sedian

Seguridad Digital
de Andalucía

Marco institucional en ciberseguridad en España y Europa

Junta de Andalucía

Índice

1. Introducción: ámbito global del ciberespacio y sus amenazas

El escenario que representa un mercado globalizado y digital se dibuja como un espacio sin límites en el que confluyen datos y voluntades tan importantes, que pueden llegar incluso a afectar e interferir en nuestra economía. Bajo este contexto, la llamada **“sociedad de la información”** integra la aparición de redes telemáticas de comunicación entre las cuales destaca especialmente, Internet.

1. Introducción: ámbito global del ciberespacio y sus amenazas

La **protección de la privacidad** siempre ha requerido un enfoque multidisciplinar, paradójicamente, según sea utilizada, la tecnología representará una amenaza o un refuerzo del espacio íntimo de cada usuario. El ámbito de la **seguridad de la información** engloba la protección tanto de la información manual como automatizada. Ello junto a las recientes modificaciones normativas en materia de protección de datos, ha colaborado con el aumento de concientización entre usuarios domésticos y profesionales en relación con el tratamiento de datos y los mecanismos adecuados para preservarlos.

1. Introducción: ámbito global del ciberespacio y sus amenazas

El contenido de la **privacidad** como manifestación del derecho a la intimidad es complejo y abarca múltiples aspectos de la vida privada de los sujetos. En España, los distintos aspectos de la privacidad han dado lugar a diversos derechos, aunque todos interrelacionados: a la vida privada, la imagen, la intimidad, la inviolabilidad de las comunicaciones y, recientemente, el derecho de protección de datos.

1. Introducción: ámbito global del ciberespacio y sus amenazas

El **ciberespacio** es un escenario con características propias marcadas por un componente tecnológico, de fácil accesibilidad, un porcentaje alto de anonimidad, conexión y dinamismo. En los últimos tiempos, las acciones negativas en el ámbito de la ciberseguridad han aumentado notablemente en número, alcance y sofisticación.

1.Introducción: ámbito global del ciberespacio y sus amenazas

Después de identificar y valorar los activos que han de protegerse, deben identificarse las posibles amenazas, las cuales tienen una naturaleza heterogénea bajo la aplicación de TIC. Las **amenazas** sobre el ciberespacio se concretan en ciberataques que pueden ser clasificados, en función de su autoría e impacto.

2. Normativa relacionada con la seguridad de la información

La naturaleza de los ciberriesgos existentes requiere la definición de una estrategia en materia de seguridad, alineada con los objetivos de cualquier actividad.

Lo que denominamos la nueva ciberseguridad se extiende más allá del campo meramente de la protección del patrimonio tecnológico para adentrarse en las esferas política, económica y social. En consecuencia será necesario prestar especial atención a las siguientes normativas:

- **RGPD (UE) 2016/679 del Parlamento Europeo y del Consejo**, de 27 de abril de 2016, 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.

2. Normativa relacionada con la seguridad de la información

- **Ley Orgánica 3/2018, de 5 de diciembre,** de Protección de Datos Personales y garantía de los derechos digitales.
- **Ley 34/2002 de 11 de junio,** de servicios de la sociedad de la información de comercio electrónico (LSSI).
- **Ley 36/2015,** de 28 de septiembre, de Seguridad Nacional.
- **Ley Firma-E,** Ley 6/2020 de 11 de noviembre reguladora de determinados aspectos de los servicios electrónicos de confianza.
- **Directiva E-Privacy:** Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

2. Normativa relacionada con la seguridad de la información

- **Directiva 2000/31/CE**, del Parlamento Europeo y del Consejo, de 8 de junio , que regula algunos elementos como el comercio electrónico en el mercado interior.
- **Orden PRA/116/2017**, de 9 de febrero, por la que se publica el Acuerdo del Consejo Seguridad Nacional de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional.
- **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.
- **Orden PRE/2740/2007**, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

