Guía de Seguridad de las TIC
CCN-STIC 806

Plan de Adecuación al ENS

Junio 2020

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.06.16 16:30:19 +02'00'

NIPO: 075-11-053-3

Fecha de Edición: junio de 2020

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Junio de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. OBJETIVO Y ALCANCE DE LA GUÍA

Esta guía va dirigida a las entidades del ámbito de aplicación del Real decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), con el objeto de proporcionar unas líneas a seguir para abordar el proceso de adecuación e implantación al ENS de los sistemas de información concernidos.

El proceso de implantación comenzará con la elaboración del Plan de Adecuación, lo que cimentará el proceso de la gestión continuada de la seguridad en la entidad mediante la designación de roles, la constitución de órganos de seguridad, así como la adquisición de compromisos de seguridad y de implantación que se reflejarán en la Política de Seguridad de la Información y el Plan de Adecuación, respectivamente.

Como es sabido, y así se recoge en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, las entidades públicas deberán tener en cuenta que cuando recurran a servicios externalizados estos deberán ser conformes al ENS, en los niveles y categoría de seguridad determinada por la entidad contratante.

Una vez finalizado este hito se llevarán a cabo las tareas de implantación de medidas de seguridad planificadas con el objetivo final de superar el proceso de Certificación del sistema, iniciando así el ciclo de mejora, mediante la revisión y mejora continua de los procesos de seguridad.

2. PLAN DE ADECUACIÓN AL ENS

El Plan de Adecuación, es el punto de partida para abordar el proceso de implantación del ENS y está compuesto por las siguientes actuaciones:

- Elaborar la **Política de Seguridad de la Información y la Normativa Interna correspondiente..**
- **Identificar los servicios** y **categorizar los sistemas de información**: valoración de servicios prestados e información tratada.
- **Determinación de la Declaración de Aplicabilidad provisional.**
- Realizar el **Análisis de Riesgos.**
- Elaborar la D**eclaración de Aplicabilidad** definitiva
- Desarrollar un **Plan de mejora de la seguridad** en base al informe de insuficiencias detectadas.

Con su elaboración se identificarán, por un lado, las personas u órganos responsables de que la implantación del ENS se lleve a cabo en la entidad y, por otro, las medidas de seguridad que será necesario implantar, con la definición de hitos y la identificación de los recursos necesarios para llevarlas a cabo.

El Plan de Adecuación será elaborado por el Responsable de Seguridad. Si el Responsable de Seguridad no está nombrado oficialmente, hará sus funciones, de

forma temporal, quien la Dirección designe, anexándose al plan de adecuación su designación formal, que incluirá las funciones temporalmente asignadas y el periodo máximo de ejercicio de estas funciones con carácter temporal.

2.1 Política de Seguridad de la Información y Normativa Interna.

La **Política de Seguridad** es un documento de alto nivel, mediante el cual la entidad define su compromiso respecto a la seguridad de la información y la de los servicios prestados. En esta Política se describirán los mecanismos implementados para la gestión continuada de la seguridad y se establecerán los responsables de velar por su cumplimiento. Entre otros contenidos, se contemplarán los siguientes:

- El compromiso de la organización con el cumplimiento de todo el articulado del Real Decreto ENS (principios básicos y requisitos mínimos).
- El marco legal y regulatorio.
- Referencia a la forma en la que la organización da cumplimiento a la normativa de protección de datos.
- Los roles de seguridad designados, sus funciones, el proceso de designación y renovación, siendo como mínimo:
    - Responsable de la Información y los Responsables de los Servicios, para aquellos sistemas de información que no sean operados por terceros públicos o privados.
    - Responsable de Seguridad y Responsable del Sistema (siempre que sea posible, se encontrarán diferenciados), la estructura del Comité de Seguridad y sus funciones.
- Los mecanismos que se han implementado para que los roles de seguridad y el Comité actúen de forma coordinada y se puedan resolver los conflictos que pudieran surgir, que podrá coincidir con el Comité de Seguridad.
- La forma en la cual se va a desarrollar la Política de Seguridad, con indicación del soporte documental que la articulará haciendo referencia al desarrollo de un sistema de gestión de la seguridad de la información documentado y con un proceso regular de aprobación. También se indicará las revisiones que se realizarán de la política y su periodicidad.

