GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

CCN
CENTRO CRIPTOLÓGICO NACIONAL

RECOMENDACIÓN

ESQUEMA NACIONAL DE SEGURIDAD

PREGUNTAS FRECUENTES

ens
Esquema Nacional de Seguridad

NOVIEMBRE 2012

ÍNDICE

1. CUESTIONES GENERALES 5

1.1. ¿QUÉ ES EL ESQUEMA NACIONAL DE SEGURIDAD (ENS)? 5
1.2. ¿POR QUÉ ES NECESARIO EL ENS? 5
1.3. ¿CUÁLES SON LOS OBJETIVOS PRINCIPALES DEL ENS? 5
1.4. ¿CUÁL ES EL ORIGEN DEL ENS?, ¿QUIÉNES HAN PARTICIPADO EN SU ELABORACIÓN? 6
1.5. TRAS LA PUBLICACIÓN DEL ENS, ¿CUÁLES SON LOS PASOS SIGUIENTES? 6
1.6. ¿PARA QUÉ SIRVEN LOS PRINCIPIOS BÁSICOS ENUNCIADOS EN EL ENS? 6
1.7. ¿QUÉ HAY QUE HACER CON LOS REQUISITOS MÍNIMOS QUE SE EXPRESAN EN EL ENS? 6

2. ÁMBITO DE APLICACIÓN, ALCANCE E IMPLANTACIÓN DEL ENS 7

2.1. ¿ES EL ENS DE OBLIGADO CUMPLIMIENTO PARA TODAS LAS ADMINISTRACIONES PÚBLICAS? 7
2.2. ¿QUÉ APLICACIONES, SERVICIOS O SISTEMAS ESTÁN COMPRENDIDOS EN EL ÁMBITO DE APLICACIÓN DEL ENS? 7
2.3. ¿CUÁNDO UN SISTEMA NO ESTARÍA COMPRENDIDO DENTRO DEL ÁMBITO DE APLICACIÓN DEL ENS? 7
2.4. ¿QUÉ RESPONSABILIDADES SE DERIVAN DEL INCUMPLIMIENTO DEL ENS? 7
2.5. ¿ES EL ENS DE APLICACIÓN TAMBIÉN A LA RELACIÓN ENTRE ADMINISTRACIONES PÚBLICAS? 8
2.6. ¿ES EL ENS DE APLICACIÓN A LAS ENTIDADES VINCULADAS O DEPENDIENTES DE LAS ADMINISTRACIONES PÚBLICAS? 8
2.7. ¿SIRVE EL ENS PARA PROTEGER LA INFORMACIÓN QUE PUDIERAN LLEGAR A INTERCAMBIARSE VARIOS SISTEMAS DE INFORMACIÓN? 8
2.8. ¿EN QUÉ MEDIDA DEBEMOS TENER EN CUENTA EL ENS CUANDO LAS ACTIVIDADES DE LOS SISTEMAS DE INFORMACIÓN TIENEN LUGAR FUERA DE LAS DEPENDENCIAS DE NUESTRO ORGANISMO O ESTÁN SUBCONTRATADOS CON EMPRESAS EXTERNAS? 9
2.9. ¿CUÁL ES EL "ÓRGANO SUPERIOR" AL QUE SE ALUDE EN EL ENS (ART. 11 Y DISPOSICIÓN TRANSITORIA)? 9
2.10. ¿CÓMO DEBEMOS ENTENDER LA SEDE ELECTRÓNICA, DESDE EL PUNTO DE VISTA DEL ENS? ¿ES UN SISTEMA DE INFORMACIÓN O ES UN DERECHO DE LOS CIUDADANOS? ¿HAY QUE COLGAR EN LA SEDE ELECTRÓNICA LA DECLARACIÓN DE CONFORMIDAD CON EL ENS? 9
2.11. ¿QUEDARÍAN EXCLUIDOS DEL ÁMBITO DE APLICACIÓN DEL ENS AQUELLOS SISTEMAS NO RELACIONADOS CON LOS CIUDADANOS *STRICTO SENSU* COMO, POR EJEMPLO, LOS IMPLICADOS EN LA GESTIÓN DE RECURSOS HUMANOS (FUNCIÓN PÚBLICA)? 10
2.12. ¿SE CONSIDERARÍAN INCLUIDOS EN EL ÁMBITO DEL ENS MEDIOS COMO LA ATENCIÓN TELEFÓNICA? 11
2.13. ¿AFECTA EL ENS A LAS RELACIONES ENTRE DISTINTOS ORGANISMOS DE LAS AA.PP., ENTENDIDAS COMO INTERCAMBIO DE INFORMACIÓN ENTRE LOS MISMOS? 11
2.14. UN SISTEMA DE BACK-OFFICE (NO VISIBLE DESDE EL EXTERIOR) UTILIZADO PARA, POR EJEMPLO, GESTIONAR PROCEDIMIENTOS SANCIONADORES DE LOS CIUDADANOS, ¿QUEDARÍA DENTRO DEL ALCANCE DEL ENS? 12
2.15. ¿ES APLICABLE EL ENS A LOS HOSPITALES PÚBLICOS? ¿Y A LAS UNIVERSIDADES PÚBLICAS? 12
2.16. ¿CUÁLES SON LAS MEDIDAS DE SEGURIDAD QUE DEBEN ADOPTAR LOS PROVEEDORES EXTERNOS QUE PROPORCIONEN SERVICIOS INFORMÁTICOS A LAS AA.PP.?, ¿DEBEN CUMPLIR CON EL ENS? (POR EJEMPLO: SERVICIOS DE ALOJAMIENTO DE SERVIDORES, SERVICIOS *CLOUD COMPUTING*, ETC.) 13
2.17. ¿ES APLICABLE EL ENS A LOS SISTEMAS UTILIZADOS POR LAS AA.PP. PARA "MECANIZAR" LA INFORMACIÓN OBTENIDA EN TRÁMITE UN PRESENCIAL? 13
2.18. ¿CÓMO SE REALIZA EL CONTROL DE LA CORRECTA APLICACIÓN DEL ENS? 14
2.19. LOS COLEGIOS PROFESIONALES, ¿ESTÁN SUJETOS A LO DISPUESTO EN EL ENS? 14

3. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y ESQUEMA NACIONAL DE SEGURIDAD 15

3.1. ¿SE PUEDEN ENTENDER EQUIVALENTES LOS NIVELES LOPD CON LOS NIVELES ENS? 15
3.2. LA DISPOSICIÓN ADICIONAL ÚNICA DEL REAL DECRETO 1720/2007, SEÑALA: "LOS PRODUCTOS DE SOFTWARE DESTINADOS AL TRATAMIENTO AUTOMATIZADO DE DATOS PERSONALES DEBERÁN INCLUIR EN SU DESCRIPCIÓN TÉCNICA EL NIVEL DE SEGURIDAD, BÁSICO, MEDIO O ALTO, QUE PERMITAN ALCANZAR DE ACUERDO CON LO ESTABLECIDO". ¿ES NECESARIO QUE ESTÉ CERTIFICADO O AUDITADO POR ALGÚN AUDITOR INDEPENDIENTE? 15
3.3. PARA EL EJERCICIO DE LOS DERECHOS ARCO (ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN) CONTEMPLADOS EN LA LOPD, LAS AA.PP. SUELEN USAR FORMULARIOS EN FORMATO PDF, EN LOS QUE SE

EXPLICA CUAL ES EL PROCEDIMIENTO QUE DEBEN SEGUIR LOS CIUDADANOS PARA EL EJERCICIO DE TALES DERECHOS. ¿SE CONSIDERAN ESTOS DERECHOS COMO PERTENECIENTES AL ENS?, ¿TIENEN QUE ESTAR ESTOS DOCUMENTOS EN LA SEDE, O SIMPLEMENTE PUEDEN ESTAR EN UNA PÁGINA WEB DE INFORMACIÓN? 15

4. EL EQUIPO HUMANO DE LA SEGURIDAD DE LA INFORMACIÓN 16

4.1. EL ARTÍCULO 15 DEL ENS EXPRESA LA NECESIDAD DE QUE LA SEGURIDAD DE LOS SISTEMAS SEA GESTIONADA POR PERSONAL CUALIFICADO. ¿SE HAN ARTICULADO O DEFINIDO LOS CRITERIOS DE CUALIFICACIÓN DE PERSONAL EN BASE A CERTIFICACIONES, TITULACIONES? 16
4.2. ¿CUÁLES SON LAS FUNCIONES QUE DEBE DESARROLLAR EL RESPONSABLE DEL SISTEMA, SEGÚN EL ENS? ¿QUIÉN DEBE SER ESTA PERSONA? 17
4.3. ¿CUÁLES SON LAS FUNCIONES QUE DEBE DESARROLLAR EL RESPONSABLE DE LA INFORMACIÓN SEGÚN EL ENS?, ¿QUIÉN DEBE SER? 18
4.4. ¿PUEDE DESIGNARSE AL RESPONSABLE DE SEGURIDAD COMO UN COMITÉ EN EL QUE SE CONTEMPLEN DISTINTOS ROLES: TÉCNICO, ORGANIZATIVO Y LEGAL?, ¿TIENE SENTIDO QUE EL RESPONSABLE DE SEGURIDAD SEA UN ALTO CARGO?, ¿CUÁL ES EL PERFIL MÁS IDÓNEO PARA ESTA FUNCIÓN? 18
4.5. ¿EL RESPONSABLE DE SEGURIDAD DEL ENS PUEDE SER LA MISMA PERSONA QUE EL RESPONSABLE DE SEGURIDAD DE LA LOPD? 19
4.6. ¿CUÁLES SON LAS FUNCIONES DEL RESPONSABLE DEL SERVICIO, SEGÚN EL ENS? ¿QUÉ NIVEL ADMINISTRATIVO LE CORRESPONDE? 19
4.7. ¿PUEDE UNA MISMA PERSONA SER RESPONSABLE DE LA INFORMACIÓN, RESPONSABLE DEL SERVICIO Y RESPONSABLE DE SEGURIDAD?, ¿QUÉ ROLES SON INCOMPATIBLES EN UNA MISMA PERSONA? 19
4.8. ¿ES OBLIGATORIA LA DIVISIÓN DE RESPONSABILIDADES CITADA EN LA GUÍA CCN-STIC 801? 20