2. Normativa relacionada con la seguridad de la información

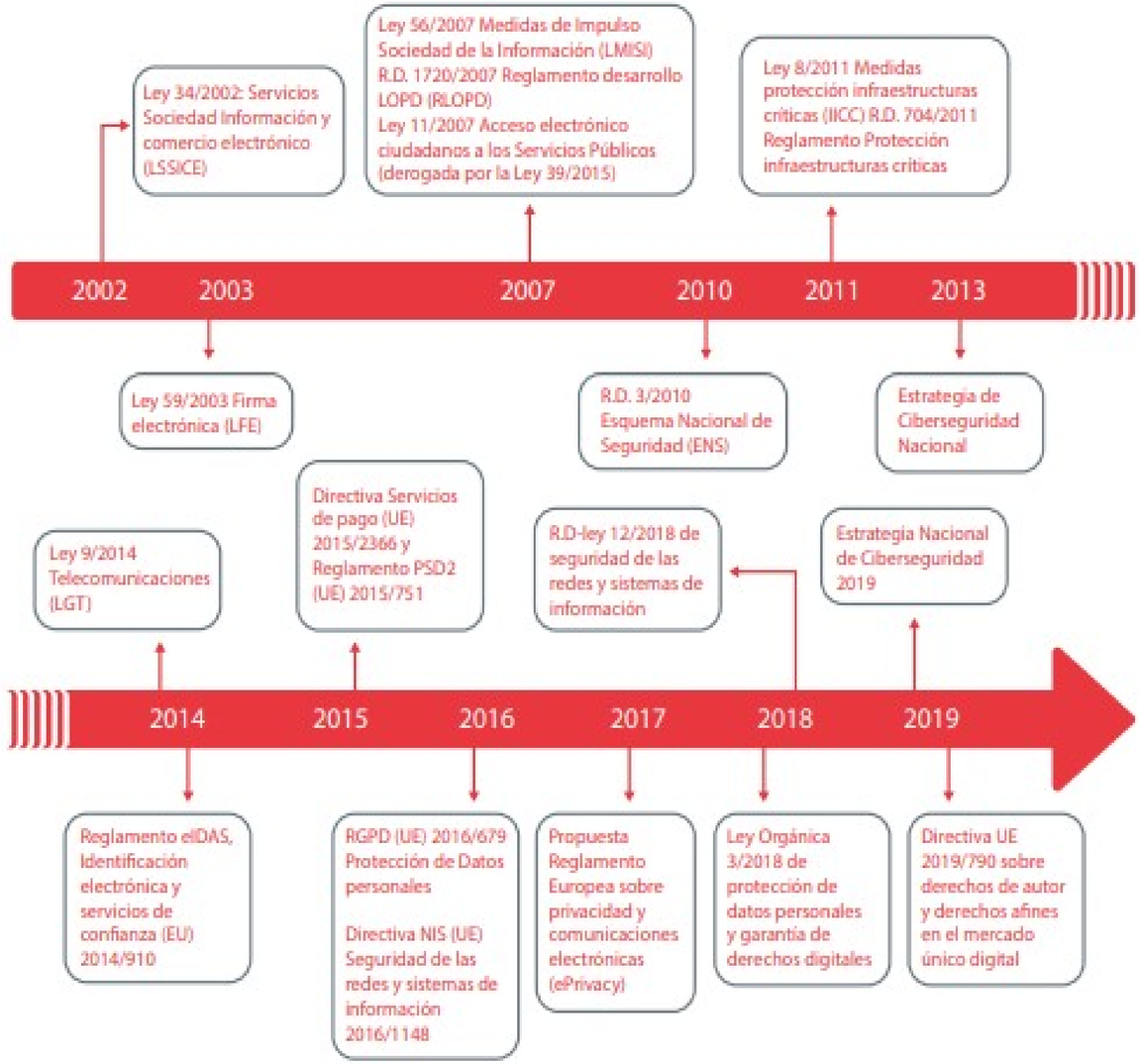


Figura 2.1: Evolución legal en materia de ciberseguridad. Fuente INCIBE

2. Normativa relacionada con la seguridad de la información

- **Ley 36/2015**, de 28 de septiembre, de Seguridad Nacional.
- **Real Decreto-ley 12/2018,** de 7 de septiembre, de seguridad de las redes y sistemas de información.
- **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.
- **Orden PRA/33/2018**, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad.

