollo y mantenimiento de sistemas
12.1 Categoría: Requerimientos de Seguridad de los Sistemas
12.1.1 Control: Análisis y Especificaciones de los Requerimientos de seguridad
12.2 Categoría: Seguridad en los Sistemas de Aplicación
12.2.1 Validación de Datos de Entrada
12.2.2 Control: Controles de Procesamiento Interno
12.2.3 Control: Autenticación de Mensajes
12.2.4 Control: Validación de Datos de Salidas
12.3 Categoría: Controles Criptográficos
12.3.1 Control: Política de Utilización de Controles Criptográficos
12.3.2 Control: Cifrado
12.3.4 Control: Firma Digital
12.3.5 Control: Servicios de No Repudio
12.3.6 Control: Protección de claves criptográficas
12.3.7 Control: Protección de Claves criptográficas: Normas y procedimientos
12.4 Categoría: Seguridad de los Archivos del Sistema
12.4.1 Control: Software Operativo
12.4.2 Control: Protección de los Datos de Prueba del Sistema
12.4.3 Control: Cambios a Datos Operativos
12.4.4 Control: Acceso a las Bibliotecas de Programas fuentes
12.5 Categoría: Seguridad de los Procesos de Desarrollo y Soporte
12.5.1 Control Procedimiento de Control de Cambios
12.5.2 Control: Revisión Técnica de los Cambios en el sistema Operativo
12.5.3 control: Restricción del Cambio de Paquetes de Software
12.5.4 Control: Canales Ocultos y Código Malicioso
12.5.6 Control: Desarrollo Externo de Software
12.6 Categoría: Gestión de vulnerabilidades técnicas
12.6.1 Control: Vulnerabilidades técnicas

13. Cláusula: Gestión de Incidentes de Seguridad
13.1 Categoría: Informe de los eventos y debilidades de la seguridad
13.1.1 Reporte de los eventos de la seguridad de información
13.1.2 Reporte de las debilidades de la seguridad
13.1.3 Comunicación de Anomalías del Software
13.2 Categoría: Gestión de los Incidentes y mejoras de la seguridad
13.2.1 Control: Responsabilidades y procedimientos
13.2.2 Aprendiendo a partir de los incidentes de la seguridad de la información
13.2.3 Procesos Disciplinarios

14. Cláusula: Gestión de la Continuidad
14.1 Categoría: Gestión de continuidad del Organismo
14.1.1 Control: Proceso de Administración de la continuidad del Organismo
14.1.2 Control: Continuidad de las Actividades y Análisis de los impactos
14.1.3 Control: Elaboración e implementación de os planes de continuidad de las Actividades del Organismo
14.1.4 Control: Marco para la Planificación de la continuidad de las Actividades del Organismo
14.1.5 Control: Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad del Organismo

15. Cláusula: Cumplimiento
15.1 Categoría: Cumplimiento de Requisitos Legales

15.1.1 Control: Identificación de la Legislación Aplicable
15.1.2 Control: Derechos de Propiedad Intelectual
15.1.3 Control: Protección de los Registros del Organismo
15.1.3 Control: Protección de Datos y Privacidad de la Información Personal
15.1.4 Control: Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información
15.1.6 Regulación de Controles para el Uso de Criptografía
15.1.7 Recolección de Evidencia
15.1.8 Delitos Informáticos
15.2 Categoría: Revisiones de la Política de Seguridad y la Compatibilidad
15.2.1 Control: Cumplimiento de la Política de Seguridad
15.2.2 Verificación de la Compatibilidad Técnica
15.3 Consideraciones de Auditorías de Sistemas
15.3.1 Controles de Auditoría de Sistemas
15.3.2 Protección de los Elementos Utilizados por la Auditoría de Sistemas
15.3.3 Sanciones Previstas por Incumplimiento.

Por su parte la DA Nº 669/2004 de la Jefatura de Gabinete de Ministros estableció la obligatoriedad **para ciertos organismos del Sector Público Nacional**[24] de:

- Dictar una política de Seguridad de la Información conforme la Política de Seguridad Modelo, o adecuar sus Políticas de Seguridad conforme al Modelo aprobado.
- Conformar un Comité de Seguridad en la Información[25].
- Designar un coordinador del Comité de Seguridad de la Información[26].
- Establecer las funciones del Comité de Seguridad de la Información.

⚠	**Advertencia / Cuestión a analizar:** De la redacción del punto "1. Introducción" de esta Política, estas obligaciones **solo resultan de aplicación** a las entidades comprendidas en los incisos a) y c) del art. 8º de la Ley 24.156; es decir: a) Administración Nacional, conformada por la Administración Central y los Organismos Descentralizados, comprendiendo en estos últimos a las Instituciones de Seguridad Social y c) Entes Públicos excluidos expresamente de la Administración Nacional, que abarca a cualquier organización estatal no empresarial, con autarquía financiera, personalidad jurídica y patrimonio propio, donde el Estado nacional tenga el control mayoritario del patrimonio o de la formación de las

[24] Solo los comprendidos en los incisos a) y c) del art. 8º de la Ley 24.156; es decir: a) Administración Nacional, conformada por la Administración Central y los Organismos Descentralizados, comprendiendo en estos últimos a las Instituciones de Seguridad Social y c) Entes Públicos excluidos expresamente de la Administración Nacional, que abarca a cualquier organización estatal no empresarial, con autarquía financiera, personalidad jurídica y patrimonio propio, donde el Estado nacional tenga el control mayoritario del patrimonio o de la formación de las decisiones, incluyendo aquellas entidades públicas no estatales donde el Estado nacional tenga el control de las decisiones.
Se excluyen, por tanto: b) Empresas y Sociedades del Estado que abarca a las Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias.d) Fondos Fiduciarios integrados total o mayoritariamente con bienes y/o fondos del Estado nacional. Serán aplicables las normas de esta ley, en lo relativo a la rendición de cuentas de las organizaciones privadas a las que se hayan acordado subsidios o aportes y a las instituciones o fondos cuya administración, guarda o conservación está a cargo del Estado nacional a través de sus Jurisdicciones o Entidades.

[25] Epígrafe 2.4 de la Política Modelo. Comité de Seguridad de la Información: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.
El Comité de Seguridad de la Información será responsable de que se gestionen los riesgos de seguridad de la información, brindando su apoyo para el desarrollo de dicho proceso y su mantenimiento en el tiempo (epígrafe 4.)

[26] Además de este coordinador, la Política Modelo recoge la figura del Responsable de Seguridad de la Información (epígrafe 2.5), señalando que: "2.5 Responsable de Seguridad de la Información: Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran."
El Responsable de Seguridad de la Información junto con los Titulares de Unidades Organizativas serán responsables del desarrollo del proceso de gestión de riesgos de seguridad de la información (epígrafe 4).

	decisiones, incluyendo aquellas entidades públicas no estatales donde el Estado nacional tenga el control de las decisiones. **Quedan excluidas, por tanto, de la aplicación de esta norma:** b) Empresas y Sociedades del Estado que abarca a las Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias. d) Fondos Fiduciarios integrados total o mayoritariamente con bienes y/o fondos del Estado nacional. Serán aplicables las normas de esta ley, en lo relativo a la rendición de cuentas de las organizaciones privadas a las que se hayan acordado subsidios o aportes y a las instituciones o fondos cuya administración, guarda o conservación está a cargo del Estado nacional a través de sus Jurisdicciones o Entidades. **De todo lo anterior se deduce que esta Política Modelo solo afectará a aquellas Infraestructuras Críticas de Información comprendidas en su ámbito de aplicación, perdiendo, en consecuencia, el carácter nacional que debería perseguir, para garantizar que todas las IC disponen de su Política de Seguridad.**

⚠	**Advertencia / Cuestión a analizar:** **En el momento de redactar este documento desconocemos cual es el grado de cumplimiento de las anteriores cuatro obligaciones en los organismos del Sector Público Nacional.**

Conviene hacer notar que el Responsable de Seguridad designado por los organismos en virtud de lo dispuesto en esta Política Modelo tiene la función de enlace con el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad, especialmente en lo relativo a la comunicación de incidentes o violaciones de seguridad.

En general, esta Política Modelo contempla las siguientes **figuras y responsables**:

El **Comité de Seguridad de la Información** del organismo:

- procederá a revisar y proponer a la máxima autoridad del Organismo para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información;
- monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes;
- tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad;
- aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información;

• garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios; • promover la difusión y apoyo a la seguridad de la información dentro del Organismo y coordinar el proceso de administración de la continuidad de las actividades del Organismo.
El **Coordinador del Comité de Seguridad de la Información** será el responsable de: • coordinar las acciones del Comité de Seguridad de la Información y de • impulsar la implementación y cumplimiento de la presente Política.
El **Responsable de Seguridad de la Información:** • cumplirá funciones relativas a la seguridad de los sistemas de información del Organismo, • lo cual incluye: la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.
Los **Propietarios de la Información y Propietarios de activos** son responsables de: • clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, • de documentar y mantener actualizada la clasificación efectuada, y • de definir qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
El **Responsable del Área de Recursos Humanos** o quien desempeñe esas funciones, cumplirá la función de: • notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. • Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad.
El **Responsable del Área Informática** cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del Organismo. Por otra parte tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.
El **Responsable del Área Legal o Jurídica** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación del Organismo con sus empleados y con terceros. Asimismo, asesorará en materia legal al Organismo, en lo que se refiere a la seguridad de la información.
Los **usuarios** de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.
La **Unidad de Auditoría Interna**, o en su defecto quien sea propuesto por el Comité de Seguridad de la Información es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

	Comentario: **Nos parece positivo que la Política Modelo incluya, defina y señale funciones de conceptos tales como la necesidad de contar con un Comité de Seguridad de la Información (y su coordinador), el Responsable de Seguridad, los propietarios de la Información y de los Activos, Responsable del Área Informática o la Unidad de Auditoría Interna. Todo ello contribuye a afianzar el marco de gobernanza de la ciberseguridad en el organismo de que se trate.**

Esta Política Modelo contempla la necesidad de **comunicación con otros organismos** especializados en temas relativos a la seguridad informática, entre ellos:

- Oficina Nacional de Tecnologías de Información (ONTI), y particularmente con la Oficina Nacional de Tecnologías de Información - Coordinación de Emergencias en Redes Teleinformáticas[27].
- Dirección Nacional de Protección de Datos Personales.

	Advertencia / Cuestión a analizar: **¿Están establecidas tales comunicaciones en las Políticas de Seguridad de cada organismo? ¿Hay evidencia de ello?**

	Advertencia / Cuestión a analizar: **Conclusión: la Política Modelo es un buen paradigma, sobre el que cabe preguntar:** - **¿Ha implantado cada organismo una Política de Seguridad de la Información Propia?** - **En caso afirmativo, ¿cómo se asegura el organismo su permanente observancia?** - **¿Supervisa la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad en todos los organismos la observancia de lo dispuesto en esta Política Modelo? ¿Qué indicadores y métricas está usando? ¿Cuáles han sido los últimos resultados?** **Hasta dónde se ha podido investigar, los únicos desarrollos derivados de esta Política que se han expresado públicamente han sido:** Disposición 678 / 2014 - POLICÍA DE SEGURIDAD AEROPORTUARIA 01-Ago-2014

[27] La Coordinación de Emergencias en Redes Teleinformáticas es una unidad de respuesta ante incidentes en redes, que centraliza y coordina los esfuerzos para el manejo de los incidentes de seguridad que afecten a los recursos informáticos del Sector Público.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA POLICÍA DE SEGURIDAD AEROPORTUARIA APRUEBASE LA "POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA POLICÍA DE SEGURIDAD AEROPORTUARIA", ELABORADA EN CUMPLIMIENTO DE LA DISPOSICIÓN PSA Nº 561/13 POR EL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DE LA POLICÍA DE SEGURIDAD AEROPORTUARIA. <u>Resolución 970 / 2014 - JEFATURA DE GABINETE DE MINISTROS</u> 05-Nov-2014 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN - CONFORMASE CONFORMASE EL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DE LA JEFATURA DE GABINETE DE MINISTROS QUE ESTARÁ INTEGRADO POR LOS TITULARES DE LAS SECRETARIAS QUE SE ENCUENTRAN BAJO LA ORBITA DEL JEFE DE GABINETE DE MINISTROS, JEFA DE GABINETE DE ASESORES, COORDINADORA DE GABINETE DE ASESORES, TITULAR DE LA UNIDAD DE AUDITORIA INTERNA Y TITULAR DE LA SUBSECRETARIA DE TECNOLOGÍAS DE GESTION DE LA SECRETARIA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA. <u>Resolución 181 / 2020 - INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS</u> 19-Nov-2020 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN - CREASE CREASE EN LA ORBITA DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS, ADMINISTRACION DESCONCENTRADA EN EL ÁMBITO DEL MINISTERIO DE ECONOMÍA, EL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN COMO ÚNICO CANAL PARA REALIZAR PROPUESTAS A LA DIRECCIÓN DEL INSTITUTO RELATIVAS A LA POLÍTICA DE SEGURIDAD, LOS PROCEDIMIENTOS INTERNOS Y LOS SISTEMAS DE PREVENCIÓN A FIN DE ASEGURAR LA HOMOGENEIDAD Y UNICIDAD DE CRITERIOS Y OBJETIVOS EN LA MATERIA.

- **<u>Decreto 577/2017. Creación del Comité de Ciberseguridad.</u>**

Por el Poder Ejecutivo Nacional (P.E.N.)

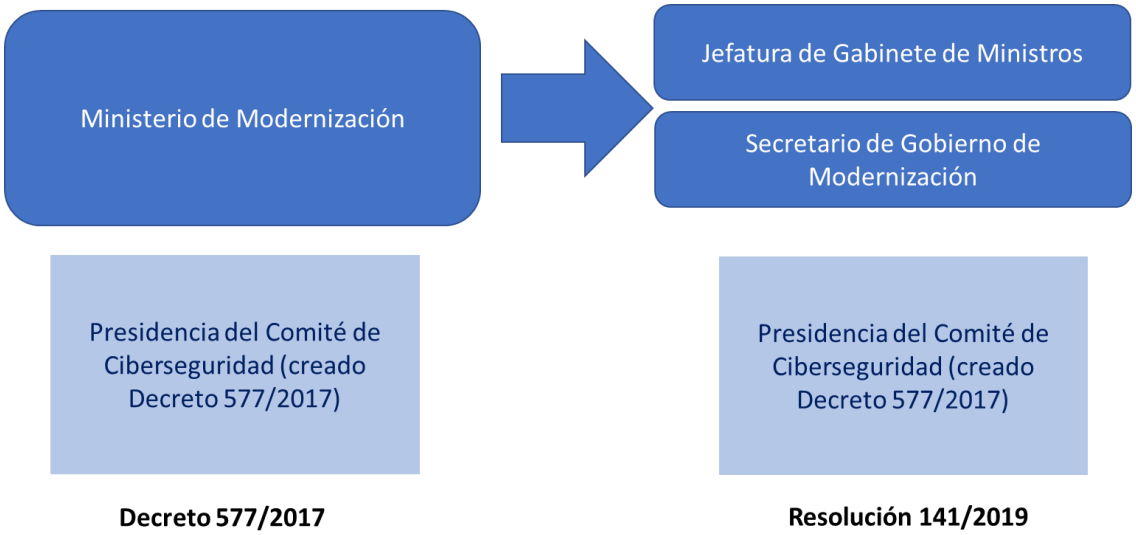
Este Decreto fue sancionado el 28 de julio de 2017 y publicado en el Boletín Nacional del 31 de Julio de 2017.

El Decreto crea el **Comité de Ciberseguridad** en la órbita del Ministerio de Modernización, que estará integrado por representantes del citado ministerio, del Ministerio de Defensa y del Ministerio de Seguridad, el cual tendrá por objetivo la elaboración de la Estrategia Nacional de Ciberseguridad. El Comité de Ciberseguridad será presidido por el Ministro de Modernización.

	Comentario: **No obstante, por posterior Resolución 141/2019 de la Jefatura de Gabinete de Ministros, se modifica la adscripción de este Comité, cuyo presidente pasa a depender del Secretario de Gobierno de Modernización, dependiente de la Jefatura de Gabinete de Ministros, lo que nos parece**

	positivo porque eleva la posición del órgano y facilita su incardinación en la ciberseguridad pública nacional.

La figura siguiente muestra la transición citada:



Este Decreto 577/2017 regulaba que el Comité de Ciberseguridad estaría formado por representantes de los ministerios de Modernización, Defensa y Seguridad, y cuyo objetivo esencial será la elaboración de la **Estrategia Nacional de Ciberseguridad**.

Como decimos, según Decreto 480/2019 (que modifica el 577/2017), el Comité de Ciberseguridad está **compuesto** por los siguientes cargos y/o representantes:

- Secretario de Gobierno de Modernización, como Vicejefe de Gabinete de la Jefatura de Gabinete de Ministros (presidente).
- Secretaría de Asuntos Estratégicos de la Jefatura de Gabinete de Ministros.
- Ministerio de Defensa.
- Ministerio de Seguridad.
- Ministerio de Relaciones Exteriores y Culto.
- Ministerio de Justicia y Derechos Humanos.

Las **funciones** del Comité de Ciberseguridad son (art. 2):

a) Desarrollar la Estrategia Nacional de Ciberseguridad, en coordinación con las áreas competentes de la Administración Pública Nacional.
b) Elaborar el plan de acción necesario para la implementación de la Estrategia Nacional de Ciberseguridad.
c) Convocar a otros organismos para que participen en la implementación de medidas en el marco del plan de acción elaborado conforme lo establecido en el punto b) precedente.
d) Impulsar el dictado de un marco normativo en materia de Ciberseguridad.
e) Fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales.
f) Participar en el desarrollo de acciones inherentes a la Ciberseguridad nacional que se le encomienden.

⚠	**Advertencia / Cuestión a analizar:** **Tratándose de un Comité con las importantes funciones que se señalan en la norma, entendemos que su composición es bastante exigua.** **Obsérvese que una Estrategia Nacional de Ciberseguridad, que nace como respuesta a la problemática de los riesgos del ciberespacio y que resulta de aplicación a toda la nación (sector público, sector privado, profesionales y ciudadanos), debe contemplar el impacto de la materialización de tales riesgos en todos los sectores concernidos, incluyendo también la economía, ciencia, cultura, educación, interior, salud, etc.**

- **Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad.**

Por la Secretaría de Gobierno de Modernización.

Esta Resolución fue sancionada el 24 de mayo de 2019 y publicada en el Boletín Nacional del 28 de Mayo de 2019.

⚠	**Advertencia / Cuestión a analizar:** **Nos parece que, por la importancia de esta norma, que viene a aprobar el instrumento político-estratégico más importante de la nación Argentina en materia de ciberseguridad pública, evidencia que el instrumento jurídico elegido posee un rango menor del deseable.**

La Resolución reconoce que el ciberespacio se ha constituido en un elemento esencial en la vida de las personas y las organizaciones, y que este nuevo paradigma, junto a sus enormes beneficios, implica también graves riesgos a la seguridad de las personas, las organizaciones y los gobiernos, estando el entorno digital amenazado por nuevas formas de delitos, la acción de grupos terroristas y la confrontación entre los Estados.

Por ello, consciente de esta realidad, el Estado Nacional ha fijado dentro de sus planes de largo plazo una serie de objetivos e iniciativas prioritarias, entre las que se encuentra dotar a nuestro país de capacidades de prevención, detección y neutralización de cualquier actividad maliciosa, contribuyendo a un ciberespacio seguro para quienes habitan nuestro país, para lo que se requiere de una **Estrategia Nacional de Ciberseguridad** en la que se establezcan los principios esenciales y los objetivos centrales de la República Argentina en torno a su proyecto para la protección del ciberespacio.

La Estrategia (art. 3) invita a las Provincias y a la Ciudad Autónoma de Buenos Aires a adherirse a dicha Estrategia.

⚠	**Advertencia / Cuestión a analizar:** **La redacción del art. 3 de la Estrategia parece dar a entender que la observancia de su contenido no es imperativa para las Provincias y para la Ciudad Autónoma de Buenos Aires. De confirmarse esto, supondría una grave merma de la esperanza de penetración de la Estrategia en la Argentina, muy especialmente en las entidades del sector público, y alentaría la publicación de una nueva Estrategia bajo el amparo de un instrumento jurídico de mayor nivel.**

Los **Principios Rectores** recogidos en la Estrategia Nacional de Ciberseguridad son:

- Respeto por los derechos y libertades individuales.
- Liderazgo, construcción de capacidades y fortalecimiento Federal (el Estado Nacional debe asumir el liderazgo y construir capacidades de detección, prevención y respuesta a incidentes cibernéticos, en coordinación con los estados provinciales, la Ciudad Autónoma de Buenos Aires, los municipios, el sector privado, el sector académico y la sociedad civil, con una adecuada articulación de las competencias y recursos involucrados).
- Integración internacional.
- Cultura de ciberseguridad y responsabilidad compartida.
- Fortalecimiento del desarrollo socioeconómico.

Por su parte, los **Objetivos** y **Acciones** que determina la Estrategia son:

Objetivos	Acciones
Objetivo 1) **Concientización** del uso seguro del Ciberespacio. En el marco del presente documento, es el proceso de formación del discernimiento en cuanto a los riesgos que conlleva el uso de las tecnologías, entender la cultura del Ciberespacio y junto a ello la adopción de hábitos basados en las mejores prácticas.	Para ello será necesario: • Crear un plan programático de concientización de alcance nacional sobre la seguridad en el Ciberespacio, abarcativo de la sociedad en su conjunto. • Fortalecer y articular con los sectores privados y las organizaciones civiles la promoción de contenidos de concientización. • Incrementar las actividades de concientización en el ámbito educativo.
Objetivo 2) **Capacitación** y educación en el uso seguro del Ciberespacio. En el marco del presente documento, es entendido como el proceso de formación y	Para ello será necesario: • Promover la formación de profesionales, técnicos e investigadores. • Desarrollar talleres y ejercicios, tanto gubernamentales como con los sectores privados y el sector civil.

adquisición de conocimientos, aptitudes y habilidades necesarias para un uso seguro del Ciberespacio.	• Fortalecer la capacitación en técnicas de prevención, detección, respuesta y resiliencia ante incidentes. • Incrementar las actividades transversales de formación en el sector académico.
Objetivo 3) Desarrollo del **marco normativo.** Adecuar y generar las normas jurídicas, marcos regulatorios, estándares y protocolos, para hacer frente a los desafíos que plantean los riesgos del ciberespacio, asegurando el respeto de los derechos fundamentales.	Para ello será necesario: • Actualizar el marco jurídico tomando en cuenta la necesidad de principios comunes mínimos con la comunidad internacional. • Actualizar el marco normativo técnico en línea con las normas técnicas y las buenas prácticas reconocidas internacionalmente.
Objetivo 4) Fortalecimiento de **capacidades de prevención, detección y respuesta**. Fortalecer las capacidades de prevención, detección y respuesta frente al uso del Ciberespacio con fines ilegales.	Para ello será necesario: • Ampliar y mejorar las capacidades de detección y análisis de ciberamenazas para una defensa y protección más eficaz de los activos digitales. • Ampliar y mejorar las capacidades de detección y respuesta ante ciberataques dirigidos contra objetivos de carácter nacional. • Optimizar y promover las capacidades de los organismos y fuerzas de seguridad con competencia en la investigación y persecución de la delincuencia, el crimen organizado y el terrorismo en el ciberespacio. • Garantizar la coordinación, cooperación y el intercambio de información entre el Estado Nacional y los estados provinciales, la Ciudad Autónoma de Buenos Aires, los municipios, el sector privado, el sector académico y la sociedad civil, con una adecuada articulación de las competencias y recursos involucrados.
Objetivo 5) Protección y recuperación de los **sistemas de información del Sector Público**. Garantizar que los sistemas de información que utiliza el Sector Público, incluyendo sus organismos descentralizados, posean un adecuado nivel de seguridad y recuperación.	Para ello será necesario: • Desarrollar las políticas públicas necesarias para garantizar la seguridad y resiliencia de los sistemas de información del Sector Público, incluyendo los mecanismos de control para la aplicación de las Políticas de Seguridad de la Información. • Trabajar coordinadamente con los responsables de seguridad informática de los Entes Reguladores y otros organismos de la Administración Pública Nacional y descentralizados, las administraciones provinciales, de la Ciudad Autónoma de Buenos Aires, de los municipios y el sector privado, en los cuales se hayan identificado sistemas de información críticos. • Impulsar la realización de auditorías y la generación de métricas, que permitan evaluar la mejora constante

	de los niveles de seguridad de los sistemas y la capacidad de resiliencia de los mismos. • Continuar el proceso de jerarquización y fortalecimiento de los recursos humanos encargados de la seguridad de los sistemas informáticos del Estado Nacional.
Objetivo 6) Fomento de la **industria de la ciberseguridad**. Promover el desarrollo de la industria nacional en los sectores vinculados a la ciberseguridad.	Para ello será necesario: • Impulsar el desarrollo de la industria de ciberseguridad nacional. • Fomentar y potenciar las capacidades tecnológicas precisas para disponer de soluciones confiables que permitan proteger adecuadamente los sistemas frente a las diferentes amenazas, fomentando las actividades de investigación, desarrollo e innovación (I+D+i) tanto a nivel público como privado.
Objetivo 7) **Cooperación Internacional.** Contribuir a la mejora de la ciberseguridad en el ámbito internacional.	Para ello será necesario: • Promover el desarrollo de acuerdos a nivel regional e internacional que contribuyan a la generación de un Ciberespacio pacífico y seguro. • Fortalecer la presencia de la República Argentina en todos los organismos internacionales, en materia de ciberseguridad. • Mantener una participación activa en todos los ámbitos académicos y técnicos internacionales en lo que se trabaje la temática.
Objetivo 8) Protección de las **Infraestructuras Críticas Nacionales de Información**. Fortalecimiento de la cooperación público-privada en resguardo de las infraestructuras críticas de la información del país.	Para ello será necesario: • Promover la definición, identificación y protección de las infraestructuras críticas nacionales de la información. • Articular los esfuerzos públicos-privados para la construcción de capacidades de detección, resguardo y respuesta ante amenazas y ataques, a partir de los recursos y responsabilidades de cada organización. • Fortalecer la cooperación en el intercambio de información ante vulnerabilidades y amenazas. • Promover esfuerzos coordinados dentro de las redes industriales con el objetivo de fortalecer y resguardar los servicios críticos y productivos.