Las entidades públicas podrán elaborar su propia Política de Seguridad o bien acogerse a la Política de la entidad de orden superior, en el caso de organismos dependientes, para aquellos servicios que son proporcionados por estas. En este caso, el Responsable de Seguridad y el Responsable del Sistema podrán ser los designados por estas. Por el contrario, los Responsables de los Servicios y los Responsables de la Información, serán designados en el Organismo en concreto.

Si el organismo dispone de una Política de Seguridad conforme a lo que se pide en el Anexo II del ENS, sección [org.1], ésta se identificará y anexará al plan de adecuación.

Si se dispone de una Política de Seguridad, pero no satisface los requisitos del Anexo II, sección [org.1]:

- Se identificará la política de aplicación.
- Se anexará al plan de adecuación.
- En el plan de mejora de la seguridad se hará constar cómo se planea adaptar la política a las exigencias del Anexo II.

Si no se dispone de una Política de Seguridad, en el plan de mejora de la seguridad se hará constar cómo se planea desarrollar la política de acuerdo a las exigencias de Anexo II.

Como apoyo adicional a estas actividades, puede utilizar las guías "CCN-STIC 801. Responsabilidades y funciones" y "CCN-STIC 805 Política de Seguridad de la Información".

La **Normativa Interna** comprenderá aquel conjunto de normas, de carácter interno a la organización, que prescribirá el comportamiento exigible a los usuarios del sistema de información en lo relativo al uso de los medios electrónicos que la entidad pone a su disposición.

La Guía CCN-STIC 821 Normas de Seguridad y sus Apéndices contienen modelos que pueden usarse a estos fines.

2.2 Identificación de los servicios, categorización de los sistemas y Declaración de Aplicabilidad provisional.

Suele ser una buena práctica, comenzar la adecuación identificando los servicios prestados por la entidad sustentados en los sistemas de información que habrán de ser conformes con el ENS.

La cumplimentación detallada del modelo de Ficha de Servicios que se incluye en el Anexo I servirá para disponer, ordenadamente, de los datos esenciales de cada servicio prestado, incluyendo los tipos de información tratados y los sistemas de información sobre los que se prestan, así como una valoración inicial del nivel de seguridad de cada una de las dimensiones de seguridad aplicables al servicio/información de que se trate.

Este procedimiento servirá eventualmente para detectar la conveniencia o no de segregar varios servicios en sistemas de información diferenciados.

Hecho lo anterior, la categoría de seguridad del sistema de información será la resultante de la valoración de los servicios analizados y de la información tratada por cada uno de ellos.

En base a ello, podremos obtener una Declaración de Aplicabilidad (relación de medidas aplicables del Anexo II del ENS) provisional.

Para ayudar en dicha identificación y valoración puede apoyarse en la guía "CCN-STIC 803 ENS. Valoración de los sistemas" y en su "ANEXO I. Valoración de sistemas en Universidades".

2.2.1 Información tratada

Habiendo identificado el sistema de información en cuestión, además de lo anterior, es conveniente disponer de una relación detallada de la información tratada por dicho sistema, junto con su valoración según lo establecido en el Anexo I del Esquema Nacional de Seguridad.

Pueden darse varias causas que impidan alcanzar plenamente el objetivo propuesto en el párrafo anterior:

- se carece de una Política de Seguridad, o esta es insuficiente,
- no está nombrado el responsable de alguna de las informaciones tratadas,
- no está aprobada formalmente la valoración de la información.

En tales casos, la valoración la realizará y argumentará el Responsable de Seguridad, a su mejor criterio, dejando constancia de los motivos o razonamientos. Esta valoración sólo es vinculante para el organismo mientras no se disponga de la valoración formal. Deberá constar un plazo límite para disponer de la valoración formal.

Si el sistema maneja datos de carácter personal, el plan de adecuación incluirá una relación detallada de dichos datos y alineará las medidas del ENS a su protección en consonancia con lo señalado en la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, atendiendo a lo preceptuado en el Reglamento (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[1].

2.2.2 Servicios prestados

Análogamente, a partir de la Ficha de servicios, se dispondrá de una relación detallada de los servicios que se prestan, junto con su valoración según lo establecido en el Anexo I del Esquema Nacional de Seguridad.

Pueden darse varias causas que impidan alcanzar plenamente el objetivo propuesto en el párrafo anterior:

- Se carece de una Política de Seguridad, o esta es insuficiente.
- No está nombrado el responsable de alguno de los servicios prestados.
- No está aprobada formalmente la valoración de la información.