5. PLAN DE ADECUACIÓN AL ENS 21

5.1. ¿QUÉ PRIMEROS PASOS SE DEBEN ADOPTAR PARA CUMPLIR EL ENS? 21
5.2. ¿EXISTE ALGÚN MODELO DE POLÍTICA DE SEGURIDAD QUE PUEDA SERVIR DE REFERENCIA? 21
5.3. ¿CUÁL ES EL IMPACTO DEL ENS EN LOS SISTEMAS ACTUALES? 22
5.4. HABIENDO CONCLUIDO EL PLAZO PREVISTO EN EL ENS PARA REDACTAR Y APROBAR EL PLAN DE ADECUACIÓN AL ENS, ¿ES NECESARIA SU REALIZACIÓN? 22
5.5. ¿SE PUEDE HACER UN PLAN DE ADECUACIÓN SIN INCLUIR LA POLÍTICA DE SEGURIDAD? 22
5.6. ¿SE PUEDE APROBAR UNA POLÍTICA DE SEGURIDAD SIN CONTEMPLAR LA ESTRUCTURA DE SEGURIDAD DE LA ORGANIZACIÓN DE LA SEGURIDAD? 22
5.7. ¿DEBE PUBLICARSE EN LA SEDE ELECTRÓNICA DEL ORGANISMO EN CUESTIÓN EL PLAN DE ADECUACIÓN AL ENS? 23
5.8. ¿PUEDE REALIZARSE UN ÚNICO PLAN DE ADECUACIÓN PARA VARIOS SISTEMAS DE INFORMACIÓN? 23
5.9. ¿CÓMO DEBE SER EL PLAN DE ADECUACIÓN AL ENS?, ¿QUIÉN DEBE RESPONSABILIZARSE DE SU CUMPLIMIENTO?, ¿QUÉ SUCEDE CUÁNDO LA EXPLOTACIÓN DE LOS SERVICIOS ESTÁ ENCOMENDADA A UN DEPARTAMENTO HORIZONTAL, QUE ATIENDE A VARIOS ORGANISMOS? 23

6. LAS GUÍAS STIC DEL CCN 24

6.1. ¿ES OBLIGATORIO PARA LAS AA.PP. SEGUIR LO QUE SE INDICA EN LAS GUÍAS STIC DEL CCN? 24
6.2. ¿QUÉ GUÍAS STIC HAY PUBLICADAS? ¿CÓMO SE PUEDE ACCEDER A ELLAS? 24

7. LA CATEGORIZACIÓN DE LOS SISTEMAS 24

7.1. ¿EN QUÉ CONSISTE LA CATEGORIZACIÓN DE LOS SISTEMAS PARA LA ADOPCIÓN DE MEDIDAS DE SEGURIDAD? 24
7.2. ¿CÓMO SE CATEGORIZAN LOS SISTEMAS? 24
7.3. EN EL ANEXO I DEL ENS SE HACE REFERENCIA EN MUCHAS OCASIONES AL "INCUMPLIMIENTO FORMAL" Y AL "INCUMPLIMIENTO MATERIAL" DE UNA LEY, LO QUE CONDICIONARÍA EL NIVEL DE SEGURIDAD QUE LE CORRESPONDERÍA A LA DIMENSIÓN DE QUE SE TRATE. 24

8. EL ANÁLISIS DE RIESGOS Y LA GESTIÓN DE RIESGOS 25

8.1. ¿ES NECESARIO REALIZAR UN ANÁLISIS DE RIEGOS, EN SENTIDO ESTRICTO? ¿NO BASTARÍA CON USAR LA EXPERIENCIA DE LOS TÉCNICOS DEL ORGANISMO PARA DETERMINAR QUÉ MEDIDAS SON LAS MÁS OPORTUNAS EN CADA CASO? 25
8.2. HERRAMIENTAS PARA EL ANÁLISIS DE RIESGOS 25
8.3. LA PRECEPTIVA DECLARACIÓN DE APLICABILIDAD, ¿HA DE REALIZARSE POR SISTEMA DE INFORMACIÓN O POR ÁREAS DE NEGOCIO? 26

9. LA AUDITORÍA DE LA SEGURIDAD 26

9.1. ¿CONTEMPLA EL ENS ALGÚN MECANISMO DE AUDITORÍA? 26
9.2. ¿ES NECESARIO REALIZAR LA AUDITORIA DE LA SEGURIDAD POR UN AUDITOR INDEPENDIENTE DE LA ORGANIZACIÓN? ¿ES POSIBLE REALIZAR ESTA DECLARACIÓN DE CONFORMIDAD VALIÉNDOSE DE UNA AUTOEVALUACIÓN RESPECTO DEL ANEXO II DEL ENS? 27

10. CERTIFICACIONES 27

10.1. ¿QUIÉN CERTIFICA QUE UN DETERMINADO PRODUCTO CUMPLE FUNCIONALMENTE CON LAS EXIGENCIAS DE SEGURIDAD QUE SE REQUIEREN? 27
10.2. ¿EXISTE ALGUNA CERTIFICACIÓN QUE ACREDITE LA ADECUACIÓN AL ENS POR PARTE DE UN ORGANISMO PÚBLICO? 28

11. MEDIDAS DE SEGURIDAD 28

11.1. ¿CÓMO SE DETERMINAN LAS MEDIDAS DE SEGURIDAD QUE HAY QUE APLICAR? 28
11.2. MP.COM.2 ¿QUÉ DEBE ENTENDERSE POR DOMINIO DE SEGURIDAD? ¿CÓMO PROTEGER SISTEMAS INTERCONECTADOS? 29
11.3. ¿ES DE APLICACIÓN EL ENS AL CORREO ELECTRÓNICO CORPORATIVO? 29

12. EL ENS Y LA NORMALIZACIÓN VOLUNTARIA RELATIVA A SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 30

12.1. ¿ES EL ENS COMPATIBLE CON UNE ISO/IEC 27001:2007?, ¿SON NORMAS SIMILARES?, ¿SON COMPLEMENTARIAS? 30
12.2. ¿CUÁL ES LA RELACIÓN ENTRE EL ENS Y LA NORMA UNE-ISO/IEC 27002:2009? 31
12.3. TENIENDO MI SERVICIO/SISTEMA CERTIFICADO CONTRA LA NORMA UNE ISO/IEC 27001:2007, ¿DEBO ENTENDER QUE YA ESTOY CUMPLIENDO CON EL ENS? 31

1. CUESTIONES GENERALES

1.1. ¿Qué es el Esquema Nacional de Seguridad (ENS)?

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 da cumplimiento a 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. Su objeto es **establecer 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.

Por tanto, la finalidad del Esquema Nacional de Seguridad es la creación de 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**, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

1.2. ¿Por qué es necesario el ENS?

El ENS es necesario para establecer **elementos comunes** relativos a la seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas, al objeto de crear las condiciones necesarias para la confianza en el uso de los citados medios electrónicos que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

1.3. ¿Cuáles son los objetivos principales del ENS?

Sus objetivos principales son los siguientes:

- **Crear las condiciones necesarias de confianza en el uso de los medios electrónicos**, a través de medidas para garantizar la seguridad de la información y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- **Establecer la política de seguridad** en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, que estará constituida por los principios básicos y los requisitos mínimos para una protección adecuada de la información.
- **Introducir los elementos comunes** que han de guiar la actuación de las Administraciones públicas en materia de seguridad de las tecnologías de la información.
- **Aportar un lenguaje común** para facilitar la interacción de las Administraciones públicas, así como la comunicación de los requisitos de seguridad de la información a la Industria.
- **Aportar un tratamiento homogéneo de la seguridad** que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan diversas entidades.
- **Facilitar un tratamiento continuado de la seguridad**.

1.4. ¿Cuál es el origen del ENS?, ¿quiénes han participado en su elaboración?

El ENS se establece en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

El ENS es el resultado de un **trabajo coordinado por el Ministerio de la Presidencia, asumido posteriormente por el Ministerio de Hacienda y Administraciones Públicas, con el apoyo del Centro Criptológico Nacional (CCN)** y la **participación de todas las Administraciones Públicas**, incluyendo las universidades públicas (CRUE), a través de los **órganos colegiados con competencias** en materia de administración electrónica: Consejo Superior de Administración Electrónica, Comité Sectorial de Administración Electrónica, Comisión Nacional de Administración Local. Participación que incluyó los **informes preceptivos** de: Ministerio de Política Territorial, Ministerio de la Presidencia, Agencia Española de Protección de Datos y Consejo de Estado.

También se ha tenido presente la opinión de las **asociaciones de la Industria del sector TIC**, las aportaciones recibidas tras la **publicación del borrador en el sitio web del Consejo Superior de Administración Electrónica** el 3 de septiembre de 2009.

1.5. Tras la publicación del ENS, ¿cuáles son los pasos siguientes?

Cabe destacar los siguientes:

- Elaboración por parte de CCN de las Guías de Seguridad CCN-STIC para mejor cumplimiento del ENS, de acuerdo con lo previsto en el artículo 29 del Real Decreto 3/2010.
- Reforzamiento de la capacidad de respuesta a incidentes de seguridad CCN-CERT, de acuerdo con las funciones previstas en los artículos 36 y 37 del citado Real Decreto 3/2010.
- Realización de las acciones de formación, en colaboración con el INAP, de acuerdo con lo previsto en la disposición adicional primera del Real Decreto 3/2010.

1.6. ¿Para qué sirven los Principios Básicos enunciados en el ENS?

Los Principios Básicos del ENS establecen unos **puntos de referencia** para tomar decisiones.

Son como la Estrella Polar cuando uno está perdido: si el camino le lleva sistemáticamente en otra dirección, probablemente el camino no sea el adecuado; si hay una bifurcación, hay que optar por la que se orienta correctamente. Mientras todo funciona correctamente, la Estrella Polar es meramente decorativa.

El ENS define los **Principios Básicos de Seguridad** como: "Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios."

1.7. ¿Qué hay que hacer con los Requisitos Mínimos que se expresan en el ENS?

Los Requisitos Mínimos deben cumplirse **siempre**. 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 del citado Anexo II son sustituidas por otras medidas compensatorias, los requisitos mínimos, en todo caso, deben cumplirse igualmente.

2. ÁMBITO DE APLICACIÓN, ALCANCE E IMPLANTACIÓN DEL ENS

2.1. ¿Es el ENS de obligado cumplimiento para todas las Administraciones Públicas?

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

- 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.

Están excluidos del ámbito de aplicación del ENS los sistemas que tratan información clasificada regulada por Ley 9/1968 de 5 de abril, de Secretos Oficiales y sus normas de desarrollo.