	Comentario: **Los contenidos de la Estrategia nos parecen adecuados, aunque creemos que la ordenación de los 8 objetivos descritos debería formularse atendiendo al grado de importancia del objetivo concreto. (Por ejemplo, entendemos que debe ser prioritaria la protección de los sistemas del sector público o las infraestructuras críticas de información (objetivos 8 y 6,**

	respectivamente), antes que otros objetivos (tales como la concientización o la capacitación, que deben considerarse como meros objetivos instrumentales dirigidos a satisfacer los primeros.)

Conviene observar cómo **el Objetivo 8 de la Estrategia se dirige a la Protección de las Infraestructuras Críticas Nacionales de Información.**

La Estrategia Nacional de Ciberseguridad crea la **Unidad Ejecutiva del Comité de Ciberseguridad**, con las siguientes **funciones**:

1. Convocar, organizar y realizar el seguimiento de las reuniones del Comité de Ciberseguridad.
2. Coordinar la labor de los Grupos de Trabajo que se creen, interactuando con los Entes Reguladores, de corresponder.
3. Elaborar los proyectos de actos administrativos y formular las propuestas de acciones, cuando así lo disponga el Secretario de Gobierno de Modernización de la Jefatura de Gabinete de Ministros, en virtud de lo dispuesto por el artículo 5° del Decreto N° 577/2017.
4. Convocar a otros organismos cuya presencia resulte conveniente, en base a las decisiones que adopte el Comité de Ciberseguridad.
5. Documentar y comunicar a través de actas, las decisiones y cursos de acción que adopte el Comité de Ciberseguridad.
6. Poner a disposición de los integrantes del Comité de Ciberseguridad los documentos que sean necesarios para el desarrollo de su actividad.
7. Mantener un registro actualizado de todos los documentos que se elaboren.
8. Brindar asistencia administrativa al Comité de Ciberseguridad y llevar adelante todas las labores encomendadas por este.

⚠	**Advertencia / Cuestión a analizar:** **Por la importancia en la operativa diaria que tendría la Unidad Ejecutiva del Comité de Ciberseguridad, quizás hubiera sido más adecuado regular su creación a través de un instrumento jurídico de rango mayor (como fue el caso de la creación del propio Comité de Ciberseguridad, creado por Decreto del Poder ejecutivo Nacional), lo que podría haberse aprovechado para publicar la propia Estrategia con tal instrumento jurídico.** **Por otro lado, desconocemos en el momento de redactar estas líneas, la composición final de dicha Unidad Ejecutiva del Comité de Ciberseguridad y si ha mantenido reuniones periódicas.**

- **<u>Resolución 1523/2019. Definición de Infraestructuras Críticas.</u>**

Por la Secretaría de Gobierno de Modernización.

Esta Resolución fue sancionada el 12 septiembre de 2019 y publicada en el Boletín Nacional del 18 de septiembre de 2019.

⚠	**Advertencia / Cuestión a analizar:** **Puesto que uno de los objetivos de esta norma es determinar los criterios de identificación de las infraestructuras críticas y los sectores afectados, quizás hubiera sido más adecuado elevar el rango normativo del instrumento jurídico utilizado (por ejemplo, elevándolo de Resolución a Decreto del Poder Ejecutivo Nacional).**

Efectivamente, esta Resolución:

- Aprueba la definición de **Infraestructuras Críticas** y de **Infraestructuras Críticas de Información,**
- Enumera los **criterios de identificación** y la **determinación de los sectores alcanzados,**
- Aprueba el **glosario de términos de ciberseguridad**.

Esta Resolución trae causa del Decreto N° 577/2017, por el que se creó el Comité de Ciberseguridad, y entre cuyas funciones se encuentra la de "fijar los lineamientos y criterios para la definición, identificación y protección de las Infraestructuras Críticas Nacionales", según lo señala el inciso e) de su artículo 2° y de la Resolución de la Secretaría de Gobierno de Modernización N° 829/2019 que aprobó la Estrategia Nacional de Ciberseguridad, la cual incluye entre sus objetivos la Protección de las Infraestructuras Críticas de Información del país.

Esta Resolución, señala que los avances tecnológicos vienen acompañados de un panorama creciente y cambiante de amenazas, que podrían afectar seriamente a **servicios esenciales** de nuestra sociedad, cuya prestación es posible gracias a la existencia de infraestructuras tecnológicas, y que estas amenazas afectan tanto las infraestructuras tecnológicas utilizadas en **ambientes organizacionales**, pero también en **entornos industriales**, cuyo impacto podría inclusive producir daño a las personas o a los activos físicos, como lo han demostrado ya casos de ciberataques registrados en otros países.

En base a ello, la Resolución considera que establecer la **definición y los criterios de identificación y proponer un agrupamiento en sectores tanto para infraestructuras de tecnologías de información como de operación**, constituye un requisito esencial para la elaboración de las normas, políticas y planes para la protección de las Infraestructuras que respaldan servicios críticos, permitiendo la identificación de sistemas, equipamiento y actores involucrados, entre otros aspectos.

El Anexo I de la Resolución define los conceptos:

Infraestructuras Críticas	Aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya

	destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente.
Infraestructuras Críticas de Información	Son las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas.

Comentario:

De las definiciones anteriores podemos colegir que resultan de aplicación tanto a las entidades del sector público como del sector privado.

Seguidamente, la Resolución señala los **criterios de identificación** de Infraestructuras Críticas, a saber:

- Impacto en la vida humana.
- Impacto económico.
- Impacto en el medio ambiente.
- Impacto en el ejercicio de los derechos humanos y de las libertades
- Impacto público o social.
- Impacto en el ejercicio de las funciones del estado.
- Impacto en la soberanía nacional.
- Impacto en mantenimiento de la integridad territorial nacional.

Advertencia / Cuestión a analizar:

En relación con los criterios anteriores, esta Resolución no concreta los umbrales a partir de los cuales cabría decir que la situación ha generado un impacto significativo, por lo que no está determinado el momento a partir del cual a una situación concreta se le puede conferir el carácter de "crítica".

En otras regulaciones nacionales se determina con más detalle estos umbrales. Por ejemplo, en el caso de España, el Anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (transposición de la Directiva Europea NIS), señala:

4. Nivel de impacto del ciberincidente

El indicador de impacto de un ciberincidente se determinará evaluando las consecuencias que tal ciberincidente ha tenido en las funciones y actividades de la organización afectada, en sus activos o en los individuos afectados. De acuerdo a ello, se tienen en cuenta aspectos como las consecuencias potenciales o materializadas que provoca una determinada amenaza en un

	sistema de información y/o comunicación, así como en la propia entidad afectada (organismos públicos o privados, y particulares). *Los criterios empleados para la determinación del nivel de impacto asociado a un ciberincidente atienden a los siguientes parámetros:* *– Impacto en la Seguridad Nacional o en la seguridad ciudadana.* *– Efectos en la prestación de un servicio esencial o en una infraestructura crítica.* *– Tipología de la información o sistemas afectados.* *– Grado de afectación a las instalaciones de la organización.* *– Posible interrupción en la prestación del servicio normal de la organización.* *– Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.* *– Pérdidas económicas.* *– Extensión geográfica afectada.* *– Daños reputacionales asociados.* *Los incidentes se asociarán a alguno de los siguientes niveles de impacto: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO, SIN IMPACTO.* *Nivel crítico:* *– Afecta apreciablemente a la Seguridad Nacional.* *– Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.* *– Afecta a una infraestructura crítica.* *– Afecta a sistemas clasificados SECRETO.* *– Afecta a más del 90 % de los sistemas de la organización.* *– Interrupción en la prestación del servicio superior a 24 horas y superior al 50 % de los usuarios.* *– El ciberincidente precisa para resolverse más de 100 Jornadas-Persona.* *– Impacto económico superior al 0,1 % del Producto Interior Bruto (PIB) actual.* *– Extensión geográfica supranacional.* *– Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.* *Nivel muy alto:* *– Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.* *– Afecta apreciablemente a actividades oficiales o misiones en el extranjero.* *– Afecta a un servicio esencial.* *– Afecta a sistemas clasificados RESERVADO.* *– Afecta a más del 75 % de los sistemas de la organización.* *– Interrupción en la prestación del servicio superior a 8 horas y superior al 35 % de los usuarios.* *– El ciberincidente precisa para resolverse entre 30 y 100 Jornadas-Persona.* *– Impacto económico entre el 0,07 % y el 0,1 % del PIB actual.*

	– Extensión geográfica superior a 4 Comunidades Autónomas (CC.AA.) o un territorio de Interés Singular (TIS, se considera como tal a las ciudades de Ceuta y Melilla y a cada una de las islas que forman los archipiélagos de las islas Baleares y las islas Canarias). *– Daños reputacionales a la imagen del país (marca España).* *– Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.* *Nivel alto:* *– Afecta a más del 50 % de los sistemas de la organización.* *– Interrupción en la prestación del servicio superior a 1 hora y superior al 10 % de usuarios.* *– El ciberincidente precisa para resolverse entre 5 y 30 Jornadas-Persona.* *– Impacto económico entre el 0,03 % y el 0,07 % del PIB actual.* *– Extensión geográfica superior a 3 CC.AA.* *– Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.* *Nivel medio:* *– Afecta a más del 20 % de los sistemas de la organización.* *– Interrupción en la presentación del servicio superior al 5 % de usuarios.* *– El ciberincidente precisa para resolverse entre 1 y 5 Jornadas-Persona.* *– Impacto económico entre el 0,001 % y el 0,03 % del PIB actual.* *– Extensión geográfica superior a 2 CC.AA.* *– Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).* *Nivel bajo:* *– Afecta a los sistemas de la organización.* *– Interrupción de la prestación de un servicio.* *– El ciberincidente precisa para resolverse menos de 1 Jornada-Persona.* *– Impacto económico entre el 0,0001 % y el 0,001 % del PIB actual.* *– Extensión geográfica superior a 1 CC.AA.* *– Daños reputacionales puntuales, sin eco mediático.* *Sin impacto:* *– No hay ningún impacto apreciable.*

Por último, la Resolución identifica los **sectores de aplicación** de las Infraestructuras Críticas, a saber:

- Energía
- Tecnologías de Información y Comunicaciones

- Transportes
- Hídrico
- Salud
- Alimentación
- Finanzas
- Nuclear
- Químico
- Espacio
- Estado

⚠	**Advertencia / Cuestión a analizar:** **Al momento de redactar el presente documento no se poseen evidencias de la relación de instalaciones/dependencias que finalmente se han considerado como Infraestructuras Críticas o Infraestructuras Críticas de Información.** **Por otro lado, nos parece adecuada la relación de sectores afectados, coincidentes con los sectores propuestos por la todavía vigente Directiva Europea NIS, aunque siempre puede ampliarse, como lo ha propuesto el actual borrador de la que será próximamente la nueva Directiva NIS europea.** **Finalmente, se echa en falta la entidad o entidades que asumirían el control directo de la situación en caso de un incidente grave, por ejemplo, un ciberataque. En la Directiva Europea NIS y en las legislaciones que la transponen a los diferentes ordenamientos jurídicos nacionales, por ejemplo, se definen y determinan las llamadas *Autoridades Competentes* (en general, tantas como sectores implicados, que cubrirán los sectores determinados y que supervisarán la aplicación de la Directiva a escala nacional) y los *CSIRT de referencia* (uno o varios, que cumplan los requisitos establecidos en la Directiva, que cubran al menos los sectores que figuran la norma y los tipos de servicios digitales que se señalan, que serán responsables de la gestión de incidentes y riesgos de conformidad con un procedimiento claramente definido.)**

- **<u>Disposición 1/2021 Creación del Centro Nacional de Respuesta a Incidentes Informáticos (CERT.AR)</u>**

Por la Dirección Nacional de Ciberseguridad

Esta Disposición fue sancionada el 19 de Febrero de 2021 y publicada en el Boletín Nacional del 22 de Febrero de 2021.

La disposición crea, en el ámbito de la **Dirección Nacional de Ciberseguridad** el **Centro Nacional de Respuesta a Incidentes Informáticos (CERT.AR),** con el objetivo de coordinar la gestión de incidentes de seguridad a nivel nacional y prestar asistencia en aquellos que afecten a las

entidades y jurisdicciones del sector público nacional definidas en el inciso a) del artículo 8° de la ley nº 24.156 y sus modificatorios y a las Infraestructuras Críticas de Información, declaradas como tales.

	Comentario: **Nos parece positivo que el CERT.AR se constituya en el ámbito de la Dirección Nacional de Ciberseguridad, puesto que esta ubicación sitúa al tratamiento y gestión de los incidentes en el mejor lugar para proponer una respuesta nacional armonizada.** **No es descartable, sin embargo, que, andando el tiempo y la experiencia, se decida, al amparo de la posible determinación de Autoridades Competentes como las descritas en la Directiva Europea NIS, la creación de otros CSIRTs de alcance sectorial o departamental.**
	No obstante, por la importancia que este CSIRT va a tener en el futuro desenvolvimiento nacional de la ciberseguridad pública, entendemos que hubiera sido preferible su creación mediante un instrumento jurídico de rango mayor que una mera Decisión Administrativa.

Obsérvese que el ámbito de aplicación de esta Disposición **solo afecta** a:

- Administración Nacional, conformada por la Administración Central y los Organismos Descentralizados, comprendiendo en estos últimos a las Instituciones de Seguridad Social, y
- Infraestructuras Críticas de Información (ICI).

Por tanto, salvo que se trate de ICI, **quedan excluidas del ámbito de aplicación** de esta Disposición:

- Empresas y Sociedades del Estado, que abarca a las Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias.
- Entes Públicos excluidos expresamente de la Administración Nacional, que abarca a cualquier organización estatal no empresarial, con autarquía financiera, personalidad jurídica y patrimonio propio, donde el Estado nacional tenga el control mayoritario del patrimonio o de la formación de las decisiones, incluyendo aquellas entidades públicas no estatales donde el Estado nacional tenga el control de las decisiones.
- Fondos Fiduciarios integrados total o mayoritariamente con bienes y/o fondos del Estado nacional.
- Organizaciones privadas a las que se hayan acordado subsidios o aportes y a las instituciones o fondos cuya administración, guarda o conservación está a cargo del Estado nacional a través de sus Jurisdicciones o Entidades.

⚠	**Advertencia / Cuestión a analizar:** **Por su importancia, entendemos que esta Disposición debería también incluir en su ámbito de aplicación, al menos, al primer grupo: Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias.**

Es importante señalar que esta Disposición Administrativa establece como responsabilidad primaria del CERT.AR la de "*Entender en los aspectos relativos a la ciberseguridad y la protección de las infraestructuras críticas de información, así como también a la generación de capacidades de prevención, detección, defensa, respuesta y recupero ante incidentes de seguridad informática del Sector Público Nacional*", siendo sus concretas **funciones**:

a) Administrar y gestionar toda la información sobre reportes de incidentes de seguridad en las entidades y jurisdicciones del Sector Público Nacional definidas en el inciso a) del artículo 8° de la Ley Nº 24.156 y sus modificatorios.

b) Asesorar técnicamente ante incidentes de seguridad en sistemas informáticos que reporten las entidades y jurisdicciones enumeradas en el artículo 1° de la presente medida.

c) Coordinar las acciones a seguir, ante incidentes de seguridad, con otros Programas y equipos de respuesta a incidentes de la República Argentina.

d) Contribuir a incrementar la capacidad de prevención, alerta, detección y recuperación ante incidentes de seguridad informática que puedan afectar activos de información críticos del país.

e) Interactuar y cooperar con equipos de similar naturaleza de otros países.

f) Llevar un registro de estadísticas y establecer métricas a nivel nacional.

g) Coordinar la gestión de incidentes de seguridad informáticos que afecten recursos críticos a nivel nacional.

h) Impulsar la formación de capacidades de prevención, detección, alerta y recuperación para la respuesta ante incidentes de seguridad informática.

i) Cooperar con los gobiernos provinciales y de la Ciudad Autónoma de Buenos Aires en la gestión de incidentes de seguridad informática.

Estas funciones del CERT.AR se incardinan en la **Dirección Nacional de Ciberseguridad**, organismo creado por Decisión Administrativa N° 1865 de fecha 14 de octubre de 2020, que aprobó la estructura organizativa de primer y segundo nivel operativo de la Jefatura de Gabinete de Ministros, en el ámbito de la Secretaría de Innovación Pública, dependiente de dicha Jefatura de Gabinete de Ministros,

La antedicha Decisión Administrativa Nº 1865/2020 señalaba las **funciones** de la **Dirección Nacional de Ciberseguridad**, a saber:

- Diseñar políticas de ciberseguridad, en coordinación con los organismos del Estado Nacional con competencia en la materia,
- Elaborar planes, programas y proyectos con perspectiva federal en materia de ciberseguridad, en el ámbito de competencia de la Secretaría de Innovación Pública,
- Participar en las acciones destinadas a implementar los objetivos fijados en la Estrategia Nacional de Ciberseguridad, articulando proyectos con las diferentes áreas del Estado Nacional involucradas,
- Asistir a la Secretaría de Innovación Pública en su participación ante el Comité de Ciberseguridad creado por Decreto N° 577/17 y sus modificatorios, y colaborar en la ejecución de las decisiones que se adopten,
- Proponer proyectos de normas relacionados con la ciberseguridad en la República Argentina, en coordinación con las áreas con competencia en la materia,
- Entender en los procesos relativos al accionar del equipo de respuesta a emergencias informáticas a nivel nacional (CERT NACIONAL).

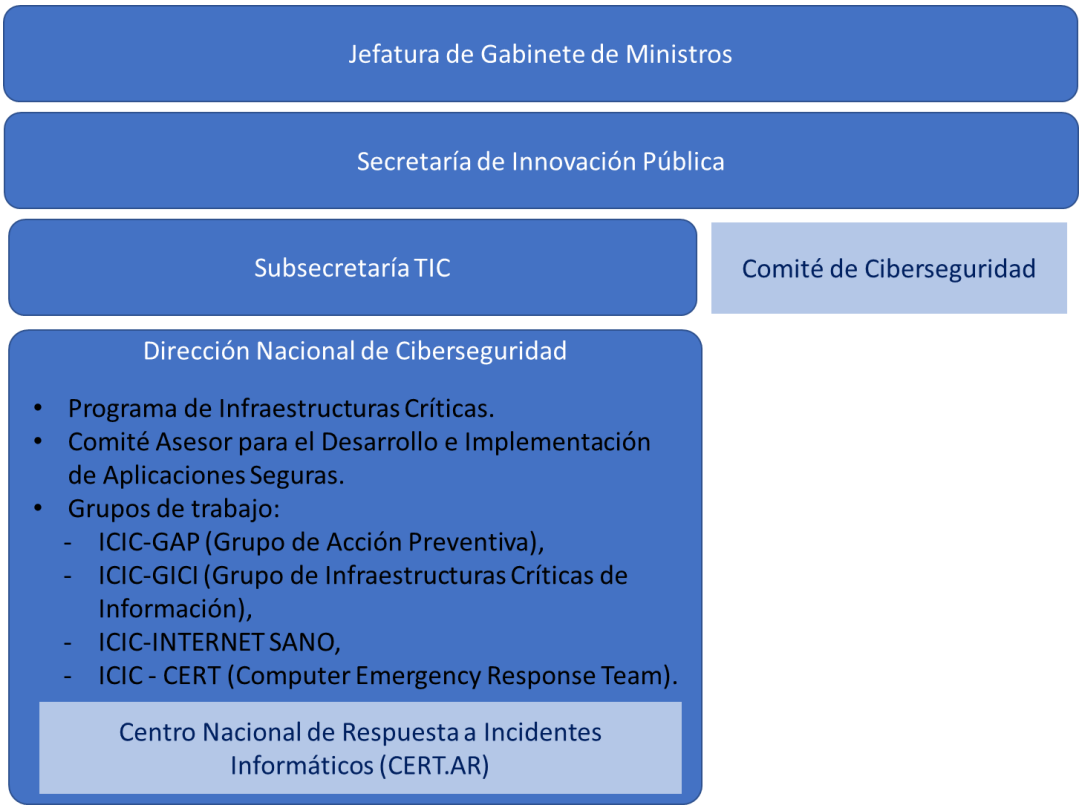
Advertencia / Cuestión a analizar:

Del análisis de las funciones encomendadas a esta Dirección Nacional de Ciberseguridad se deduce que posee unas atribuciones centradas más en los aspectos normativos y procedimentales de la ciberseguridad pública que en los operativos. Esta situación obliga a disponer de un organismo que aglutine la respuesta operativa a la problemática de la ciberseguridad pública en Argentina, en lo que habitualmente se conoce como un Centro Nacional de ciberseguridad, como más adelante veremos.

Asimismo, esta Disposición Administrativa Nº 1865/2020 **deroga la Disposición Nº2/2013 que creó la Oficina Nacional de Tecnologías de Información (ONTI).**

Posteriormente, mediante Disposición 6/2021, de la Dirección Nacional de Ciberseguridad de la Jefatura de Gabinete de Ministros, se crea el **Comité Asesor para el Desarrollo e Implementación de Aplicaciones Seguras**, en la órbita de la citada Dirección Nacional de Ciberseguridad.

Con todo ello, la estructura organizativa actual y el encuadramiento del CERT.AR se muestra en la figura siguiente:



⚠	**Advertencia / Cuestión a analizar:** **Conviene hacer notar que la estructura mostrada en la figura anterior hace descansar en un órgano de cuarto nivel la ejecución del Programa de Infraestructuras Críticas de Información del país. Convendría elevar su ubicación jerárquica a un vinel superior.**

- **<u>Decisión Administrativa 641/2021. Requisitos mínimos de seguridad de la información para organismos</u>**

Por la Jefatura de Gabinete de Ministros.