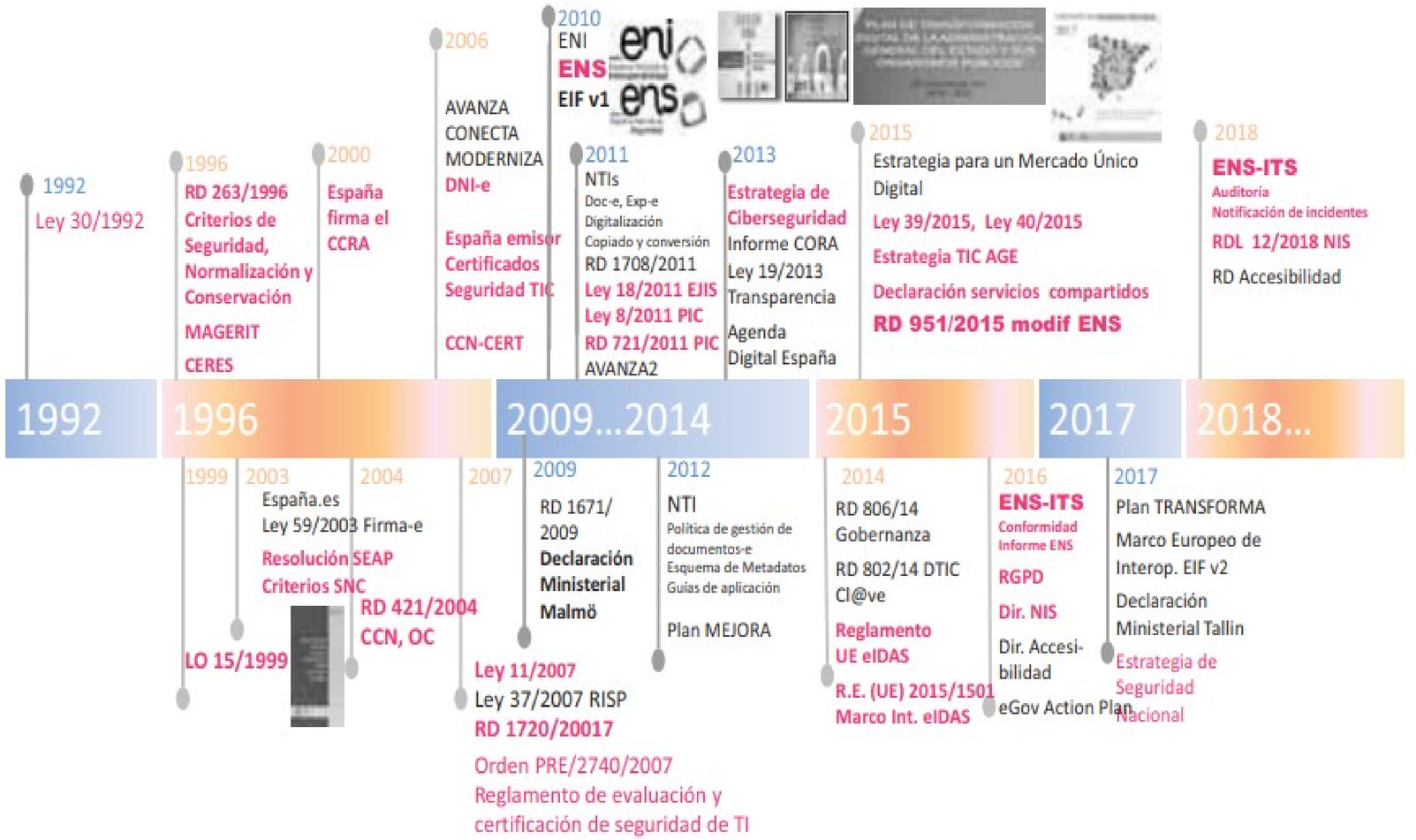
3. Esquema Nacional de Seguridad

Principios básicos y requisitos mínimos

El **Esquema Nacional de Seguridad** tiene como objeto establecer de las condiciones necesarias de confianza en el uso de los medios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios entre los ciudadanos y las Administraciones públicas.

Es de obligado cumplimiento para todas las organizaciones que forman parte de la Administración Pública y lo constituyen una serie de principios básicos y requisitos mínimos con el fin de proteger adecuadamente la información, para ello, se tendrán en cuenta las recomendaciones de la Unión Europea y la situación tecnológica de las diferentes Administraciones públicas.

Análisis evolutivo en materia ciberseguridad en España



Fuente: Amutio Gómez, M.; “El Esquema Nacional de Seguridad, al servicio de la Ciberseguridad”.

3. Esquema Nacional de Seguridad

¿Qué es el ENS?

El Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** establece la **política de seguridad** en la utilización de medios electrónicos y está constituido por **principios básicos y requisitos mínimos** que permitan una protección adecuada de la información.

Tiene por finalidad crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos.

Figura 3.1: Contenido del Esquema Nacional de Seguridad
Fuente: Centro Criptológico Nacional

