FECHA DE RECEPCIÓN: 20/05/16
FECHA DE APROBACIÓN: 07/06/16

La ciberseguridad pública como garantía del ejercicio de derechos

Public cybersecurity as guarantee of the exercise of rights

Carlos Manuel Galán*
Carlos Galán Cordero**

Resumen:
El desarrollo de los derechos fundamentales recogidos en los textos de las Declaraciones Universales y en las Constituciones normativas de los estados democráticos exige que los sistemas de información que sustentan su ejercicio se encuentren permanentemente operativos. Sin embargo, esta necesidad se ve, incesantemente, puesta en compromiso por multitud de ciberataques que, en el fondo de la cuestión, pretenden socavar el libre ejercicio de tales derechos.
Es en este entorno donde la ciberseguridad pública, entendida como el conjunto de normas, métodos, procedimientos y herramientas, encuentra su razón de ser y se configura como el único medio adecuado para garantizar una convivencia ajustada a los postulados del Estado de Derecho.

Abstract:
The development of fundamental human rights contained in the texts of the Universal Declarations and the Constitutions of democratic states requires that information systems that support its exercise are permanently operational. However, this need is constantly violated by many cyberattacks that, in the heart of the matter, seek to undermine the free exercise of such rights.
It is in this environment where public cybersecurity, understood as the set of legal regulations, methods, procedures and tools, finds its reason for being and is configured as the only appropriate means of ensuring social coexistence in accordance with the principles of the Rule of Law.

Palabras clave:
Ciberseguridad - Ciberataques - Derechos Humanos - Estrategia

Keywords:
Cibersecurity - Ciberattacks - Human Rights - Cibersecurity Strategy

Sumario:

* Doctor en Informática por la Universidad Politécnica de Madrid (España); Licenciado en Derecho por la Universidad Complutense; es Abogado y Presidente de la Agencia de Tecnología Legal. Ha sido asesor del Ministerio del Interior de España, donde presidió la Comisión de Informática y Comunicaciones de la Seguridad de los Juegos Olímpicos de Barcelona '92. Fue Director General de la Agencia de Certificación Electrónica y, en la actualidad, además de ser Profesor de la Universidad Carlos III de Madrid, colabora con el Centro Criptológico Nacional del Centro Nacional de Inteligencia de España, dónde, habiendo formado parte del equipo de redacción de la Estrategia de Ciberseguridad Nacional, desarrolla su trabajo en materias relativas a la Ciberseguridad y el Derecho. Contacto: cgalan@der-pu.uc3m.es

** Licenciado en Derecho por la Universidad Autónoma de Madrid (España) y Abogado del Ilustre Colegio de Abogados de Madrid; Máster en Relaciones Internacionales y Comunicación; Máster en Dirección de la Empresa Audiovisual; Responsable del Área de Derecho de la Información, Comunicación y Seguridad de la Agencia de Tecnología Legal.

1. La dependencia tecnológica de la sociedad

El primer cuarto del Siglo XXI, constituye un lugar común de insistir en la dependencia de las sociedades occidentales de sus sistemas de información, ya sean estos públicos o privados. La actividad cotidiana de los ciudadanos, de los profesionales, de las empresas, de las entidades públicas, del Estado, en suma, depende de que ese conjunto de herramientas tecnológicas a las que hemos denominado sistemas de información (computadores y redes de comunicaciones, esencialmente), propiedad u operados por el sector público, por las organizaciones privadas o por los propios ciudadanos, se permanezcan operativos y en condiciones de prestar los servicios que de ellos se esperan.

Efectivamente, en España, en la actualidad, servicios esenciales tales como la energía, los transportes, las finanzas, la sanidad, el comercio, la Defensa y la seguridad, el procedimiento administrativo e, incluso, el ocio, se desarrollan o se gestionan, de forma mayoritaria, por medios electrónicos, y lo harán todavía más en el futuro[1], de manera análoga al comportamiento seguido por los países que conforman nuestro entorno. La importancia de garantizar la continuidad operativa de los sistemas que soportan estos servicios esenciales ha quedado, claramente, reflejada en la regulación sobre Protección de Infraestructuras Críticas, contempla doce sectores estratégicos de especial atención: Administración Pública, Espacio, Industria nuclear, Industria Química, Instalaciones de Investigación, Agua, Energía, Salud, Tecnologías de la Información y las Comunicaciones, Transporte, Alimentación y Sistema financiero y tributario[2].

Por tanto, y tratándose de un camino sin retorno, la llamada "digitalización de la sociedad" exige garantizar que las herramientas tecnológicas utilizadas tienen la capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas prestan o hacen accesibles (lo que se ha denominado *resiliencia*)[3].

La necesidad de asegurar el normal funcionamiento de los sistemas de información se desprende del hecho de que -como así vienen señalando los anuales *Informes de Ciberamenazas y Tendencias*[4] publicados por el **Centro Criptológico Nacional (CCN)** de España -organismo gubernamental nacional adscrito al **Centro Nacional de Inteligencia (CNI)** y, competencialmente, responsable de velar por la ciberseguridad de los sistemas de información de las entidades públicas y aquellos otros que tratan información clasificada-, la realidad evidencia día a día el volumen y la virulencia de los ciberataques contra la seguridad de tales sistemas, muy especialmente aquellos de los que son víctimas los gobiernos, las administraciones públicas y las empresas poseedoras de patrimonio tecnológico de todo el mundo, advirtiéndose un incremento inusitado de las acciones de **ciberespionaje** llevadas a cabo por los propios estados, con la pretensión de obtener información valiosa o sensible desde los puntos de vista político, estratégico o económico.

Por otro lado, la universalización del uso de los medios electrónicos en la actividad habitual de las sociedades avanzadas representa un enorme estímulo para ciertos sujetos y organizaciones delincuenciales, que ven con satisfacción cómo la "superficie de ataque" se ensancha, al tiempo que lo hacen los beneficios derivados de su comportamiento delictivo. La comisión de tales acciones en el ciberespacio, cuando revisten las características del

1 Buena prueba de ello lo constituyen las recientes Ley 39/2015, de Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/2015, de Régimen Jurídico del Sector Público, ambas de 1 de octubre, que confieren al uso de los procedimientos electrónicos en las relaciones de las entidades públicas con los ciudadanos y de estas entre sí, respectivamente, el medio prioritario y habitual.