Esta Decisión Administrativa fue sancionada el 25 de junio de 2021 y publicada en el Boletín Nacional del 28 de junio de 2021.

Esta Decisión Administrativa aprueba los **Requisitos Mínimos de Seguridad de la Información** para los Organismos del Sector Público Nacional, y cuyo **ámbito de aplicación** alcanza a las entidades de la letra a) del art. 8 de la Ley 24.156 Administracion Financiera y Sistemas de C, es decir a la Administración Nacional, conformada por la Administración Central y los Organismos Descentralizados, comprendiendo en estos últimos a las Instituciones de Seguridad Social.

Por tanto, **quedan excluidas** del ámbito de esta Decisión Administrativa:

- Empresas y Sociedades del Estado que abarca a las Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales

donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias.

- Entes Públicos excluidos expresamente de la Administración Nacional, que abarca a cualquier organización estatal no empresarial, con autarquía financiera, personalidad jurídica y patrimonio propio, donde el Estado nacional tenga el control mayoritario del patrimonio o de la formación de las decisiones, incluyendo aquellas entidades públicas no estatales donde el Estado nacional tenga el control de las decisiones.
- Fondos Fiduciarios integrados total o mayoritariamente con bienes y/o fondos del Estado nacional.
- Organizaciones privadas a las que se hayan acordado subsidios o aportes y a las instituciones o fondos cuya administración, guarda o conservación está a cargo del Estado nacional a través de sus Jurisdicciones o Entidades.

a los que, no obstante, se invita a adherirse.

⚠	**Advertencia / Cuestión a analizar:** **Por su importancia, entendemos que esta Disposición debería también incluir en su ámbito de aplicación, al menos, al primer grupo: Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias.**

Esta Decisión Administrativa incluye como **Anexo** la relación de Requisitos Mínimos, entre cuyos epígrafes destacan:

Objetivos específicos:

- Proteger los derechos de los titulares de datos personales o propietarios de información que es tratada por el Sector Público Nacional.
- Proteger la información, los datos personales y activos de información propios del conjunto de organismos que componen el Sector Público Nacional.
- Promover una política pública que enmarque una conducta responsable en materia de seguridad de la información de los organismos que conforman el Sector Público Nacional, sus agentes y funcionarios.
- Evidenciar el compromiso e interés de quienes componen el Sector Público Nacional en pos del desarrollo.

Directrices:

- Política de Seguridad de la Información del organismo.
- Aspectos Organizativos de la Seguridad.
- Seguridad Informática de los Recursos Humanos.

- Gestión de Activos.
- Autenticación, Autorización y Control de Accesos.
- Uso de herramientas criptográficas.
- Seguridad física y ambiental.
- Seguridad operativa.
- Seguridad en las comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Relación con proveedores.
- Gestión de incidentes de seguridad.
- Aspectos de seguridad para la continuidad de la gestión.
- Cumplimiento.

Advertencia / Cuestión a analizar:
El mantenimiento de la ciberseguridad en los organismos comprendidos en el alcance de esta norma, además de resultar obligatoria, exigiría contar con un Esquema de Evaluación y Certificación de la Ciberseguridad, al que deberían someterse todas las entidades destinatarias de la norma.
Este es el caso, por ejemplo, del Esquema Nacional de Seguridad de España (Real Decreto 311/2022, heredero del Real Decreto 3/2010) y del modelo que está siguiendo la Unión Europea para disponer de Esquemas de Evaluación y Certificación de la Ciberseguridad.

Esta Decisión Administrativa **exige** que:

- Las entidades y jurisdicciones del Sector Público Nacional comprendidas en el ámbito de aplicación de esta norma deberán aprobar sus Planes de Seguridad en el plazo máximo de noventa (90) días desde su entrada en vigor, que deberán establecer los plazos en que se dará cumplimiento a cada uno de los Requisitos Mínimos de Seguridad de la Información para los Organismos del Sector Público Nacional establecidos en el Anexo I citado, plazo que no podrá ser posterior al 31 de diciembre de 2022.

Advertencia / Cuestión a analizar:

¿Se ha cumplido este plazo? ¿Cuántas entidades han aprobado sus propios Planes de Seguridad?

- Dichos Planes de Seguridad deberán ser remitidos a la Dirección Nacional de Ciberseguridad de la Secretaría de Innovación Pública, dependiente de la Jefatura de Gabinete de Ministros y/o a la que en el futuro la reemplace, dentro de un plazo máximo de noventa (90) días desde la entrada en vigor de la norma.

⚠	**Advertencia / Cuestión a analizar:** **¿Se ha hecho? ¿Qué organismos lo han hecho?**

- Las máximas autoridades de las entidades y jurisdicciones comprendidas en el ámbito de aplicación de la norma deberán asignar las funciones relativas a la seguridad de sus sistemas de información al área con competencia en la materia e informar, mediante Comunicación Oficial a través del Sistema de Gestión Documental Electrónica (GDE) a la Dirección Nacional de Ciberseguridad de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros el nombre, apellido y datos de contacto del responsable del área designada, dentro del plazo de sesenta (60) días corridos desde la entrada en vigor de la norma.

⚠	**Advertencia / Cuestión a analizar:** **¿Se ha hecho? ¿Qué organismos lo han hecho?**

- Las entidades y jurisdicciones comprendidas en el ámbito de aplicación de la norma deberán adoptar las medidas preventivas, detectivas y correctivas destinadas a proteger la información que reciban, generen o gestionen como asimismo sus recursos.

⚠	**Advertencia / Cuestión a analizar:** **¿Se ha hecho? ¿Qué organismos lo han hecho?**

- Las entidades y jurisdicciones del ámbito de aplicación de la norma deberán reportar a la Dirección Nacional de Ciberseguridad de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros los incidentes de seguridad que se produzcan dentro de sus ámbitos, dentro de las cuarenta y ocho (48) horas de tomado conocimiento de su ocurrencia o de su potencial ocurrencia.

⚠	**Advertencia / Cuestión a analizar:** **¿Se ha hecho? ¿Qué organismos lo han hecho?**

5. RESUMEN DE HALLAZGOS, CONCLUSIONES Y PLAN DE ACCIÓN

5.1 Resumen de hallazgos: advertencias y/o cuestiones a analizar

A lo largo del presente informe hemos venido recogiendo los aspectos positivos que, a nuestro juicio, demuestra la realidad jurídica e institucional de la argentina en materia de tratamiento de la ciberseguridad de sus IC, y también aquellas otras cuestiones que pueden constituir un riesgo para alcanzar la eficacia y eficiencia de tal tratamiento o que merecen una reflexión adicional.

De estas últimas (Advertencias y/o cuestiones a analizar) reproducimos aquellas que nos han parecido más significativas.

Sobre la Resolución 580/2011 (Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad – Creación):

- No se dispone de evidencias que reflejen hasta qué punto de se han desarrollado los objetivos específicos del Plan Nacional de Infraestructuras Críticas de Información y Ciberseguridad en las posteriores actuaciones -de naturaleza jurídica u operativa.
- De la redacción de la letra c) de las funciones encomendadas a la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad cabe deducir que la adhesión al Programa Nacional de Infraestructuras Críticas es opcional y voluntario para las organizaciones. Si esto es así, la ausencia de un marco regulatorio común y obligatorio para todas las Infraestructuras Críticas de Información, ya se encuentren en manos públicas o privadas, dificulta una protección armonizada de dichas infraestructuras, pudiendo poner en riesgo el mantenimiento de la ciberseguridad nacional.
- Las funciones encomendadas a la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad citadas no contemplan la implementación de todos los objetivos específicos del Plan Nacional de Infraestructuras Críticas de Información y Ciberseguridad, señalados anteriormente.

Sobre la Disposición ONTI 3/2013. Aprobación de la Política Modelo de Seguridad de la Información:

- Llama la atención que una norma de la importancia de esta, que supone sentar las bases para disponer de una “Política de Seguridad de la Información”, de alcance público, haya sido dictada por un instrumento de rango jurídico menor, como es el caso de las Decisiones Administrativas.
- De la redacción del punto “1. Introducción” de la Política de Seguridad de la Información, estas obligaciones solo resultan de aplicación a las entidades comprendidas en los incisos a) y c) del art. 8º de la Ley 24.156; es decir: a) Administración Nacional, conformada por la Administración Central y los Organismos Descentralizados, comprendiendo en estos últimos a las Instituciones de Seguridad Social y c) Entes Públicos excluidos expresamente de la Administración Nacional, que abarca a cualquier organización estatal no empresarial, con autarquía financiera, personalidad jurídica y patrimonio propio, donde el Estado nacional tenga el control mayoritario del patrimonio o de la formación de las decisiones, incluyendo aquellas entidades públicas no estatales donde el Estado nacional tenga el control de las decisiones.

Quedan excluidas, por tanto, de la aplicación de esta norma: b) Empresas y Sociedades del Estado que abarca a las Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias. d) Fondos Fiduciarios integrados total o mayoritariamente con bienes y/o fondos del Estado nacional. Serán aplicables las normas de esta ley, en lo relativo a la rendición de cuentas de las organizaciones privadas a las que se hayan acordado subsidios o aportes y a las instituciones o fondos cuya administración, guarda o conservación está a cargo del Estado nacional a través de sus Jurisdicciones o Entidades.

De todo lo anterior se deduce que esta Política Modelo solo afectará a aquellas Infraestructuras Críticas de Información comprendidas en su ámbito de aplicación, perdiendo, en consecuencia, el carácter nacional que debería perseguir, para garantizar que todas las IC disponen de su Política de Seguridad.

- No se dispone de evidencias del grado de cumplimiento de las cuatro obligaciones expresadas en la Política de Seguridad Modelo en los organismos del Sector Público Nacional.
- No se dispone de evidencias del establecimiento de las comunicaciones en las Políticas de Seguridad de cada organismo.
- No se dispone de evidencias sobre: 1. El grado de aprobación en cada organismo de la Política de Seguridad; 2. En caso afirmativo, medios para asegurar su permanente observancia; 3. El grado de supervisión de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad en todos los organismos la observancia de lo dispuesto en la Política Modelo; 4. Indicadores y métricas usadas; 5. Resultados alcanzados.

Sobre el Decreto 577/2017. Creación del Comité de Ciberseguridad:

- Tratándose de un Comité con las importantes funciones que se señalan en la norma, entendemos que su composición es bastante exigua. Obsérvese que una Estrategia Nacional de Ciberseguridad, que nace como respuesta a la problemática de los riesgos del ciberespacio y que resulta de aplicación a toda la nación (sector público, sector privado, profesionales y ciudadanos), debe contemplar el impacto de la materialización de tales riesgos en todos los sectores concernidos, incluyendo también la economía, ciencia, cultura, educación, interior, salud, etc.

Sobre la Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad:

- Nos parece que, por la importancia de esta norma, que viene a aprobar el instrumento político-estratégico más importante de la nación Argentina en materia de ciberseguridad pública, evidencia que el instrumento jurídico elegido posee un rango menor del deseable.
- La redacción del art. 3 de la Estrategia parece dar a entender que la observancia de su contenido no es imperativa para las Provincias y para la Ciudad Autónoma de Buenos Aires. De confirmarse esto, supondría una grave merma de la esperanza de penetración de la Estrategia en la Argentina, muy especialmente en las entidades del sector público, y alentaría la publicación de una nueva Estrategia bajo el amparo de un instrumento jurídico de mayor nivel.

- Por la importancia en la operativa diaria que tendría la Unidad Ejecutiva del Comité de Ciberseguridad, quizás hubiera sido más adecuado regular su creación a través de un instrumento jurídico de rango mayor (como fue el caso de la creación del propio Comité de Ciberseguridad, creado por Decreto del Poder ejecutivo Nacional), lo que podría haberse aprovechado para publicar la propia Estrategia con tal instrumento jurídico. Por otro lado, desconocemos en el momento de redactar estas líneas, la composición final de dicha Unidad Ejecutiva del Comité de Ciberseguridad y si ha mantenido reuniones periódicas.

Sobre la Resolución 1523/2019. Definición de Infraestructuras Críticas:

- Puesto que uno de los objetivos de esta norma es determinar los criterios de identificación de las infraestructuras críticas y los sectores afectados, quizás hubiera sido más adecuado elevar el rango normativo del instrumento jurídico utilizado (por ejemplo, elevándolo de Resolución a Decreto del Poder Ejecutivo Nacional).
- En relación con los criterios para la identificación de las Infraestructuras Críticas, esta Resolución no concreta los umbrales a partir de los cuales cabría decir que la situación ha generado un impacto significativo, por lo que no está determinado el momento a partir del cual a una situación concreta se le puede conferir el carácter de "crítica".
- No se dispone de evidencias de la relación de instalaciones/dependencias que finalmente se han considerado como Infraestructuras Críticas o Infraestructuras Críticas de Información.
- Aunque parece adecuada la relación de sectores afectados, coincidentes con los sectores propuestos por la todavía vigente Directiva Europea NIS (aunque siempre puede ampliarse, como lo ha propuesto el actual borrador de la que será próximamente la nueva Directiva NIS europea), se echa en falta la entidad o entidades que asumirían el control directo de la situación en caso de un incidente grave, por ejemplo, un ciberataque. En la Directiva Europea NIS y en las legislaciones que la transponen a los diferentes ordenamientos jurídicos nacionales, por ejemplo, se definen y determinan las llamadas Autoridades Competentes (en general, tantas como sectores implicados, que cubrirán los sectores determinados y que supervisarán la aplicación de la Directiva a escala nacional) y los CSIRT de referencia (uno o varios, que cumplan los requisitos establecidos en la Directiva, que cubran al menos los sectores que figuran la norma y los tipos de servicios digitales que se señalan, que serán responsables de la gestión de incidentes y riesgos de conformidad con un procedimiento claramente definido.)

Sobre la Disposición 1/2021 Creación del Centro Nacional de Respuesta a Incidentes Informáticos (CERT.AR):

- Por la importancia que este CSIRT va a tener en el futuro desenvolvimiento nacional de la ciberseguridad pública, entendemos que hubiera sido preferible su creación mediante un instrumento jurídico de rango mayor que una mera Decisión Administrativa.
- Por su importancia, entendemos que esta Disposición debería también incluir en su ámbito de aplicación, al menos, al primer grupo: Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias.

- Del análisis de las funciones encomendadas a la Dirección Nacional de Ciberseguridad se deduce que posee unas atribuciones centradas más en los aspectos normativos y procedimentales de la ciberseguridad pública que en los operativos. Esta situación obliga a disponer de un organismo que aglutine la respuesta operativa a la problemática de la ciberseguridad pública en Argentina, en lo que habitualmente se conoce como un Centro Nacional de ciberseguridad.

Sobre la Decisión Administrativa 641/2021. Requisitos mínimos de seguridad de la información para organismos:

- Por su importancia, entendemos que esta Disposición debería también incluir en su ámbito de aplicación, al menos, al primer grupo: Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias.
- El mantenimiento de la ciberseguridad en los organismos comprendidos en el alcance de esta norma, además de resultar obligatoria, exigiría contar con un Esquema de Evaluación y Certificación de la Ciberseguridad, al que deberían someterse todas las entidades destinatarias de la norma. Este es el caso, por ejemplo, del Esquema Nacional de Seguridad de España (Real Decreto 311/2022, heredero del Real Decreto 3/2010) y del modelo que está siguiendo la Unión Europea para disponer de Esquemas de Evaluación y Certificación de la Ciberseguridad.
- No se dispone de evidencias: del cumplimiento del plazo de 90 días dado por la norma para que las entidades de su ámbito de aplicación aprueben sus Planes de Seguridad, del del número de entidades que lo han hecho, de su remisión a la Dirección Nacional de Ciberseguridad, de la designación de las funciones relativas a la seguridad de los sistemas, de la adopción de las medidas preventivas, detectivas y correctivas señaladas en la norma o de los reportes de los incidentes de seguridad.

5.2 Conclusiones generales

Todo lo anterior puede concretarse en las siguientes conclusiones esenciales:

(I) Se carece de una dirección operativa nacional de la ciberseguridad.

Como se ha señalado con anterioridad (Decisión Administrativa N° 1865 de fecha 14 de octubre de 2020), del análisis de las funciones que la regulación argentina encomienda a la Dirección Nacional de Ciberseguridad se deduce que posee unas atribuciones centradas más en los aspectos normativos y procedimentales de la ciberseguridad pública que en los operativos.

Por otro lado, las funciones encomendadas en su momento a la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad citadas no contemplan la implementación de todos los objetivos específicos del Plan Nacional de Infraestructuras Críticas de Información y Ciberseguridad, señalados anteriormente.

Esta situación aconseja disponer de un organismo que aglutine la respuesta operativa a la problemática de la ciberseguridad pública en Argentina, en lo que habitualmente se conoce como Centro Nacional de Ciberseguridad.

Efectivamente, habiendo diseñado de forma adecuada los eslabones estratégico (Comité de Ciberseguridad) y táctico (CERT.AR), el modelo actual carece de una entidad de gobierno central de la ciberseguridad desde el punto de vista operativo. Es decir, una entidad que se responsabilice de la adecuada dirección centralizada (atendiendo siempre a la estrategia marcada por los órganos superiores) en materia de recursos, métodos, procedimientos, herramientas, I+D+i, sensibilización, formación y cooperación nacional e internacional en materia de ciberseguridad, sus tecnologías y sus condicionantes jurídicos.

Una entidad que, asimismo, deberá asistir al Gobierno mediante asesoramiento en materia de ciberseguridad para la elaboración de políticas, leyes y actualizaciones de la normativa existente, permitiendo la coherencia en la aplicación de dichas políticas a nivel nacional.

En la actualidad, por lo recogido en el presente informe, estas actividades no parecen estar adecuadamente centralizadas o armonizadas, pudiendo acometerse desde distintas unidades administrativas, lo que puede poner en peligro la debida coordinación, propiciando en consecuencia ineficacia en la gestión de los recursos -públicos y privados-, y, lo que es peor, la posibilidad cierta de ofrecer resultados dispares, incoherentes o, incluso, contradictorios.

Por otro lado, cuando se detectan incidentes a gran escala, no está del todo claro qué organismo es el responsable. Del mismo modo, cuando se produce un incidente, las empresas no tienen claro si deben comunicarlo, a quién deben comunicarlo, o si existe un CSIRT de referencia al que tienen que comunicárselo, con qué herramienta y bajo qué premisas.

Por este motivo convendría, como parte de un modelo de gestión orientado al usuario, un modelo de "ventanilla única" en base a un **Centro Nacional de Ciberseguridad** que racionalice la coordinación operativa ante un incidente, además de otras funciones.

(II) Se carece del imprescindible análisis del ecosistema de la ciberseguridad, comprensivo de todos los actores implicados: sector público, privado y ciudadanos.

Como antes se señalaba, esta actividad, cuando eventualmente se decide acometer, se viene realizando en la actualidad por varias instituciones, públicas y privadas, centros de investigación y Universidades, sin la debida coordinación, alimentando un modelo disfuncional.

(III) Dispersión de la respuesta ante las amenazas y de los procedimientos de prevención, detección y respuesta.

La respuesta a los ciberataques exige, por la propia naturaleza de la amenaza, eficacia e inmediatez. Sin embargo, el actual modelo de respuesta operativa, debido en gran parte a su juventud, no ha alcanzado todavía el pleno desarrollo, lo que podría suponer que, en determinados casos, la respuesta llegue tarde; incrementando las consecuencias de los ataques, desde todos los puntos de vista: políticos (cuando se trata de campañas de desinformación o interferencia extrajera), sociales y económicos.

La necesidad de contar con metodologías, herramientas y plataformas comunes es condición imprescindible para asegurar que los ciberataques y los ciberincidentes son adecuadamente tratados, en tiempo y forma, garantizando una respuesta rápida, eficaz y eficiente.

(IV) Limitado intercambio de información.

Constituyendo los ciberataques y las ciberamenazas una actividad global, que no puede tratarse de manera aislada, y de la que todas las partes -públicas, privadas o ciudadanos- pueden ser víctima, se hace imprescindible articular métodos, procedimientos y herramientas para

garantizar que lo que es conocido por una entidad pueda, de manera inmediata, ser conocido por todas aquellas entidades que, disponiendo de las autorizaciones precisas, puedan requerir de tal conocimiento para hacer frente a las amenazas, bajo el principio universal de "compartir para ganar".

El modelo actual hace que esta necesidad se vea muy limitada, cuando no inexistente.

(V) Ausencia de métodos, procedimientos y herramientas comunes.

En la actualidad, los organismos públicos con competencias en la provisión de servicios de ciberseguridad, para sí mismos o para su comunidad de intereses, suelen hacer uso de herramientas individuales propietarias que impiden o dificultan una postura común a las amenazas del ciberespacio.

Como se ha señalado, es necesario disponer de una base sólida de métodos, procedimientos y herramientas, incluyendo las jurídicas, de uso común por todas las partes, que garanticen un conocimiento adecuado de las ciberamenazas y sus riesgos, y permitan una respuesta rápida y eficaz a los ciberataques, garantizando una posición homogénea en materia de formación e Investigación, Desarrollo e Innovación.

(VI) Debilidad en la defensa de los intereses de la Argentina.

Como es lógico suponer, todo lo anterior conlleva una significativa debilidad en la defensa de los legítimos intereses de la Argentina, desde todos los puntos de vista: político, social, industrial, o económico.

(VII) Ineficacia en la asignación y gestión de los fondos públicos.

No se puede terminar este breve repaso a los condicionantes más significativos a los que este documento pretende hacer frente sin mencionar, pese a su obviedad, que todo lo anterior comporta que los siempre escasos fondos destinados a la ciberseguridad metodológica, tecnológica y operativa vengan siendo ineficazmente asignados y gestionados.

Solo la presencia de un órgano como el que se propone, el Centro Nacional de Ciberseguridad, puede ser capaz de ofrecer una respuesta eficaz y eficiente en la asignación y gestión de dichos presupuestos.

5.3 Hoja de ruta y acciones subsiguientes

En base a lo anterior, las acciones que entendemos deben priorizar las actuaciones del Gobierno de Argentina en materia de Ciberseguridad de las Infraestructuras Críticas de Información, son las siguientes:

1. Reforzar la implantación de la **Estrategia Nacional de Ciberseguridad** en todos los sectores nacionales.
2. Reforzar el nivel estratégico de la ciberseguridad nacional, con la potenciación -en miembros y funciones- del Comité de Ciberseguridad, para lo que proponemos una nueva denominación: **Consejo Nacional de Ciberseguridad**, cuya presidencia debe ostentar, de manera formal, el Presidente de la Nación Argentina y, por delegación, el Jefe de Gabinete de Ministros, y cuya composición deberá comprender todos los departamentos ministeriales afectados. Este órgano dictará, al máximo nivel, la política

de ciberseguridad de la nación argentina, propiciando el desarrollo e implantación de las regulaciones necesarias.

3. Reforzar el nivel estratégico de la ciberseguridad nacional (incluyendo a las Infraestructuras Críticas de Información) con la creación del **Centro Nacional de Ciberseguridad**, en los términos expuestos con anterioridad, bajo la órbita de la Jefatura de Gabinete de Ministros.
4. Reforzar el nivel táctico de la ciberseguridad nacional (incluyendo a las Infraestructuras Críticas de Información) con la potenciación del CERT.ar nacional, en funciones y recursos.
5. Acomodar el marco jurídico de la ciberseguridad a los instrumentos normativos adecuados y exigir su cumplimiento a todos los sectores implicados.
6. Desarrollar un **Esquema Nacional de Evaluación y Certificación de la Ciberseguridad** (obligatorio para las entidades del sector público y las Infraestructuras Críticas).
7. Ajustar la definición y los umbrales de determinación de las Infraestructuras Críticas de Información.
8. Reforzar los procedimientos para la definición de la Notificación, Seguimiento y Gestión de los incidentes de ciberseguridad y las herramientas a usar, incluyendo a todos las entidades de los sectores designados como críticos.