2.2. ¿Qué aplicaciones, servicios o sistemas están comprendidos en el ámbito de aplicación del ENS?

Como 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.

Cualquier caso que se aleje de la lista anterior conviene examinarlo con detalle y determinar si se encuentra o no comprendido dentro del marco de la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos. Si es así, habrá que entender que también le es de aplicación lo dispuesto en el ENS.

2.3. ¿Cuándo un sistema no estaría comprendido dentro del ámbito de aplicación del ENS?

Sólo en el caso de que el sistema:

- No esté relacionado con el ejercicio de derechos por medios electrónicos, o
- No esté relacionado con un cumplimiento de deberes por medios electrónicos, o
- No esté relacionado con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo.

Las AA.PP. podrán determinar incluir tal sistema en el ámbito de aplicación del ENS.

En cualquier otro caso, la aplicación del ENS al sistema en cuestión es obligatoria.

2.4. ¿Qué responsabilidades se derivan del incumplimiento del ENS?

Las responsabilidades derivadas del incumplimiento del ENS serían las que correspondieren a cada caso concreto, en virtud de lo dispuesto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2.5. ¿Es el ENS de aplicación también a la relación entre Administraciones Públicas?

Desde luego. El ámbito de aplicación del ENS es el establecido en el artículo 2 de la Ley 11/2007. En él se señala que también es de aplicación a las relaciones entre las distintas Administraciones Públicas. Quedan excluidos los sistemas que manejan información clasificada.

2.6. ¿Es el ENS de aplicación a las entidades vinculadas o dependientes de las Administraciones Públicas?

A la luz de la Ley 11/2007, la Ley 30/1992 y la Ley 6/1997, cabe interpretar lo siguiente:

- El ENS es aplicable a las entidades de derecho público vinculadas o dependientes de las Administraciones Públicas (AGE, CC.AA. y EE.LL.), aunque puede ser necesario un análisis caso por caso.
- Ciertos 'organismos públicos', según la disposición adicional décima de la Ley 6/1997 están vinculados a la AGE y, por tanto, entran dentro del ámbito de aplicación del ENS.
- Lo mismo ocurre con otras entidades empresariales vinculadas o dependientes de la AGE.
- Las Universidades Públicas son Administración Pública vinculada (que no dependiente) a las administraciones de las Comunidades Autónomas y, por tanto, les aplica el ENS.
- En el caso de los órganos constitucionales (Casa Real, Congreso, Senado, Consejo General del Poder Judicial, Tribunal Constitucional, Defensor del Pueblo, Tribunal de Cuentas, Consejo Económico y Social) la aplicación del ENS, o no, sería una decisión propia.
- No obstante, como se ha dicho más arriba, hay que analizar caso por caso para determinar si se trata de una entidad de derecho público vinculada o dependiente de alguna de las Administraciones Públicas. No parece necesario que ejerzan potestades administrativas, ni que su actividad esté sujeta a la Ley 30/1992 por imperativo de ésta.

2.7. ¿Sirve el ENS para proteger la información que pudieran llegar a intercambiarse varios Sistemas de Información?

Naturalmente.

La aplicación de las medidas de seguridad (Anexo II del ENS) pertinentes a cada caso (Sistema de Información de que se trate en cada momento) nos permiten securizar el tratamiento de la información que en cada momento es tratada por cada Sistema de Información, dependiendo, naturalmente, del nivel de seguridad en cada una de sus dimensiones, de la categoría de seguridad del Sistema de Información y siempre desde la confianza que nos aporta la realización previa de un buen Análisis de Riesgos.

Obsérvese que el nivel de seguridad de la Información lo determina el Responsable de la Información, que puede pertenecer a la misma organización del Sistema de Información securizado o a otro distinto y exterior.

Sea como fuere, el Sistema de Información “usuario” debe “heredar” las condiciones de seguridad impuestas por el “propietario” de la información.

2.8. ¿En qué medida debemos tener en cuenta el ENS cuando las actividades de los Sistemas de Información tienen lugar fuera de las dependencias de nuestro organismo o están subcontratados con empresas externas?

El ENS es una norma de obligado cumplimiento para todos los Sistemas de Información de las AA.PP., independientemente de su ubicación.

Por tanto, debemos exigir el cumplimiento del ENS no sólo a los Sistemas de Información que estén operados por personal de las AA.PP. y/o en dependencias de las AA.PP., sino también a aquellos otros que, estando operados por terceros –e, incluso, en dependencias de terceros- desarrollan funciones, misiones, cometidos o servicios para las AA.PP.

2.9. ¿Cuál es el "órgano superior" al que se alude en el ENS (art. 11 y Disposición Transitoria)?

A efectos del ENS, debemos entender por **órgano superior**, los siguientes:

- En la Administración General del Estado: Ministros y, en su caso, Secretarios de Estado.
- En la Administración de las Comunidades Autónomas: Consejeros y, en su caso, Viceconsejeros.
- En la Administración Local: Presidentes de Diputaciones Provinciales, Alcaldes y, en su caso, Tenientes de Alcalde.

Obsérvese que los órganos superiores que menciona el ENS se corresponden con aquellos órganos administrativos entre cuyas competencias se encuentra la determinación y asignación presupuestaria del organismo, circunstancia lógica, a la vista de que el cumplimiento del ENS supondrá, en la mayoría de los casos, la debida asignación presupuestaria que requiere su implantación.

2.10. ¿Cómo debemos entender la Sede Electrónica, desde el punto de vista del ENS? ¿Es un Sistema de Información o es un derecho de los ciudadanos? ¿Hay que colgar en la Sede Electrónica la declaración de conformidad con el ENS?

La Ley 11/2007 y sus normas de desarrollo, vienen a señalar aquellos elementos para los que es necesario adoptar las medidas de seguridad que el ENS concreta. Estos elementos son los siguientes:

1. Sedes electrónicas.
2. Registros electrónicos.
3. Sistemas de Información accesibles electrónicamente por los ciudadanos.
4. Sistemas de Información para el ejercicio de derechos.
5. Sistemas de Información para el cumplimiento de deberes.
6. Sistemas de Información para recabar información y estado del procedimiento administrativo.

Lo anterior significa que la seguridad de la Sede Electrónica debe contemplarse, conjuntamente, desde su **doble función**: como punto de acceso (requiriendo medidas de seguridad diferenciadas) y como elemento a partir del cual los ciudadanos pueden tener acceso a una multiplicidad de servicios (que requerirán, cada uno de ellos, el tratamiento diferenciado que aconseje su preceptivo análisis de riesgos).

Así pues, la Sede Electrónica, requerirá de cautelas de seguridad diferenciadas, particulares y, en general, distintas, de cada uno de los servicios a los que puedan accederse a través de ella.

(Hagamos un símil: la Sede Electrónica es el portal de un hotel con varias dependencias/habitaciones, y cada dependencia/habitación es un sistema/servicio individualizado al que puede acceder la persona que entra en el edificio. Las medidas de seguridad (por ejemplo, control de acceso) serán distintas si el visitante sólo pretende acceder a la recepción del hotel, a la cafetería, a la caja fuerte, o a la habitación donde se aloja el Presidente del Gobierno.)

Finalmente, en la Sede Electrónica nunca se deberá publicar información o documentos que puedan evidenciar vulnerabilidades o brechas de seguridad que puedan ser explotadas por agentes externos/internos.

2.11. ¿Quedarían excluidos del ámbito de aplicación del ENS aquellos sistemas no relacionados con los ciudadanos *stricto sensu* como, por ejemplo, los implicados en la gestión de recursos humanos (función pública)?

Como hemos señalado en otros lugares, el ámbito de aplicación del ENS alcanza 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.

Evidentemente, los funcionarios o empleados públicos son siempre ciudadanos (cosa que, a la inversa, no siempre es verdad). Ahora bien, cuando la Ley 11/2007 está hablando de *ciudadano*, lo hace bajo el principio y la interpretación de *destinatario, beneficiario o parte en los procedimientos administrativos para los que la unidad administrativa en cuestión tiene competencias públicas encomendadas.*

La gestión de Recursos Humanos de un organismo público no goza de ese carácter "público" de sus actuaciones administrativas, puesto que se trata, más bien, de una relación "privada" entre el propio funcionario y el organismo del que depende o en el que presta sus servicios.

Así pues, la relación del funcionario o empleado público con su Administración puede presentar dos formas claramente diferenciadas:

1. Relación administrativa pública: aquella en la que el funcionario o empleado público se relaciona con su Administración como un ciudadano más.
2. Relación privada (laboral, por ejemplo): aquella en la que el funcionario o empleado público se relaciona con su Administración como consecuencia de un vínculo previo no extensible al resto de los ciudadanos.

La conformidad con la Ley 11/2007 y sus normas de desarrollo alcanza específicamente a la primera de las antedichas relaciones.

Por tanto, el sin duda deseable ejercicio electrónico de derechos por pare de los funcionarios o empleados públicos, en tanto se relacionen con sus AA.PP. en virtud de una relación funcionarial o laboral, deberá satisfacerse dando sin embargo prioridad a aquellas actuaciones administrativas que posean el antedicho carácter público.

2.12. ¿Se considerarían incluidos en el ámbito del ENS medios como la atención telefónica?

El art. 8 de la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos señala:

> *"1. Las Administraciones Públicas deberán habilitar **diferentes canales** o medios para la prestación de los servicios electrónicos, garantizando en todo caso el acceso a los mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos, en la forma que estimen adecuada.*
> *2. La Administración General del Estado garantizará el acceso de todos los ciudadanos a los servicios electrónicos proporcionados en su ámbito a través de un sistema de **varios canales** que cuente, al menos, con los siguientes medios:*
> *a) Las oficinas de atención presencial que se determinen…*
> *b) Puntos de acceso electrónico…*
> *c) **Servicios de atención telefónica** que, en la medida en que los criterios de seguridad y las posibilidades técnicas lo permitan, faciliten a los ciudadanos el acceso a las informaciones y servicios electrónicos a los que se refieren los apartados anteriores."*

Por tanto, la **atención telefónica** (usada con las debidas garantías), está comprendida dentro de los canales que podrán ser utilizados por los ciudadanos para el ejercicio de sus derechos.

Por otro lado, como es sabido, el objetivo fundamental del ENS es eliminar o minimizar el impacto que un incidente de seguridad tendría en el desenvolvimiento del organismo de que se trate en cada caso.

Así, el art. 43.3 del ENS se refiere al **impacto**, cuando señala:

"3. La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos."