[1] Recordar que, en tanto no sea transpuesta a nuestro ordenamiento jurídico la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, siguen vigentes, exclusivamente para el tratamiento de este tipo de datos, la Ley Orgánica 15/1999 y el Real Decreto 1720/2007 que la desarrolla, tal y como señala la Disposición transitoria cuarta de la LOPDGDD.

En tales casos, la valoración la realizará y argumentará el Responsable de Seguridad, a su mejor criterio, dejando constancia de los motivos o razonamientos. Esta valoración sólo es vinculante para el organismo mientras no se disponga de la valoración formal. Deberá constar un plazo límite para disponer de la valoración formal.

2.2.3 Nivel de seguridad y Categoría de seguridad.

Como se ha señalado, una vez identificados los servicios y la información, se procederá a realizar su valoración en base a lo dispuesto en el Anexo I del RD ENS. Este proceso consiste en la determinación del impacto que tendría en la organización un incidente de seguridad que afectara a la información tratada o a los servicios prestados en cada una de las dimensiones de seguridad (Confidencialidad [C], Integridad [I], Trazabilidad [T], Autenticidad [A], Disponibilidad [D]) y se mide en tres niveles BAJO, MEDIO O ALTO. La valoración de los servicios y la información la realizan sus respectivos responsables, los cuales podrán contar con la opinión del Responsable de Seguridad y/o del Responsable del Sistema. Una vez valorados los servicios e información, nos encontramos en condiciones de proceder a la determinación de la **Categoría del Sistema**, pudiendo ser BÁSICA, MEDIA o ALTA, de acuerdo a lo indicado en el Anexo I del Real Decreto ENS. La categorización de los sistemas se plasmará en un documento que deberá ser aprobado por el Responsable del Sistema.

2.3 Análisis de riesgos

El **análisis de riesgos** se desarrollará conforme a lo dispuesto en el art. 13 y Anexo II (sección [op.pl.1]) del ENS, para la categoría establecida para el sistema. Para su realización se recomienda utilizar la metodología MAGERIT - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica[2] -. Esta metodología permite estudiar los riesgos que soporta un sistema de información, determinando de este modo las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

En el análisis de riesgos se valorarán las salvaguardas presentes en la fecha de aprobación del plan de adecuación.

Para realizar el análisis de riesgos podemos utilizar la herramienta de referencia PILAR, que implementa la metodología MAGERIT, en cualquiera de sus versiones (PILAR, PILAR Basic, µPILAR y online a través de la plataforma INÉS). Las Guías CCN-STIC-470 PILAR, proporcionan manuales de uso en sus diferentes versiones.

2.4 Declaración de aplicabilidad definitiva

Atendiendo a los resultados del anterior análisis de riesgos, en el que se habrán tenido en cuenta las exigencias derivadas de la normativa de protección de datos, el

[2] MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA en http://rm-inv.enisa.europa.eu/methods_tools/m_magerit.html

Responsable de Seguridad elaborará una relación de las medidas del ENS que son de aplicación al sistema (o a cada sub-sistema, si se ha recurrido a una segregación de sistemas), de acuerdo a los valores máximos de seguridad obtenidos en cada una de las dimensiones de seguridad y/o de acuerdo a la categoría del sistema, y las medidas de seguridad adicionales resultante del análisis de riesgos

Habitualmente, se recurrirá a las medidas detalladas en el Anexo II, enriquecidas o matizadas por características determinadas del sistema o exigencias derivadas del tratamiento de datos de carácter personal.

La inaplicabilidad de una medida requerida por el Anexo II, en función de la valoración del sistema, deberá estar motivada.

Cuando se recurra a medidas compensatorias, se indicará el motivo, así como las medidas que sustituye, tal y como se recoge en la Guía CCN-STIC 819 Medidas Compensatorias.

Las medidas se complementarán con aquellas que sean pertinentes a la vista del análisis de riesgos realizado. Téngase en cuenta que, tanto el ENS como la reglamentación de protección de datos de carácter personal, establecen una serie de medidas mínimas que deben ampliarse cuando sea prudente hacerlo.

La Declaración de Aplicabilidad se plasmará en un documento que debe ser aprobado formalmente por el Responsable de Seguridad. Para realizarla podemos tomar como referencia el Informe de Buenas Prácticas CCN-CERT BP/14 Declaración de aplicabilidad ENS y su anexo.