ANEXO I: APROXIMACIÓN A LA GOBERNANZA DE LA CIBERSEGURIDAD EN DIFERENTES PAÍSES.

En los siguientes epígrafes describiremos brevemente cómo se ha abordado la ciberseguridad de las infraestructuras críticas desde los modelos de gobernanza adoptados por diferentes países de la órbita occidental, haciendo especial énfasis en dos aspectos fundamentales: el modelo de gobernanza de la ciberseguridad pública en el país de que se trate y la normativa legal que desarrolla tal modelo, con lo que se persigue tener una idea razonable de cual viene siendo el comportamiento de estos países en un área tan crítica como la ciberseguridad de las infraestructuras esenciales del país.

Para ello, se han escogido tres países: Estados Unidos, Reino Unido y España, suficientemente representativos de los más significativos esfuerzos por gobernar, institucional y legalmente, la ciberseguridad nacional.

AI.1 Estados Unidos

Marco regulatorio

Cronológicamente, la ciberseguridad pública de los EEUU se ha venido regulando en las siguientes normas esenciales:

2003 Homeland Security Presidential Directive 7 _ CISA
2013 Executive Order 13636 - Improving Critical Infraestructure Cybersecurity
2014 Public Law Federal - Information Security Modernization
2014 Public Law Public - Cybersecurity Enhancement Act
2015 Executive Order 13702 - Creating National Strategic Computing Initiative
2016 Circular a-130 OMB managing Information as a Strategic Resource
2016 Executive Order 13718 - Commission on Enhancing National Cybersecurity
2017 Executive Order 13800 - Strengthening the Cybersecurity of Federal networks and Critical Infraestructure
2018 Public Law Federal - Cybersecurity and Infraestructure Security Agency
2020 Executive Order 13905 - Strengthening National Resilience Through responsible Use
2021 Executive Order 14028 - Improving the Nation's Cybersecurity

Se resumen seguidamente las más importantes.

2016 Executive Order 13718 – Commission on Enhancing National Cybersecurity

Principios, conclusiones e imperativos:

La orden ejecutiva pedía a la Comisión que abordara una amplia gama de temas de ciberseguridad: gobernanza federal, infraestructuras críticas, investigación y desarrollo de la ciberseguridad, personal de ciberseguridad, gestión de la identidad y autenticación, Internet de las cosas, concienciación y educación del público, y ciberseguridad de los gobiernos estatales y locales. A medida que avanzaban sus trabajos, la Comisión decidió añadir a esta lista las cuestiones relacionadas con los seguros y el ámbito internacional.

Para guiar sus recomendaciones dentro de estos imperativos, la Comisión identificó diez Principios Fundamentales:

- La creciente convergencia, interconexión, interdependencia y naturaleza global de los sistemas cibernéticos y físicos significa que la ciberseguridad debe gestionarse mejor en todos los contextos: internacional, nacional, organizativo e individual.
- Como líder mundial en innovación, Estados Unidos debe ser un abanderado de la ciberseguridad. Este liderazgo requiere la inversión en investigación y la colaboración con otras naciones, incluyendo las normas internacionales de ciberseguridad.
- El gobierno federal es el máximo responsable de la defensa y la seguridad de la nación y tiene importantes responsabilidades operativas en la protección de las infraestructuras críticas de la nación, que cambian rápidamente. El gobierno también tiene roles de misión cibernética que necesitan ser aclarados, incluyendo una mejor definición de los roles y responsabilidades del gobierno (incluyendo las agencias individuales), y abordando las capacidades faltantes o débiles, así como identificando y creando la capacidad que se necesita para realizar estas actividades.
- La colaboración entre el sector privado y el gobierno antes, durante y después de un evento es esencial para crear y mantener un entorno cibernético defendible y resistente.
- La responsabilidad, la autoridad, la capacidad y la rendición de cuentas en materia de ciberseguridad y gestión de riesgos cibernéticos deben ser explícitas y estar alineadas con las estrategias de gestión de riesgos y gobernanza de cada empresa.
- La ciberseguridad efectiva depende de la concienciación, la educación y el compromiso de los consumidores y los trabajadores para proteger su experiencia digital. Este esfuerzo debe ser un proceso continuo y hacer avanzar la comprensión y las capacidades de los individuos como participantes vitales en la configuración de su propia ciberseguridad -y la de la nación-. No obstante, en la medida de lo posible, la carga de la ciberseguridad debe alejarse en última instancia del usuario final -los consumidores, las empresas, las infraestructuras críticas y otros- hacia soluciones de alto nivel que incluyan una mayor disuasión de las amenazas, productos y protocolos más seguros y un ecosistema de Internet más seguro.
- Dado que el comportamiento humano y la tecnología están entrelazados y son vitales para la ciberseguridad, las tecnologías y los productos deben facilitar la acción segura y dificultar la acción menos segura.
- La seguridad, la privacidad y la confianza deben ser consideraciones primordiales desde el principio, cuando se conciben las nuevas tecnologías y políticas relacionadas con la ciberseguridad, y no cuestiones auxiliares que se tengan en cuenta después de su desarrollo. La mejora de la privacidad y la confianza, impulsada por la transparencia y la responsabilidad, contribuirá a la preservación de las libertades civiles.
- A pesar de sus recursos a menudo limitados, las pequeñas y medianas empresas son partes interesadas esenciales en cualquier esfuerzo por mejorar la ciberseguridad -en particular, a la luz de su papel en la cadena de suministro- y sus necesidades deben ser mejor atendidas.
- Para mejorar la ciberseguridad es necesario ofrecer la combinación adecuada de incentivos, con una fuerte dependencia de las fuerzas del mercado y de las acciones gubernamentales de apoyo. Los incentivos deben ser siempre preferibles a la regulación, que sólo debe considerarse cuando los riesgos para la seguridad pública son importantes y el mercado no puede mitigarlos adecuadamente.

A través de varias reuniones públicas, la Comisión escuchó a una amplia gama de expertos y líderes del gobierno y del sector privado y, combinados con su propia experiencia y la de su personal, identificó varias conclusiones clave:

- Las empresas tecnológicas están sometidas a una importante presión del mercado para innovar y salir al mercado rápidamente, a menudo a expensas de la ciberseguridad.
- Las organizaciones y sus empleados requieren entornos de trabajo flexibles y móviles.
- Muchas organizaciones y personas siguen sin hacer lo básico.
- El ataque y la defensa adoptan las mismas innovaciones.
- El atacante tiene ventaja.
- La complejidad tecnológica crea vulnerabilidades.

- Abundan las interdependencias y los riesgos en la cadena de suministro.
- Los gobiernos dependen operativamente del ciberespacio tanto como el sector privado.
- Confianza en los fundamentos.

Basándose en la variedad de temas y conclusiones y con el fin de crear enfoques significativos basados en los Principios Fundamentales, la Comisión desarrolló seis "Imperativos" en torno a los cuales estructurar sus recomendaciones y los elementos de acción asociados. Estos imperativos son

- Proteger, defender y asegurar la infraestructura de la información y las redes digitales actuales
- Innovar y acelerar la inversión para la seguridad y el crecimiento de las redes digitales y la economía digital
- Preparar a los consumidores para prosperar en la era digital
- Desarrollar las capacidades del personal de ciberseguridad
- Equipar mejor al gobierno para que funcione de forma eficaz y segura en la era digital
- Garantizar una economía digital global abierta, justa, competitiva y segura

El informe de la Comisión presenta un puñado de temas clave que la administración entrante probablemente reconozca:

- La ciberseguridad es un reto global y omnipresente tanto para el gobierno como para el sector privado y, como tal, requiere un enfoque de soluciones inclusivo, transparente y basado en estándares;
- La ciberseguridad es fundamental para la economía mundial y, por lo tanto, el mercado tiene el papel principal en la configuración y el desarrollo de tecnología segura e innovadora;
- El papel del gobierno debe ser limitado, pero claramente definido y coherente con su misión actual e histórica de proteger a la nación y fomentar una economía digital segura.

Queda por ver el grado de aplicación de estas recomendaciones por parte de la administración entrante, pero el carácter bipartidista de las Comisiones, combinado con la importante aportación de los líderes del sector privado, es digno de mención y puede influir positivamente en su aceptación.

2017 Executive Order 13800 – Strengthening the Cybersecurity of Federal networks and Critical Infraestructure

El 11 de mayo de 2017, el presidente Trump emitió la Orden Ejecutiva 13800, Fortalecimiento de la ciberseguridad de las redes federales y la infraestructura crítica, para mejorar la postura y las capacidades cibernéticas de la nación ante la intensificación de las amenazas a la ciberseguridad. La OE 13800 centra los esfuerzos federales en la modernización de la infraestructura de tecnología de la información federal, la colaboración con los gobiernos estatales y locales y los socios del sector privado para asegurar más plenamente la infraestructura crítica, y la colaboración con los aliados extranjeros.

El trabajo realizado para aplicar la OE 13800 refleja la sólida colaboración de todo el Gobierno Federal y de los socios del sector para salvaguardar la seguridad de las infraestructuras críticas y reducir el riesgo de ciberseguridad nacional.

<u>Informe al Presidente sobre la modernización de las TI federales:</u>

El DHS, en colaboración con el Consejo Americano de Tecnología (ATC), la Oficina de Gestión y Presupuesto (OMB) y las principales partes interesadas del Gobierno, preparó el Informe al Presidente sobre la modernización de las TI federales. Las prioridades de actuación establecidas en el informe incluyen (1) salvaguardar los Activos de Alto Valor (HVAs) de alto riesgo, (2) promover la modernización y consolidación de la infraestructura de red, incluyendo los programas de Conexión de Internet de Confianza (TIC) y Sistema Nacional de Protección de la Ciberseguridad (NCPS) del DHS, y (3) ampliar el

uso de los servicios compartidos, incluyendo el programa de Diagnóstico y Mitigación Continua (CDM) del DHS, para permitir un mayor uso y adopción de los servicios en la nube y móviles.

El DHS participa activamente en la aplicación de medidas para mejorar la postura general de ciberseguridad de la empresa federal, modernizar la empresa federal de TI y crear una asociación más sólida entre el Gobierno y la industria.

Apoyo a las infraestructuras críticas de mayor riesgo:

El DHS, en coordinación con las agencias sectoriales pertinentes, identifica y mantiene anualmente una lista de entidades de infraestructuras críticas que cumplen los criterios especificados en la Sección 9 de la Executive Order 13636, Improving Critical Infrastructure Cybersecurity, utilizando un enfoque basado en el riesgo. Las entidades de la Sección 9 poseen u operan infraestructuras críticas "en las que un incidente de ciberseguridad podría resultar razonablemente en efectos regionales o nacionales catastróficos para la salud o seguridad pública, la seguridad económica o la seguridad nacional".

El DHS, en coordinación con el Secretario de Defensa, el Fiscal General, el Director de Inteligencia Nacional, el Director de la Oficina Federal de Investigación y los jefes de las agencias sectoriales apropiadas, identificó las autoridades y capacidades que el Gobierno Federal podría emplear para apoyar los esfuerzos de ciberseguridad de las entidades de la Sección 9. Además, el DHS y sus socios contrataron a estas entidades para evaluar cómo las autoridades y capacidades podrían emplearse para apoyar los esfuerzos de gestión de riesgos de ciberseguridad.

Las conclusiones y recomendaciones de este trabajo se comunicaron al Presidente para apoyar mejor a las entidades de la Sección 9 en sus esfuerzos de gestión de riesgos de ciberseguridad, para incluir:

- Establecer una oficina de programas del DHS para reforzar el apoyo a las entidades de la Sección 9 y mejorar la coordinación del apoyo interinstitucional;
- Mejorar el acceso a la información clasificada;
- Revisar la metodología para explorar un enfoque más basado en las funciones para identificar las entidades de la Sección 9;
- Mejorar la comunicación y la coordinación de los incidentes;
- Mejorar el intercambio de información intersectorial con las entidades de la Sección 9;
- Exploración de incentivos para que las entidades del sector privado ejerzan el debido cuidado en la protección de su información y sistemas de información, lo que podría incluir la notificación de incidentes de ciberseguridad al Gobierno;
- Establecer una iniciativa público-privada para contrarrestar las vulnerabilidades de la cadena de suministro y reducir el riesgo de los proveedores en materia de ciberseguridad; y
- Explorar nuevas tecnologías para reducir el riesgo cibernético.

El DHS dirigirá un grupo de trabajo interinstitucional que se centrará en la aplicación de las recomendaciones y se comprometerá con cada entidad de la Sección 9 para garantizar su comprensión de los programas y recursos disponibles.

Supporting Transparency in the Marketplace:

El DHS, en coordinación con el Departamento de Comercio, recibió el encargo de examinar la suficiencia de las políticas y prácticas federales existentes para promover la adecuada transparencia de las prácticas de gestión de riesgos de ciberseguridad en el mercado, centrándose en las entidades de infraestructuras críticas que cotizan en bolsa. El informe resultante se elaboró en un breve plazo de 90 días a través de un proceso de colaboración interinstitucional; una participación limitada de la industria privada; y una revisión bibliográfica de fuentes secundarias que abordan la suficiencia de las políticas y prácticas federales existentes para promover la transparencia de los riesgos de ciberseguridad y las prácticas de gestión de riesgos y la eficacia de los sistemas de transparencia en general para promover

los objetivos políticos. En el marco de la revisión bibliográfica se identificaron 96 fuentes diferentes y varias políticas y prácticas federales. Los resultados asociados proporcionan una visión de la eficacia de los sistemas de transparencia; la suficiencia de las políticas y prácticas federales existentes; e informa de los futuros debates políticos sobre la transparencia del mercado y la mejora de los resultados de la ciberseguridad.

Resiliencia contra las redes de bots y otras amenazas automatizadas y distribuidas:

El DHS ha trabajado estrechamente con el Departamento de Comercio para liderar un proceso abierto y transparente con el fin de identificar y promover la acción de las partes interesadas para mejorar la resistencia del ecosistema de Internet y las comunicaciones y fomentar la colaboración con el objetivo de reducir drásticamente las amenazas perpetuadas por los ataques automatizados y distribuidos.
El informe, Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats, resume las oportunidades y los desafíos para reducir la amenaza de las redes de bots, y ofrece acciones de apoyo que deben ser tomadas tanto por el Gobierno como por el sector privado para reducir la amenaza de los ataques automatizados y distribuidos. El informe se centra en seis temas principales:

- Los ataques automatizados y distribuidos son un problema global.
- Existen herramientas eficaces, pero no se utilizan ampliamente.
- Los productos deben estar protegidos durante todas las etapas del ciclo de vida.
- Se necesita concienciación y educación.
- Los incentivos del mercado deben estar más alineados.
- Los ataques automatizados y distribuidos son un reto para todo el ecosistema.

El informe, elaborado con amplias aportaciones de las partes interesadas y los expertos, enumera cinco objetivos complementarios que mejorarían la resistencia del ecosistema de Internet. Las acciones recomendadas incluyen actividades en curso que deberían continuarse o ampliarse, así como nuevas iniciativas, como un esfuerzo para aumentar la transparencia de los componentes de software y una campaña pública para apoyar la concienciación sobre la seguridad del IoT.

Evaluación de las capacidades de respuesta a incidentes de interrupción de la electricidad:

El DHS también colaboró estrechamente con el Departamento de Energía para llevar a cabo una evaluación del posible alcance y duración de un apagón prolongado asociado a un incidente cibernético significativo, así como una evaluación de la preparación y las lagunas en la capacidad de Estados Unidos para gestionar y mitigar las consecuencias de un incidente cibernético contra el subsector eléctrico. Esta evaluación concluyó que los Estados Unidos están, en general, bien preparados para gestionar la mayoría de las interrupciones de la electricidad, aunque hay áreas particulares en las que las consideraciones catastróficas y las amenazas emergentes revelan lagunas de capacidad contra los ciberataques.

Para subsanar estas lagunas, la evaluación describe áreas que abarcan desde la mejora de las comunicaciones públicas entre los funcionarios de todos los niveles, la ampliación de los conocimientos técnicos en materia de ciberseguridad y el intercambio de información, hasta la integración y el aumento de las capacidades de planificación y análisis para las interrupciones a largo plazo y las posibles consecuencias e impactos resultantes de dichas interrupciones. Además, la integración temprana de la ciberseguridad en el diseño del sistema, la financiación de las inversiones en ciberseguridad, en particular para las empresas de servicios públicos más pequeñas, y el desarrollo de una fuerte fuerza de trabajo apoyarían de manera integral la preparación nacional de la infraestructura eléctrica del país.

Desarrollo de la fuerza de trabajo estadounidense en ciberseguridad:

El Departamento de Comercio y el DHS evaluaron el alcance y la suficiencia de los esfuerzos realizados en el pasado para educar y formar a la futura mano de obra estadounidense en materia de ciberseguridad y proporcionar un informe que identifique las conclusiones y recomendaciones sobre cómo apoyar el crecimiento y el mantenimiento de estos futuros empleados de ciberseguridad en los sectores público y privado. Para llevar a cabo este trabajo, se convocó a expertos en educación y desarrollo de la mano de obra en ciberseguridad de los departamentos de Defensa, Trabajo y Educación, así como de la Oficina de Gestión de Personal, la Fundación Nacional de la Ciencia y otros organismos pertinentes, para debatir y presentar el estado de los esfuerzos existentes para hacer crecer y ampliar la mano de obra en ciberseguridad del país. Para garantizar una amplia aportación, se convocó un taller público a nivel nacional y se emitió una solicitud pública de información (RFI).

El grupo de trabajo interinstitucional, dirigido por el Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio y el DHS, recopiló los resultados en un informe para el Presidente, en el que se identifican cuatro conclusiones clave: (1) la fuerza de trabajo en ciberseguridad de EE. (2) es necesario ampliar el grupo de candidatos a la ciberseguridad mediante la reconversión profesional y el aumento de la participación de mujeres, minorías y veteranos; (3) hay escasez de profesores de ciberseguridad en los niveles primario y secundario, de profesorado en la enseñanza superior y de instructores de formación; y (4) faltan datos completos y fiables sobre las necesidades de puestos de trabajo en ciberseguridad y los programas de educación y formación.

El informe detalla cinco recomendaciones clave para abordar las conclusiones:

- El Gobierno Federal debería liderar el lanzamiento de una llamada a la acción nacional de alto perfil para llamar la atención y movilizar los recursos del sector público y privado para abordar las necesidades de mano de obra en ciberseguridad;
- La Administración debería centrarse y recomendar la autorización a largo plazo y las asignaciones suficientes para programas de educación y desarrollo de la fuerza de trabajo de ciberseguridad eficaces y de alta calidad;
- Los sectores público y privado deberían transformar, elevar y sostener el entorno de aprendizaje para hacer crecer una fuerza de trabajo de ciberseguridad dinámica y diversa a través de enfoques de reciclaje, aprendizaje práctico, experimental y basado en el trabajo, incluyendo aprendizajes, experiencias de investigación, programas de cooperación, prácticas, formación virtual y entornos de evaluación, y proporcionando una mayor ayuda financiera para la educación y la formación en ciberseguridad;
- Los sectores público y privado deberían alinear la educación y la formación con las necesidades de la fuerza de trabajo en ciberseguridad de los empleadores, aplicando el Marco de la Fuerza de Trabajo en Ciberseguridad de la Iniciativa Nacional para la Educación en Ciberseguridad (NICE), desarrollando trayectorias de modelos de carrera en ciberseguridad y estableciendo un centro de intercambio de información sobre la educación, la formación y los programas e iniciativas de desarrollo de la fuerza de trabajo en ciberseguridad.
- Los sectores público y privado deben establecer y potenciar medidas que demuestren la eficacia y el impacto de las inversiones en mano de obra de ciberseguridad a través de métricas y mecanismos de evaluación robustos para seguir y determinar la cantidad y la calidad de las personas educadas, formadas y preparadas para realizar tareas de ciberseguridad en el lugar de trabajo.
- Lea el documento Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future Capabilities.

2018 Public law No: 115-278 (11.16.2018) Cybersecurity and Infraestructure Security Agency

(Art. 2) Este proyecto de ley modifica la Ley de Seguridad Nacional de 2002 para rediseñar la Dirección de Protección Nacional y Programas del Departamento de Seguridad Nacional (DHS) como Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA). Transfiere los recursos y las responsabilidades de la dirección a la CISA.

La CISA estará dirigida por el Director de Ciberseguridad Nacional y Seguridad de las Infraestructuras. (Se trata de funcionario civil de alto nivel en el Department of Homeland Security. El Director, como jefe de la CISA, es el principal asistente y asesor del Secretario de Seguridad Nacional y del Subsecretario de Seguridad Nacional para todos los programas del DHS destinados a reducir el riesgo de la nación ante el terrorismo y las catástrofes naturales. El Director es nombrado por el Presidente con el consentimiento del Senado.

El cargo fue creado en noviembre de 2018, en sustitución del cargo de Subsecretario de Seguridad Nacional para la Protección y los Programas Nacionales.

. Sus responsabilidades incluirán: dirigir los programas de ciberseguridad y seguridad de infraestructuras críticas, las operaciones y la política asociada; y llevar a cabo las responsabilidades del DHS en relación con las normas antiterroristas de las instalaciones químicas.

El proyecto de ley detalla la estructura organizativa de la agencia.

(Art. 3) El proyecto de ley transfiere dentro del DHS la Oficina de Gestión de la Identidad Biométrica a la Dirección de Gestión.

También requiere que el DHS transfiera el Servicio Federal de Protección a un componente, dirección u oficina apropiada del DHS tras la finalización de una revisión en curso de la Oficina de Responsabilidad del Gobierno.

(Sec. 4) El DHS informará sobre su papel de liderazgo en el despliegue de la ciberseguridad basada en la nube para los departamentos y agencias federales civiles.

2020 Executive Order 13905 – Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing (PNT) Services

EEl posicionamiento, la navegación y la temporización (PNT) son necesarios para el funcionamiento de las infraestructuras críticas del país. Ya sea para uso civil, comercial o militar, casi todos los sectores dependen de una información PNT precisa para prestar sus servicios. Sin embargo, el uso del Sistema de Posicionamiento Global (GPS) como fuente principal, y en muchos casos única, de datos PNT hace que estos sectores sean vulnerables a la interrupción intencionada o no de la señal GPS. Para complicar las cosas, los avances tecnológicos han hecho que la capacidad de emitir señales falsas de GPS sea relativamente sencilla, poniendo aún más en riesgo los sistemas dependientes de PNT.

Una de las principales prioridades del CISA es comprender cómo se utiliza la PNT en todas las Funciones Críticas Nacionales (NCF), y cómo las funciones que dependen de los servicios PNT pueden ser más seguras y resistentes. Esta comprensión informará los esfuerzos de reducción de riesgos de CISA, como la creación de un marco de conformidad para los receptores GPS y el apoyo al Instituto Nacional de Normas y Tecnología (NIST) en el desarrollo de perfiles PNT. El marco de conformidad establecerá parámetros clave para evaluar la seguridad y la resistencia de los receptores GPS. En colaboración con los fabricantes de equipos, los usuarios finales y otras agencias federales, el DHS desarrollará un léxico común que defina las expectativas de seguridad para la industria. Estas normas permitirán a los usuarios finales comprender mejor las capacidades de los receptores PNT, lo que a su vez permitirá a los usuarios tomar decisiones de riesgo mejor informadas.

A medida que surjan servicios PNT alternativos, el DHS trabajará con la industria para entender cómo su adopción afecta a las infraestructuras críticas y a los NCF. Además, la CISA seguirá liderando los esfuerzos del DHS para trabajar con los socios federales y la comunidad de infraestructuras críticas para promover el uso responsable del GPS y otras fuentes PNT.

El objetivo de la O.E. era identificar y promover el uso responsable de los servicios PNT por parte del Gobierno Federal y los propietarios y operadores de infraestructuras críticas.