Por tanto, si un incidente de seguridad sobre los **canales de atención telefónica** pudiera tener repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos, nos encontraríamos con que tales canales estarían dentro del ámbito contemplado en el ENS.

2.13. ¿Afecta el ENS a las relaciones entre distintos organismos de las AA.PP., entendidas como intercambio de información entre los mismos?

Ya hemos dicho que el ENS afecta, especialmente, a las Sedes y Registros Electrónicos, los Sistemas de Información accesibles electrónicamente por los ciudadanos, los Sistemas de Información para el ejercicio de derechos o para el cumplimiento de deberes y los Sistemas de Información para recabar información y estado del procedimiento administrativo.

Por tanto, si el intercambio de información entre distintos organismos de las AA.PP. tiene como objetivo último estos fines, tal intercambio deberá estar sometido a lo dispuesto en el ENS.

Por último, conviene señalar que, muy especialmente en el caso de intercambio de información entre organismos públicos, hay que tener en cuenta igualmente lo dispuesto en el Real Decreto 4/2010, que regula el Esquema Nacional de Interoperabilidad, como garantía fundamental de que la información intercambiada será adecuada a los propósitos perseguidos.

2.14. Un sistema de back-office (no visible desde el exterior) utilizado para, por ejemplo, gestionar procedimientos sancionadores de los ciudadanos, ¿quedaría dentro del alcance del ENS?

Naturalmente.

Obsérvese que, en el caso descrito, el ejercicio de los derechos de los ciudadanos quedaría limitado si, debido a algún incidente de seguridad en tal sistema, se impidiera o perturbara la interposición del correspondiente recurso, conocer el estado de su tramitación, alteración del cómputo de los plazos, etc.

Aunque se trate de un Sistema de Información no visible desde el exterior, su correcto funcionamiento incide directamente en el normal desenvolvimiento del procedimiento administrativo. Por tanto, le es de aplicación plena lo dispuesto en el ENS.

2.15. ¿Es aplicable el ENS a los Hospitales públicos? ¿Y a las Universidades públicas?

El art. 3 del ENS señala:

> *"El ámbito de aplicación del presente real decreto será el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio.*
>
> *Están excluidos del ámbito de aplicación indicado en el párrafo anterior los sistemas que tratan información clasificada regulada por Ley 9/1968, de 5 de abril, de Secretos Oficiales y normas de desarrollo."*

Por la parte que ahora interesa, el citado art. 2.1 de la Ley 11/2007, señala:

> *"La presente Ley, en los términos expresados en su disposición final primera , será de aplicación: a) A las Administraciones Públicas, entendiendo por tales la Administración General del Estado, las 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."*

Para determinar el alcance de la expresión "*entidades de derecho público vinculadas o dependientes de las mismas*", que aparece en el artículo 2 anterior, habrá que relacionarla con lo establecido en el artículo 2.2. de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en la que parece inspirada.

En concreto, el artículo 2.2. de la citada Ley 30/1992 señala:

> *"Las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las Administraciones Públicas tendrán asimismo la consideración de Administración Pública. Estas Entidades sujetarán su actividad a la presente Ley cuando ejerzan potestades administrativas, sometiéndose en el resto de su actividad a lo que dispongan sus normas de creación*".

Finalmente, señalar que el art. 2.2 de la Ley 11/2007, prescribe:

> *"La presente Ley no será de aplicación a las Administraciones Públicas en las actividades que desarrollen en régimen de derecho privado."*

Así pues, si el Hospital o Universidad de que se trate posee la consideración de entidad de derecho público (vinculada o dependiente, de la Administración General del Estado, de las Comunidades Autónomas o de las Entidades Locales), le será de plena aplicación lo dispuesto en el ENS en aquellas actividades que no desarrolle en régimen de derecho privado.

2.16. ¿Cuáles son las medidas de seguridad que deben adoptar los proveedores externos que proporcionen servicios informáticos a las AA.PP.?, ¿deben cumplir con el ENS? (Por ejemplo: servicios de alojamiento de servidores, servicios *cloud computing*, etc.)

La Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en su artículo 15, señala la posibilidad de que, cuando por razones de eficacia o cuando no se posean los medios técnicos idóneos para su desempeño, la realización de actividades de carácter **material, técnico o de servicios**, de la competencia de los órganos administrativos o de las entidades de derecho público, pueda recaer sobre personas físicas o jurídicas sujetas a derecho privado.

En tales casos, la realización de las actividades indicadas, no supone cesión de titularidad de la competencia ni de los elementos sustantivos de su ejercicio, siendo responsabilidad del órgano o entidad de la Administración contratante dictar cuantos actos o resoluciones de carácter jurídico den soporte o en los que se integre la concreta actividad material objeto de la actividad.

Por tanto, las medidas de seguridad que deben adoptar los proveedores de servicios no las fija el propio proveedor, sino que serán las determinadas por la Administración contratante, en virtud de la naturaleza de los servicios prestados.

Finalmente, recordar una vez más que es responsabilidad de la Administración contratante la suscripción del correspondiente **contrato de prestación del servicio** (incluyendo, en su caso, los Acuerdos de Nivel de Servicio a los que hubiere lugar), que deberá contener todas las estipulaciones necesarias para dar cumplimiento a lo dispuesto en el ENS, en virtud de la naturaleza del servicio prestado.

2.17. ¿Es aplicable el ENS a los sistemas utilizados por las AA.PP. para "mecanizar" la información obtenida en trámite un presencial?

Como es sabido, el ENS se aplicará por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Las únicas **exclusiones expresas** de la aplicación del ENS son los sistemas que tratan información clasificada, las actividades que desarrollen las Administraciones públicas en régimen de derecho privado y aquellas actividades que no sean para gestionar el ejercicio de sus competencias.

Además, sólo cuando se trate de sistemas no relacionados con el ejercicio de derechos, con el cumplimiento de deberes por medios electrónicos, y con el acceso de los ciudadanos a la información y procedimientos administrativos por medios electrónicos, la Administración correspondiente podrá determinar la no aplicación de lo dispuesto en el ENS (art. 30 ENS).

Por tanto, si las AA.PP. optan por utilizar las tecnologías de la información en el desarrollo de su actividad administrativa, les resulta de aplicación el Esquema Nacional de Seguridad, con las exclusiones indicadas.

En relación con la pregunta, y como quiera que los equipos y sistemas informáticos que se usan en el trámite presencial forman parte de las tecnologías de la información, su utilización comporta la necesidad de someterse al ENS, con independencia de que el acceso sea local, o sea remoto.

2.18. ¿Cómo se realiza el control de la correcta aplicación del ENS?

Existen varios controles:

- Los ordinarios de cumplimiento de cada unidad administrativa (art. 40).
- Los que pueda articular el Comité Sectorial de Administración Electrónica para conocer el estado de las principales variables de seguridad (art. 35).
- Los derivados de las auditorías (art. 34) y,
- Eventualmente, los que pudieran emanar del CCN, en el ámbito de sus competencias.

2.19. Los Colegios Profesionales, ¿están sujetos a lo dispuesto en el ENS?

Según el texto de la vigente Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales, los Colegios Profesionales son Corporaciones de Derecho Público, amparadas por la Ley y reconocidas por el Estado, con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines; relacionándose con la Administración a través del Departamento ministerial competente (art. 2.3) y, en su caso, con la Comunidad Autónoma correspondiente.

Si bien la Ley 11/2007, de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos, establece, genéricamente, que el ámbito de aplicación de la norma alcanza a las Administraciones Públicas, entendiendo por tales la Administración General del Estado, las 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 (art. 2.1.a), no es menos cierto que es la propia Ley 11/2007, en primera instancia, la que limita su propio alcance, cuando señala, en su art. 2.2, que "*La presente Ley no será de aplicación a las Administraciones Públicas en las actividades que desarrollen en régimen de derecho privado*".

A esta primera limitación, establecida en la propia Ley 11/2007, vertebradora de la Administración Electrónica y de la que traen causa, entre otras, los Esquemas Nacionales de Seguridad e Interoperabilidad, hay que sumar la expresada en el propio Real Decreto 3/2010, cuando señala, en su art. 30: "*Las Administraciones públicas podrán determinar aquellos sistemas de información a los que no les sea de aplicación lo dispuesto en el presen te real decreto por tratarse de sistemas no relacionados con el ejercicio de derechos ni con el cumplimiento de deberes por medios electrónicos ni con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, de acuerdo con lo previsto en la ley 11/2007 de 22 de junio*".

Por tanto, si entre las funciones, servicios o actividades que desarrollan, prestan o acometen los Colegios Profesionales sujetos a la Ley 2/1974, se encuentran aquellos que están relacionados con:

- 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/o estado del procedimiento administrativo.

Entonces, a tales servicios o actividades, le será de plena aplicación lo dispuesto en el ENS, no siendo aplicable, sin embargo, a aquellas otras actividades que desarrollaran al margen de las enumeradas o al amparo del derecho privado.

3. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y ESQUEMA NACIONAL DE SEGURIDAD

3.1. ¿Se pueden entender equivalentes los niveles LOPD con los niveles ENS?

Las denominaciones BÁSICO/MEDIO/ALTO, que utilizan tanto el ENS como el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal), no poseen la misma semántica. Es decir: no son intercambiables ni significan lo mismo.

Así, mientras que para el RD 1720/2007 los niveles de seguridad se determinan por la pertenencia del dato a un nivel concreto, para el ENS la categoría del sistema se sustenta en el impacto que un incidente de seguridad podría tener en relación con la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio y el respeto a la legalidad y a los derechos de los ciudadanos (y en sus dimensiones: integridad, confidencialidad, trazabilidad, disponibilidad y autenticidad).

Por tanto, puesto que su determinación obedece a procedimientos distintos, cada sistema/servicio/tratamiento debe cualificarse independientemente: para su conformidad con la normativa de Protección de Datos de Carácter Personal y para con lo dispuesto en el ENS.

3.2. La Disposición Adicional Única del Real Decreto 1720/2007, señala: "Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido". ¿Es necesario que esté certificado o auditado por algún auditor independiente?

El RD 1720/2007 sólo exige que en las normas técnicas del producto en cuestión aparezca la mención del nivel de seguridad que es capaz de alcanzar el software en cuestión. No prescribe, por tanto, ninguna auditoría.

Sin embargo, existen productos software que han sometido (o están sometiendo) al análisis de auditores externos y/o independientes esta cuestión, con la idea de exhibir el resultado de tal auditoría no sólo en las normas técnicas del producto, sino también en sus páginas web, etc.