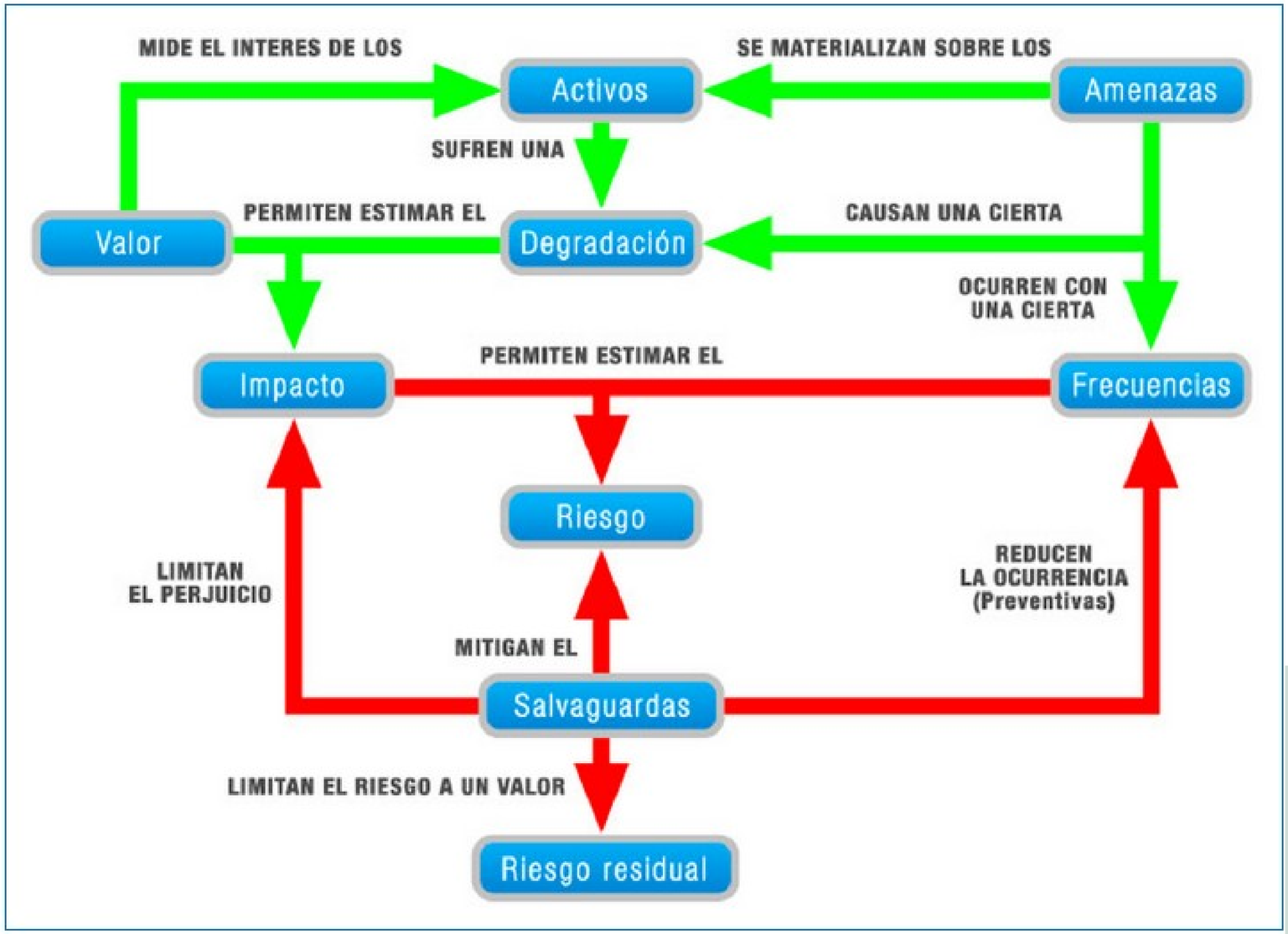
3. Esquema Nacional de Seguridad

¿Cuáles son los principios básicos del ENS?

De acuerdo con el ENS, las decisiones en materia de seguridad deberán tomarse teniendo en cuenta los siguientes **principios básicos**:

- Seguridad integral.
- Gestión de riesgos.
- Prevención, reacción y recuperación.
- Líneas de defensa.
- Reevaluación periódica.
- Función diferenciada.