La O.E. ordena al gobierno federal y a los propietarios y operadores de infraestructuras críticas que tomen medidas para identificar y promover el uso responsable de los servicios PNT. El DHS está bien posicionado para ejecutar la OE de PNT. En 2018, el Secretario del DHS firmó la estrategia de PNT del DHS que sincroniza los esfuerzos interinstitucionales de PNT en todo el Departamento para aumentar la resiliencia mediante la mejora de la coordinación y la colaboración dentro del DHS y el sector privado.

Esta OE es un gran paso adelante para abordar el riesgo de esta capacidad; centrándose no solo en fuentes más seguras de PNT, sino en sistemas más seguros que dependen de los datos de PNT.

2021 Executive Order 14028 – Improving the Nation's Ccybersecurity

Objetivos:

- Eliminar los obstáculos para compartir información sobre amenazas entre el gobierno y el sector privado.
- La OE garantiza que los proveedores de servicios informáticos puedan compartir información con el gobierno y les exige que compartan cierta información sobre infracciones.
- Modernizar e implementar estándares de ciberseguridad más fuertes en el Gobierno Federal.
- La OE ayuda a que el Gobierno Federal pase a tener servicios en la nube seguros y una arquitectura de confianza cero, y obliga a desplegar la autenticación multifactorial y el cifrado en un plazo determinado.
- Mejorar la seguridad de la cadena de suministro de software
- La OE mejorará la seguridad de los programas informáticos estableciendo normas de seguridad básicas para el desarrollo de los programas informáticos vendidos al Gobierno, lo que incluye exigir a los desarrolladores que mantengan una mayor visibilidad de sus programas informáticos y que pongan los datos de seguridad a disposición del público.
- También crea un programa piloto para crear una etiqueta del tipo "estrella de la energía" para que el gobierno -y el público en general- puedan determinar rápidamente si el software fue desarrollado de forma segura.
- Establecer una Junta de Revisión de la Ciberseguridad
- La OE establece una Junta de Revisión de la Ciberseguridad, copresidida por líderes del gobierno y del sector privado, con autoridad para reunirse después de un incidente cibernético significativo para analizar lo sucedido y hacer recomendaciones concretas para mejorar la ciberseguridad. Esta junta sigue el modelo de la Junta Nacional de Seguridad del Transporte, que se utiliza después de los accidentes aéreos y otros incidentes.
- Crear un manual estandarizado para responder a las vulnerabilidades e incidentes de ciberseguridad
- La OE crea un libro de jugadas estandarizado y un conjunto de definiciones para la respuesta a incidentes de cibervulnerabilidad por parte de los departamentos y agencias federales. El libro de jugadas garantizará que todas las agencias federales cumplan con un determinado umbral y estén preparadas para tomar medidas uniformes para identificar y mitigar una amenaza, y servirá como una plantilla para que el sector privado utilice en la coordinación de los esfuerzos de respuesta.
- Mejorar la detección de incidentes de ciberseguridad en las redes del Gobierno Federal.
- La OE mejora la capacidad de detectar actividades cibernéticas maliciosas en las redes federales al habilitar un sistema de detección y respuesta de puntos finales (EDR) en todo el gobierno y mejorar el intercambio de información dentro del gobierno federal.
- Mejora de las capacidades de investigación y remediación
- La OE crea requisitos de registro de eventos de ciberseguridad para los departamentos y agencias federales con el fin de mejorar la capacidad de una organización para detectar intrusiones, mitigar las que están en curso y determinar el alcance de un incidente después del hecho.

Marco institucional

Los componentes esenciales del marco de gobernanza institucional de la ciberseguridad en los EEUU están residenciados en el Department of Homeland Security.

El Department of Homeland security está dirigido por el Secretario de Seguridad Nacional con la asistencia del Subsecretario.

Contiene las siguientes Agencias:

- Servicios de Ciudadanía e Inmigración: Tramita y examina las solicitudes de ciudadanía, residencia y asilo de los extranjeros. (Los pasaportes de los ciudadanos estadounidenses son expedidos por el Departamento de Estado, no por el Departamento de Seguridad Nacional.)
- Aduanas y Protección de Fronteras: Agencia policial que hace cumplir las leyes de Estados Unidos a lo largo de sus fronteras internacionales (aéreas, terrestres y marítimas), incluyendo su aplicación de las leyes de inmigración, aduanas y agricultura de Estados Unidos, mientras se encuentra en todos los puertos de entrada y patrulla entre ellos.
- Servicio de Inmigración y Aduanas: Agencia de aplicación de la ley dividida en dos oficinas:
  - Homeland Security Investigations (HSI), que investiga las violaciones de más de 400 leyes estadounidenses y reúne información sobre actividades delictivas nacionales e internacionales que amenazan la seguridad del país; y
  - Enforcement and Removal Operations (ERO) hace cumplir las infracciones administrativas de la Ley de Inmigración y Nacionalidad deteniendo, deportando y expulsando a los infractores de la ley de inmigración de Estados Unidos.
- Administración de Seguridad del Transporte: Es responsable de la seguridad de la aviación (nacional e internacional, sobre todo de los controles de pasajeros en los aeropuertos), así como de la seguridad del transporte terrestre y marítimo.
- Guardia Costera de Estados Unidos: Servicio militar responsable de la aplicación de la ley, la seguridad marítima, la defensa nacional, la movilidad marítima y la protección de los recursos naturales.
- Servicio Secreto de los Estados Unidos: Agencia de aplicación de la ley encargada de dos misiones distintas y críticas para la seguridad nacional:
  - Misión de investigación - La misión de investigación del USSS es salvaguardar los sistemas de pago y financieros de los Estados Unidos de una amplia gama de delitos financieros y electrónicos.
  - Misión de protección: la misión de protección del USSS es garantizar la seguridad del Presidente de los Estados Unidos, del Vicepresidente de los Estados Unidos, de sus familiares directos y de los jefes de Estado extranjeros.
- Agencia Federal de Gestión de Emergencias: agencia que supervisa la respuesta del gobierno federal a las catástrofes naturales como terremotos, huracanes, tornados, inundaciones e incendios forestales.

Asimismo, contiene los siguientes Grupos Consultivos:

- Consejo Consultivo de Seguridad Nacional: Gobierno estatal y local, primeros intervinientes, sector privado y académicos

- Consejo Consultivo de la Infraestructura Nacional: Asesora sobre la seguridad de los sistemas de información públicos y privados
- Comité Consultivo de Ciencia y Tecnología para la Seguridad Nacional: Asesora al Subsecretario de Ciencia y Tecnología.
- Consejo Asesor de la Asociación de Infraestructuras Críticas: Coordina la protección de las infraestructuras con el sector privado y otros niveles de gobierno
- Consejo de Coordinación Interinstitucional sobre Preparación para Emergencias y Personas con Discapacidades
- Grupo de Trabajo sobre Nuevos Americanos: "Un esfuerzo interinstitucional para ayudar a los inmigrantes a aprender inglés, adoptar el núcleo común de la cultura cívica estadounidense y convertirse en estadounidenses de pleno derecho".

Otros Componentes:

- Oficina de Lucha contra las Armas de Destrucción Masiva: Contrarrestar los intentos de los terroristas u otros actores de la amenaza de llevar a cabo un ataque contra los Estados Unidos o sus intereses utilizando un arma de destrucción masiva. La secretaria Kirstjen Nielsen creó la Oficina CWMD en diciembre de 2017 consolidando principalmente la Oficina de Detección Nuclear Doméstica y una parte de la Oficina de Asuntos Sanitarios, así como otros elementos del DHS.
- Centro de formación de las fuerzas de seguridad federales: Instalaciones de formación de las fuerzas de seguridad interinstitucionales situadas en Georgia, Nuevo México y Carolina del Sur.
- Dirección Nacional de Protección y Programas: reducción de riesgos, que abarca tanto las amenazas físicas como las virtuales y sus elementos humanos asociados.
    - Servicio Federal de Protección: Agencia federal de seguridad y aplicación de la ley que protege e investiga los delitos contra los edificios federales, las propiedades, los activos y los intereses del gobierno federal de Estados Unidos.
    - Sistema Nacional de Comunicaciones
- Dirección de Ciencia y Tecnología: Investigación y desarrollo
- Dirección de Gestión: Responsable de los presupuestos internos, la contabilidad, el control del rendimiento y los recursos humanos
- Oficina de Estrategia, Política y Planes: Planificación y coordinación de políticas a largo plazo
    - Oficina de Estadísticas de Inmigración
- Oficina de Inteligencia y Análisis: Identifica y evalúa las amenazas basándose en la información de diversos organismos
- Oficina de Coordinación de Operaciones: Supervisa diariamente la situación de la seguridad nacional, coordina las actividades con las autoridades estatales y locales y la infraestructura del sector privado
- La Oficina del Secretario incluye la Oficina de Privacidad, la Oficina de Derechos y Libertades Civiles, la Oficina del Inspector General, el Defensor del Pueblo de los Servicios de Ciudadanía e Inmigración, la Oficina de Asuntos Legislativos, la Oficina del Asesor General, la Oficina de Asuntos Públicos, la Oficina de Control de Estupefacientes (CNE), la Oficina de la Secretaría Ejecutiva (ESEC) y la Oficina del Asesor Militar.
- Agencia de Ciberseguridad y Seguridad de las Infraestructuras

Desde el punto de vista operativo, en la actualidad, la responsabilidad de la ciberseguridad pública reside en la **Cybersecurity and Infraestructure Security Agency (CISA),** una agencia pública federal norteamericana, dependiente del Department of Homeland Security (DHS), creada en 2018 por decisión del Presidente Trump, firmando la *Cybersecurity and Infrastructure Security Agency Act,* y que hereda las actividades del National Protection and Programs Directorate (NPPD).

Sus departamentos son los siguientes:

- Cybersecurity Division
- National Council of Statewide Interoperability Coordinators (NCSWIC)
- Infrastructure Security Division
- Emergency Communications Division
- National Risk Management Center
- Integrated Operations Division
- Stakeholder Engagement Division
- National Emergency Technology Guard (inactive, but can be activated by the director of CISA)
- National Initiative for Cybersecurity Careers and Studies

Las áreas de trabajo de la CISA son las siguientes:

- Partenariado: CISA fomenta asociaciones innovadoras y de colaboración que permiten a las partes interesadas del gobierno y del sector privado tomar decisiones e inversiones informadas y voluntarias en materia de gestión de riesgos.
- Intercambio de información y datos: CISA comparte información con sus socios de infraestructuras críticas y sirve como centro nacional de información sobre ciberseguridad y comunicaciones, amenazas físicas como atentados y situaciones de tiradores activos, e intercambio de datos en tiempo casi real.
- Desarrollo de capacidades: CISA proporciona creación de capacidades, asistencia técnica, herramientas, ejercicios, programas de formación y esfuerzos de concienciación que mejoran la comprensión de los riesgos comunes y las posibles estrategias de mitigación para la comunidad de infraestructuras críticas.
- Gestión y respuesta a incidentes: CISA actúa como líder federal para las actividades de respuesta a incidentes cibernéticos con el sector privado, los gobiernos estatales, regionales y y las agencias federales. También coordina con socios del sector público y privado el apoyo a los eventos especiales de seguridad nacional, como la Super Bowl, y ofrece estrategias de gestión de riesgos para ayudar a las partes interesadas a gestionar las consecuencias de los riesgos emergentes y futuros.
- Evaluación y análisis de riesgos: CISA recopila y analiza los datos de riesgo para informar y priorizar las actividades de gestión de riesgos con el fin de priorizar las infraestructuras críticas y las Funciones Críticas Nacionales asociadas.
- Defensa de la red: CISA utiliza procesos, herramientas y tecnologías para evaluar las amenazas cibernéticas y físicas para las personas y la propiedad, y las posibles consecuencias de esas amenazas.
- Comunicaciones de emergencia: CISA mejora las comunicaciones interoperables de seguridad pública en todos los niveles de gobierno.

CISA lidera un esfuerzo de colaboración para garantizar la seguridad, resistencia y fiabilidad de los sistemas cibernéticos de la nación, impulsando los esfuerzos nacionales a través de la colaboración con el sector privado, el mundo académico y los socios gubernamentales para crear una fuerza de trabajo cibernética diversa, fomentar el desarrollo y el uso de tecnologías seguras y promover las mejores prácticas.

CISA detecta y previene los riesgos de ciberseguridad siempre que sea posible compartiendo información, desplegando tecnologías de detección y prevención, publicando productos técnicos y orientaciones, y proporcionando capacidades de respuesta a incidentes y de "caza" para minimizar los impactos de los incidentes identificados y de un panorama de amenazas en evolución. Para elevar la línea de base de la ciberseguridad federal, CISA proporciona servicios de infraestructura crítica, gobernanza de SLTT y creación de capacidades, información y asistencia para permitir una gestión más completa de los riesgos de ciberseguridad de las funciones críticas.

Funciones en seguridad de las Infraestructuras Críticas:

CISA es responsable de ayudar a salvaguardar las infraestructuras críticas de la nación mediante la mejora de la capacidad de las partes interesadas para mitigar los riesgos. A medida que los mundos físico y cibernético convergen, CISA aprovecha un enfoque integrado de la seguridad trabajando con empresas, comunidades y gobiernos a todos los niveles para ayudar a que las infraestructuras críticas de la nación sean más resistentes a las amenazas cibernéticas y físicas. CISA coordina el esfuerzo nacional para gestionar los riesgos físicos de las infraestructuras críticas, haciendo hincapié en las medidas de protección rentables y fáciles de aplicar que mitigan una multitud de amenazas, incluidas las asociadas a la violencia selectiva y a los extremistas violentos domésticos, y colabora con las partes interesadas del gobierno y del sector privado que poseen u operan la mayoría de las infraestructuras críticas de la nación.

Comunicaciones de emergencia:

La CISA apoya y promueve las comunicaciones utilizadas por el personal de respuesta a emergencias y los funcionarios del gobierno para mantener a Estados Unidos a salvo, seguro y resistente. CISA lidera los esfuerzos de comunicaciones operables e interoperables de seguridad pública y seguridad nacional y preparación para emergencias (NS/EP) de la nación.

CISA proporciona formación, coordinación, herramientas y orientación para ayudar a sus socios federales, estatales, locales, tribales, territoriales y de la industria a desarrollar sus capacidades de comunicaciones de emergencia. Los programas y servicios de CISA coordinan la planificación, la preparación y la evaluación de las comunicaciones de emergencia para garantizar comunidades más seguras y mejor preparadas en todo el país.

Gestión de riesgos:

CISA recopila y analiza la información sobre riesgos para identificar y priorizar las actividades de gestión de riesgos. CISA desarrolla estrategias de gestión de riesgos que refuerzan las infraestructuras críticas y abordan los riesgos para las Funciones Críticas Nacionales, tanto emergentes como a largo plazo. Las iniciativas incluyen: Seguridad y Resiliencia Electoral; Gestión de Riesgos de la Cadena de Suministro de las Tecnologías de la Información y la Comunicación; Quinta Generación (5G) de Redes Móviles; Ciberseguridad para el Pulso

Electromagnético y las Perturbaciones Geomagnéticas, Posicionamiento, Navegación y Cronometraje, y Ciberseguridad de las Tuberías.

Operaciones integradas:

La CISA ofrece servicios que permiten a las partes interesadas y a los socios de la comunidad de infraestructuras críticas mejorar la seguridad y la resistencia de la nación. La CISA consolida y coordina la difusión oportuna de información sobre amenazas cibernéticas y físicas; proporciona un contexto de inteligencia específico para incidentes y productos para apoyar la toma de decisiones; y a través de 10 centros regionales, proporciona la entrega de programas y servicios de la CISA para apoyar a las partes interesadas mientras trabajan para preparar, responder, recuperar y mitigar los efectos de los incidentes.

Participación de las partes interesadas:

CISA fomenta asociaciones innovadoras y de colaboración que permiten a las partes interesadas del gobierno y del sector privado tomar decisiones e inversiones informadas y voluntarias en materia de gestión de riesgos. La agencia busca aumentar la preparación de la nación a través de esfuerzos de comunicación multicanal que construyan la confianza y la comprensión del público para que las partes interesadas y el público estadounidense respondan favorablemente cuando sean llamados a actuar.

AI.2 Reino Unido

Marco regulatorio

Para hacer que el Reino Unido sea más seguro y ayudar a prevenir este tipo de ataques, el gobierno pretende, a través de una nueva legislación, adoptar un enfoque más fuerte para conseguir que las empresas de riesgo mejoren su resistencia cibernética como parte de su nueva National Cyber Strategy[28] de 2.600 millones de libras.

Actualización de la normativa NIS:

La normativa Network and Information Systems (NIS)[29] entró en vigor en 2018 para mejorar la ciberseguridad de las empresas que prestan servicios esenciales como el agua, la energía, el transporte, la sanidad y las infraestructuras digitales. Las organizaciones que no pongan en marcha medidas eficaces de ciberseguridad pueden ser multadas con hasta 17 millones de libras.

El Gobierno quiere actualizar la normativa NIS y ampliar la lista de empresas que entran en el ámbito de aplicación para incluir a los proveedores de servicios gestionados (MSP) que prestan servicios especializados en línea y digitales. Los MSP incluyen servicios de seguridad, servicios en el lugar de trabajo y externalización de TI. Estas empresas son cruciales para impulsar el crecimiento del sector digital del país, de 150.600 millones de libras, y tienen acceso privilegiado a las redes y sistemas de sus clientes.

La normativa NIS exige a los proveedores de servicios esenciales que realicen evaluaciones de riesgo y pongan en marcha medidas de seguridad razonables y proporcionadas para proteger su

[28] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022
[29] https://www.legislation.gov.uk/uksi/2018/506

red. Tienen que informar de los incidentes significativos y disponer de planes para asegurarse de que se recuperan rápidamente de ellos.

Aunque la normativa se aplica a algunos servicios digitales como los mercados en línea, los motores de búsqueda en línea y la computación en la nube, se ha producido un aumento en el uso y la dependencia de los servicios digitales para satisfacer necesidades corporativas como el almacenamiento de información, el procesamiento de datos y la ejecución de software.

Una investigación realizada por el Departamento de Digital, Cultura, Medios de Comunicación y Deporte[30] muestra que sólo el 12% de las organizaciones revisan los riesgos de ciberseguridad procedentes de sus proveedores inmediatos y sólo una de cada veinte empresas (el 5%) aborda las vulnerabilidades en su cadena de suministro más amplia.

El Gobierno ha lanzado recientemente (19.1.2022) una consulta sobre la modificación del Reglamento SRI que incluye propuestas para:

- Ampliar el ámbito de aplicación del Reglamento SRI" para incluir los servicios gestionados. Éstos suelen ser prestados por empresas que gestionan servicios informáticos en nombre de otras organizaciones.
- Exigir a las grandes empresas que informen mejor de los incidentes cibernéticos a reguladores como Ofcom, Ofgem y la ICO, incluyendo la obligación de notificar a los reguladores todos los ataques de ciberseguridad que sufran, no sólo los que afecten a sus servicios.
- Dar al gobierno la capacidad de preparar el futuro de las regulaciones NIS actualizándolas y, si es necesario, incluir en el ámbito de aplicación a más organizaciones en el futuro que proporcionen apoyo crítico a los servicios esenciales.
- Transferir todos los costes relevantes en los que incurren los reguladores para hacer cumplir la normativa SRI del contribuyente a las organizaciones cubiertas por la legislación para crear un sistema de financiación más flexible y reducir la carga de los contribuyentes.
- Actualizar el régimen regulatorio para que los proveedores de servicios digitales más críticos en la economía tengan que demostrar proactivamente que están siguiendo la normativa NIS a la OIC, y adoptar un enfoque más ligero con el resto de proveedores digitales.

Marco institucional

En marzo de 2022, el Gobierno creó y financió el UK Cyber Security Council[31], un nuevo organismo independiente para dirigir la ciberfuerza laboral y equipararla a profesiones establecidas como la ingeniería.

[30] https://www.gov.uk/government/news/businesses-urged-to-act-as-two-in-five-uk-firms-experience-cyber-attacks-in-the-last-year

[31] https://www.gov.uk/government/news/new-uk-cyber-security-council-to-be-official-governing-body-on-training-and-standards#:~:text=The%20UK%20Cyber%20Security%20Council,build%20back%20better%20and%20safer.

Las propuestas de hoy otorgarían a este Consejo la capacidad de definir y reconocer los títulos de los puestos de trabajo cibernéticos y vincularlos a las cualificaciones y certificaciones existentes. Las personas tendrían que cumplir las normas de competencia establecidas por el Consejo antes de poder utilizar un título de trabajo específico en toda la gama de especialidades de la ciberseguridad.

Esto facilitaría a los empresarios la identificación de las cibercapacidades específicas que necesitan en sus organizaciones y crearía una información más clara sobre las trayectorias profesionales de los jóvenes y de los profesionales actuales, sin crear barreras innecesarias para el acceso y la progresión.

Las propuestas incluyen la creación de un registro de profesionales, similar al que existe en las profesiones médicas y jurídicas, en el que figuren los profesionales reconocidos como éticos, debidamente cualificados o de alto nivel.

La protección de las IC del Reino Unido en materia de ciberseguridad está residenciada en el CNI (Critical National Infrestructure) Hub, adscrito al National Cyber Security Centre (NCSC)[32].

La misión del NCSC es hacer del Reino Unido el lugar más seguro para vivir y trabajar en línea. Un aspecto fundamental de esta misión es la colaboración con las organizaciones que prestan los servicios esenciales de los que dependen nuestros ciudadanos y empresas cada día: la Infraestructura Nacional Crítica (CNI) del Reino Unido, abarcando desde las redes de comunicaciones hasta las redes de energía.

En el Reino Unido hay 13 sectores de Infraestructuras Nacionales Críticas:

- Productos químicos
- Civil Nuclear
- Comunicaciones
- Defensa
- Servicios de emergencia
- Energía
- Finanzas
- Alimentación
- Gobierno
- Salud
- Espacio
- Transporte
- Agua

El gobierno británico define las infraestructuras críticas del Reino Unido como: "*Aquellos elementos críticos de la Infraestructura (instalaciones, sistemas, sitios, propiedades, información, personas, redes y procesos), cuya pérdida o compromiso tendría un impacto perjudicial importante en la disponibilidad, la prestación o la integridad de los servicios esenciales, provocando graves consecuencias económicas o sociales o la pérdida de vidas*".

[32] Ver epígrafe ___ de este documento.

La Infraestructura Nacional Crítica del Reino Unido incluye tanto organizaciones del sector público como del sector privado.

Los sectores de Defensa, Servicios de Emergencia, Gobierno y Sanidad se consideran predominantemente del sector público. Puede encontrar información sobre el sector público aquí en el sitio web del NCSC.

No obstante, gran parte de la CNI del Reino Unido es propiedad del sector privado, y no del gobierno británico. El NCSC tiene un equipo dedicado a apoyar la ciberseguridad dentro de cada sector CNI para ayudar a proteger sus servicios esenciales.

Garantizar que los sistemas más críticos del Reino Unido sean ciberresistentes es una prioridad absoluta para el NCSC, con el fin de proteger nuestros servicios esenciales para que no sean atacados o explotados por los adversarios. Nuestro trabajo abarca la creación de espacios de confianza para la innovación y el intercambio de las mejores prácticas de ciberseguridad en toda la CNI, así como la aportación de conocimientos técnicos para apoyar proyectos pioneros.

El NCSC apoya al CNI del Reino Unido mediante los servoicios que se han mecionado en este documento.

AI.3 Francia

Marco regulatorio

Como se especifica en la Ley n°2013-1168 de 18 de diciembre de 2013, "*el Primer Ministro define la política y coordina la acción del Gobierno en materia de seguridad y defensa de los sistemas de información. A tal efecto, tendrá a su disposición la autoridad nacional de seguridad de los sistemas de información*", la ANSSI, dependiente de la Secretaría General de Defensa y Seguridad Nacional.