2 Anexo de la Ley 8/2011, de 28 de abril, por la que se establecen las medidas de protección de las infraestructuras críticas, en desarrollo de 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.

3 Como así recoge el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la administración electrónica.

4 *Informe de Amenazas 2015 y Tendencias 2016*, accesible a través de www.ccn-cert.cni.es

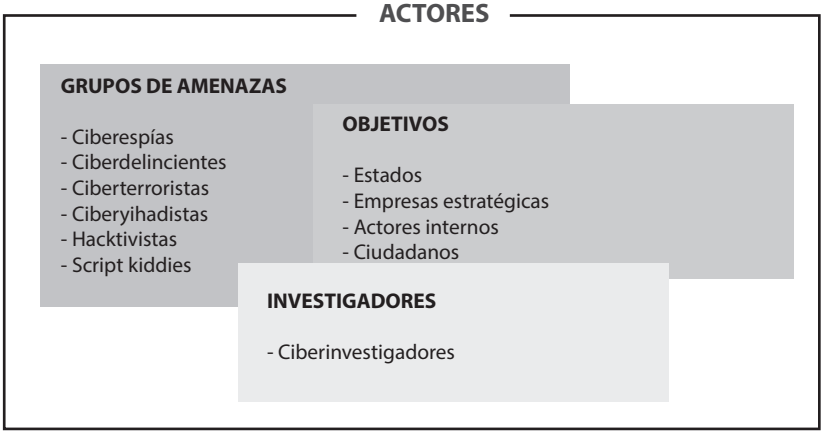
delito, es lo que se ha denominado **ciberdelincuencia**, habiéndose desarrollado en los últimos años un nuevo modelo de negocio: el *Ciberdelito como Servicio*[5].

Aunque ciberespionaje y ciberdelincuencia han venido siendo las más significativas amenazas de los últimos años y, en su consecuencia, constituyendo la mayor preocupación de los gobiernos, los servicios de inteligencia y los cuerpos policiales de todo el mundo, no podemos olvidar que el activismo antisocial desarrollado en Internet -lo que se ha denominado **hacktivismo-,** junto con la potencial amenaza que constituye el **ciberterrorismo**, siguen constituyendo una fuente de enorme de inquietud para las organizaciones públicas y privadas de los países más desarrollados[6].

Además de lo anterior, recientemente, ha surgido una nueva amenaza: el **ciberyihadismo**, que, usando métodos, procedimientos y herramientas del terrorismo, el hacktivismo y la ciberguerra, constituye ya una realidad y supone una de las mayores amenazas con las que se enfrentarán las sociedades occidentales en los próximos años. Las importantes vías de financiación de estos grupos -al socaire de ISIS o Daesh- hacen que ya no constituya un problema insalvable para los atacantes la adquisición de los conocimientos y las herramientas precisas para el desarrollo de ciberataques o la contratación de los elementos humanos requeridos para su acometimiento.

Finalmente, la persistencia de distintos conflictos armados en todo el mundo, en los que se han visto involucrados no sólo los ejércitos convencionales sino también unidades paramilitares y tropas adoctrinadas a través de fanatismos y radicalismos de raíz religiosa, han propiciado que las acciones que hemos denominado como **ciberguerra** se hagan especialmente presentes. Estos últimos años han dejado claro que las redes y los sistemas informáticos constituyen un nuevo espacio para la confrontación militar.

Figura 1. Actores (agentes y víctimas) de las ciberamenazas



El cuadro siguiente muestra una aproximación general a los actores mencionados, sus capacidades y motivaciones[7].

5 *Crime-as-a-Service*. Es decir, la puesta a disposición por parte de terceros, de herramientas tecnológicas o infraestructuras para la comisión de acciones delictivas.

6 Como, por ejemplo, lo demuestran las iniciativas legislativas de la Unión Europea: Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección; o la norteamericanas de protección de sus Infraestructuras Críticas: la *National Cybersecurity and Critical Infrastructure Protection Act* ("NCCIP") de 2013 (H.R. 3696); la *Cyber Intelligence Sharing and Protection Act* ("CISPA") de 2013 (H.R. 624); la *Cybersecurity Information Sharing Act* ("CISA") (S. 2588), y la *Cyber Information Sharing Tax Credit Act* (S. 2717).

7 Fuente: Ciberamenazas 2015 y Tendencias 2016 (CCN-CERT IA-09/16), Centro Criptológico Nacional de España (Centro Nacional de Inteligencia).

Cuadro 1. Agentes de las amenazas: capacidades y motivaciones

ACTOR	MOTIVACIÓN	NIVEL DE CONOCIMIENTOS	OBJETIVO
Estados	Contra-terrorismo o protección de la seguridad nacional. Terrorismo, como segunda opción. Mejora de su posición geopolítica o estratégica.	Alto	• Instituciones gubernamentales o de las Administraciones Públicas. • Industrias de la Defensa o empresas con alto patrimonio tecnológico. • Organizaciones que constituyen un escalón para alcanzar otros objetivos.
Ciberdelincuentes profesionales	Beneficio económico (directo o indirecto)	Alto - Medio	• Ofrecer productos y servicios con muchos detalles sobre datos de identidad o financieros. • Básicamente, cualquiera puede ser un objetivo, si puede obtenerse beneficio económico.
Terroristas	Lograr alteraciones en la sociedad, mediante el uso del terror. Influir en la toma de decisiones políticas.	Medio - Bajo	• Objetivos de alto impacto o repercusión pública, con significativas bases ideológicas o simbólicas.
Ciberyihadistas	Lograr la penetración de su ideología	Bajo - Medio	• Objetivos que representen el ideario ideológico a combatir.
Cibervándalos y script kiddies	Picardía. Búsqueda de desafíos.	Bajo	• Muy variado.
Hacktivistas	Acercarse a sus objetivos ideológicos.	Medio	• Medios de comunicación. • Objetivos relacionados con sus aspiraciones. • A veces, totalmente al azar, a la vista de vulnerabilidades detectadas.
Actores internos	Venganza, o beneficios económicos o ideológicos (en ocasiones, dirigidos desde el exterior).	Alto - Bajo	• Entorno de trabajo, actual o anterior.
Ciber-investigadores	Revelación de debilidades (y su propio perfil)	Medio	• Variados.
Organizaciones privadas	Obtener o vender información valiosa.	Alto - Bajo	• Competidores, clientes, público en general.