Diagrama de gestión de riesgos de la ciberseguridad en España



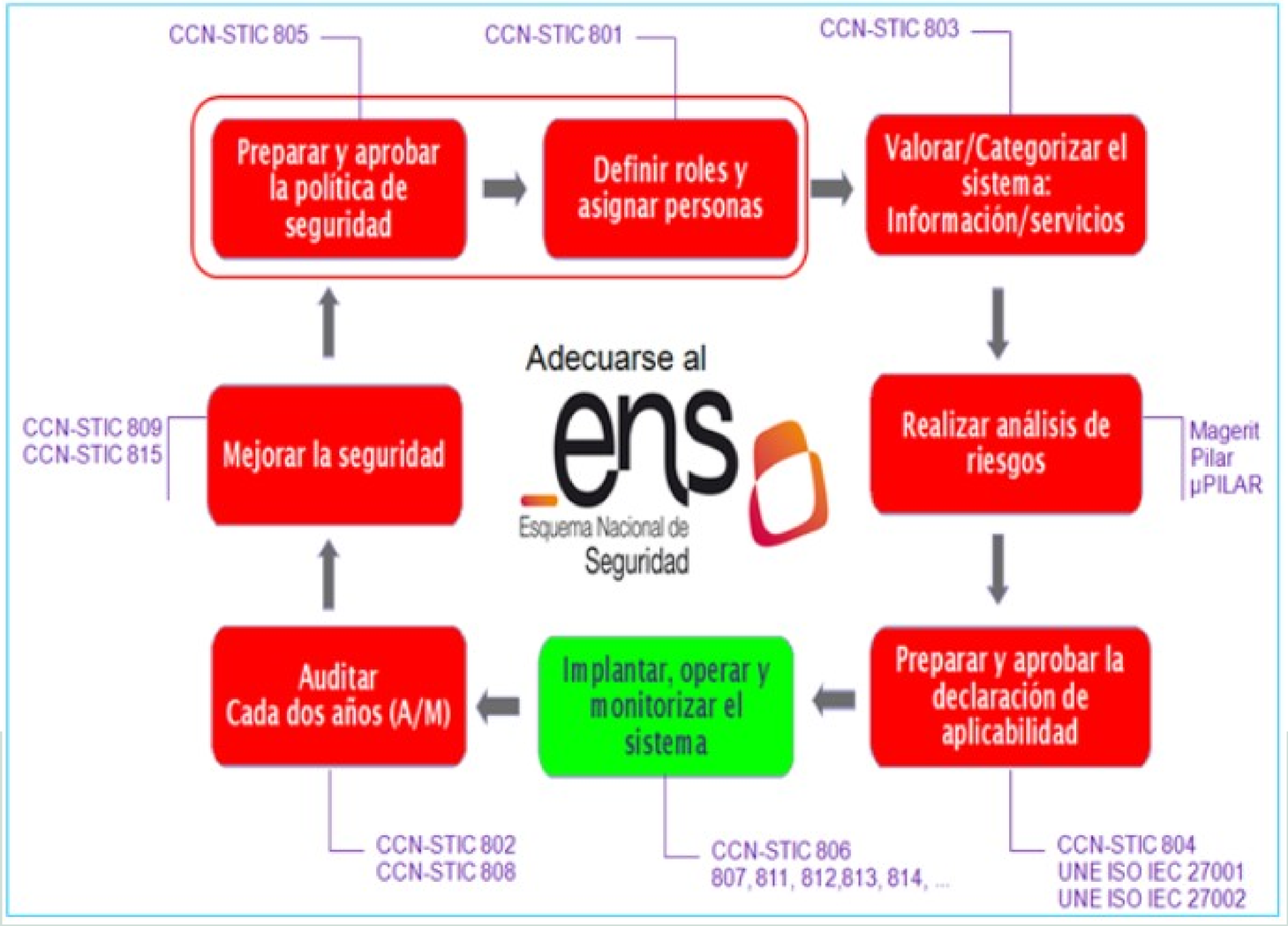
Fuente: Centro Criptológico Nacional

3. Esquema Nacional de Seguridad

¿Cómo se aplican los requisitos mínimos que se expresan en el ENS?

Los **Requisitos Mínimos** son de obligatorio cumplimiento. Lo más habitual es que se plasmen por medio de la aplicación de las medidas de seguridad establecidas en el **Anexo II del ENS**; pero si, por alguna razón, motivada y documentada, las medidas de seguridad son sustituidas por otras medidas compensatorias, los requisitos mínimos, en todo caso, deben cumplirse igualmente.

Adecuación al Esquema Nacional de Seguridad en el ámbito de la Administración electrónica



Fuente: Centro Criptológico Nacional

3. Esquema Nacional de Seguridad

¿El ENS es de cumplimiento obligatorio solo para las Administraciones Públicas?

El **ámbito de aplicación** del Esquema Nacional de Seguridad es el establecido en el artículo 2 de la Ley 11/2007:

- A la Administración General del Estado, Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.
- A los ciudadanos en sus relaciones con las Administraciones Públicas.
- A las relaciones entre las distintas Administraciones Públicas.

3. Esquema Nacional de Seguridad

¿El ENS es de cumplimiento obligatorio solo para las Administraciones Públicas?

Por regla general, podemos afirmar que el **ENS es de aplicación** a:

- Sedes electrónicas.
- Registros electrónicos.
- Sistemas de Información accesibles electrónicamente por los ciudadanos.
- Sistemas de Información para el ejercicio de derechos.
- Sistemas de Información para el cumplimiento de deberes.
- Sistemas de Información para recabar información y estado del procedimiento administrativo.

4. Directiva sobre seguridad de las redes y sistemas de información

La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 conocida y denominada en adelante como **directiva NIS** se encuentra dirigida a establecer medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Aquellas Administraciones Públicas que operen servicios esenciales aplicarán directamente la Directiva NIS. En el mismo extremo será responsabilidad de cada Estado miembro garantizar la seguridad de las redes y del sistema de información de las administraciones públicas que no estén incluidas en el ámbito de aplicación de esta Directiva.

4. Directiva sobre seguridad de las redes y sistemas de información

A fin de alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información, cada Estado miembro deberá disponer de una **Estrategia nacional de seguridad de las redes y sistemas de información** que fijen los objetivos estratégicos y las medidas concretas que haya que aplicar.

Entre las medidas de gestión del riesgo figuran aquellas cuya finalidad es determinar todo riesgo de incidentes, prevenir, detectar y gestionar incidentes y mitigar sus repercusiones. La seguridad de las redes y sistemas de información comprende la seguridad de los datos conservados, transmitidos y procesados.

4. Directiva sobre seguridad de las redes y sistemas de información

Esboza **el marco institucional de la ciberseguridad**, que desarrollará la Estrategia Nacional, compuesto por:

1- Las autoridades públicas competentes con funciones de vigilancia y régimen sancionador.

2- Contenido Estratégico: entre otras cuestiones, las establecidas en el art. 7 de la Directiva NIS.
Ley 36/2015: Enfoque de seguridad nacional

3- Punto de contacto único, art. 13 RDL: Consejo de Seguridad Nacional a través del Departamento de Seguridad Nacional.

5. Estrategia Nacional de Ciberseguridad

La Estrategia Nacional de Ciberseguridad se sustenta e inspira en los mismos principios rectores de la Seguridad Nacional: **unidad de acción, anticipación, eficiencia y resiliencia**. Particularmente, la Estrategia Nacional de Ciberseguridad 2019 establece la posición de España ante una nueva concepción de la ciberseguridad que atiende y responde a las necesidades actuales de todos los usuarios.

Aprobada el 30 de abril de 2019, **este documento desarrolla y afianza las previsiones de la Estrategia de Seguridad Nacional de 2017** en este ámbito.

5. Estrategia Nacional de Ciberseguridad

La Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad, se integra de cinco capítulos en función de los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas:

- **El ciberespacio como espacio común global**, afianza la elaboración de la Estrategia Nacional de Ciberseguridad 2019, así como las principales características que impulsan su desarrollo.
- **Las amenazas y desafíos en el ciberespacio**, clasificadas en dos categorías: amenazas a activos que forman parte del ciberespacio; y por otro, aquellos que usan el ciberespacio como medio para realizar actividades maliciosas e ilícitas.
- **Propósito, principios y objetivos para la ciberseguridad**, aplica los principios rectores de la Estrategia de Seguridad Nacional 2017 (Unidad de acción, Anticipación, Eficiencia y Resiliencia) a cinco objetivos específicos.