La Estrategia Nacional de Seguridad Digital, presentada el 16 de octubre de 2015 por el primer ministro Manuel Valls, tiene como objetivo apoyar la transición digital de la sociedad francesa.

Fue objeto de un trabajo interministerial coordinado por la ANSSI.

Responde a los nuevos retos derivados de la evolución de los usos digitales y las amenazas relacionadas con ellos con cinco objetivos:

- Garantizar la soberanía nacional
- Dar una respuesta contundente contra los actos de cibermaldad
- Informar al público en general
- Hacer de la seguridad digital una ventaja competitiva para las empresas francesas
- Reforzar la voz de Francia en la escena internacional.

Con la Estrategia Nacional de Seguridad Digital, el Estado se compromete con la seguridad de los sistemas de información para avanzar, mediante una respuesta colectiva, hacia una confianza digital que favorezca la estabilidad del Estado, el desarrollo económico y la protección de los ciudadanos.

La seguridad de los sistemas de información (ISS) y el Libro Blanco sobre Defensa y Seguridad Nacional de 2008:

El Libro Blanco identificó el riesgo de un ataque informático contra las infraestructuras nacionales como una de las principales amenazas más probables en los próximos quince años, y destacó el impacto potencialmente muy fuerte de tales ataques en la vida de la nación. Nuestra dependencia de los procesos informáticos crece constantemente con el desarrollo de la sociedad de la información y el creciente uso de las tecnologías de la información en los procesos centrales del Estado y la sociedad.

En consecuencia, el Libro Blanco invitaba al Estado a desarrollar una capacidad de prevención y reacción ante los ataques informáticos y a hacer de ello una prioridad importante en su sistema de seguridad nacional. En particular, en el ámbito de la defensa de los sistemas de información, subrayó la necesidad de una capacidad de detección precoz de los ataques informáticos y de una organización capaz de contrarrestar tanto los ataques más sutiles como los más masivos. En el ámbito de la prevención, propuso un mayor uso de productos y redes de seguridad de alto nivel, así como la creación de un conjunto de competencias para las administraciones y los operadores de infraestructuras vitales.

La ANSSI fue creada de acuerdo con las orientaciones de este Libro Blanco sobre la defensa y la seguridad nacionales. Para proponer la estrategia nacional en materia de seguridad de los sistemas de información, se creó un comité estratégico de sistemas de información mediante el decreto de creación de la ANSSI.

Además de la creación de la ANSSI, el Libro Blanco preveía la creación de un observatorio zonal de seguridad de los sistemas de información (OzSSI) en cada zona de defensa y seguridad. La misión de estos observatorios es transmitir, en todo el territorio nacional, las medidas adoptadas para mejorar la seguridad de los sistemas de información.

El Libro Blanco de Defensa y Seguridad Nacional de 2013 y LPM:

En 2013, ante el aumento de la cantidad y sofisticación de los ciberataques contra los sistemas de información de muchas empresas nacionales y del Estado, se publicó un nuevo Libro Blanco. Marca un punto de inflexión: el Estado ya no se conforma con satisfacer sus propias necesidades de ciberseguridad, sino que ahora tiene en cuenta las de los operadores vitales para la nación.

Este refuerzo implica para los sistemas de información más críticos de estos operadores

- el cumplimiento de las normas de seguridad que deben aplicarse
- la implantación de sistemas adecuados de detección de ataques;
- la obligación de notificar los incidentes significativos;
- la capacidad del Estado de verificar el nivel de seguridad de estos sistemas mediante auditorías y, en caso de crisis grave, de imponer las medidas necesarias.

Promulgada el 19 de diciembre de 2013, la Ley de Programación Militar (LPM) nº 2013-1168 sigue las directrices marcadas por el Libro Blanco de Defensa y Seguridad Nacional de 2013. Constituye la herramienta legislativa que permitirá a los operadores públicos y privados críticos para la nación protegerse mejor y a la ANSSI -y a otros servicios del Estado- apoyarlos mejor en caso de ciberataque. El artículo 22 prevé la adopción de medidas para reforzar la seguridad de los operadores vitales y otorga al Primer Ministro nuevas prerrogativas.

Las estrategias de ciberseguridad:

En febrero de 2011, la Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI) publicó la primera estrategia francesa de defensa y seguridad de los sistemas de información.

Para protegerse de los ciberataques y garantizar la seguridad de los ciudadanos franceses, las empresas y la nación en el ciberespacio, la estrategia francesa establece cuatro objetivos estratégicos:

- ser una potencia mundial en ciberdefensa y pertenecer al primer círculo de las grandes naciones en este ámbito, manteniendo su autonomía;
- garantizar la libertad de decisión de Francia protegiendo la información soberana
- reforzar la ciberseguridad de las infraestructuras nacionales vitales;
- y garantizar la seguridad en el ciberespacio.

El documento que presenta estos cuatro objetivos estratégicos y las siete áreas de esfuerzo que se derivan de ellos permitirá a todos los ciudadanos comprender lo que está en juego y el alcance de la acción gubernamental.

Lanzada en febrero de 2021, la segunda estrategia cibernética nacional forma parte del plan de inversiones Francia 2030. Detalles de esta estrategia y primeros logros.

Triplicar la facturación del sector cibernético y crear 37.000 puestos de trabajo de aquí a 2025: esta es la ambición de la estrategia nacional de aceleración de la ciberseguridad, con un plan de más de mil millones de euros.

Esta estrategia se basa en cuatro ejes

- desarrollar soluciones de ciberseguridad soberanas e innovadoras
- reforzar los vínculos y las sinergias entre los agentes del sector
- apoyar a la demanda (particulares, empresas, autoridades locales y el Estado), en particular sensibilizando a los franceses sobre la ciberseguridad, promoviendo al mismo tiempo las ofertas nacionales
- formar a más jóvenes y profesionales en profesiones de ciberseguridad.

Francia también cuenta con una red de CERTs, organismos oficiales encargados de prestar servicios de prevención de riesgos y asistencia en la gestión de incidentes. Estos CERT (Computer Emergency Response Teams) son centros de alerta y reacción ante ataques informáticos, destinados a las empresas y/o administraciones, pero cuya información es generalmente accesible para todos.

Marco institucional

La Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI) fue creada por el Decreto nº 2009-834 de 7 de julio de 2009 (Diario Oficial de 8 de julio de 2009), en forma de departamento con competencia nacional.

El modelo francés en el que se basa la actividad de la ANSSI distingue claramente entre misiones defensivas y ofensivas y se concreta en el papel de la agencia como autoridad nacional en materia de ciberdefensa y ciberseguridad. Esta autoridad se apoya en una base legal que indica las responsabilidades y el ámbito de actuación de la agencia.

La ANSSI ha sustituido a la Dirección Central de Seguridad de los Sistemas de Información (DCSSI) de la Secretaría General de Defensa y Seguridad Nacional (SGDSN), al tiempo que ha reforzado sus competencias, personal y recursos.

La ANSSI es la autoridad nacional para la seguridad y la defensa de los sistemas de información y constituye un conjunto de competencias que asiste a las administraciones y operadores de vital importancia.

Se encarga de promover las tecnologías, los sistemas y los conocimientos técnicos nacionales. Contribuye al desarrollo de la confianza en la tecnología digital.

El centro de transmisión gubernamental, situado bajo la autoridad de la SGDSN, asiste a la ANSSI a través de la puesta en marcha de medios de mando y enlace seguros requeridos por el Presidente de la República y el Gobierno

De acuerdo con las directrices del Libro Blanco de la Defensa y la Seguridad Nacional de 2013, la ANSSI contribuye a orientar la investigación nacional y europea sobre la seguridad de los sistemas de información.

Cuando es necesario, la ANSSI se beneficia de la experiencia de un comité estratégico formado por funcionarios de alto nivel de la administración. La misión de este comité es proponer la estrategia del Estado en este ámbito.

Desarrollos:

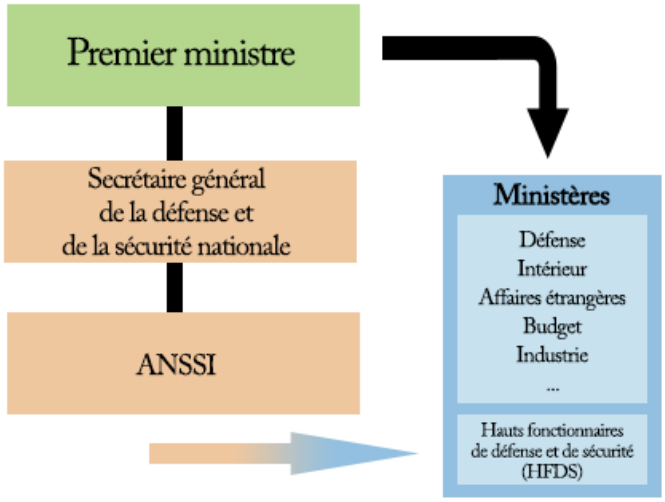
La Ley de Programación Militar promulgada el 19 de diciembre de 2013 reforzó las misiones de la ANSSI. Su artículo 22 prevé la adopción de medidas para reforzar la seguridad de los operadores de vital importancia y otorga a la ANSSI nuevas prerrogativas: en nombre del Primer Ministro, podrá imponer a las OIV medidas de seguridad y controles de sus sistemas de información más críticos. Además, el artículo 22 establece la obligatoriedad de comunicar las incidencias observadas por la OIV en estos sistemas.

El artículo 34 de la ley n°2018-607, relativo a la programación militar para los años 2019 a 2025, completa a su vez las misiones de la agencia. Especifica la implantación de sistemas de detección durante eventos susceptibles de afectar a la seguridad de los sistemas de información del Estado, de las autoridades públicas y de los operadores públicos y privados, así como la recogida de información técnica relativa a estos incidentes, y el apoyo en la respuesta a los mismos.

La seguridad de la información es responsabilidad de cada ministro en el área de la que es responsable.

Está asistido por un Alto Funcionario de Defensa y Seguridad (HFDS) cuyas competencias están recogidas en el Código de Defensa. El HFDS depende directamente del ministro y cuenta con un departamento especializado.

El HFDS se encarga de dirigir la política de seguridad de los sistemas de información y de supervisar su aplicación. Nombra a un responsable de la seguridad de los sistemas de información (FSSI) para que le ayude en estas tareas.



AI.4 España, en el marco regulatorio de la Unión Europea

Desde el punto de vista de la gobernanza de la ciberseguridad en España debemos fijar nuestra atención en dos elementos esenciales: el órgano y su producto; es decir: el Consejo de Ciberseguridad Nacional y la Estrategia Nacional de Ciberseguridad.

El **Consejo Nacional de Ciberseguridad** es el órgano colegiado de apoyo al Consejo de Seguridad Nacional en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, en el marco de la Ley 50/1997, de 27 de noviembre, del Gobierno, creándose por Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013, estando presidido por la Secretaria de Estado Directora del Centro Nacional de Inteligencia (CNI) y Directora del Centro Criptológico Nacional (CCN).

Como se señala en la página web del Departamento de Seguridad Nacional (DSN), Secretaría Técnica y órgano de trabajo permanente del Consejo, su composición refleja el espectro de los ámbitos de los departamentos, organismos y agencias del sector público con competencias en materia de ciberseguridad, para coordinar aquellas actuaciones que deban abordarse de forma conjunta, pudiendo requerir la presencia de otros actores cuya intervención para alguna sesión concreta se considere necesaria.

En la actualidad, forman el Consejo Nacional de Ciberseguridad:

- Secretaria de Estado Directora del Centro Nacional de Inteligencia (Presidencia).
- Director del Departamento de Seguridad Nacional (Vicepresidencia).
- Departamento de Seguridad Nacional (Secretaría).
- Ministerio de Asuntos Exteriores, Unión Europea y Cooperación.
- Ministerio de Defensa.
- Ministerio del Interior.
- Ministerio de Industria, Comercio y Turismo.
- Ministerio de Política Territorial.
- Ministerio de Ciencia e Innovación.
- Centro Nacional de Inteligencia.
- Ministerio de Derechos Sociales y Agenda 2030.

- Ministerio de Sanidad.
- Ministerio de Asuntos Económicos y Transformación Digital.
- Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática.
- Ministerio de Transportes, Movilidad y Agenda Urbana.
- Ministerio de Hacienda y Función Pública, y
- Ministerio de Justicia.

Sus **funciones** son las siguientes:

- Apoyar la toma de decisiones del Consejo de Seguridad Nacional en materia de ciberseguridad mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.
- Reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias relacionadas con el ámbito de la ciberseguridad, así como entre los sectores público y privado.
- Contribuir a la elaboración de propuestas normativas en el ámbito de la ciberseguridad para su consideración por el Consejo de Seguridad Nacional.
- Prestar apoyo al Consejo de Seguridad Nacional en su función de verificar el grado de cumplimiento de la Estrategia de Seguridad Nacional en lo relacionado con la ciberseguridad y promover e impulsar sus revisiones.
- Verificar el grado de cumplimiento de la Estrategia de Ciberseguridad Nacional e informar al Consejo de Seguridad Nacional.
- Realizar la valoración de 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 y evaluar los resultados de su ejecución, todo ello en coordinación con los órganos y autoridades directamente competentes.
- Contribuir a la disponibilidad de los recursos existentes y realizar los estudios y análisis sobre los medios y capacidades de las distintas Administraciones Públicas y Agencias implicadas con la finalidad de catalogar las medidas de respuesta eficaz en consonancia con los medios disponibles y las misiones a realizar, todo ello en coordinación con los órganos y autoridades directamente competentes y de acuerdo con las competencias de las diferentes Administraciones Públicas implicadas en el ámbito de la ciberseguridad.
- Facilitar la coordinación operativa entre los órganos y autoridades competentes cuando las situaciones que afecten a la Ciberseguridad lo precisen y mientras no actúe el Comité Especializado de Situación.
- Todas aquellas otras funciones que le encomiende el Consejo de Seguridad Nacional.

Como se desprende de la lista anterior, el Consejo Nacional de Ciberseguridad se centra en reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, facilitando la toma de decisiones mediante el análisis, estudio y propuesta de iniciativas tanto en los ámbitos nacional e internacional.

Uno de los resultados derivados de la función de este Consejo es la redacción y aprobación de las diferentes Estrategias Nacionales.

Por lo que toca a la ciberseguridad, la más reciente es la regulada por Orden PCI/487/2019, de 26 de abril, por la que se publica la **Estrategia Nacional de Ciberseguridad 2019**, aprobada por el Consejo de Seguridad Nacional[33], y en cuya redacción participaron todos los miembros del Consejo Nacional de Ciberseguridad, además de un Comité de Expertos de asociaciones profesionales, empresas y del mundo académico.

Esta Estrategia Nacional de Ciberseguridad desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad, considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas para conseguirlo. Así, tras señalar la importancia del ciberespacio como espacio común global y esbozar sus amenazas y riesgos, la Estrategia, siguiendo el modelo iniciado por su antecedente de 2013, determina los objetivos de ciberseguridad nacional y las líneas de acción para alcanzarlos.

El cuadro siguiente muestra dichos **objetivos** y **líneas de acción**:

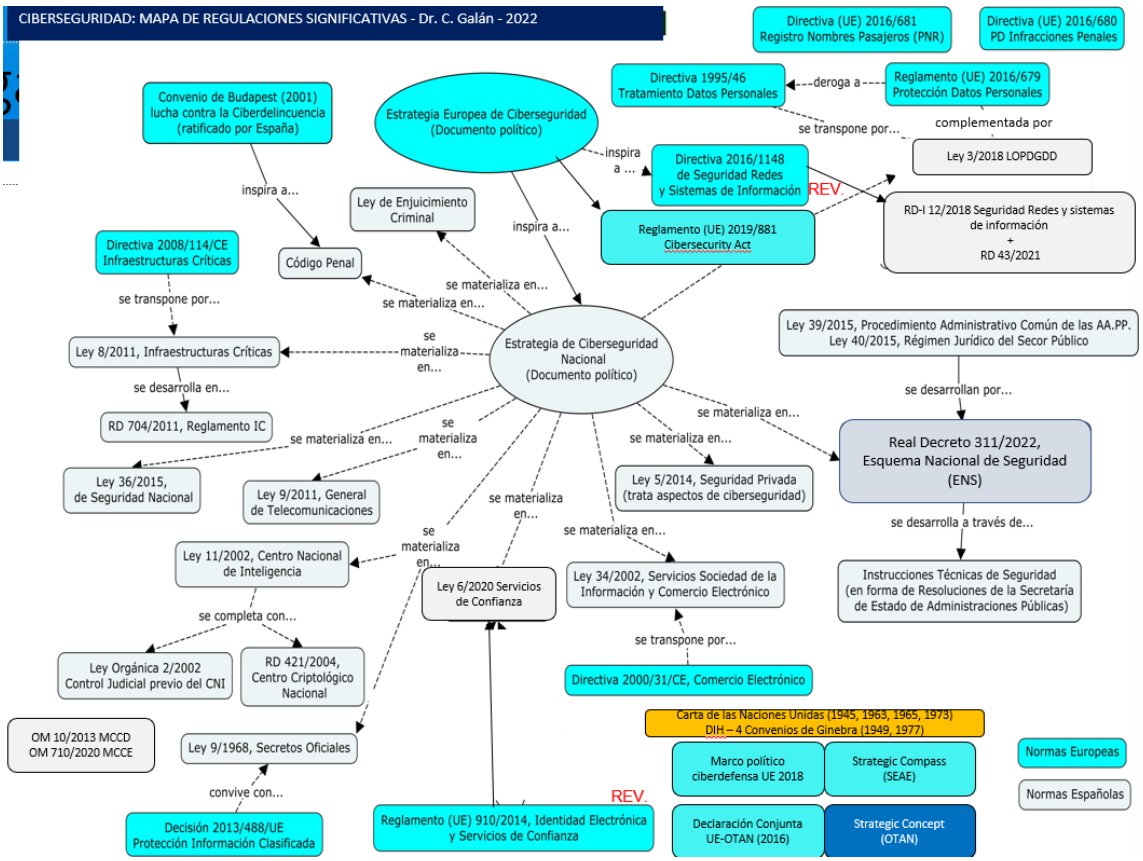
OBJETIVOS	LÍNEAS DE ACCIÓN[34]
OB.1 – Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público.	LA.1 - Reforzar las capacidades ante las amenazas provenientes del ciberespacio.
	LA.2 – Garantizar la seguridad y resiliencia de los activos estratégicos para España.
OB.2 – Uso seguro y fiable del ciberespacio frente a un uso ilícito o malicioso.	LA.3 – Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio.
OB.3 – Protección del ecosistema empresarial y social de los ciudadanos.	LA.4 – Impulsar la ciberseguridad de ciudadanos y empresas.
OB.4 – Cultura y compromiso con la ciberseguridad y protección de las capacidades humanas y tecnológicas.	LA.5 – Potenciar la industria española de ciberseguridad y la generación y retención de talento, para el fortalecimiento de la autonomía digital.
	LA.7 – Desarrollar una cultura de ciberseguridad.
OB.5 – Seguridad del ciberespacio en el ámbito internacional.	LA.6 – Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales.

[33] La primera Estrategia Nacional de Ciberseguridad, publicada en 2013, determinó los objetivos de ciberseguridad como Estado y las líneas de acción a desarrollar para alcanzarlos, sentando el modelo que se ha replicado en la estrategia vigente, alineando a nuestro país en la órbita de los países occidentales más avanzados en la materia. El Dr. Carlos Galán ha tenido el privilegio de formar parte del equipo de redacción de ambas estrategias nacionales.

[34] Cada una de las Líneas de Acción contempla un conjunto de medidas concretas que, por su extensión, no reproducimos aquí.

Si contemplamos la ciberseguridad como el conjunto de medidas dirigidas a satisfacer las exigencias de las que hemos denominado *dimensiones de la ciberseguridad* (disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y su conformidad legal) encontramos un significativo número de regulaciones que, en mayor o menor medida, generales o sectoriales, abordan tal problemática.

La figura siguiente, sin pretender en modo alguno ser exhaustiva, recoge las más significativas de ellas[35].



Ante la imposibilidad material de comentar cada una de las normas señaladas en la figura anterior, nos centraremos en las que entendemos más alineadas con el propósito del presente trabajo.

La Directiva NIS y su transposición al ordenamiento jurídico nacional. Las Propuestas de nuevas Directivas NIS2.0 y de Resiliencia de Entidades Críticas.

La conocida como Directiva NIS (**Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión**) fue publicada en el

[35] Alguna regulación, como examinamos más adelante, se encuentra en proceso de revisión (señalada con REV) en el momento de redactar este trabajo.

DOUE el 19 de julio de ese mismo año, y consideraba esencial que todos los Estados miembros de la UE poseyeran unas capacidades mínimas y una estrategia que garanticen un elevado nivel de seguridad de las redes y sistemas de información en su territorio, especialmente en lo tocante a lo que la norma europea definió como *operadores de servicios esenciales* y *proveedores de servicios digitales*, lo que debía traducirse en la adopción de un conjunto de medidas de ciberseguridad exigibles a tales entidades, tendentes a mejorar el funcionamiento del mercado interior.

Los destinatarios últimos de la norma se muestran en el cuadro siguiente:

Operadores de servicios esenciales, de los sectores…[36]
Energía: electricidad, crudo y gas.
Transporte: aéreo, ferrocarril, marítimo y fluvial y carretera.
Banca.
Infraestructuras de los mercados financieros.
Sector sanitario: entornos de asistencia sanitaria (entre ellos hospitales y clínicas privadas).
Suministro y distribución de agua potable.
Infraestructura digital: IXP, Proveedores de servicios DNS y Registros de nombres de dominio de primer nivel.
Proveedores de servicios digitales
Mercados en línea.
Motores de búsqueda en línea.
Servicios de computación en la nube.

Los **criterios** para la identificación de los operadores esenciales fueron:

d) Presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales;
e) La prestación de dicho servicio depende de las redes y sistemas de información, y
f) Un incidente tendría efectos perturbadores significativos en la prestación de dicho servicio.

La Directiva NIS, en resumen:

a) Establece la obligación para todos los Estados miembros de adoptar una **estrategia nacional de seguridad** de las redes y sistemas de información;
b) Crea un **Grupo de Cooperación** para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;
c) Crea una red de equipos de respuesta a incidentes de seguridad informática (Red de CSIRT[37]), con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz;

[36] Siempre que sean: a) una entidad presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales; b) la prestación de dicho servicio depende de las redes y sistemas de información, y c) un incidente tendría efectos perturbadores significativos en la prestación de dicho servicio.
[37] *Computer Security Incident Response Team*

d) Establece **requisitos en materia de seguridad** y **notificación** para los operadores de servicios esenciales y para los proveedores de servicios digitales;
e) Establece obligaciones para que los Estados miembros designen **autoridades nacionales competentes**, **puntos de contacto únicos** y **CSIRT** con funciones relacionadas con la seguridad de las redes y sistemas de información.

El 8 de septiembre de 2018, el Boletín Oficial del Estado publicaba el **Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información**, cumpliendo el mandato de transposición de la Directiva NIS.

Aunque la Directiva de la que traía causa limitaba su ámbito de aplicación a los denominados "operadores de servicios esenciales" y los "proveedores de servicios digitales", la norma española aprovechó el mandato para ampliar su alcance a sectores no expresamente incluidos en la europea (sin que ello suponga una derogación encubierta o un desplazamiento normativo de la legislación española vigente). Ejemplos significativos de esta ampliación lo constituyen los **prestadores de servicios de confianza** o los **operadores de redes y servicios de comunicaciones electrónicas**, que entran a formar parte de los destinatarios de la norma, en cuanto puedan ser designados operadores críticos.

Conviene señalar, llegado este punto, el esfuerzo desarrollado por el grupo de trabajo de redacción del RD-ley para cohonestar en aquel momento las tres normas estatales de especial significación en materia de (ciber)seguridad: el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS)[38], la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras Críticas y la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional[39].