3.3. Para el ejercicio de los derechos ARCO (acceso, rectificación, cancelación y oposición) contemplados en la LOPD, las AA.PP. suelen usar formularios en formato PDF, en los que se explica cual es el procedimiento que deben seguir los ciudadanos para el ejercicio de tales derechos. ¿Se consideran estos derechos como pertenecientes al ENS?, ¿tienen que estar estos documentos en la Sede, o simplemente pueden estar en una página web de información?

Como hemos dicho en otros lugares, el ámbito de aplicación del ENS se extiende 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.

El ejercicio de los derechos ARCO es, como su propio nombre indica, un derecho de los ciudadanos. Por tanto, el ejercicio de tales derechos debe ser objeto del ENS.

Obsérvese que las medidas de seguridad que serán de aplicación a cada sistema/servicio deben estar ponderadas respecto de los riesgos que la organización asume. En este caso, toda vez que se trata de una mera información al usuario (información que podrá encontrarse en la Sede Electrónica, como expresión del ejercicio de un derecho) las cautelas que deben tomarse parecen simples: asegurar la disponibilidad de la información, su integridad y su autenticidad, estás dos últimas dimensiones pueden satisfacerse firmando electrónicamente los PDF o incorporándoles un CSV (Código Seguro de Verificación) mediante el cual los interesados puedan verificar su autenticidad mediante la consulta a la página web del organismo.

4. EL EQUIPO HUMANO DE LA SEGURIDAD DE LA INFORMACIÓN

4.1. El artículo 15 del ENS expresa la necesidad de que la seguridad de los sistemas sea gestionada por personal cualificado. ¿Se han articulado o definido los criterios de cualificación de personal en base a certificaciones, titulaciones?

Dos cuestiones son importantes aquí:

- El principio de la seguridad como **función diferenciada**, que se trata en el artículo 10.

  "Artículo 10. La seguridad como función diferenciada.
  En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.
  El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
  La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.
  La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos."

- El requisito de **profesionalidad** que se trata en el artículo 15.

  "Artículo 15. Profesionalidad.
  1. La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.
  2. El personal de las Administraciones públicas recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Administración.
  3. Las Administraciones públicas exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados."

4.2. ¿Cuáles son las funciones que debe desarrollar el Responsable del Sistema, según el ENS? ¿Quién debe ser esta persona?

El **Responsable del Sistema** es un puesto operativo, no un cargo directivo o de gobierno. Suele recibir también la denominación de Responsable de Producción o Explotación, de manera que en él viene a recaer la responsabilidad de la prestación material del servicio.

Según se manifiesta en la Guía CCN-STIC-801, el **Responsable del Sistema** deberá asumir las siguientes responsabilidades:

- Desarrollar, operar y mantener del Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Velar por el cumplimiento de las obligaciones del Administrador de Seguridad del Sistema (ASS).
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Además, el responsable del sistema puede *acordar* la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada**.**

Por tanto, este profesional debe poseer los conocimientos técnicos adecuados, así como la capacidad de gestionar la actividad de los operadores o técnicos de sistemas que tenga a su cargo (si los hubiere).

Por otro lado, nada impide que esta función sea asumida por una persona (o personas) externas a la propia organización (previa formalización contractual) y que pueda reportar al Comité de Seguridad o a los Responsables TIC del organismo. Hacemos notar de nuevo que puede delegarse la función, no la responsabilidad, que será siempre del organismo público.

4.3. ¿Cuáles son las funciones que debe desarrollar el Responsable de la Información según el ENS?, ¿quién debe ser?

Según se manifiesta en la Guía CCN-STIC-801, , el **Responsable de la Información** es la persona (u órgano colegiado con responsabilidad unitaria identificable) que tiene la potestad de establecer los requisitos de la información en materia de seguridad, o, en terminología del ENS, la persona que determina los niveles de seguridad de la información.

Por tanto, lo lógico será que el Responsable de la Información se corresponda con algún funcionario o empleado público (de carrera o de libre designación, según los casos) perteneciente a los niveles de gobierno del organismo público en cuestión (por ejemplo, cargos directivos en la AGE). Nótese que la información de alto nivel que se maneja en un órgano de la Administración Pública o Entidad de Derecho Público cae habitualmente dentro de un grupo reducido de tipos de información, tipos que son muy estables en el tiempo. La valoración se realiza una vez en una fase inicial de implantación del ENS y puede permanecer inalterable durante años.

Como en otras figuras, nada impide que esta responsabilidad pueda recaer en un órgano colegiado (presidido por una persona física, que será la que asumirá la responsabilidad formal de sus actos.) Por ejemplo, tal es el caso del Pleno de un Ayuntamiento, cuando determina y aprueba la valoración hecha de una determinada información y, en su consecuencia, aceptando el riesgo residual que pudiera permanecer tras el preceptivo Análisis de Riesgos y obtención de la Declaración de Aplicabilidad.

Aunque la aprobación formal de los niveles corresponda al responsable de la información, se puede recabar una propuesta al Responsable de Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

4.4. ¿Puede designarse al Responsable de Seguridad como un Comité en el que se contemplen distintos roles: técnico, organizativo y legal?, ¿tiene sentido que el Responsable de Seguridad sea un alto cargo?, ¿cuál es el perfil más idóneo para esta función?

Efectivamente, la seguridad comporta en muchas ocasiones la **concurrencia de perfiles profesionales distintos**: físicos, técnicos, informáticos, jurídicos, organizativos, etc.

Hay ejemplos de organizaciones de tamaño importante (por ejemplo, una Comunidad Autónoma) donde es un hecho (sobre todo cuando existen unidades administrativas que tienen la responsabilidad de prestar servicios tecnológicos comunes a una multiplicidad de otros órganos) que la figura del Responsable de Seguridad esté encarnada en tal unidad administrativa, que, bajo la dirección de una persona física, engloba en su seno a una multiplicidad de perfiles, capaces todos ellos de dar adecuada respuesta a las necesidades de seguridad cuya responsabilidad tengan encomendadas.

(Obsérvese que esta encomienda requiere la preceptiva publicación de la norma habilitante correspondiente).

Por tanto, debemos **entender la palabra "persona" que cita repetidamente el ENS, más bien como la "personificación" de la potestad atribuida a un órgano**, potestad que, obviamente, en última instancia, dependerá de la persona física titular de tal órgano administrativo.

En otras palabras, la finalidad última del ENS en relación con este asunto es evitar que la responsabilidad se diluya en comités o unidades administrativas -más o menos formales- análogas, sino que, por el contrario, la responsabilidad última deber recaer sobre una persona física (que podrá ser, nada lo impide, el Presidente de un Comité de Seguridad).

De todo lo anterior se deduce que el Responsable de Seguridad no es un cargo de gobierno. Su función esencial es planificar lo que se ha de hacer en materia de seguridad, así como supervisar que se haya hecho adecuadamente. Suele poseer un perfil técnico.

Lógicamente –como así prescribe el ENS- la función del Responsable de Seguridad debe estar claramente diferenciada de la del Responsable del Sistema (también llamado Responsable de Explotación).

Aunque es frecuente que el Responsable de Seguridad posea un nivel administrativo inferior al Responsable del Sistema, lo idóneo sería que ambas figuras se mantuvieran en el mismo nivel administrativo. En todo caso, conviene que el Responsable de Seguridad no dependa orgánicamente del Responsable del Sistema, para asegurar la adecuada independencia que debe guiar sus actuaciones.

4.5. ¿El Responsable de Seguridad del ENS puede ser la misma persona que el Responsable de Seguridad de la LOPD?

Formalmente nada lo impide.

Debemos hacer constar que ambos perfiles requieren una formación muy específica y diferenciada. (Por ejemplo, el Responsable de Seguridad ENS es un perfil eminentemente tecnológico, mientras que el Responsable de Seguridad LOPD debe poseer, además, el conocimiento jurídico pertinente). Por tanto, dándose la circunstancia de que la persona designada goce de la formación adecuada en ambas responsabilidades, no existe inconveniente.

Independientemente de lo anterior, sobre todo en organizaciones de tamaño significativo, debe entenderse como más conveniente que ambos responsables (en el caso de personas físicas) sean distintos, pudiendo formar parte, eso sí, de un Comité de Seguridad de amplio espectro y cuyo titular será el Responsable formal de ambas funciones.

4.6. ¿Cuáles son las funciones del Responsable del Servicio, según el ENS? ¿Qué nivel administrativo le corresponde?

El Responsable del Servicio determina los requisitos de los servicios prestados.

Puede ser un apersona concreta o un órgano corporativo que revestirá la forma de órgano colegiado. A menudo puede ocurrir que se encuentre en una posición jerárquicamente dependiente del Responsable de la Información.

Esta estructura refleja el hecho habitual de que un Servicio hereda los requisitos de la información que maneja, sin perjuicio de las exigencias en materia de disponibilidad que convenga añadir.

4.7. ¿Puede una misma persona ser Responsable de la Información, Responsable del Servicio y Responsable de Seguridad?, ¿qué roles son incompatibles en una misma persona?

Ya hemos visto que el ENS prohíbe, explícitamente, que el Responsable del Sistema sea la misma persona que el Responsable de Seguridad. Obviamente, quien está legitimado para pronunciarse sobre la idoneidad de las medidas de seguridad adoptadas para securizar un Sistema, no puede ser la misma persona encargada de su explotación.

Hecha esta salvedad, nos preguntamos hasta qué punto el resto de las responsabilidades enunciadas en el ENS son susceptibles de ser asumidas de manera unificada.

Desde el punto de vista formal, nada lo impide. Sin embargo, desde el punto de vista funcional, esta coincidencia no es lógica.

Obsérvese, en primer lugar, que la Información puede ser generada por el propio organismo, o provenir de un organismo externo. Si la información se *importa* desde un organismo externo, será el Responsable de la Información de aquel organismo el que señalará su nivel de seguridad y, en su consecuencia, marcará las medidas de seguridad que habrá de adoptar el organismo receptor de la información.

Por otro lado, obsérvese que una misma información puede alimentar varios servicios, que podrán tener, cada uno su propio Responsable del Servicio.

Finalmente, y aunque no se trate de un caso frecuente, obsérvese que un mismo servicio puede ser explotado por uno o varios sistemas de información distintos, para cada uno de los cuales puede haber sido designado un Responsable de Seguridad distinto.