Estas realidades, cada una en su contexto, suponen, como veremos, un grave atentado contra los derechos fundamentales personales, que es necesario considerar y hacer frente.

2. Los derechos fundamentales en peligro y la respuesta

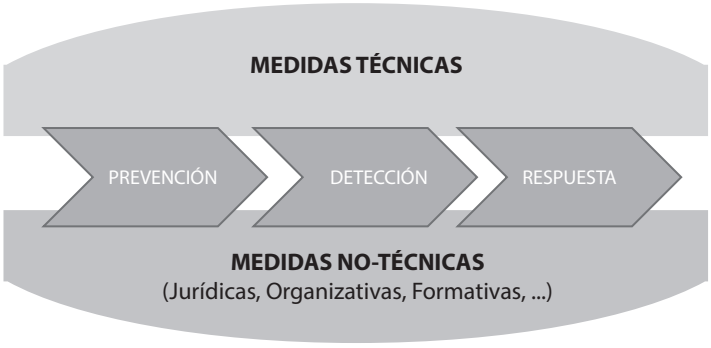
La Constitución española -al igual que otros textos, nacionales o internacionales, de expresión de derechos y libertades- proclama un conjunto de derechos fundamentales, que pueden verse, claramente, perturbados por una multiplicidad de acciones hostiles desarrolladas en el ciberespacio.

Así, la dignidad de la persona, la libertad ideológica o de expresión, la intimidad, el honor, los servicios sociales o, incluso, la propiedad privada, entre otros derechos, pueden verse, claramente, comprometidos cuando los sistemas de información que sustentan su ejercicio práctico dejan de funcionar o lo hacen de manera irregular, como consecuencia de las acciones deliberadas que los agentes de las amenazas desarrollan, pretendiendo satisfacer los intereses descritos.

España -al igual que muchos otros países- no ha sido un oasis en este mapa de ciberataques. Por el contrario, nuestro país ha sido uno de los más castigados por las acciones de los agentes de las ciberamenazas, especialmente, en materia de ciberespionaje y ciberdelincuencia organizada.

Ante esta situación se hace imprescindible disponer de medidas capaces de hacer frente a esta realidad que, cuanto menos, amenaza con desestabilizar nuestra forma de vida. En ciberseguridad, pueden adoptarse dos grandes tipos de medidas: **técnicas** y **no-técnicas** (jurídicas, organizativas, formativas, etc.), y todas ellas en las diferentes fases en las que pueden aplicarse: **prevención** (antes de que se produzca el ciberincidente)**, detección** (al objeto de detectar la presencia de un ciberataque)[8] y **respuesta** (erradicación y recuperación, esencialmente), tal y como se muestra en la figura siguiente[9].

Figura 2. Medidas de ciberseguridad



Sea como fuere, las medidas adoptadas en cada caso deben ser, constantemente, evaluadas, adaptándose a las nuevas circunstancias: nuevos tipos de ataque, nuevos vectores, nuevas vulnerabilidades, nuevas tecnologías, nuevos dispositivos, etc.

Ante este panorama, los esfuerzos públicos dirigidos a erradicar o, cuanto menos, a mitigar los riesgos, han tenido que incrementarse. La **Estrategia de Ciberseguridad Nacional de España (ECSN)**, hecha pública a finales de 2013, y desarrollada a través del **Plan Nacional de Ciberseguridad,** constituye el hilo conductor de aquellos esfuerzos, presentes y futuros. La ECSN, en su calidad de documento estratégico nacional y, en su consecuencia, de aplicación a todo el Estado, exige contemplar varios requisitos.

En primer lugar, no es un documento aislado, antes bien, debe estar engarzado adecuadamente en el marco propuesto por la **Estrategia de Seguridad Nacional de 2013**[10], atendiendo a:

- Las amenazas y los riesgos de operar en el ciberespacio.
- Los intereses nacionales.
- Los Tratados y Convenios internacionales de los que España era parte.

Y todo ello, en el contexto estratégico mundial de la ciberseguridad, recogido -con dispar acierto-, en la veintena de estrategias nacionales que diferentes países habían publicado con anterioridad.

Los **Principios Rectores** que marcaron la redacción de la ECSN fueron -y siguen siendo- los siguientes:

- **Liderazgo nacional y coordinación**: el ámbito y la complejidad de los desafíos del ciberespacio requiere, además de un liderazgo nacional decidido, la adecuada coordinación de las capacidades y competencias involucradas.

8 Estas medidas son especialmente importantes. La mayor parte de los más sofisticados ciberataques actuales, especialmente los denominados APT (*Advenced Persistent Threats*), pueden producirse y mantenerse durante largos periodos de tiempo sin ser detectados.

9 Fuente: Dr. C. Galán, "Esquema Nacional de Seguridad: razones para una actualización", en *III Congreso Internacional de Innovación Tecnológica y Administración Pública*. (Toledo: Universidad de Castilla-La Mancha, Nov., 2015).

10 Presidencia del Gobierno de España. *Estrategia de Seguridad Nacional. Un proyecto compartido*. (2013). http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

- **Responsabilidad compartida**: todos los agentes públicos y privados con responsabilidad en materia de ciberseguridad, incluyendo también a los propios ciudadanos, han de sentirse implicados. Para ello, se precisa de una intensa coordinación entre los diferentes organismos de las AA.PP. y una adecuada cooperación público-privada capaz de compatibilizar iniciativas y propiciar el intercambio de información.
- **Cooperación Internacional**: el carácter transfronterizo de las amenazas hace que sea esencial promover la cooperación global, puesto que muchas de las posibles medidas sólo resultarán eficaces si se adoptan internacionalmente.
- **Proporcionalidad, racionalización y eficacia**: es necesario gestionar los riesgos derivados del uso de la tecnología de forma dinámica, equilibrando oportunidades y amenazas, asegurando la proporcionalidad en las medidas de protección adoptadas, que habrán de ser elementos habilitantes de la confianza y no trabas al desarrollo de nuevos servicios.