El modelo de gobernanza recogido en este RD-ley se sustenta en el esquema de competencias que las vigentes Estrategias de Seguridad y Ciberseguridad nacionales han dibujado: el Consejo de Seguridad Nacional, el Consejo Nacional de Ciberseguridad, las Autoridades Competentes y los CSIRT de referencia, confiriendo a las así denominadas Autoridades Competentes las funciones de supervisión, vigilancia y sancionadora, reservando para los CSIRT de referencia las funciones más operativas, tales como el análisis de riesgos y la conducción operativa nacional de la respuesta a incidentes, actuación nacional amparada en lo dispuesto en el art. 1491.29ª de nuestra Constitución, que confiere al Estado las competencias exclusivas en materia de seguridad nacional, siendo la ciberseguridad una de sus manifestaciones, como hemos señalado antes.

Estos CSIRT de referencia constituyen, a nuestro entender, la piedra angular sobre la que descansa el tratamiento de la ciberseguridad, pues, más allá de las funciones otorgadas legalmente a las Autoridades Competentes, materializan los mecanismos de prevención, detección y respuesta a los incidentes, funciones que, a partir de la entrada en vigor de este nuevo RD-ley, vienen exigiendo de todos ellos la máxima coordinación, como asimismo prevé la norma, que confiere al CCN-CERT (del Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia) la función de coordinador nacional en los supuestos de especial gravedad.

[38] Recientemente derogado por Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
[39] Recordamos que los sectores estratégicos definidos en la Ley 8/2011, de 28 de abril, son: Administración; Espacio; Industria Nuclear; Industria Química; Instalaciones de Investigación; Agua; Energía; Salud; TIC; Transporte; Alimentación y Sistema Financiero y Tributario.

La figura siguiente muestra un esquema simplificado del marco general de reparto de competencias que dicho RD-ley dibujó originariamente[40].

			CSIRT DE REFERENCIA		AUTORIDAD COMPETENTE
OPERADORES DE SERVICIOS ESENCIALES	ES OPERADOR CRÍTICO	Pertenece al Sector Público	CCN-CERT	ESPDEF-CERT Cooperación o incidencia en la Defensa Nacional. (Requiere desarrollo reglamentario)	CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD (CNPIC) (Secretaría de Estado de Seguridad – M. Interior)
		No pertenece al Sector Público	INCIBE-CERT		
	NO ES OPERADOR CRÍTICO	Pertenece al Sector Público	CCN-CERT		CENTRO CRIPTOLÓGICO NACIONAL (CCN) (Ministerio de Defensa)
		No pertenece al Sector Público	INCIBE-CERT		AUTORIDAD SECTORIAL CORRESPONDIENTE (Requiere desarrollo reglamentario)
PROVEEDORES DE SERVICIOS DIGITALES	ES OPERADOR CRÍTICO	Pertenece al Sector Público	CCN-CERT		CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD (CNPIC) (Secretaría de Estado de Seguridad – M. Interior)
		No pertenece al Sector Público	INCIBE-CERT		
	NO ES OPERADOR CRÍTICO	Pertenece al Sector Público	CCN-CERT		CENTRO CRIPTOLÓGICO NACIONAL (CCN) (Ministerio de Defensa)
		No pertenece al Sector Público	INCIBE-CERT		SECRETARIA DE ESTADO PARA EL AVANCE DIGITAL (Ministerio de Economía y Empresa)

Pese a tratarse de una norma en vigor y, por tanto, ejecutiva, el Real Decreto-ley pospuso a su desarrollo reglamentario determinadas cuestiones que veremos más adelante.

En la actualidad, son numerosas las regulaciones de sustrato tecnológico que prescriben la notificación de incidentes al organismo competente de que se trate en cada caso. Esta diversidad, de la que en muchas ocasiones es sujeto obligado la misma entidad, alienta y justifica la existencia de una Plataforma Común para la notificación de incidentes, capaz de dar respuesta, a través de un solo proceso (contemplando la notificación inicial, las intermedias y la final) dirigido automáticamente a cada autoridad competente por razón de la legislación afectada, lo que puede constituir, a nuestro juicio, una de las medidas más innovadoras de este Real Decreto-ley en materia de ciberseguridad, a imagen de lo que ha venido desarrollando en CCN-CERT en el Sector Público con la plataforma LUCIA.

El RD-ley exhibe un régimen de infracciones especialmente riguroso. Un solo ejemplo: en determinadas circunstancias, tipifica como muy grave la falta de adopción de las medidas para subsanar las deficiencias detectadas o el incumplimiento reiterado de la obligación de notificar los incidentes.

El desarrollo reglamentario al que antes nos hemos referido tuvo lugar por **Real Decreto 43/2021, de 26 de enero**, que vino a regular los siguientes aspectos:

[40] Recientemente, el Real Decreto-ley 6/2022, de 29 de marzo, por el que se adoptan medidas urgentes en el marco del Plan Nacional de respuesta a las consecuencias económicas y sociales de la guerra en Ucrania, actualiza la denominación dada a la Secretaría de Estado para el Avance Digital por la actual Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital e introduce un nuevo apartado en el artículo 16 con algunas cautelas adicionales dirigidas a los operadores de servicios esenciales y proveedores de servicios digitales que, pese a no ser operadores críticos se encuentren comprendidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, que utilizan servicios ofrecidos por proveedores de servicios digitales, en particular servicios de computación en nube, podrán exigir a los proveedores de tales servicios medidas de seguridad adicionales, más estrictas que las que dichos proveedores han adoptado en cumplimiento de la legislación en materia de seguridad de las redes y sistemas de información, sabiendo que las citadas medidas podrán ser exigidas mediante obligaciones contractuales, previo informe preceptivo y vinculante del Centro Criptológico Nacional.

- La identificación de los factores específicos en los sectores de los operadores de servicios esenciales para determinar si un incidente podría tener efectos perturbadores significativos.
- En la determinación de las Autoridades Competentes, la autoridad sectorial correspondiente por razón de la materia, cuando no se trate de operadores críticos.
- Dentro de las funciones de las Autoridades Competentes, el establecimiento de canales de comunicación con los operadores de servicios esenciales y los proveedores de servicios digitales, y los protocolos de actuación para la coordinación con los CSIRT de referencia.
- La identificación de los operadores de servicios esenciales con incidencia en la Defensa Nacional.
- La determinación de los supuestos de especial gravedad que requieran de la coordinación nacional del CCN-CERT.
- La determinación de los mecanismos de coordinación de los CSIRT de referencia con la Oficina de Coordinación Cibernética del Centro Nacional de Protección de Infraestructuras y Ciberseguridad del Ministerio del Interior, cuando las actividades de respuesta puedan afectar a un operador crítico.
- La determinación de las medidas técnicas y de organización que deberán adoptar los operadores de servicios esenciales y los proveedores de servicios digitales.
- La fijación de los plazos para la designación y comunicación a la Autoridad Competente por parte de los operadores de servicios esenciales, de la persona, unidad u órgano colegiado responsable de la seguridad de la información y la identificación de sus funciones.
- La determinación, a efectos de notificación, de los sucesos o incidencias que podrían afectar a las redes y sistemas de información, aun cuando todavía no lo hayan hecho.
- La determinación de las medidas necesarias relativas a la notificación de incidentes por parte de los operadores de servicios esenciales.
- El órgano de la autoridad competente para la imposición de sanciones en el caso de infracciones graves o leves.

En el momento de redactar estos párrafos, las instituciones de la Unión Europea están desarrollando el borrador de lo que será la nueva Directiva, a la que informalmente se ha denominado **Propuesta de Directiva NIS2.0**.

Efectivamente, durante la segunda mitad de 2020, la Comisión Europea llevó a cabo una evaluación de los resultados alcanzados con la Directiva NIS, incluyendo una consulta pública que concluyó, desde diversos ámbitos, la necesidad de mejorar la transposición de la norma, su alcance y su definición.

Como consecuencia de ello, la Comisión presentó una propuesta de revisión[41] que trataba de mejorar algunos problemas que la Directiva NIS no había resuelto y que, como se ha dicho[42], aparecían en la antedicha evaluación, tales como la reducida ciberresiliencia empresarial, la diferente implementación según los países, el bajo conocimiento situacional y la carencia de respuestas comunes.

[41] Propuesta de Directiva COM (2020) 823 (final) de la Comisión de 16 de diciembre sobre medidas para un alto nivel común de Ciberseguridad en la UE y Anexos sobre entidades esenciales e importantes.
[42] Arteaga. F. "La evaluación y la revisión de la Directiva NIS: la directiva NIS2.0". R. I. Elcano (Feb., 2021)

En su exposición de motivos, la Comisión reconoce que:

- El ámbito de aplicación de la Directiva NIS se ha quedado pequeño debido al avance de la digitalización y la conectividad en los últimos años y no incluye a servicios digitales relevantes.
- Tampoco incluye a todos los actores relevantes porque los criterios de la Directiva y de las transposiciones nacionales para identificar los proveedores de servicios digitales no han sido claros.
- Por las mismas razones, el procedimiento para la notificación de incidentes por los proveedores de servicios esenciales no es el mismo y las sanciones y exigencia de obligaciones varía en cada Estado miembro.
- El intercambio de información entre actores públicos y privados sigue siendo muy bajo y poco sistematizado.
- La disparidad de los recursos presupuestarios y humanos disponibles por los Estados miembros condiciona su nivel de madurez y su capacidad de ciberresiliencia.

La nueva Propuesta refleja así el deseo de la Comisión de extender el ámbito de aplicación de la norma europea a otros actores, tales como los suministradores de servicios o redes públicas de comunicación, los de contenidos o datos, los de plataformas de redes sociales y los dedicados a fomentar la confianza en los anteriores o a las Administraciones Públicas, los servicios postales, la gestión de aguas, el espacio, la alimentación, entre otros, eliminando la clasificación actual de operadores de servicios esenciales y proveedores de servicios digitales, sustituyéndolos por **entidades esenciales** y **entidades importantes.**

A la fecha de redacción de estas líneas, la adscripción por sectores de las entidades contempladas en la Propuesta de Directiva NIS2.0 es la siguiente:

Entidades Esenciales	Entidades Importantes
- Energía (Electricidad, Calefacción y refrigeración urbana, Crudo, Gas, Hidrógeno) - Transporte (Aire, Ferrocarril, Agua, Carretera). - Banca. - Infraestructuras de los mercados financieros. - Salud. - Agua potable. - Aguas residuales.	- Servicios postales y de mensajería. - Gestión de residuos. - Fabricación, producción y distribución de productos químicos. - Producción, transformación y distribución de alimentos. - Fabricación[44]. - Proveedores digitales (Mercados en línea, Motores de búsqueda en línea, Plataformas de servicios de redes sociales.) - Investigación.

[44] Fabricación de productos sanitarios y productos sanitarios para diagnóstico in vitro; productos informáticos, electrónicos y ópticos; maquinaria y equipos n.c.o.p.; vehículos de motor, remolques y semirremolques y otro material de transporte.

- Infraestructura Digital[43]. - Administraciones públicas. - Espacio.	

En ambos grupos, el nuevo texto obliga a los estados a supervisar (mediante actuaciones *ex ante* o *ex post*, atendiendo a su adscripción) las medidas de seguridad que hayan de adoptarse por las entidades afectadas, que, en caso de incumplimiento, conllevarían importantes sanciones.

De nuevo el análisis de riesgos previo, como método para la determinación de las medidas de seguridad adecuadas, se configura como un elemento esencial, también de esta nueva norma, al igual que ya lo viene siendo, por ejemplo, en el caso español con el Esquema Nacional de Seguridad.

Por último, también al tiempo de redactar estos párrafos, y dando respuesta a los llamamientos a la acción por parte del Consejo[45] y del Parlamento[46] para revisar el actual enfoque de seguridad de las entidades críticas y garantizar una mayor armonización con la Directiva NIS, se encuentra en proceso de redacción la **Propuesta de Directiva del Parlamento Europeo y del Consejo, relativa a la resiliencia de las entidades críticas** (denominada informalmente Directiva RES)[47] cuyo objeto es mejorar la prestación en el mercado interior de servicios esenciales para el mantenimiento de funciones sociales o actividades económicas vitales, aumentando la resiliencia de las entidades críticas que prestan tales servicios, haciendo frente al aumento de la interconexión entre el mundo físico y digital mediante un marco legislativo con sólidas medidas de resiliencia, tanto para los aspectos cibernéticos como físicos, tal como se establece en la Estrategia para una Unión de la Seguridad[48].

Como señala su texto introductorio, la propuesta refleja los enfoques nacionales que ponen el acento en las interdependencias intersectoriales y transfronterizas, en las que la protección es solo un elemento junto con la prevención y mitigación de riesgos, la continuidad de las actividades y la recuperación (resiliencia).

Así pues, esta Propuesta de Directiva tiene por objeto:

[43] Entre ellas: - Proveedores de Puntos de Intercambio de Internet - Proveedores de servicios de DNS, excluidos los operadores de servidores de nombres raíz - Registros de nombres de TLD - Proveedores de servicios de computación en la nube - Proveedores de servicios de centros de datos - Proveedores de redes de entrega de contenidos - Proveedores de servicios de confianza a los que se refiere el punto (19) del artículo 3 del Reglamento (UE) n.º 910/2014(1) - Proveedores de redes públicas de comunicaciones electrónicas a los que se refiere el punto (8) del artículo 2 de la Directiva (UE) 2018/1972(2) o proveedores de servicios de comunicaciones electrónicas a los que se refiere el punto (4) del artículo 2 de la Directiva (UE) 2018/1972 cuando sus servicios estén disponibles al público. Gestión de servicios de TIC (B2B); Gestión de servicios de TIC (B2B); Proveedores de servicios gestionados (MSP) - Proveedores de servicios de seguridad gestionados (MSSP).

[45] Conclusiones del Consejo, de 10 de diciembre de 2019, sobre las acciones complementarias para aumentar la resiliencia y luchar contra las amenazas híbridas (doc. 14972/19).

[46] Informe sobre las conclusiones y recomendaciones de la Comisión Especial sobre Terrorismo del Parlamento Europeo (2018/2044 (INI)).

[47] Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la resiliencia de las entidades críticas. Bruselas, 16.12.2020 - COM(2020) 829 final - 2020/0365 (COD).

[48] COM(2020) 605.

a) Establecer la obligación de los Estados miembros de adoptar determinadas medidas destinadas a garantizar la prestación en el mercado interior de servicios esenciales para el mantenimiento de funciones sociales o actividades económicas vitales, en particular para identificar las entidades y entidades críticas que deberán considerarse equivalentes en determinados aspectos y para permitirles cumplir sus obligaciones;
b) Establecer obligaciones de las entidades críticas destinadas a aumentar su resiliencia y mejorar su capacidad de prestar esos servicios en el mercado interior;
c) Establecer normas sobre la supervisión y ejecución de las entidades críticas, y la supervisión específica de las entidades críticas consideradas de particular importancia europea.

Siendo su ámbito de aplicación cualquiera de las entidades (públicas o privadas) de uno de los tipos mencionados en su Anexo, y que asimismo haya sido identificada como "entidad crítica" por un Estado miembro de conformidad con el artículo 5 de la misma, los tipos de entidades relacionados con el sector **Infraestructura Digital** son los siguientes:

- Los proveedores de puntos de intercambio de Internet (de la Directiva NIS2.0).
- Los proveedores de servicios de DNS (de la Directiva NIS2.0).
- Los registros de nombres del dominio de primer nivel (de la Directiva NIS2.0).
- Los proveedores de servicios de computación en nube (de la Directiva NIS2.0).
- Los proveedores del servicio de centros de datos (de la Directiva NIS2.0).
- Los proveedores de redes de distribución de contenidos (de la Directiva NIS2.0).
- Los proveedores de servicios de confianza a que se refiere el artículo 3, punto 19), del Reglamento (UE) n.º 910/2014 (Reglamento eIDAS).
- Los proveedores de redes públicas de comunicaciones electrónicas a que se refiere artículo 2, punto 8), de la ya estudiada Directiva 2018/1972/UE (Código Europeo de Comunicaciones Electrónicas) o los proveedores de servicios de comunicaciones electrónicas en el sentido del artículo 2, punto 4), de la Directiva (UE) 2018/1972, en la medida en que sus servicios estén a disposición del público.

Entre los cuales también se encuentran los proveedores de redes públicas de comunicaciones electrónicas.

La ciberseguridad pública: el Esquema Nacional de Seguridad.

La Constitución española de 1978, en su artículo 103.1, proclama: "*La Administración Pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Ley y al Derecho*."

Así pues, y amparado genéricamente en el principio irrenunciable de la eficacia, el despliegue de los servicios que el Sector Público (Administraciones Públicas y Sector Público Institucional) debe prestar a los ciudadanos, especialmente cuando se usan las Tecnologías de la Información y la Comunicación (TIC), exige contar –para dar cumplida respuesta a aquella exigencia constitucional- con los procedimientos administrativos, métodos y herramientas más adecuados que vengan a garantizar a todos sus destinatarios: ciudadanos y empresas, pero también el resto del Sector Público, la seguridad y confiabilidad de sus actos.

Efectivamente, de poco serviría poseer unas magníficas tecnologías que posibilitaran el tratamiento y la comunicación de millones de datos si los actores implicados en la vida de los

procedimientos administrativos no percibieran los sistemas de información en los que se sustenta su relación como infraestructuras seguras y tan confiables como la misma esencia que sus actividades requiere.

No cabe duda –como así se ha afirmado-, que el mejor servicio al ciudadano constituye la razón de las reformas que, tras la aprobación de la Constitución, se han ido acometiendo en España para configurar una Administración moderna que haga de los principios de eficacia y eficiencia su razón última, y siempre con la mirada puesta en los ciudadanos y en los intereses generales.

Tal interés constituyó la principal razón de ser de la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP, en adelante), eje vertebrador originario de la que se ha dado en llamar *Administración electrónica*, persiguiendo estar a la altura de nuestra época y del adecuado posicionamiento de nuestras Administraciones Públicas en el marco europeo e internacional. La publicación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP, en adelante) y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP, en adelante), que derogan la anterior, consolidan la primacía del uso de los medios electrónicos en el desenvolvimiento de las entidades públicas.

El reconocimiento general de la relación electrónica en y con el Sector Público plantea varias cuestiones que es necesario contemplar:

- La progresiva utilización de medios electrónicos suscita la cuestión de la privacidad de los datos que se facilitan electrónicamente en relación con un expediente.
- Los legitimados tienen derecho de acceso al estado de tramitación del procedimiento administrativo, así como examinar los documentos de los que se compone. Lo mismo debe suceder, como mínimo, en un expediente iniciado electrónicamente o tramitado de esta forma. Dicho expediente debe permitir el acceso en línea a los interesados para verificar su situación, sin mengua de las garantías de privacidad.
- En todo caso, la progresiva utilización de comunicaciones electrónicas, derivada del reconocimiento del derecho a comunicarse electrónicamente con la Administración, suscita la cuestión no ya de la adaptación de ésta -recursos humanos y materiales a una nueva forma de relacionarse con los ciudadanos-, sino también la cuestión de la manera de adaptar sus formas de actuación y tramitación de los expedientes y, en general, racionalizar, simplificar y adaptar los procedimientos, aprovechando la nueva realidad que imponen las TIC.
- El hecho de reconocer el derecho (obligación, en algunos casos) de los ciudadanos a comunicarse electrónicamente con la Administración, plantea, en primer lugar, la necesidad de definir claramente la sede administrativa electrónica con la que se establecen las relaciones, promoviendo un régimen de identificación, autenticación, contenido mínimo, protección jurídica, accesibilidad, disponibilidad y responsabilidad.

Son muchos los preceptos contenidos en nuestras leyes administrativas de referencia (Ley 39/2015 y Ley 40/2015, ambas de 1 de octubre) que insisten en la necesidad de que el desenvolvimiento de las entidades del Sector Público, tanto si obedece al desarrollo del procedimiento como si responde al ejercicio general de sus competencias, debe tener lugar en el marco de un entorno que contemple todas las medidas de seguridad que sean precisas para garantizar a los administrados y a las propias entidades públicas, la integridad, confidencialidad,

autenticidad y trazabilidad de la información tratada y la disponibilidad de los servicios prestados, en el marco del respeto a la legislación vigente.

La Ley 39/2015, de 1 de octubre, recoge, entre los derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo "*a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas*". Realiza, además, diversas menciones al cumplimiento de las garantías y medidas de seguridad, cuando se refiere a los registros, archivo de documentos y copias.

Por su parte, la Ley 40/2015, de 1 de octubre, que recoge en su artículo 156 el Esquema Nacional de Seguridad, así mismo menciona la seguridad al referirse a las relaciones de las administraciones por medios electrónicos, la sede electrónica, el archivo electrónico de documentos, los intercambios electrónicos en entornos cerrados de comunicaciones y las transmisiones de datos entre Administraciones Públicas.

El Esquema Nacional de Seguridad (ENS), operado en la actualidad por **Real Decreto 311/2022, de 3 de mayo**, constituye uno de los mejores ejemplos europeos de tratamiento de la ciberseguridad.

El vigente ENS, actualizado y heredero del originariamente regulado en el Real Decreto 3/2010, de 8 de enero, ha tenido los siguientes objetivos:

- Alinear el ENS al marco normativo y al contexto estratégico existente para garantizar la seguridad en la administración digital, tratando de reflejar con claridad su ámbito de aplicación en beneficio de la ciberseguridad y de los derechos de los ciudadanos, así como actualizar las referencias al marco legal vigente y revisar la formulación de ciertas cuestiones a la luz de éste, conforme a la Estrategia Nacional de Ciberseguridad 2019, de forma que se logre simplificar, precisar o armonizar los mandatos del ENS, eliminar aspectos que hayan podido considerarse excesivos, o añadir aquellos otros que se identifican como necesarios.
- Introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios. Ello aconseja la inclusión en el ENS del concepto de "Perfil de Cumplimiento Específico" que, aprobado por el Centro Criptológico Nacional, permita alcanzar una adaptación del ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.
- Facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, los requisitos mínimos y las medidas de seguridad.

Conviene recordar que el ámbito subjetivo de aplicación de esta norma es la totalidad de las entidades comprendidas en el denominado Sector Público, en los términos en que se define en el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma, siendo también exigible a los sistemas de información de las entidades del sector privado, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas, lo que alcanza también, aunque de una

forma instrumental, a los operadores de telecomunicaciones, extendiéndose también a la cadena de suministro de los antedichos contratistas o proveedores, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

En resumen, el ENS está constituido por los **principios básicos** y **requisitos mínimos** necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

PRINCIPIOS BÁSICOS	REQUISITOS MÍNIMOS
• Seguridad como proceso integral. • Gestión de la seguridad basada en los riesgos. • Prevención, detección, respuesta y conservación. • Existencia de líneas de defensa. • Vigilancia continua. • Reevaluación periódica. • Diferenciación de responsabilidades.	• Organización e implantación del proceso de seguridad. • Análisis y gestión de los riesgos. • Gestión de personal. • Profesionalidad. • Autorización y control de los accesos. • Protección de las instalaciones. • Adquisición de productos de seguridad y contratación de servicios de seguridad. • Mínimo privilegio. • Integridad y actualización del sistema. • Protección de la información almacenada y en tránsito. • Prevención ante otros sistemas de información interconectados. • Registro de la actividad y detección de código dañino. • Incidentes de seguridad. • Continuidad de la actividad. • Mejora continua del proceso de seguridad.

El ENS contempla la adopción por parte de las entidades de su ámbito de aplicación de medidas concretas, de naturaleza organizativa y técnica, según la siguiente distribución:

Como señala el propio Real Decreto, lo dispuesto en él, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

Por último, el ENS confiere a la Secretaría General de Administración Digital (de la Secretaría de Estado para la Digitalización y la Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital) y al Centro Criptológico Nacional (adscrito al Centro Nacional de Inteligencia del Ministerio de Defensa), en sus respectivas competencias, la responsabilidad de velar por la adecuada implantación, desarrollo y seguimiento del ENS en las entidades de su ámbito de aplicación.