Como resumen diremos que, dejando a salvo lo preceptuado por el ENS, en relación con la exigencia de diferenciación personal entre el Responsable del Sistema y el Responsable de Seguridad, la posibilidad de hacer coincidir en una única persona las responsabilidades de la información, los servicios y la seguridad, se hará tanto más inconveniente cuanto mayor sea la multiplicidad de las informaciones manejadas y los servicios prestados, o cuanto mayor relación o interdependencia tengan los sistemas de información del organismo con otros sistemas de información exteriores.

4.8. ¿Es obligatoria la división de responsabilidades citada en la Guía CCN-STIC 801?

Aunque su confección obedece a criterios amplia e internacionalmente reconocidos, los contenidos de las Guías CCN-STIC son recomendaciones, no mandatos imperativos.
La división de responsabilidades expresada en la Guía CCN-STIC 801 responde al mandato del art. 10 del ENS, cuando señala:

> *"En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.*
> *El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.*
> *La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.*
> *La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos."*

La división de responsabilidades enunciada en la Guía CCN-STIC 801 es una recomendación, desarrollada para el mejor cumplimiento de lo dispuesto en el ENS, recomendación que se contiene de nuevo en la medida de seguridad "Segregación de funciones y tareas [op.acc.3]." del Anexo II y que vuelve a encontrarse, como uno de los objetivos de la Auditoría de Seguridad, en el Anexo III.1.

Llegado este punto, merece la pena insistir en la precisa exigencia que enuncia el antedicho art. 10 del ENS, cuando prohíbe que la función del Responsable de Seguridad recaiga en la misma persona que el Responsable del Servicio.

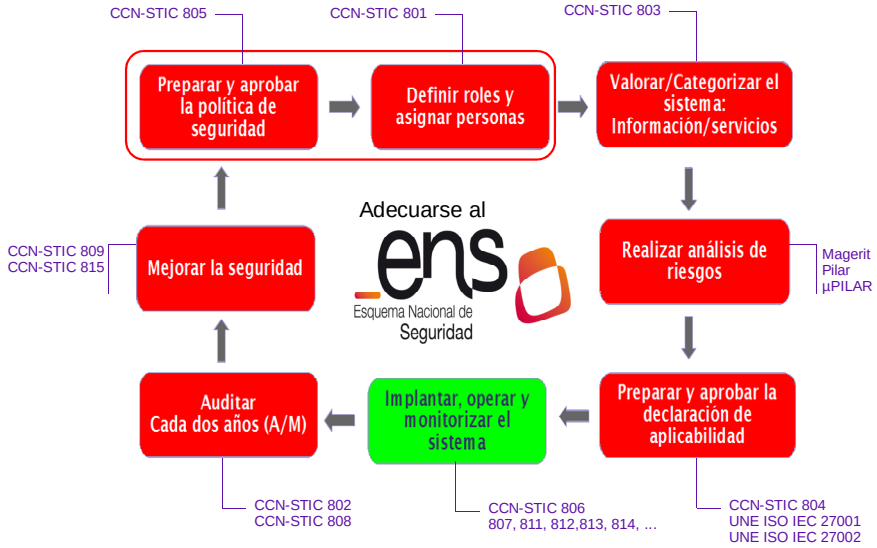
5. PLAN DE ADECUACIÓN AL ENS

5.1. ¿Qué primeros pasos se deben adoptar para cumplir el ENS?

En la disposición transitoria del Real Decreto 3/2010 se articula un mecanismo escalonado para la adecuación a lo previsto en el Esquema Nacional de Seguridad de manera que los sistemas de las administraciones deberán estar adecuados a este Esquema en unos plazos en ningún caso superiores a 48 meses desde la entrada en vigor del mismo.

Una adecuación ordenada al Esquema Nacional de Seguridad requiere el tratamiento de las siguientes cuestiones:

- Preparar y aprobar la política de seguridad, incluyendo la definición de roles y la asignación de responsabilidades.
- Categorizar los sistemas atendiendo a la valoración de la información manejada y de los servicios prestados.
- Realizar el análisis de riesgos, incluyendo la valoración de las medidas de seguridad existentes.
- Preparar y aprobar la Declaración de aplicabilidad de las medidas del Anexo II del ENS.
- Elaborar un plan de adecuación para la mejora de la seguridad, sobre la base de las insuficiencias detectadas, incluyendo plazos estimados de ejecución.
- Implantar operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad correspondiente.



5.2. ¿Existe algún modelo de Política de Seguridad que pueda servir de referencia?

Los aspectos principales del contenido de la Política de Seguridad se apuntan en el Anexo II del ENS, en la medida de seguridad [org.1]. A saber:

> *"La política de seguridad será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el artículo 11, y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:*
> *a) Los objetivos o misión de la organización.*
> *b) El marco legal y regulatorio en el que se desarrollarán las actividades.*

c) Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
d) La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso."

5.3. ¿Cuál es el impacto del ENS en los sistemas actuales?

En la disposición transitoria del Real Decreto 3/2010 se articula un mecanismo escalonado para la adecuación a lo previsto en el Esquema Nacional de Seguridad de manera que los sistemas de las administraciones deberán estar adecuados a este Esquema en unos plazos en ningún caso superiores a 48 meses desde la entrada en vigor del mismo.

5.4. Habiendo concluido el plazo previsto en el ENS para redactar y aprobar el Plan de Adecuación al ENS, ¿es necesaria su realización?

Naturalmente.

Que la Disposición Transitoria del ENS prescriba que, si a los doce meses de la entrada en vigor del Esquema Nacional de Seguridad, hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un plan de adecuación que marque los plazos de ejecución de lo prescrito en el ENS, no significa que, transcurridos los antedichos doce meses, no haya que realizar el citado Plan.

Obsérvese que, en esencia, las actividades contempladas en el Plan de Adecuación, tal y como se enuncian en la Guía CCN-STIC 806, siempre constituyen el punto de partida de todo proceso de adecuación legal de los Sistemas de Información de las organizaciones públicas a lo dispuesto en el ENS.

5.5. ¿Se puede hacer un Plan de Adecuación sin incluir la Política de Seguridad?

Rotundamente, no.

La redacción –y aprobación- de la Política de Seguridad de la organización es una condición previa e indispensable para abordar un proceso de conformidad legal al ENS coherente y con garantías de éxito.

5.6. ¿Se puede aprobar una Política de Seguridad sin contemplar la Estructura de Seguridad de la Organización de la Seguridad?

No tendría sentido.

Obsérvese que una Política de Seguridad contiene, necesariamente, la estructura organizativa encargada de dirigir y materializar su implantación, y velar por su cumplimiento.

Esto no significa que la antedicha Estructura de Seguridad deba ser rígida o estar totalmente dimensionada desde un principio. Suele suceder con frecuencia que, tras el preceptivo Análisis de Riesgos y la ulterior Declaración de Aplicabilidad, se llegue a la conclusión de que la adopción coherente de determinadas medidas de seguridad requiere el concurso de elementos nuevos en la Estructura de Seguridad de la organización, no contemplados en un primer momento.

5.7. ¿Debe publicarse en la Sede Electrónica del organismo en cuestión el Plan de Adecuación al ENS?

La Disposición Transitoria Primera (Adecuación de sistemas y servicios) del ENS, señala la obligación de contar (antes del 30 de enero de 2011, fecha en la que se cumplen los primeros doce meses tras la entrada en vigor de la norma) del preceptivo Plan de Adecuación de los sistemas y servicios que sean objeto del ENS. Nada prescribe la norma, sin embargo, en relación con la publicación del citado Plan de Adecuación, que sí debe ser aprobado por los órganos superiores del organismo.

Obsérvese, además, que la publicación del Plan de Adecuación en la Sede Electrónica del organismo sería claramente contraproducente desde el punto de vista de la seguridad, toda vez que se estarían dando "pistas" *urbi et orbi* respecto del nivel de seguridad de los sistemas de información del organismo, cuestión nada deseable y que vendría a introducir riesgos adicionales.

5.8. ¿Puede realizarse un único Plan de Adecuación para varios Sistemas de Información?

En todo lo que sea común, **no hay inconveniente en que el Plan de Adecuación contemple, de manera única, aquellos aspectos de seguridad comunes** que pudieran afectar a una multiplicidad de sistemas y servicios, siempre que, cuando así fuere demandado o pertinente, se pudiera analizar separadamente cada uno de ellos y analizar su grado de adaptación con relación a la planificación realizada.

5.9. ¿Cómo debe ser el Plan de Adecuación al ENS?, ¿quién debe responsabilizarse de su cumplimiento?, ¿qué sucede cuándo la explotación de los servicios está encomendada a un departamento horizontal, que atiende a varios organismos?

En primer lugar, debemos entender que si cada Centro Directivo es el responsable último de la prestación de los servicios que tiene encomendados, **es precisamente cada Centro Directivo el que debe asumir la responsabilidad de la gobernanza de la ejecución del Plan de Adecuación** (así como del preceptivo Análisis de Riesgos y la aceptación de la subsiguiente Declaración de Aplicabilidad).

Una vez desarrollado el Análisis de Riesgos (por cada sistema/servicio o conjunto homogéneo de ellos) y obtenida la correspondiente Declaración de Aplicabilidad, **será también responsabilidad del Centro Directivo en cuestión asegurarse de que las medidas de seguridad correspondientes** (y dimanantes de la Declaración de Aplicabilidad previa) se adoptan convenientemente, según lo disponga el correspondiente Plan de Adecuación; adopción de medidas de seguridad que, en algún caso (especialmente, las de naturaleza técnica), recaerá en el Departamento de Explotación (pudiendo ser este un Departamento horizontal que preste servicio a varios organismos, Centros Directivos, unidades administrativas complejas, etc.)

Cuando esto sea así, es conveniente que estos **compromisos y competencias se plasmen por escrito,** adoptando la forma administrativa que corresponda a cada caso, con la instrucción/refrendo del superior jerárquico común a los organismos implicados (clientes internos) y al Departamento de Explotación Horizontal (proveedor interno).

6. LAS GUÍAS STIC DEL CCN

6.1. ¿Es obligatorio para las AA.PP. seguir lo que se indica en las Guías STIC del CCN?

El art. 29 del ENS señala la utilidad de las Guías CCN-STIC. En concreto, dice: *"Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones."*

No se trata, por tanto, de normas imperativas, sino de la expresión de metodologías y recomendaciones para el adecuado cumplimiento de lo dispuesto en el ENS. Recomendaciones que tendrán especial significación para aquel organismo administrativo afectado por un incidente grave de seguridad, motivado por la inobservancia de las recomendaciones descritas.