Y todos ellos, **respetando y fortaleciendo la protección de los valores y derechos emanados de la Constitución y las leyes.**

3. Los objetivos perseguidos por la ECSN

Los objetivos últimos de la ECSN son los mostrados en el cuadro siguiente.

Cuadro 2. Objetivos de la Estrategia de Ciberseguridad Nacional de España

Objetivo Global:	**Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, y respuesta a los ciberataques.**
Política de Ciberseguridad	Para alcanzar la seguridad del ciberespacio, se promoverá una Política de Ciberseguridad Nacional mediante el desarrollo del adecuado marco normativo y el impulso de una Estructura que aglutine y coordine a todas las instituciones y agentes con responsabilidad en la materia. Esta Estructura se articulará bajo el principio de eficiencia y sostenibilidad en el uso de los recursos, garantizando unas óptimas capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta de los Sistemas de Información y Telecomunicaciones ante posibles ciberataques. El fortalecimiento de la ciberseguridad proporcionará a las Administraciones Públicas, al tejido industrial y empresarial, a la comunidad científica y a los ciudadanos en general, una mayor confianza en el uso de las TIC. Para ello, los organismos públicos responsables trabajarán en coordinación con el sector privado y con los propios ciudadanos, para garantizar la seguridad y la confiabilidad de los sistemas que sustentan la llamada Sociedad de la Información. Asimismo, en defensa del interés nacional, la Política de Ciberseguridad Nacional estará alineada con iniciativas similares a las de los países de nuestro entorno, así como con las organizaciones europeas e internacionales competentes, en particular, con la Estrategia de Ciberseguridad de la Unión Europea. Finalmente, de cara a garantizar la protección de los sistemas y la resiliencia de los servicios de las Administraciones Públicas y las Infraestructuras Críticas, así como la disponibilidad de productos confiables, será necesario potenciar, impulsar y reforzar las capacidades nacionales de investigación y desarrollo en ciberseguridad de las TIC. En este sentido, España, manteniendo su política de diversificación y neutralidad tecnológica, velará por la utilización de componentes que estén certificados conforme a normas internacionalmente reconocidas. Las consideraciones hechas en este objetivo global se aplicarán al resto de los objetivos.
Objetivo I:	**Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia.**
Administraciones Públicas	Buena parte de los sistemas TIC de las Administraciones Públicas españolas, la información contenida en ellos y los servicios que prestan, constituyen activos nacionales estratégicos. Resulta imprescindible potenciar la implantación de un marco nacional, coherente e integrado, de políticas, procedimientos y normas técnicas que ayuden a garantizar la protección de la información pública, sus sistemas y servicios, así como de las redes que los soportan. Este marco será clave para desarrollar e implantar servicios, cada vez más seguros. La adaptación de los sistemas de las Administraciones Públicas a esta realidad pasa por implantar servicios de seguridad en las mismas, mejorando y ejercitando su capacidad de prevención, detección y respuesta ante incidentes, desarrollando nuevas herramientas y manteniendo actualizado el ordenamiento jurídico.

	Asimismo, además de mejorar las capacidades de los sistemas militares de Defensa y de inteligencia es necesario reforzar la seguridad de los Sistemas de Información y Comunicación estratégicos, adaptándolos a los nuevos riesgos y amenazas del ciberespacio. Las Administraciones Públicas se involucrarán, activamente, en un proceso de mejora continua respecto de la protección de sus sistemas TIC. Los poderes públicos están obligados a ser ejemplares en la gestión de la ciberseguridad.
Objetivo II: **Sector privado e Infraestructuras Críticas**	**Impulsar la seguridad y resiliencia de los Sistemas de Información y Telecomunicaciones usados por el sector empresarial en general y los operadores de Infraestructuras Críticas en particular.**
	En aplicación del principio de responsabilidad compartida, las Administraciones Públicas deben mantener estrechas relaciones con las empresas que gestionan los Sistemas de Información y Telecomunicaciones relevantes para los intereses nacionales, intercambiando el conocimiento que permita una adecuada coordinación entre ambos y la mutua comprensión del entorno de la ciberseguridad. En este sentido, merece especial mención las acciones para asegurar la Protección del Patrimonio Tecnológico de España, entendido como aquellos activos materiales o inmateriales que sustentan la propiedad intelectual e industrial del sector empresarial, que conforman nuestro presente y condicionan el desarrollo futuro. Es de interés también determinar el impacto que para España puede tener una potencial interrupción o destrucción de las redes y sistemas que proporcionan servicios esenciales a la sociedad. Puesto que el sector privado posee la titularidad de buena parte de estos sistemas, las medidas que se adopten en materia de ciberseguridad deberán estar alineadas con los requisitos expresados en la normativa reguladora de Protección de Infraestructuras Críticas, para alcanzar un conjunto integrado de medidas de aplicación a los sectores afectados.
Objetivo III: **Ámbito judicial y policial**	**Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio.**
	Las TIC constituyen un medio, un fin o una combinación de ambos, utilizado tanto por las organizaciones terroristas como por las delictivas para lograr sus objetivos. A esto debe unirse, la posibilidad, cada vez mayor, de utilizar el ciberespacio como un objetivo en sí mismo para la perpetración de ataques contra servicios esenciales o Infraestructuras Críticas. En ambos casos deben potenciarse los mecanismos de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación en torno a estas formas de criminalidad. La actuación policial y judicial del Estado en materia de ciberseguridad deberá adecuarse a los patrones de conducta y a las modalidades delictivas de los terroristas y delincuentes en el ciberespacio, cuyos objetivos suelen ser coincidentes con los tradicionales, pero no su metodología. Para afrontar, adecuadamente, estas amenazas, que traspasan en muchos casos las fronteras de los Estados, es imprescindible el fortalecimiento de la cooperación judicial y policial internacional, articulando los instrumentos adecuados de colaboración e intercambio de información y la armonización de las legislaciones nacionales, con el desarrollo y mantenimiento de una regulación sólida y eficaz. Igualmente, se hace necesario fomentar la colaboración ciudadana, facilitando los procedimientos de acceso y transmisión de la información de interés policial. El éxito en la lucha contra el terrorismo y la delincuencia en el ciberespacio exige la articulación de los mecanismos necesarios que mejoren las capacidades de las instituciones policiales y los organismos judiciales competentes.
Objetivo IV: **Sensibilización**	**Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio.**
	El Gobierno de España, reconociendo la importancia de construir y mantener la confianza en los Sistemas de Información y Telecomunicaciones que usan los ciudadanos, profesionales, empresas y organismos del sector público, acometerá las acciones de información y sensibilización necesarias para asegurar que todos conocen los riesgos de operar en el ciberespacio y poseen los conocimientos y el acceso a las herramientas que posibilitan su protección. Al mismo tiempo, las empresas deben ser conscientes de la responsabilidad en la seguridad de sus sistemas, la protección de la información de sus clientes y proveedores y la confiabilidad de los servicios que prestan. Mantener la confianza del consumidor es fundamental para el éxito de la economía digital. Lo mismo cabe decir de las Administraciones Públicas y de sus relaciones con los ciudadanos. Por tanto, una función esencial es promover una sólida cultura de ciberseguridad, que proporcione a todos los actores la conciencia y la confianza necesarias para maximizar los beneficios de la Sociedad de la Información y reducir al mínimo su exposición a los riesgos del ciberespacio, mediante la adopción de medidas razonables que garanticen la protección de sus datos, así como la conexión segura de sus sistemas y equipos. La gestión eficaz de los riesgos derivados del ciberespacio debe edificarse sobre una sólida cultura de ciberseguridad. Ello requiere de los usuarios una sensibilización respecto de los riesgos que entraña operar en este medio, así como el conocimiento de las herramientas para la protección de su información, sistemas y servicios.