- **Propósito, principios y objetivos para la ciberseguridad**, aplica los principios rectores de la Estrategia de Seguridad Nacional 2017 (Unidad de acción, Anticipación, Eficiencia y Resiliencia) a cinco objetivos específicos.

Fuente: Foro Nacional de Ciberseguridad

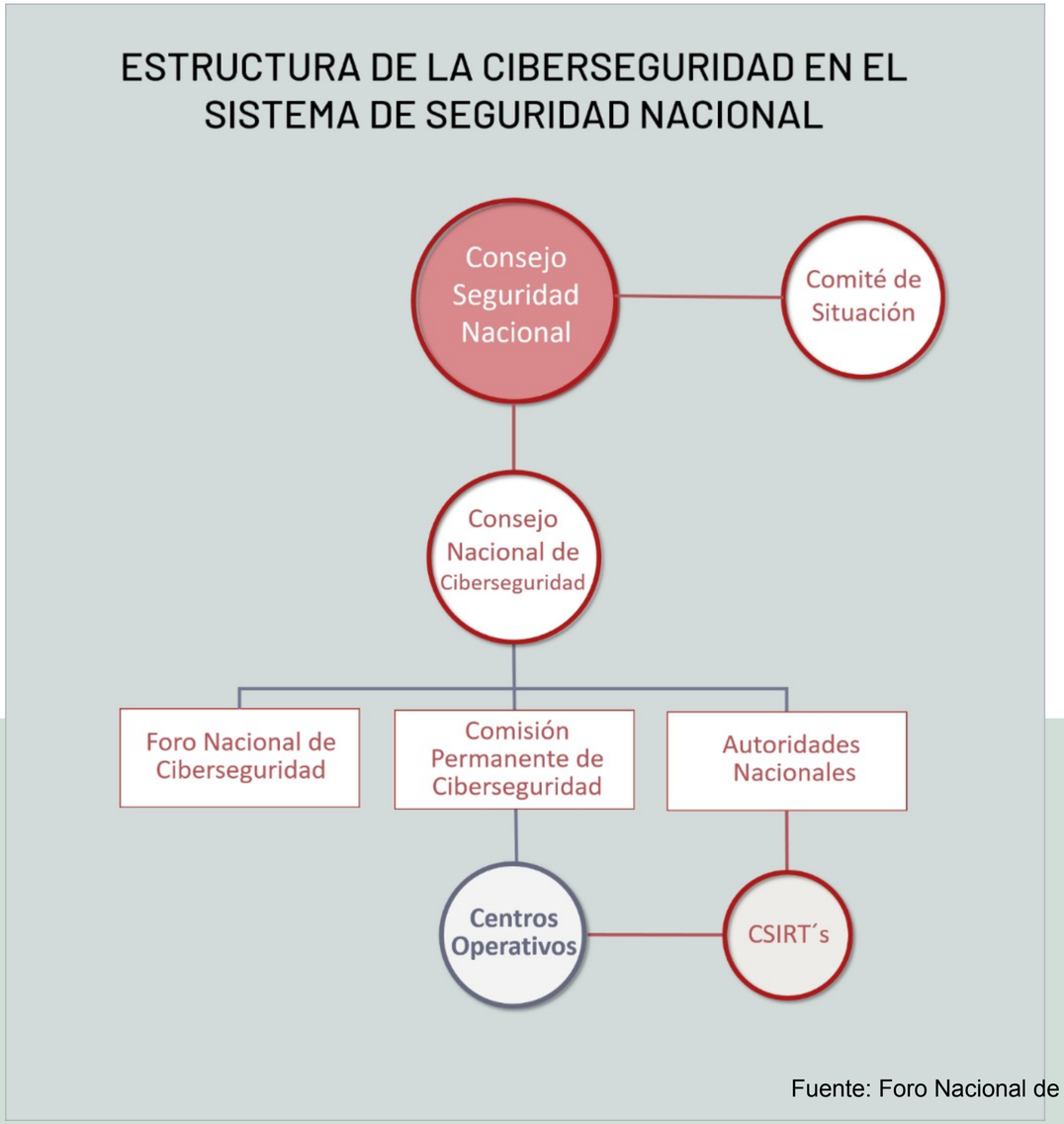
5. Estrategia Nacional de Ciberseguridad

Fuente: Foro Nacional de Ciberseguridad

- **Líneas de acción y medidas, donde se establecen siete líneas de acción** que afianzan la elaboración de la Estrategia Nacional de Ciberseguridad 2019.

5. Estrategia Nacional de Ciberseguridad

- **La ciberseguridad en el Sistema de Seguridad Nacional,** su estructura se compone de tres órganos: el Consejo de Seguridad Nacional, el Consejo Nacional de Ciberseguridad y el Comité de Situación.



Fuente: Foro Nacional de Ciberseguridad

6. Otras normativas vinculadas a la ciberseguridad

Frente a posibles riesgos y/o amenazas, resulta necesario implementar un **Sistema de Gestión de Seguridad de la Información** (SGSI).