En el caso de las Entidades Locales, se disponen de Perfiles Específicos de Cumplimiento a los pueden acogerse**,** siendo entonces de aplicación la declaración de aplicabilidad asociada a este perfil en concreto. Su adopción deberá estar argumentada formalmente.

Estos perfiles se encuentran en los documentos:

- PCE CCN-STIC 883A Perfil Cumplimiento Específico Ayuntamientos-Abstract.
- PCE CCN-STIC 883B-Perfil Cumplimiento Específico Ayuntamientos - 20.000.
- PCE CCN-STIC 883C- Perfil Cumplimiento Específico Ayuntamientos + 20.000.
- PCE CCN-STIC 883D- Perfil Cumplimiento Específico Diputaciones.

2.5 Plan de mejora de la seguridad

El **informe de deficiencias del sistema (gap analysis)**, recogerá el estado de cumplimiento de las medidas de seguridad, reflejando el nivel actual de madurez de las medidas de la declaración de aplicabilidad. Este informe se puede completar también con aquellas medidas que será necesario implantar para garantizar el cumplimiento de la normativa de protección de datos.

El informe contendrá, por tanto, lo que se consideran riesgos residuales del sistema que deberán ser aceptados formalmente por los Responsables de los Servicios y por los Responsables de la Información.

Si no están designados dichos responsables o si la aceptación del riesgo no es formal, el Responsable de Seguridad tomará la decisión a su mejor criterio, indicando las circunstancias que le llevan a ello y motivando sus decisiones de aceptación, o no, del riesgo residual.

Finalmente, será necesario identificar las tareas que será necesario realizar para subsanar las deficiencias del sistema, planificarlas y asignarles los recursos necesarios (personales y/o económicos, según sea el caso). Las plasmará en un documento denominado **Plan de mejora de la seguridad**, que deberá ser aprobado formalmente por el Comité de Seguridad, comprometiéndose, de este modo la organización con la mejora de la seguridad.

Por tanto:

1. El plan de mejora de la seguridad constará de una serie de actuaciones destinadas a subsanar las deficiencias detectadas.
2. Cada actuación prevista incluirá:
    - Las deficiencias que subsana.
    - El plazo previsto de ejecución, indicando fecha de inicio y fecha de terminación, así como los principales hitos intermedios.
    - Una estimación del coste que supondrá.
3. Las fechas de inicio pueden limitarse al año en que se prevé acometer la actuación.
4. La fecha de terminación se puede calcular en función del tiempo que se ha estimado para ejecutar la actuación.
5. El coste puede ser estimativo o basarse en ofertas ya disponibles.

3. INTERCONEXIÓN DE SISTEMAS

Cuando un sistema maneja información de terceros o presta servicios a terceros, la valoración de la información y los servicios será la determinada por dicho tercero.

Para la realización del Plan de Adecuación, se requiere conocer la valoración realizada por los responsables del otro sistema. Si se carece de dicha valoración, el Responsable de Seguridad establecerá unos valores a su mejor criterio y los hará constar como “compromiso de prestación de servicios”. Si, en el futuro, los responsables del otro sistema elevan las exigencias en materia de seguridad, se recurrirá a la realización de un “plan de adecuación incremental” que contemple las actuaciones encaminadas a subsanar las insuficiencias derivadas del nuevo escenario.

Cuando un sistema utiliza sistemas de terceros para manejar información o para prestar servicios, la valoración propia será impuesta al tercero que colabora, que la

tendrá en cuenta en su propio plan. Si el prestatario está sujeto al cumplimiento del Esquema Nacional de Seguridad, incorporará estos requisitos a su propio plan de adecuación o a su propia declaración de conformidad.