6.2. ¿Qué Guías STIC hay publicadas? ¿Cómo se puede acceder a ellas?

El CCN mantiene el repositorio de Guías-STIC, permanentemente actualizado, en el siguiente enlace: https://www.ccn-cert.cni.es/

7. LA CATEGORIZACIÓN DE LOS SISTEMAS

7.1. ¿En qué consiste la categorización de los sistemas para la adopción de medidas de seguridad?

La **proporcionalidad** es uno de los principios del ENS. Es necesario **categorizar** los sistemas para determinar las medidas de seguridad, que deben ser proporcionadas a la naturaleza de la información que se maneja, de los servicios que se prestan y de los riesgos a los que están expuestos.

Para ello, se contempla la categorización de los sistemas en **tres escalones**, en función del impacto que tendría un incidente que afectara a la seguridad de la información o los servicios, en alguna de las dimensiones de seguridad: autenticación, integridad, confidencialidad, disponibilidad y trazabilidad.

Este impacto se mide atendiendo a la repercusión que tendría el incidente respecto al logro de los objetivos, a la protección de los activos, al cumplimiento de las obligaciones de servicio por parte del departamento correspondiente y al respeto a la legalidad y a los derechos del ciudadano.

7.2. ¿Cómo se categorizan los sistemas?

Véase el Anexo I del ENS. Allí se indican los pasos a seguir.

7.3. En el Anexo I del ENS se hace referencia en muchas ocasiones al "incumplimiento formal" y al "incumplimiento material" de una ley, lo que condicionaría el nivel de seguridad que le correspondería a la dimensión de que se trate.

Sin pretender examinar todas las posibilidades y consecuencias jurídicas de ambos términos, diremos, a los efectos del ENS, lo siguiente:

- Se entiende que existe **incumplimiento material** de una ley, cuando el obligado a observarla no lo hace. Es decir: no cumple con la obligación expresada en la norma y, por consiguiente, no se alcanza el objetivo perseguido por la misma.

- Se entiende que existe **incumplimiento formal** de una ley, cuando el obligado a llega efectivamente a cumplirla, pero haciéndolo sin acomodarse al procedimiento explícitamente señalado en la norma (o implícitamente contemplado por ella). En este caso, por tanto, puede alcanzarse el objetivo perseguido por la norma, pero no de la manera (forma) que prescribe el precepto. En general, se trata de un incumplimiento menos grave que el anterior.

8. EL ANÁLISIS DE RIESGOS Y LA GESTIÓN DE RIESGOS

8.1. ¿Es necesario realizar un Análisis de Riegos, en sentido estricto? ¿No bastaría con usar la experiencia de los técnicos del organismo para determinar qué medidas son las más oportunas en cada caso?

La excesiva confianza en las capacidades personales y en la experiencia es, en sí misma, un riesgo.

Aunque nuestra experiencia en materia de Seguridad de la Información sea dilatada, debemos entender que los procesos de Análisis de Riesgos, realizados adecuadamente, se llevan a cabo usando metodologías contrastadas que evitan que un exceso de confianza nos conduzca a errores, imprecisiones, olvidos, etc., que podrían tener consecuencias desastrosas para nuestros sistemas o servicios.

Todos los modelos y referentes de seguridad -nacionales e internacionales- coinciden en sostener que el edificio de la seguridad y, en definitiva, la confianza, se construyen sobre la base del Análisis y la Gestión de Riesgos. ¿Cómo podría modularse, de no ser así, el equilibrio entre la información que se maneja, los servicios que se prestan, los riesgos a los que están expuestos y la adopción de las medidas adecuadas y proporcionadas para la protección de la información y los servicios?

Obsérvese que, incluso cuando se seleccionan las medidas apropiadas, también es necesario graduarlas o asignarles un determinado nivel. (Por ejemplo, optar por usar un mecanismo de usuario/contraseña, tarjeta con certificados o autenticación con biometría, en el acceso a un Sistema de Información).

Podemos afirmar que el Análisis y la Gestión de Riesgos son la base de la Seguridad TIC. Las Directrices de seguridad de la OCDE, las normas internacionales ISO/IEC 27001/27002, las normas NIST, etc., todas ellas sustentan su aplicación a un preceptivo análisis y ulterior gestión de riesgos.

Para obtener una información más completa de las prácticas europeas habituales en Gestión de Riesgos, puede consultarse la página web http://www.enisa.europa.eu/act/rm

Por este motivo, el art. 6 del ENS señala como obligatorio, para todos los sistemas afectados por el ENS, el desarrollo de un Análisis de Riesgos, al que deberá seguir el correspondiente proceso de Gestión de Riesgos (art. 13).

Realizar un Análisis y Gestión de Riesgos no es, por tanto, una medida opcional: es una exigencia de obligado cumplimiento.

8.2. Herramientas para el Análisis de Riesgos

Usar una herramienta, que nos sirva de ayuda para desarrollar eficazmente un Análisis de Riesgos, es sin duda una buena opción.

Añadiremos, no obstante, un par de precisiones sobre el uso de tales herramientas:

1. Conviene que la herramienta de Análisis de Riesgos esté suficientemente contrastada, mejor aún si existe una comunidad amplia de usuarios (públicos y privados) que la

usan con regularidad y que tienen la posibilidad de intercambiar sus experiencias sobre ella.

2. En el caso de las AA.PP. es especialmente importante que tales herramientas estén basadas en la metodología MAGERIT, en su calidad de método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos, de aplicación en la Administración General del Estado, Autonómica y Local.

En este sentido, debemos señalar que la herramienta PILAR, suministrada gratuitamente por el CCN a todas las AA.PP. españolas, se ha mostrado como una ayuda extraordinariamente eficaz en tal sentido.

Finalmente, hay que mencionar los cursos on-line y presenciales sobre Seguridad de la Información, que son accesibles a través del Portal del CCN (https://www.ccn.cni.es/), y que constituyen una ayuda de primera magnitud como elemento de apoyo en la implantación de Sistemas de Seguridad en nuestras AA.PP.

8.3. La preceptiva Declaración de Aplicabilidad, ¿ha de realizarse por Sistema de Información o por Áreas de Negocio?

La Declaración de Aplicabilidad es uno de los elementos que se obtienen como resultado de un Análisis de Riesgos previo. Por tanto, como su propio nombre indica, la Declaración de Aplicabilidad deberá aplicarse al Sistema de Información que le ha dado origen.

En términos prácticos, podrá realizarse un Análisis de Riesgos para todo el conjunto de sistemas y, a posteriori, desarrollar una o varias Declaraciones de Aplicabilidad, asignando a cada una de ellas los activos que trate cada sistema independiente.

La posibilidad coherente de realizar un único Análisis de Riesgos se da cuando todos los Sistemas de Información sometidos al Análisis de Riesgos pertenezcan al mismo **Dominio de Seguridad**, es decir, aquel conjunto de sistemas sometidos a una Política de Seguridad de la Información común, esto es: homogéneos desde el punto de vista de medidas que hay que aplicar.

La herramienta PILAR, distribuida por el CCN, permite este estudio separado por dominios de seguridad.

A efectos prácticos, puede resultar útil desarrollar primero los sistemas horizontales (infraestructuras compartidas), para seguir con los sistemas verticales, que pueden ir añadiéndose como “familia de servicios”.

9. LA AUDITORÍA DE LA SEGURIDAD

9.1. ¿Contempla el ENS algún mecanismo de auditoría?

El ENS alienta y propicia una **gestión continua de la seguridad**. Todas las actuaciones deben estar formalizadas permitiendo una auditoría de la seguridad, prevista en el artículo 34 del ENS.

Esta auditoría de la seguridad se describe en el Anexo III del ENS, indicándose que la seguridad de los sistemas de información – que debe estar formalizada por medio de un sistema de gestión de seguridad de la información- debe ser auditada, al menos cada dos años, para las categorías media y alta.

Como resultado de esta auditoría, se determinarán las posibles deficiencias existentes y deberán ponerse en marcha las correspondientes acciones correctoras por el Responsable de Seguridad.

9.2. ¿Es necesario realizar la auditoria de la seguridad por un auditor independiente de la organización? ¿Es posible realizar esta declaración de conformidad valiéndose de una autoevaluación respecto del Anexo II del ENS?

Cuando se están evaluando sistemas/servicios cuya categoría sea de nivel MEDIO o ALTO, **la norma señala que se hace necesario pasar una auditoría bienal, realizada por personal (cualificado, obviamente) independiente del servicio/sistema que esté auditando** (véase la definición de "auditoría de la seguridad", contenida en el Glosario del ENS).

Por tanto, de esta interpretación, parece quedar claro que aquellas personas que han tomado parte en el diseño, desarrollo, explotación, etc., del sistema o servicio de que se trate, no gozan de las aconsejables garantías de imparcialidad que requiere una auditoría con las debidas garantías (exigencia que aparece, de manera análoga, en los requisitos de las auditorías internas en la norma ISO 27001).

Esta exigencia se rebaja cuando se están evaluando sistemas categorizados como de nivel BAJO, en cuyo caso el ENS no prescribe ninguna auditoría, sino una auto-evaluación, que (salvaguardando el nivel de conocimiento exigido que deben poseer los profesionales que la realicen) no imponen la exigencia anterior.

Por tanto, si la Responsabilidad de la Seguridad está asignada a una unidad administrativa unipersonal o Pluripersonal con un único responsable (siendo, por tanto, la encargada de adoptar y gestionar las medidas de seguridad que sean preceptivas en cada caso), no podrá ser esa misma unidad administrativa quién realice las antedichas auditorías.

10. CERTIFICACIONES

10.1. ¿Quién certifica que un determinado producto cumple funcionalmente con las exigencias de seguridad que se requieren?

El **CCN**, como Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (según lo dispuesto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional), emite esta certificación funcional en base a criterios establecidos y reconocidos como estándar internacional: los llamados "*Information Technology Security Evaluation Criteria (ITSEC)*" y "*Common Criteria for Information Technology Security Evaluation*", estos últimos publicados también como norma ISO/IEC 15408.

Esta certificación es la culminación de un proceso de evaluación de las funciones de seguridad de un producto o sistema (objeto de evaluación) que, siguiendo una metodología, también estándar, realiza un laboratorio independiente, acreditado y capacitado técnicamente para tal fin. Se trata de comprobar que el objeto de evaluación realiza correcta y eficazmente la funcionalidad de seguridad que se describe en su documentación.