Este sistema es una parte del sistema global de gestión, basado en un análisis de los riesgos del negocio, que permite asegurar la información frente a la pérdida de:

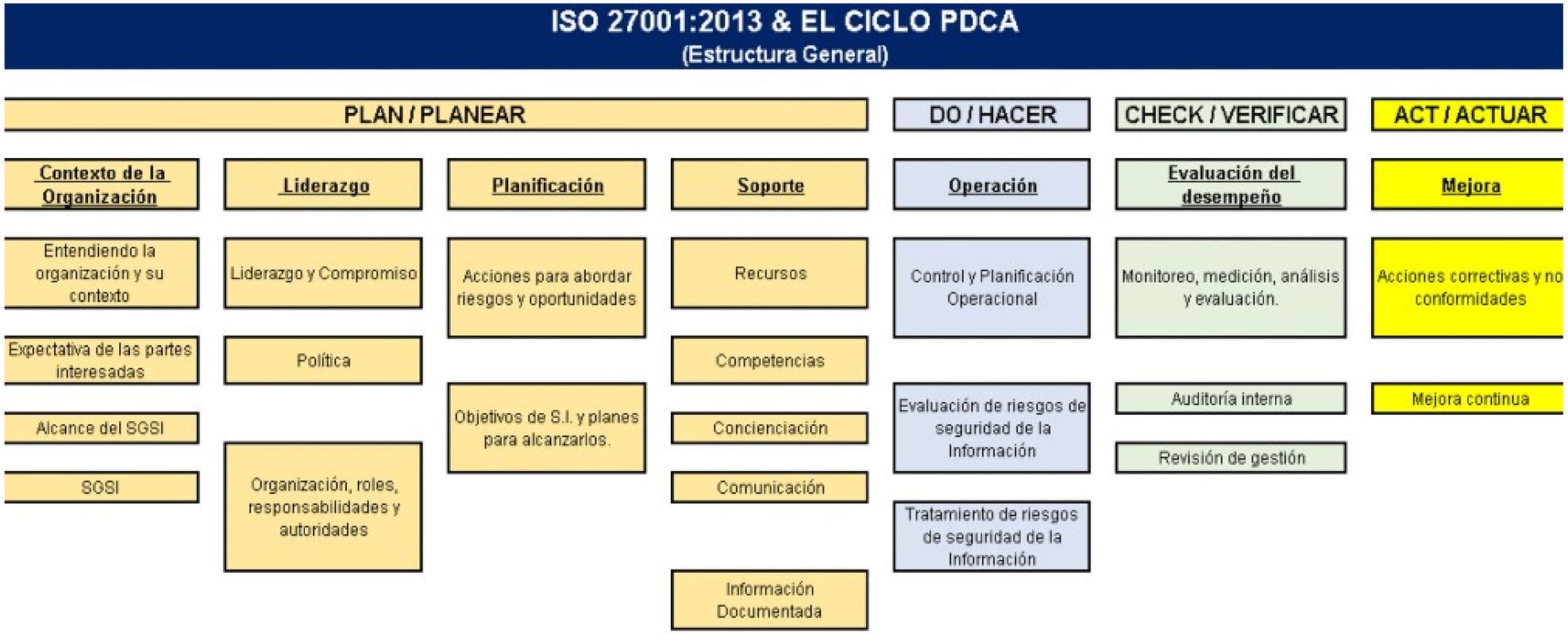
6. Otras normativas vinculadas a la ciberseguridad

Familia de Normas ISO 27000

La Organización Internacional de Estandarización (ISO) recoge un extenso número de normas dentro de la familia de **ISO 27000**.

La Seguridad de la información ha sido definida por la norma ISO/IEC 27000 como la preservación de la confidencialidad, integridad y disponibilidad de la información.

Aplicando el ciclo PDCA al SGSI



6. Otras normativas vinculadas a la ciberseguridad

Familia de Normas ISO 27000

ISO/IEC 27000: aporta las bases de por qué es importante la implantación de un SGSI