Objetivo V: **Capacitación**	**Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad.**
	Dada la importancia estratégica de la seguridad en el ciberespacio, es, absolutamente, prioritario disponer del personal cualificado a todos los niveles: órganos de gobierno, directivo, operativo, técnico y judicial. Es importante, además, fomentar y potenciar las capacidades tecnológicas precisas para disponer de soluciones nacionales confiables que permitan proteger, adecuadamente, los sistemas frente a las diferentes amenazas. Para alcanzar esta confianza, se requiere fomentar y mantener una actividad de I+D+i en materia de ciberseguridad de manera efectiva. Para ello será necesaria una adecuada coordinación del conjunto de agentes implicados en las TIC, facilitando la colaboración entre empresas y organismos públicos de investigación e impulsando proyectos de evaluación y certificación de la seguridad. La cualificación del personal encargado de la dirección, gestión e implantación de la ciberseguridad se erige en un objetivo fundamental, especialmente en las Administraciones Públicas y las Infraestructuras Estratégicas y Críticas de interés nacional. Además, la utilización de productos con la seguridad verificada constituye un elemento adicional relevante de protección.
Objetivo VI: **Ámbito Internacional**	**Contribuir a la mejora de la ciberseguridad en el ámbito internacional.**
	Se promoverá y apoyará el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales de Seguridad y Defensa en las que participa España, y se colaborará en la capacitación de Estados que lo necesiten, mediante la política de cooperación al desarrollo, ayudándoles a implantar una cultura de la ciberseguridad. Se fomentará la cooperación en el marco de la UE y con organizaciones internacionales y regionales como, la Agencia Europea de Defensa (EDA), la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), el Centro Europeo de Ciberdelincuencia, adscrito a Europol, la Organización de Naciones Unidas (ONU), la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Organización del Tratado del Atlántico Norte (OTAN) y la Organización para la Cooperación y Desarrollo Económicos (OCDE), entre otras. Junto a los países de nuestro entorno estratégico, se promoverán los esfuerzos dirigidos a conseguir un ciberespacio seguro y fiable, mediante el refuerzo de la colaboración internacional, creando relaciones de confianza para el intercambio de información y datos esenciales en materia de ciberseguridad, y el desarrollo de iniciativas propias de cooperación y desarrollo. Asimismo se llevarán a cabo actuaciones orientadas a impulsar la adopción de estándares internacionales de ciberseguridad y su elevación progresiva.

La determinación de los objetivos abarca, como puede observarse, la totalidad de los intereses nacionales, ya sean de naturaleza pública o privada. Esto es así porque el carácter transversal de las ciberamenazas no admite distinciones de este tipo en una estrategia integradora de carácter estatal. Además, no conviene olvidar que, al margen de los objetivos perseguidos por los agentes de las amenazas, un ataque que tiene su origen en un determinado sistema puede, con relativa facilidad y por mor de la interconexión las redes, propagarse a otros muchos, independientemente de si se trata de sistemas pertenecientes a sectores homogéneos o no.

Cabe destacar la importancia conferida por la ECSN a la seguridad de los sistemas de información de las Administraciones Públicas, al que dedica el primero de sus objetivos específicos. Con independencia del carácter de Sector Estratégico que pueden llegar a poseer determinados sistemas del sector público -como así se recoge en la Ley 8/2011, de 28 de abril, que establece las medidas de protección de las Infraestructuras Críticas[11]-, los sistemas de información de las entidades públicas constituyen elementos de vital importancia para el mantenimiento del orden político, económico y social de España. Más adelante entraremos en los aspectos regulatorios de detalle que han venido marcando el devenir de la ciberseguridad aplicada a tales sistemas públicos.