La protección de las infraestructuras críticas

La **Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas (ICE)** y la evaluación de la necesidad de mejorar su protección, constituyó un primer paso en el proceso de identificación y designación de las ICE y de evaluación de la necesidad de mejorar su protección.

Efectivamente, existen en la UE una serie de infraestructuras críticas (IC) cuya perturbación o destrucción podrían tener repercusiones importantes, posiblemente con consecuencias transfronterizas intersectoriales derivadas de la interdependencia de las infraestructuras interconectadas, por lo que se hacía necesario proceder a la identificación y designación de tales ICE atendiendo a un procedimiento común, incluyendo las necesidades de seguridad para estas infraestructuras, lo que debe efectuarse conforme a un planteamiento mínimo común, lo que implica que en todas las ICE designadas deberán existir **planes de seguridad del operador** o medidas equivalentes que incluyan la identificación de los elementos importantes, una

evaluación de riesgos y la identificación, selección y orden de preferencia de las contramedidas y procedimientos.

La Directiva realiza las siguientes **definiciones**:

Infraestructura Crítica (IC)	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 y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones;
Infraestructura crítica europea (ICE)	La infraestructura crítica situada en los Estados miembros cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros. La magnitud de la incidencia se valorará en función de criterios horizontales, como los efectos de las dependencias intersectoriales en otros tipos de infraestructuras;
Análisis de riesgos	El estudio de hipótesis de amenazas, para evaluar las vulnerabilidades y las posibles repercusiones de la perturbación o destrucción de infraestructuras críticas;
Información sensible sobre protección de infraestructuras críticas	Datos específicos sobre una infraestructura crítica que, de revelarse, podrían utilizarse para planear y actuar con el objetivo de provocar una perturbación o la destrucción de instalaciones de infraestructuras críticas;
Protección	Todas las actividades destinadas a garantizar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar una amenaza, riesgo o vulnerabilidad;
Propietarios u operadores de infraestructuras críticas europeas	Las entidades responsables de las inversiones o del funcionamiento diario de un elemento, sistema o parte del mismo, designado como ICE con arreglo a la Directiva.

La Directiva deja a la libre determinación de cada Estado Miembro la identificación, conforme al procedimiento establecido en su Anexo III, las ICE potenciales que se ajusten a los criterios horizontales y sectoriales y a las definiciones dadas.

Los **criterios horizontales** que la Directiva señala y que deben tomarse en consideración para la determinación de las ICE deberán incluir:

d) El número de víctimas (valorado en función del número potencial de víctimas mortales o de heridos);

e) El impacto económico (valorado en función de la magnitud de las pérdidas económicas o el deterioro de productos o servicios, incluido el posible impacto medioambiental);

f) El impacto público (valorado en función de la incidencia en la confianza de la población, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida de servicios esenciales).

Los umbrales de tales criterios horizontales atenderán a la gravedad de las repercusiones en relación con la perturbación o destrucción de una infraestructura dada. Los umbrales concretos que se aplicarán a los criterios horizontales los determinará cada Estado miembro en función de

la infraestructura crítica considerada, que informará anualmente a la Comisión del número de infraestructuras por sector sobre las que se hayan determinado los umbrales de dichos criterios.

Los **criterios sectoriales** tendrán en cuenta las características de los diferentes sectores de las ICE.

En el Anexo I de la Directiva se contiene la relación de sectores concernidos por la norma:

Lista de sectores con ICE

Sector	Subsector	
I Energía	1. Electricidad	Infraestructuras e instalaciones de generación y transporte de electricidad, en relación con el suministro de electricidad
	2. Petróleo	Producción de petróleo, refino, tratamiento, almacenamiento y distribución por oleoductos
	3. Gas	Producción de gas, refino, tratamiento, almacenamiento y transporte por gasoductos Terminales de GNL
II Transportes	4. Transporte por carretera 5. Transporte por ferrocarril 6. Transporte aéreo 7. Transporte por vías navegables interiores 8. Transporte marítimo (costero y de altura) y puertos	

La Directiva recoge la necesidad de que exista un **Procedimiento para el Plan de Seguridad del Operador (PSO),** que se muestra en el cuadro siguiente:

PROCEDIMIENTO PSO - ICE

El PSO identificará los elementos infraestructurales críticos y las soluciones de seguridad que existen o se están poniendo en práctica para su protección. El procedimiento PSO ICE incluirá al menos:

1) La identificación de elementos importantes;
2) La realización de un análisis de riesgos basado en los principales supuestos de amenaza, las vulnerabilidades de cada elemento y la repercusión potencial, y
3) La identificación, selección y orden de preferencia de las contramedidas y procedimientos, distinguiendo entre:
   - Medidas de seguridad <u>permanentes</u>, que identifiquen las inversiones y medios indispensables en materia de seguridad que puedan emplearse en cualquier circunstancia. Esta rúbrica incluirá información sobre medidas de carácter general, como medidas técnicas (incluida la instalación de medios de detección, control de acceso, protección y prevención); medidas organizativas (incluidos los procedimientos de alertas y gestión de crisis); medidas de control y verificación; comunicación; concienciación y formación, y seguridad de los sistemas de información,
   - Medidas de seguridad <u>graduales</u>, que podrán activarse en función de los diferentes niveles de riesgo y de amenaza.

Además de ello, la Directiva señala la necesidad de designar un **Responsable de Seguridad y Enlace,** que ejercerá la función de punto de contacto para cuestiones de seguridad entre el propietario u operador de ICE y la autoridad competente del Estado miembro.

Dada la complejidad de la materia, su incidencia sobre la seguridad de las personas y sobre el funcionamiento de las estructuras básicas nacionales e internacionales, y en cumplimiento de lo estipulado por la referida Directiva 2008/114/CE, se hizo preciso elaborar una norma cuyo objeto debía ser, por un lado, regular la protección de las infraestructuras críticas nacionales contra ataques deliberados de todo tipo (tanto de carácter físico como cibernético) y, por otro lado, la definición de un sistema organizativo de protección de dichas infraestructuras que aglutine a las Administraciones Públicas y entidades privadas afectadas.

Esta norma es la **Ley 8/2011, de 28 de abril, de medidas para la Protección de las Infraestructuras Críticas.**

La, así denominada, Ley PIC contiene las siguientes **definiciones**:

Servicio esencial	El servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.
Sector estratégico	Cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Su categorización viene determinada en el anexo de esta norma.
Subsector estratégico	Cada uno de los ámbitos en los que se dividen los distintos sectores estratégicos, conforme a la distribución que contenga, a propuesta de los Ministerios y organismos afectados, el documento técnico que se apruebe por el Centro Nacional de Protección de las Infraestructuras Críticas.
Infraestructuras estratégicas	Las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.
Infraestructuras críticas	Las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.
Infraestructuras críticas europeas:	Aquellas infraestructuras críticas situadas en algún Estado miembro de la Unión Europea, cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros, todo ello con arreglo a la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.
Zona crítica	Aquella zona geográfica continua donde estén establecidas varias infraestructuras críticas a cargo de operadores diferentes e interdependientes, que sea declarada como tal por la Autoridad competente. La declaración de una zona crítica tendrá por objeto facilitar la mejor protección y una mayor coordinación entre los diferentes operadores

	titulares de infraestructuras críticas o infraestructuras críticas europeas radicadas en un sector geográfico reducido, así como con las Fuerzas y Cuerpos de Seguridad del Estado y las Policías Autonómicas de carácter integral.
Criterios horizontales de criticidad	Los parámetros en función de los cuales se determina la criticidad, la gravedad y las consecuencias de la perturbación o destrucción de una infraestructura crítica se evaluarán en función de: 1. El número de personas afectadas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública. 2. El impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios. 3. El impacto medioambiental, degradación en el lugar y sus alrededores. 4. El impacto público y social, por la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.
Análisis de riesgos	El estudio de las hipótesis de amenazas posibles necesario para determinar y evaluar las vulnerabilidades existentes en los diferentes sectores estratégicos y las posibles repercusiones de la perturbación o destrucción de las infraestructuras que le dan apoyo.
Interdependencias	los efectos que una perturbación en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el propio sector y en otros sectores, y las repercusiones de ámbito local, autonómico, nacional o internacional.
Protección de infraestructuras críticas	El conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia.
Información sensible sobre protección de infraestructuras estratégicas	Los datos específicos sobre infraestructuras estratégicas que, de revelarse, podrían utilizarse para planear y llevar a cabo acciones cuyo objetivo sea provocar la perturbación o la destrucción de éstas.
Operadores críticos	Las entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica con arreglo a la presente Ley.
Nivel de Seguridad	Aquel cuya activación por el Ministerio del Interior está prevista en el Plan Nacional de Protección de Infraestructuras Críticas, de acuerdo con la evaluación general de la amenaza y con la específica que en cada supuesto se efectúe sobre cada infraestructura, en virtud del cual corresponderá declarar un grado concreto de intervención de los diferentes organismos responsables en materia de seguridad.

Catálogo Nacional de Infraestructuras Estratégicas	La información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras existentes en el territorio nacional.

Como pieza básica de este sistema, la Ley creó el **Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)** como órgano de asistencia al Secretario de Estado de Seguridad en la ejecución de las funciones que se le encomiendan a éste como órgano responsable del sistema.

La finalidad de esta norma es, por lo tanto, el establecimiento de medidas de protección de las infraestructuras críticas que proporcionen una base adecuada sobre la que se asiente una eficaz coordinación de las Administraciones Públicas y de las entidades y organismos gestores o propietarios de infraestructuras que presten servicios esenciales para la sociedad, con el fin de lograr una mejor seguridad para aquéllas.

Sobre esta base, se sustentarán el **Catálogo Nacional de Infraestructuras Estratégicas** (conforme a la comunicación del Consejo de la Unión Europea de 20 de octubre de 2004, que señala que cada sector y cada Estado miembro deberá identificar las infraestructuras que son críticas en sus respectivos territorios) y el **Plan Nacional de Protección de Infraestructuras Críticas**, como principales herramientas en la gestión de la seguridad de nuestras infraestructuras.

Si bien el contenido material de la Ley es eminentemente organizativo, especialmente en lo concerniente a la composición, competencias y funcionamiento de los órganos que integran el Sistema de Protección de Infraestructuras Críticas, así como en todo lo relativo a los diferentes planes de protección, se optó por dotar a esta norma de rango legal, de acuerdo con el criterio del Consejo de Estado, a fin de poder cubrir suficientemente aquellas obligaciones que la Ley impone y que requieren de una cobertura legal específica.

La Ley PIC regula lo que define como **Sistema de Protección de Infraestructuras Críticas**, que se compone de una serie de instituciones, órganos y empresas, procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos.

Atendiendo a lo dispuesto en la Ley PIC, son **agentes del Sistema**, con las funciones que se determinen reglamentariamente, los siguientes:

a) La Secretaría de Estado de Seguridad del Ministerio del Interior.

b) El Centro Nacional para la Protección de las Infraestructuras Críticas.

c) Los Ministerios y organismos integrados en el Sistema, que serán los incluidos en el anexo de la propia Ley.

d) Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.

e) Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.

f) Las Corporaciones Locales, a través de la asociación de Entidades Locales de mayor implantación a nivel nacional.

g) La Comisión Nacional para la Protección de las Infraestructuras Críticas.

h) El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

i) Los operadores críticos del sector público y privado.

Además, la Ley PIC crea la **Comisión Nacional para la Protección de las Infraestructuras Críticas**, como órgano colegiado adscrito a la Secretaría de Estado de Seguridad, y que será la competente para aprobar los diferentes Planes Estratégicos Sectoriales así como para designar a los operadores críticos, a propuesta del Grupo de Trabajo Interdepartamental para la Protección de Infraestructuras Críticas.

Por su parte, la norma recoge una serie de **obligaciones para los operadores críticos,** entre ellas:

a) Asesorar técnicamente al Ministerio del Interior, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo, actualizando los datos disponibles con una periodicidad anual y, en todo caso, a requerimiento del citado Ministerio.

b) Colaborar, en su caso, con el Grupo de Trabajo en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgos sobre los sectores estratégicos donde se encuentren incluidos.

c) Elaborar el Plan de Seguridad del Operador en los términos y con los contenidos que se determinen reglamentariamente.

d) Elaborar, según se disponga reglamentariamente, un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo.

e) Designar a un Responsable de Seguridad y Enlace en los términos de la presente Ley.

f) Designar a un Delegado de Seguridad por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior, comunicando su designación a los órganos correspondientes.

g) Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial y adoptar las medidas de seguridad que sean precisas en cada Plan, solventando en el menor tiempo posible las deficiencias encontradas.

Finalmente, la Ley PIC recoge los **Instrumentos de Planificación del Sistema,** requiriendo la adopción y aplicación de los siguientes planes de actuación:

a) El Plan Nacional de Protección de las Infraestructuras Críticas.

b) Los Planes Estratégicos Sectoriales.

c) Los Planes de Seguridad del Operador.

d) Los Planes de Protección Específicos.

e) Los Planes de Apoyo Operativo.

El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, es el encargado de elaborar el **Plan Nacional de Protección de las Infraestructuras Críticas**, siendo éste el documento estructural que permite dirigir y coordinar las actuaciones precisas para proteger las infraestructuras críticas en la lucha contra el terrorismo.

Los **Planes Estratégicos Sectoriales** serán elaborados por el Grupo de Trabajo y aprobados por la Comisión, e incluirán, por sectores, los criterios definidores de las medidas a adoptar para hacer frente a una situación de riesgo.

Los **Planes de Seguridad del Operador** y los **Planes de Protección Específicos** deberán ser elaborados por los operadores críticos respecto a todas sus infraestructuras clasificadas como Críticas o Críticas Europeas, tratándose de instrumentos de planificación a través de los cuales aquéllos asumen la obligación de colaborar en la identificación de dichas infraestructuras, especificar las políticas a implementar en materia de seguridad de las mismas, así como implantar las medidas generales de protección, tanto las permanentes como aquellas de carácter temporal que, en su caso, vayan a adoptar para prevenir, proteger y reaccionar ante posibles ataques deliberados contra aquéllas.

Finalmente, los **Planes de Apoyo Operativo** deberán ser elaborados por el Cuerpo Policial estatal o, en su caso, autonómico, con competencia en la demarcación, para cada una de las infraestructuras clasificadas como Críticas o Críticas Europeas dotadas de un Plan de Protección Específico, debiendo contemplar las medidas de vigilancia, prevención, protección o reacción a prestar, de forma complementaria a aquellas previstas por los operadores críticos.

Respecto de los roles personales, la Ley PIC regula la figura del **Responsable de Seguridad y Enlace**, nombrado por los operadores críticos, cuyo nombramiento deberá ser comunicado al Ministerio del Interior, y que deberá contar con la habilitación de *Director de Seguridad* expedida por el Ministerio del Interior según lo previsto en la normativa de seguridad privada o con la habilitación equivalente, según su normativa específica.

Por su parte, los operadores con Infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior deberán comunicar a las Delegaciones del Gobierno o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la existencia de un **Delegado de Seguridad** para dicha infraestructura.

Los sectores estratégicos, así como los Ministerios/Organismos del sistema regulados en el texto originario de la Ley PIC son los mostrados en el cuadro siguiente:

Sector	Ministerio/Organismo del sistema
Administración	Ministerio Presidencia. Ministerio Interior. Ministerio Defensa. Centro Nacional de Inteligencia. Ministerio Política Territorial y Administración Pública.

Espacio	Ministerio Defensa.
Industria nuclear	
	Ministerio Industria, Turismo y Comercio. Consejo de Seguridad Nuclear.
Industria química	Ministerio Interior.
Instalaciones de investigación.	Ministerio Ciencia e Innovación. Ministerio Medio Ambiente, y Medio Rural y Marino.
Agua	Ministerio Medio Ambiente, y Medio Rural y Marino. Ministerio Sanidad, Política Social e Igualdad.
Energía	Ministerio Industria, Turismo y Comercio.
Salud	Ministerio Sanidad, Política Social e Igualdad. Ministerio Ciencia e Innovación.
Tecnologías de la Información y las Comunicaciones (TIC)	Ministerio Industria, Turismo y Comercio. Ministerio Defensa. Centro Nacional de Inteligencia. Ministerio Ciencia e Innovación. Ministerio Política Territorial y Administración Pública.
Transporte	Ministerio Fomento.
Alimentación	Ministerio Medio Ambiente, y Medio Rural y Marino. Ministerio Sanidad, Política Social e Igualdad. Ministerio Industria, Turismo y Comercio.
Sistema financiero y tributario	Ministerio Economía y Hacienda.

Esta ley se desarrolla por medio del **Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de infraestructuras críticas.**

Este Real Decreto contiene las cuestiones generales relativas a su objeto y ámbito de aplicación, y dedica un artículo a la figura del **Catálogo Nacional de Infraestructuras Estratégicas**, como instrumento de la Secretaría de Estado de Seguridad del Ministerio del Interior que debe aglutinar todos los datos y la valoración de la criticidad de las citadas infraestructuras y que será empleado como base para planificar las actuaciones necesarias en materia de seguridad y protección de las mismas, al nutrirse de las aportaciones de los propios operadores.

Además de ello, su Título II está plenamente dedicado al **Sistema de Protección de Infraestructuras Críticas,** y desarrolla, entre otras, las previsiones legales relativas a los órganos creados por la Ley, esto es, el **Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC),** al que atribuye las siguientes **funciones:**

Funciones del CNPIC

a) Asistir al Secretario de Estado de Seguridad en la ejecución de sus funciones en materia de protección de infraestructuras críticas, actuando como órgano de contacto y coordinación con los agentes del Sistema.

b) Ejecutar y mantener actualizado el Plan Nacional de Protección de las Infraestructuras Críticas conforme a lo previsto en el artículo 16 de este reglamento.

c) Determinar la criticidad de las infraestructuras estratégicas incluidas en el Catálogo.

d) Mantener operativo y actualizado el Catálogo, estableciendo los procedimientos de alta, baja y modificación de las infraestructuras, tanto nacionales como europeas, que en él se incluyan en virtud de los criterios horizontales y de los efectos de interdependencias sectoriales a partir de la información que le suministren los operadores y el resto de agentes del Sistema, así como establecer su clasificación interna.

e) Llevar a cabo las siguientes funciones respecto a los instrumentos de planificación previstos en este reglamento:

- Dirigir y coordinar los análisis de riesgos que se realicen por los organismos especializados, públicos o privados, sobre cada uno de los sectores estratégicos en el marco de los Planes Estratégicos Sectoriales, para su estudio y deliberación por el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.
- Establecer los contenidos mínimos de los Planes de Seguridad de los Operadores, de los Planes de Protección Específicos y de los Planes de Apoyo Operativo y supervisar el proceso de elaboración de éstos, recomendando, en su caso, el orden de preferencia de las contramedidas y los procedimientos a adoptar para garantizar su protección ante ataques deliberados.
- Evaluar, tras la emisión de los correspondientes informes técnicos especializados, los Planes de Seguridad del Operador y proponerlos, en su caso, para su aprobación, al Secretario de Estado de Seguridad, u órgano en quien delegue.
- Analizar los Planes de Protección Específicos facilitados por los operadores críticos respecto a las diferentes infraestructuras críticas o infraestructuras críticas europeas de su titularidad y proponerlos, en su caso, para su aprobación, al Secretario de Estado de Seguridad, u órgano en quien delegue.
- Validar los Planes de Apoyo Operativo diseñados para cada una de las infraestructuras críticas existentes en el territorio nacional por el Cuerpo Policial estatal o, en su caso, autonómico competente, previo informe, respectivamente, de las Delegaciones del Gobierno en las Comunidades Autónomas o de las Comunidades Autónomas que tengan competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.

f) Elevar al Secretario de Estado de Seguridad, u órgano en quien delegue, las propuestas para la declaración de una zona como crítica que se efectúen.

g) Implantar, bajo el principio general de confidencialidad, mecanismos permanentes de información, alerta y comunicación con todos los agentes del Sistema.

h) Recopilar, analizar, integrar y valorar la información sobre infraestructuras estratégicas procedente de instituciones públicas, servicios policiales, operadores y de los diversos

instrumentos de cooperación internacional para su remisión al Centro Nacional de Coordinación Antiterrorista del Ministerio del Interior o a otros organismos autorizados.

i) Participar en la realización de ejercicios y simulacros en el ámbito de la protección de las infraestructuras críticas.

j) Coordinar los trabajos y la participación de expertos en los diferentes grupos de trabajo y reuniones sobre protección de infraestructuras críticas, en los ámbitos nacional e internacional.

k) Ser, en el ámbito de la Protección de las Infraestructuras Críticas, el Punto Nacional de Contacto con organismos internacionales y con la Comisión Europea, así como elevar a ésta, previa consulta al Centro Nacional de Coordinación Antiterrorista, los informes sobre evaluación de amenazas y tipos de vulnerabilidades y riesgos encontrados en cada uno de los sectores en los que se hayan designado infraestructuras críticas europeas, en los plazos y condiciones marcados por la Directiva.

l) Ejecutar las acciones derivadas del cumplimiento de la Directiva 2008/114/CE en representación de la Secretaría de Estado de Seguridad.

La figura siguiente muestra el organigrama del CNPIC.

Además de ello, la norma regula en detalle la **Comisión Nacional para la Protección de las Infraestructuras Críticas,** presidida por el Secretario de Estado de Seguridad**,** a la que confiere las siguientes **funciones**:

a) Preservar, garantizar y promover la existencia de una cultura de seguridad de las infraestructuras críticas en el ámbito de las Administraciones públicas.

b) Promover la aplicación efectiva de las disposiciones de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas por parte de todos los sujetos responsables del sistema de protección de infraestructuras críticas, a partir de los informes emitidos al respecto por parte del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

c) Llevar a cabo las siguientes actuaciones a propuesta del Grupo de Trabajo:

- Aprobar los Planes Estratégicos Sectoriales.

- Designar a los operadores críticos.
- Aprobar la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico, estableciendo sus objetivos y sus marcos de actuación.

d) Impulsar aquéllas otras tareas que se estimen precisas en el marco de la cooperación interministerial para la protección de las infraestructuras críticas.

Siendo sus **miembros**:

a) En representación del Ministerio del Interior:
   - El Director General de la Policía y de la Guardia Civil.
   - El Director General de Protección Civil y Emergencias.
   - El Director del CNPIC, que ejercerá las funciones de Secretario de la Comisión.

b) En representación del Ministerio de Defensa, el Director General de Política de Defensa.

c) En representación del Centro Nacional de Inteligencia, un Director General designado por el Secretario de Estado-Director de aquél.

d) En representación del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis, su Director.

e) En representación del Consejo de Seguridad Nuclear, el Director Técnico de Protección Radiológica.

f) En representación de cada uno de los ministerios integrados en el Sistema, una persona con rango igual o superior a Director General, designada por el titular del Departamento ministerial correspondiente en razón del sector de actividad material que corresponda.

El Real Decreto regula asimismo el **Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas**, cuyas **funciones** son:

a) Elaborar, con la colaboración de los agentes del Sistema afectados y el asesoramiento técnico pertinente, los diferentes Planes Estratégicos Sectoriales para su presentación a la Comisión, conforme a lo previsto en el Título III, Capítulo II, del reglamento.

b) Proponer a la Comisión la designación de los operadores críticos por cada uno de los sectores estratégicos definidos.

c) Proponer a la Comisión la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico, supervisando, coordinando y efectuando el seguimiento de los mismos y de sus trabajos e informando oportunamente de los resultados obtenidos a la Comisión.

d) Efectuar los estudios y trabajos que, en el marco de este reglamento, le encomiende la Comisión. Para ello podrá contar, si es necesario, con el apoyo de personal técnico especializado.

Además, este reglamento de desarrollo de la Ley PIC trata los instrumentos de planificación, centrándose en los **Planes** antes citados, regulando su proceso de elaboración, aprobación y registro, así como sus contenidos materiales.

Finalmente, la norma concluye con precisiones adicionales en torno a la seguridad de las comunicaciones y a las figuras del **Responsable de Seguridad y Enlace** y del **Delegado de Seguridad** de la infraestructura crítica.