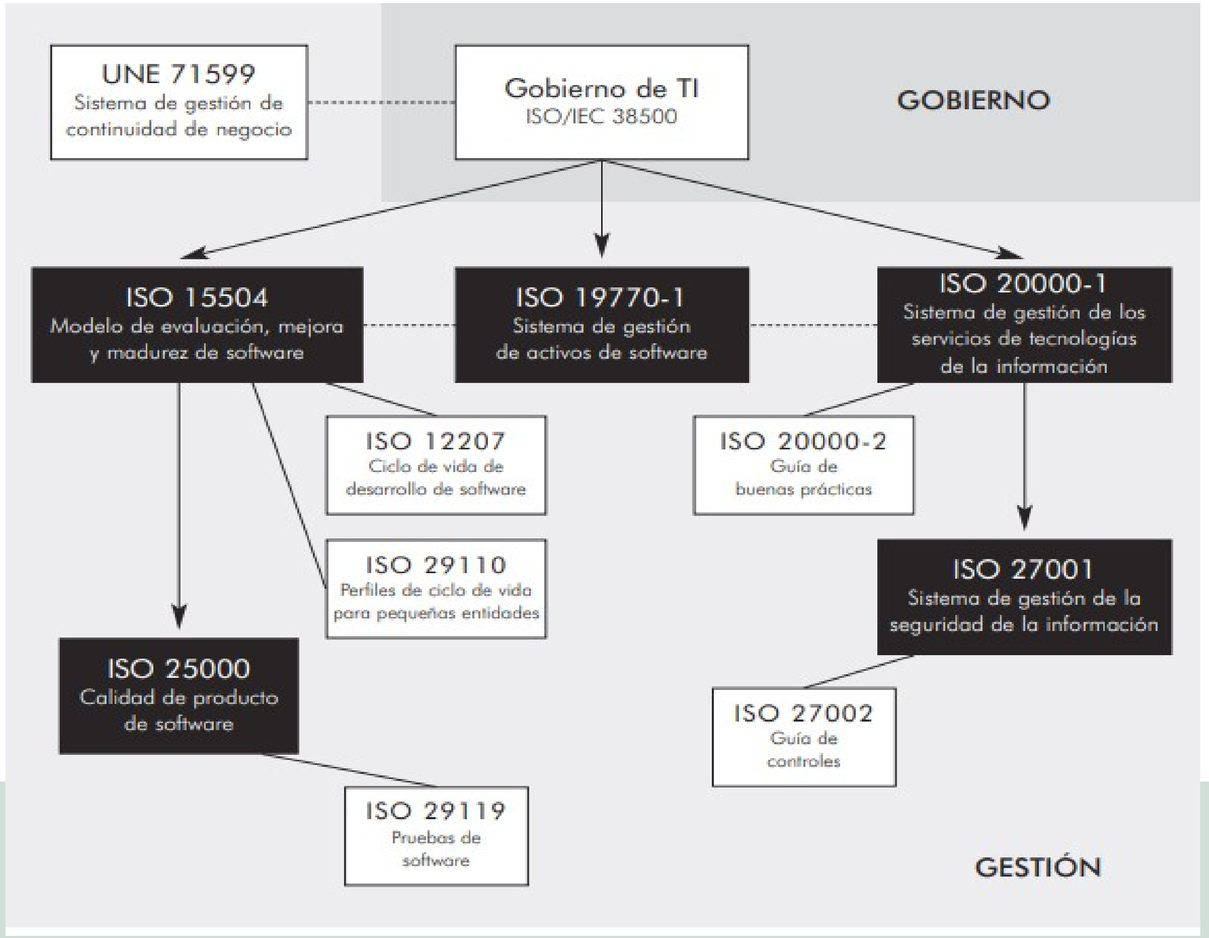
ISO/IEC 27001: contiene los requisitos del sistema de gestión de seguridad de la información.

ISO/IEC 27002: Es una guía de buenas prácticas.

ISO/IEC 27003: guía de aspectos críticos necesarios para el diseño e implementación de un SGS

ISO/IEC 27004: métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI.

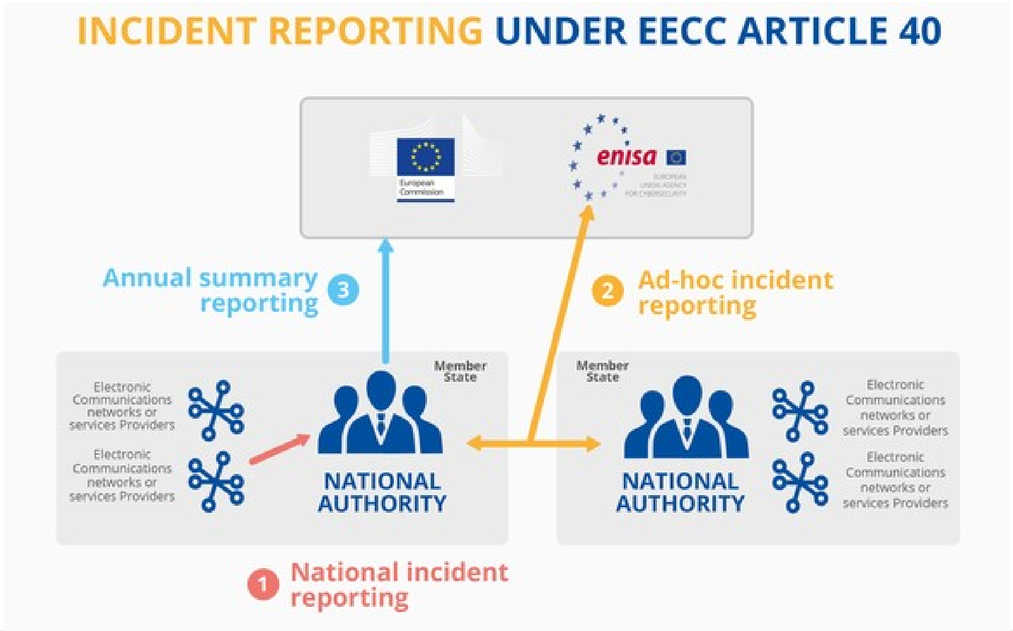
Modelo de gestión de las tecnologías y sistema de la información



Fuente: Aenor

7. Autoridades competentes en materia de Ciberseguridad.

7. Autoridades competentes en materia de Ciberseguridad.



RESPUESTA A INCIDENTES DE CIBERSEGURIDAD

FORO NACIONAL DE CIBERSEGURIDAD

CSIRT.es

Equipos de Respuesta a Incidentes de Seguridad

Conclusiones

sedian Seguridad Digital de Andalucía