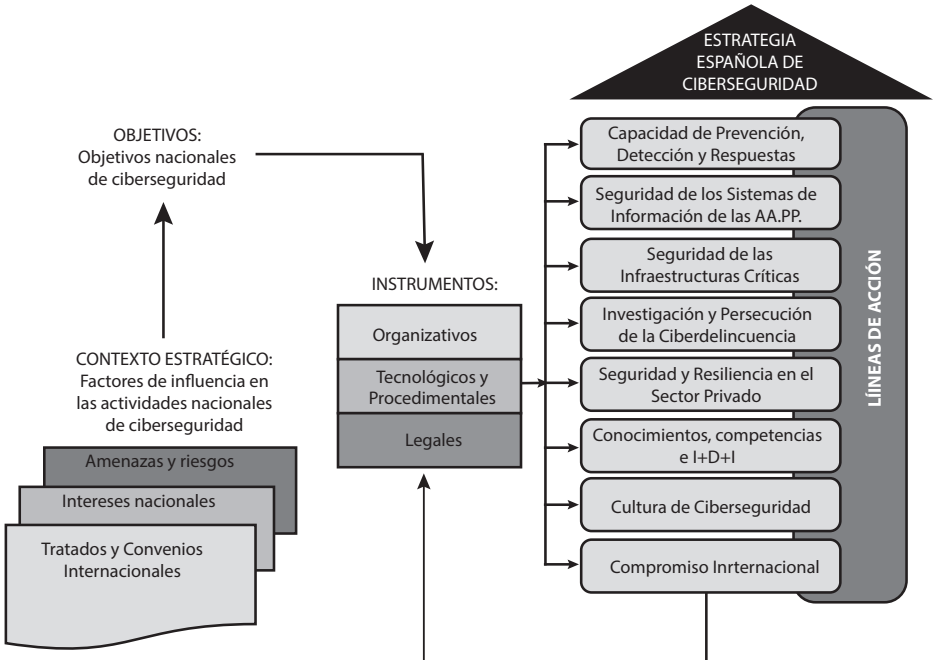
4. Las líneas de acción

Para alcanzar los objetivos fijados, la ECSN define una serie de **Líneas de Acción**, que recogen las actividades concretas que deben acometerse en el horizonte temporal de aplicación de la Estrategia (no menor de cinco años).

11 Como es sabido, esta norma define doce sectores estratégicos: Administración, Espacio, Industria nuclear, Industria química, Instalaciones de investigación, Agua, Energía, Salud, Tecnologías de la Información y las Comunicaciones (TIC), Transporte, Alimentación y Sistema financiero y tributario.

El **Modelo de Desarrollo de la ECSN** es el mostrado en la figura siguiente.

Figura 3. Modelo de desarrollo de la ECSN[12]



La figura anterior muestra cómo, persiguiendo unos Objetivos Nacionales, y atendiendo al precitado Contexto Estratégico en el que se desenvuelve nuestra sociedad y a los instrumentos que pueden usarse (herramientas de naturaleza tecnológica, organizativa o regulatoria), se alcanza a determinar unas concretas Líneas de Acción que, como decimos, fijarán unas tareas asimismo concretas para alcanzar aquellos objetivos.

Las Líneas de Acción que contempla la ECSN son las reseñadas en el cuadro siguiente.

Cuadro 3. Líneas de Acción de la ECSN

LÍNEA DE ACCIÓN 1 ***Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas***	Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional.
LÍNEA DE ACCIÓN 2 ***Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas***	Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.
LÍNEA DE ACCIÓN 3 ***Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas***	Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.
LÍNEA DE ACCIÓN 4 ***Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia***	Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.
LÍNEA DE ACCIÓN 5 ***Seguridad y resiliencia de las TIC en el sector privado***	Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.

12 Fuente: Documentos de trabajo (no clasificados) de la ECSN.

LÍNEA DE ACCIÓN 6 ***Conocimientos, Competencias e I+D+i***	Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad.
LÍNEA DE ACCIÓN 7 ***Cultura de ciberseguridad***	Concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.
LÍNEA DE ACCIÓN 8 ***Compromiso Internacional***	Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales.

Obsérvese de nuevo la importancia conferida a los sistemas de información de las Administraciones Públicas, a las que se dedica, íntegramente, la LA2, con especial mención al **Esquema Nacional de Seguridad**, verdadero eje vertebrador de la ciberseguridad pública.

Efectivamente, el Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** en el ámbito de la Administración electrónica[13], en desarrollo de lo previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y atendiendo a lo recogido en el apartado 2 del artículo 156 de la más reciente Ley 40/2015, de 1 de octubre, de Régimen Jurídico del sector Público, regula el Esquema Nacional de Seguridad (ENS), cuyo objeto es establecer la política de seguridad en la utilización de los medios electrónicos del ámbito de la norma, estando constituido esencialmente por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información y la prestación de los servicios públicos.

No obstante lo anterior, el ENS ha venido precisando de un desenvolvimiento armónico que asegure la correcta interpretación de aquellos principios, exigencia que se materializa a través de las **Instrucciones Técnicas de Seguridad** reguladas en el apartado 2 del artículo 29 del Real Decreto 3/2010, de 8 de enero, piezas normativas esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en su texto.

Así, estas Instrucciones Técnicas de Seguridad, enumeradas en la Disposición Adicional cuarta del citado Real Decreto, entran a regular aspectos concretos que la realidad cotidiana ha mostrado especialmente significativos, tales como: Informe del Estado de la Seguridad; Notificación de incidentes de Seguridad; Auditoría de la Seguridad; Conformidad con el Esquema Nacional de Seguridad; Adquisición de Productos de Seguridad; Criptología de empleo en el Esquema Nacional de Seguridad; Interconexión en el Esquema Nacional de Seguridad y Requisitos de Seguridad en entornos externalizados, sin perjuicio de las propuestas que pueda acordar el Comité Sectorial de Administración Electrónica, según lo establecido en el precitado artículo 29.2 de la norma reguladora del ENS[14].