4. ANEXO I. Ficha de Servicio.

Ficha de Descripción del Servicio

Nombre del Servicio	
Código[3]	**Denominación**

Descripción del Servicio

Datos (información) que trata					
Datos personales				**Datos no-personales**	
Dato	**¿Categorías especiales de datos? (S/N)**[4]	**Origen del Dato**	**Destinatarios previstos**	**Dato**	**Origen del Dato**

[3] El código usado será: {SF/SI}nn, siendo SF (Servicio Finalista: descrito en las funciones del organismo), SI (Servicio Instrumental: de apoyo a la consecución de los Servicios Finalistas), nn (desde el 00 al 99)

[4] Datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física. (Art. 9 RGPD)

Tipo de Servicio (Formulario web, aplicaciones, servicio externo, …)

Componentes del servicio	
Componentes del Servicio (servidores virtuales, servidor web, servidores externos,…)	**Ubicación** (CPD, …)

Esquema de la Arquitectura técnica de prestación del Servicio

Dependencias entre Servicios	
¿Depende de otro(s) Servicio(s)?	
Cód. – Nombre del Servicio	**Descripción de la dependencia**
¿Dependen otro(s) Servicio(s) de éste?	
Cód. – Nombre del Servicio	**Descripción de la dependencia**

Responsables
Responsible funcional del Servicio

Aproximación inicial a la valoración de los Niveles de Seguridad				
CONFIDENCIALIDAD (C)	**INTEGRIDAD (I)**	**TRAZABILIDAD (T)**	**AUTENTICIDAD (A)**	**DISPONIBILIDAD (D)**

(D): Tiempo máximo de interrupción del servicio: B-Baja (24 horas) / M-Media (Entre 4 y 24 horas) / A-Alta (Menos de 4 horas)

Asignación de los niveles de seguridad a los servicios finalistas

El Anexo I del ENS señala los criterios para la determinación de los niveles de seguridad, en cada una de las dimensiones.
En concreto, señala:

2. Dimensiones de la seguridad.
A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se tendrán en cuenta las siguientes dimensiones de la seguridad, que serán identificadas por sus correspondientes iniciales en mayúsculas:

a) Confidencialidad (C).
b) Integridad (I).
c) Trazabilidad (T).
d) Autenticidad (A).
e) Disponibilidad (D).

3. Determinación del nivel requerido en una dimensión de seguridad.
Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) Nivel **BAJO**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio limitado:
1º La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque éstas sigan desempeñándose.
2º El sufrimiento de un daño menor por los activos de la organización.
3º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
4º Causar un perjuicio menor a algún individuo, que aun siendo molesto pueda ser fácilmente reparable.
5º Otros de naturaleza análoga.

b) Nivel **MEDIO**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio grave:

1º La reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque éstas sigan desempeñándose.
2º El sufrimiento de un daño significativo por los activos de la organización.
3º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
4º Causar un perjuicio significativo a algún individuo, de difícil reparación.
5º Otros de naturaleza análoga.

c) Nivel **ALTO**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio muy grave:

1º La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.
2º El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.
3º El incumplimiento grave de alguna ley o regulación.
4º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5º Otros de naturaleza análoga.

Cuando un sistema maneje diferentes informaciones y preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

La definición de las **dimensiones de seguridad** son las utilizadas en el Anexo IV-Glosario del ENS. A saber:

Confidencialidad (C)	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
Integridad (I)	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
Trazabilidad (T)	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Autenticidad (A)	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
Disponibilidad (D)	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

ANEXO II. Glosario de términos y abreviaturas

Análisis de riesgos

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal

Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el Reglamento (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.

Información

Caso concreto de un cierto tipo de información.

Information. An instance of an information type. FIPS 199.

Política de seguridad

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos. ENS.

Responsable de la Información

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. CNSS Inst. 4009.

Responsable de la Seguridad

El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

The **Computer Security Program Manager** (and support staff) directs the organization's day-today management of its computer security program. This individual is also responsible for coordinating all security-related interactions among organizational elements involved in the computer security program as well as those external to the organization. NIST Special Publication 800-12.

Information systems security manager (ISSM). Individual responsible for a program, organization, system, or enclave's information assurance program. CNSS Inst. 4009.

Responsable del Servicio

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del Sistema

Persona que se encarga de la explotación del sistema de información.

Information System Owner (or Program Manager). Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. CNSS Inst. 4009, Adapted

Servicio

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de Información

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. ENS.

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. 44 U.S.C., Sec. 3502; OMB Circular A-130, Appendix III.

ABREVIATURAS

ENS	Esquema Nacional de Seguridad

4.1 Referencias

Ley Orgánica 3/2018

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Reglamento UE 2016/697

Reglamento (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

RD 3/2010

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. BOE de 29 de enero de 2010.

RD 4/2010

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

RD 951/2015

Real Decreto 951/2015, de 23 de octubre, de modificación del 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.

Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.