El ámbito de actuación del Organismo de Certificación comprende a las entidades públicas o privadas que quieran ejercer de laboratorios de evaluación de la seguridad de las TI en el marco del Esquema, y a las entidades públicas o privadas fabricantes de productos o sistemas de TI que quieran certificar la seguridad de dichos productos en el marco del Esquema y

cuando dichos productos o sistemas sean susceptibles de ser incluidos en el ámbito de actuación del Centro Criptológico Nacional.

Tanto la acreditación de los laboratorios de evaluación como la certificación de los productos y sistemas se realizan de acuerdo a lo dispuesto en el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado por la Orden PRE/2740/2007, de 19 de septiembre, y en los procedimientos propios del Esquema, todos públicos, establecidos por el Organismo de Certificación.

10.2. ¿Existe alguna certificación que acredite la adecuación al ENS por parte de un organismo público?

En la actualidad no existe tal certificación, emitida por un organismo público.

Nada impide, sin embargo, que empresas privadas especializadas, con la cualificación adecuada, a instancias del organismo público de que se trate, y tras pasar con éxito el organismo público la Auditoría a que se refiere el ENS, puedan emitir un certificado de conformidad , con el alcance temporal y ámbito que se determine.

Este certificado es una declaración de naturaleza privada, teniendo los efectos que, a los documentos privados, confiere nuestra legislación.

Finalmente, hay que señalar que la Guía CCN-STIC-809, hablando de los distintivos de seguridad, señala que la publicidad de estos distintivos a los que sean acreedores los sistemas, los órganos o las entidades de derecho público respecto a los mismos, reunirán los requisitos establecidos para la declaración de conformidad, referidas al distintivo de seguridad correspondiente, añadiendo, de forma clara, los datos relativos a la entidad que los emite y el ámbito a que se refiere. Entre los distintivos se incluirán certificaciones de accesibilidad, interoperabilidad, menciones de calidad de cualesquiera de las Administraciones públicas, de organizaciones internacionales o de organismos privados.

11. MEDIDAS DE SEGURIDAD

11.1. ¿Cómo se determinan las medidas de seguridad que hay que aplicar?

De acuerdo con el Anexo II del ENS la secuencia de actuaciones es la siguiente:_

1. Para la selección de las medidas de seguridad se seguirán los pasos siguientes:

a) Identificación de los tipos de activos presentes.

b) Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.

c) Determinación del nivel correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.

d) Determinación de la categoría del sistema, según lo establecido en el Anexo I.

e) Selección de las medidas de seguridad apropiadas de entre las contenidas en este Anexo, de acuerdo con las dimensiones de seguridad y sus niveles, y, para determinadas medidas de seguridad, de acuerdo con la categoría del sistema.

2. A los efectos de facilitar el cumplimiento de lo dispuesto en este anexo, cuando en un sistema de información existan sistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse la información y los servicios afectados.

3. La relación de medidas seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad del sistema.

11.2. mp.com.2

¿Qué debe entenderse por dominio de seguridad? ¿Cómo proteger sistemas interconectados?

Debemos entender por **Dominio de Seguridad** aquel conjunto de sistemas sometidos a una Política de Seguridad de la Información común, esto es: homogéneos desde el punto de vista de medidas que hay que aplicar.

La medida mp.com.2 señala, en esencia, que el enlace entre los sistemas interconectados debe estar cifrado cuando se materializa a través de redes ajenas, por ejemplo: a través de redes públicas.

Además de lo anterior, cuando se interconecten sistemas instalados en diferentes dominios de seguridad, bajo distintas responsabilidades y en los casos en que sea necesario, las medidas de seguridad locales se acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema.

11.3. ¿Es de aplicación el ENS al correo electrónico corporativo?

En la medida en que el correo electrónico corporativo se utilice -en todo o en parte- para la prestación de servicios o el desarrollo de las competencias o potestades de la entidad, resultará de aplicación lo dispuesto en el ENS.

Por otro lado, debemos tener presente lo dispuesto en el ENS en relación con la protección del correo electrónico, cuando dispone:

5.8.1 Protección del correo electrónico (e-mail) [mp.s.1].

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

a) La información distribuida por medio de correo electrónico, se protegerá, tanto en el cuerpo de los mensajes, como en los anexos.
b) Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.
c) Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:
1.º Correo no solicitado, en su expresión inglesa «spam».
2.º Programas dañinos, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
3.º Código móvil de tipo «applet».
d) Se establecerán normas de uso del correo electrónico por parte del personal determinado. Estas normas de uso contendrán:
1.º Limitaciones al uso como soporte de comunicaciones privadas.
2.º Actividades de concienciación y formación relativas al uso del correo electrónico.

Cuando el servicio de correo electrónico se presta externamente, habrá que asegurar que el prestador del servicio cumple con lo señalado anteriormente, cirunstancia que suele acometerse mediante la suscripción del correspondiente Contrato y Acuerdo de Nivel de Servicio, que se complementará con la facultad de la entidad de auditar la prestación del servicio y la adopción de las preceptivas medidas de seguridad.

12. EL ENS Y LA NORMALIZACIÓN VOLUNTARIA RELATIVA A SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

12.1. ¿Es el ENS compatible con UNE ISO/IEC 27001:2007?, ¿son normas similares?, ¿son complementarias?

El Esquema Nacional de Seguridad es una norma jurídica, el Real Decreto 3/2010, que se encuentra al servicio de la realización del derecho de los ciudadanos a relacionarse por medios electrónicos con las Administraciones Públicas establecido en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y es de obligado cumplimiento para las Administraciones Públicas. El ENS , sustentado en principios internacionales de seguridad de la información, trata la PROTECCIÓN de la información, los sistemas y los servicios.

El ENS contempla y exige la gestión continuada de la seguridad, para lo cual cabe aplicar un sistema de gestión. Véanse los principios básicos relativos a 'La seguridad como un proceso integral' (art. 5) y a la 'Reevaluación periódica' (art. 9); los requisitos mínimos relativos a 'Organización e implantación del proceso de seguridad' (art. 12), 'Mejora continua del proceso de seguridad' (art. 26); véase también el anexo III sobre Auditoría de la seguridad que desarrolla el artículo 34 y que incluye entre los términos considerar en la auditoría de la seguridad de los sistemas de información de una organización "f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección."

Para satisfacer los citados principios básicos y requisitos mínimos se puede aplicar un modelo de tipo PCDA para lo cual la normalización voluntaria ofrece herramientas como la norma UNE ISO/IEC 27001:2007 "Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. (ISO/IEC 27001:2005)".

Como es sabido, la norma UNE ISO/IEC 27001:2007 contiene los requisitos para la construcción (y ulterior certificación, en su caso) de un Sistema de Gestión de Seguridad de la Información. En el Anexo A de esta norma se enumeran los controles que desarrolla la norma ISO 27002. Ambas normas, por tanto, deben examinarse de manera complementaria.

Por tanto, en conclusión:

- El ENS es una norma jurídica, el Real Decreto 3/2010, que se encuentra al servicio de la realización de derechos de los ciudadanos y es de aplicación obligatoria a todas las Administraciones Públicas.
- El ENS que trata la 'protección' de la información y los servicios, contempla y exige la gestión continuada de la seguridad, para lo cual cabe aplicar un sistema de gestión.
- La normalización nacional e internacional, de cumplimiento voluntario, ofrece herramientas como la norma UNE ISO/IEC 27001:2007 que es una norma de 'gestión' que contiene los requisitos para la construcción de un sistema de gestión de seguridad de la información, contra la que puede, en su caso, de forma voluntaria, certificarse una entidad (pública o privada) mediante un proceso de auditoría realizado por un auditor certificado externo.
- Si bien cabe señalar que aquellas organizaciones que se encuentren certificadas contra ISO 27001 tienen una buena parte del camino recorrido para lograr su conformidad con el ENS, toda vez que las medidas de protección que señala el ENS coinciden, en lo sustancial, con los controles que prevé la norma internacional.

- Por tanto, el Esquema Nacional de Seguridad y la norma UNE ISO/IEC 27001:2007 difieren en su naturaleza, en su ámbito de aplicación, en su obligatoriedad y en los objetivos que persiguen.

12.2. ¿Cuál es la relación entre el ENS y la norma UNE-ISO/IEC 27002:2009?

La norma UNE-ISO/IEC 27002:2009 es un conjunto de controles de seguridad para sistemas de información genéricos.

Aunque muchas de las medidas de seguridad indicadas en el anexo II del ENS coinciden con controles de UNE-ISO/IEC 27002:2009, el ENS es más preciso y establece un sistema de protección proporcionado a la información y servicios a proteger para racionalizar la implantación de medidas de seguridad y reducir la discrecionalidad.

La norma **UNE-ISO/IEC 27002:2009** carece de esta proporcionalidad, quedando a la mejor opinión del auditor que certifica la conformidad con la norma UNE ISO/IEC 27001:2007.

Por otra parte, el ENS contempla diversos aspectos de especial interés en relación con la protección de la información y los servicios de administración electrónica (por ejemplo, aquellos relativos a la firma electrónica) no recogidos en la norma **UNE-ISO/IEC 27002:2009**.

12.3. Teniendo mi Servicio/Sistema certificado contra la norma UNE ISO/IEC 27001:2007, ¿debo entender que ya estoy cumpliendo con el ENS?

Rotundamente, no.

Como ya se ha explicado en una pregunta anterior, el Esquema Nacional de Seguridad y la norma UNE ISO/IEC 27001:2007 difieren en su naturaleza, en su ámbito de aplicación, en su obligatoriedad y en los objetivos que persiguen. El ENS es una norma jurídica, el Real Decreto 3/2010, que se encuentra al servicio de la realización de derechos de los ciudadanos, de aplicación obligatoria a todas las Administraciones Públicas, y que trata la 'protección' de la información y los servicios. ISO 27001 es una norma de **gestión** que indica cómo llegar a tener un Sistema de Gestión de Seguridad de la Información (para ello se apoya en las recomendaciones de ISO 27002). Mientras que la norma UNE ISO/IEC 27001:2007, de carácter voluntario, es una norma de 'gestión' que contiene los requisitos para la construcción de un sistema de gestión de seguridad de la información, contra la que puede, en su caso, de forma voluntaria, certificarse una entidad.

Sin embargo, cabe precisar que quién haya certificado su Servicio/Sistema conforme a la norma UNE ISO/IEC 27001:2007 está muy cerca de asegurar el cumplimiento del ENS, cuya conformidad debe alcanzarse siguiendo la metodología descrita en los Anexos I, II y III del Real Decreto 3/2010.