5. El marco jurídico de la ciberseguridad

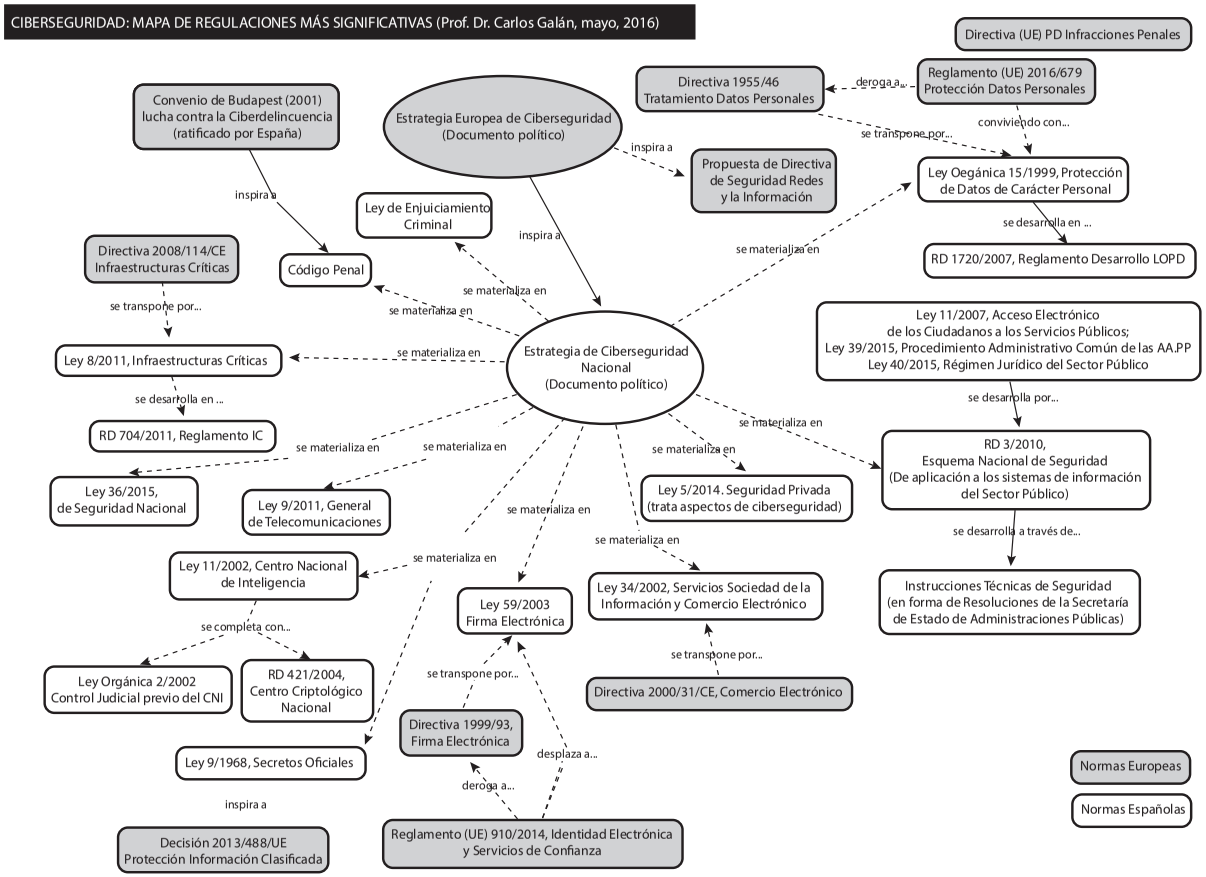
En España, el marco jurídico de la ciberseguridad, entendido como el conjunto de regulaciones que vienen a ordenar de un modo u otro el adecuado uso de los sistemas de información para la prevención o tratamiento de los ciberincidentes (accidentales o deliberados), es muy extenso.

La figura siguiente muestra, gráficamente, lo más significativo de la diversidad regulatoria estatal que, a la fecha de la redacción de este trabajo, sustenta la ciberseguridad en España, tanto como objeto o como sujeto del Derecho.

13 Recientemente, actualizado por Real Decreto 951/2015, de 23 de octubre.

14 Obviamente, estas Instrucciones Técnicas de Seguridad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, las infraestructuras que los apoyan, la evolución tecnológica y los riesgos derivados de operar en el ciberespacio.

Figura 4. Mapa de las regulaciones estatales más significativas en materia de ciberseguridad



A efectos de sistematización, podemos clasificar la normativa más significativa que, en la actualidad, entra a regular la seguridad -en un sentido amplio- cuando se utilizan medios electrónicos, en los **grupos normativos esenciales** que muestra el cuadro siguiente:

Cuadro 3. Grupos normativos esenciales de la ciberseguridad

	Grupo Normativo	Norma
I	Marco estratégico-político	- Estrategia de Ciberseguridad de la Unión Europea (2013)[15]. - Estrategia de Seguridad Nacional (2013)[16]. - Estrategia de Ciberseguridad Nacional (2013)[17].
II	Conformidad con los Derechos Fundamentales personales	- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD)[18], y sus normas de desarrollo (especialmente, el Real Decreto 1720/2007, Reglamento de desarrollo de la LOPD[19]). - Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[20]. - Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos[21].
III	Seguridad Nacional	- Ley 36/2015, de Seguridad Nacional[22]. - Decisión 2013/488/UE, Información Clasificada[23]. - Ley 9/1968, de Secretos Oficiales[24]. - Ley 11/2002, del Centro Nacional de Inteligencia[25]. - Ley Orgánica 2/2002, Control Judicial previo del Centro Nacional de Inteligencia[26]. - Real Decreto 421/2004, Centro Criptológico Nacional[27].
IV	Seguridad de los Servicios Públicos	- Ley 11/2007, de Acceso Electrónico de los Ciudadanos los Servicios Públicos[28]. - Ley 39/2015, de Procedimiento Administrativo Común de las Administraciones Públicas[29]. - Ley 40/2015, de Régimen Jurídico del Sector Público[30]. - Real Decreto 3/2010, Esquema Nacional de Seguridad[31], y normativa derivada (esencialmente, las Instrucciones Técnicas de Seguridad).
V	Seguridad Privada y de servicios de comunicaciones	- Ley 5/2014, Seguridad Privada[32]. - [propuesta] Directiva Europea de Seguridad de las Redes y de la Información[33]. - Ley 9/2014, General de Telecomunicaciones[34].
VI	Seguridad de las Infraestructuras Críticas	- Directiva 2008/114/CE, de Protección de Infraestructuras Críticas[35]. - Ley 8/2011, de Protección de Infraestructuras Críticas[36], y sus normas de desarrollo (esencialmente, el Real Decreto 704/2011, Reglamento de Protección de Infraestructuras Críticas[37]).
VII	Seguridad Sociedad de la Información y Comercio electrónico	- Directiva 2000/31/CE, Comercio Electrónico[38]. - Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico[39].

15 European Commissión, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", en Joint Communicat*ion to he European Parlamente, The Council, The European Economic and Social Committee and the Committee of the regions, (Brussels, 2013).* http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667

16 Presidencia del Gobierno de España. Estrategia *de Seguridad Nacional. Un proyecto compartido. (2013).* http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

17 Presidencia del Gobierno de España. Estrategia *de Seguridad Nacional. Un proyecto compartido. (2013).* http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

18 https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

19 http://www.boe.es/buscar/act.php?id=BOE-A-2008-979

20 http://www.boe.es/diario_boe/txt.php?id=DOUE-L-2016-80807

21 http://www.boe.es/diario_boe/txt.php?id=DOUE-L-2016-80808

22 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10389

23 http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013D0488&from=EN

24 https://www.boe.es/diario_boe/txt.php?id=BOE-A-1968-444

25 https://www.boe.es/buscar/act.php?id=BOE-A-2002-8628

26 http://www.boe.es/buscar/doc.php?id=BOE-A-2002-8627

27 https://www.boe.es/buscar/doc.php?id=BOE-A-2004-5051

28 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-12352

29 https://boe.es/diario_boe/txt.php?id=BOE-A-2015-10565

30 http://boe.es/diario_boe/txt.php?id=BOE-A-2015-10566

31 https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330

32 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-3649

33 La propuesta, a fecha de redacción del presente texto, puede encontrarse en: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666

34 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-4950

35 http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008L0114

36 http://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630

37 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-8849

38 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:Es:HTML

39 https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

	Grupo Normativo	Norma
VIII	Seguridad jurídica penal y procesal	- Convenio de Budapest de lucha contra la ciberdelincuencia (2001)[40]. - Ley Orgánica 10/1995, Código Penal[41]. - Real Decreto 14.09.1882, Ley de Enjuiciamiento Criminal[42].
IX	Seguridad instrumental	- Reglamento (UE) 910/2014, Identidad Electrónica y Servicios de Confianza[43]. - Ley 59/2003, Firma Electrónica[44].

Obviamente, el esquema anterior irá completándose y actualizándose en los próximos años, en paralelo al progreso de los servicios -públicos o privados- prestados con medios electrónicos, a la evolución tecnológica, a los nuevos estándares internacionales sobre seguridad, a medida que vayan consolidándose las infraestructuras que los apoyan y todo ello en virtud de los nuevos y cambiantes escenarios de las ciberamenazas.

6. Conclusiones

De la lectura de los epígrafes anteriores podemos extraer varias conclusiones.

En primer lugar, como hemos visto, la Seguridad -también, la Ciberseguridad- no es un concepto de fronteras perfectamente definidas. Muy al contrario, en su configuración intervienen, se superponen, se integran y, en ocasiones, se erosionan mutuamente, conceptos, métodos, procedimientos, herramientas y regulaciones que construyen una realidad multiforme y multidisciplinar.

En segundo lugar, la Ciberseguridad ya no es una opción. La dependencia de las sociedades occidentales de sus sistemas de información (públicos y privados) es de tal magnitud que no puede abordarse ningún proyecto de interés nacional que no contemple la seguridad de los sistemas de información, la información tratada y los servicios prestados, como requisitos tan importantes como la propia prestación de aquellos servicios.

Y en tercer lugar, la Seguridad -la Ciberseguridad, también- no constituye una categoría absoluta ni, una vez alcanzada, admite alteración. Al contrario: la seguridad es un concepto definido por los intereses sociales, políticos o económicos que la procuran en cada momento, del mismo modo que la mutación de aquellos intereses y el entorno cambiante en el que se asientan obligan a revisar cíclica e incesantemente la naturaleza de los activos a proteger, los riesgos a los que están sometidos y las medidas de seguridad adoptadas para mitigarlos.

Los países más avanzados en materia de ciberseguridad -entre los que ya se encuentra España-, han diseñado estrategias nacionales (de repercusión internacional) tendentes a afrontar los retos que supone operar en el ciberespacio. De nuestra actividad, de nuestro celo, de nuestra profesionalidad, en suma, depende que los servicios públicos españoles, presentes y futuros, posean el nivel de confiabilidad que nos permita crecer como Estado, como ciudadanos y como personas.

El cumplimiento escrupuloso de lo señalado en nuestra Estrategia de Ciberseguridad Nacional, y el puntual acometimiento de las actividades y tareas contempladas en cada una de sus Líneas de Acción constituyen obligaciones permanentes e impostergables, elementos coadyuvantes a la postre de la exigible garantía de los derechos y libertades públicos.

40 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221
41 https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
42 https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036
43 https://www.boe.es/doue/2014/257/L00073-00114.pdf
44 http://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399

7. Bibliografía

Anexo de la Ley 8/2011. 2011. por la que se establecen las medidas de protección de las infraestructuras críticas, en desarrollo de 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.

Carlos Galán, "Esquema Nacional de Seguridad: razones para una actualización", en *III Congreso Internacional de Innovación Tecnológica y Administración Pública*. (Toledo: Universidad de Castilla-La Mancha, Nov., 2015).

Ciberamenazas 2015 y Tendencias 2016 (CCN-CERT IA-09/16), Centro Criptológico Nacional de España (Centro Nacional de Inteligencia).

Directiva 2008/114/CE del Consejo. 2008. Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección; o la norteamericanas de protección de sus Infraestructuras.

European Commissión, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", *en Joint Communication to he European Parlamente, The Council, The European Economic and Social Committee and the Committee of the regions,* (Brussels, 2013). http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667

Informe de Amenazas 2015 y Tendencias 2016, accesible a través de www.ccn-cert.cni.es

Ley 39/2015. 2015. Ley de Procedimiento Administrativo Común de las Administraciones Públicas.

Ley 40/2015. 2015. de Régimen Jurídico del Sector Público.

Presidencia del Gobierno de España. *Estrategia de Seguridad Nacional. Un proyecto compartido*. (2013). http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinal accesiblebpdf.pdf

Real Decreto 3/2010. 2010. Por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la administración electrónica.