CCN-CERT

BP/14

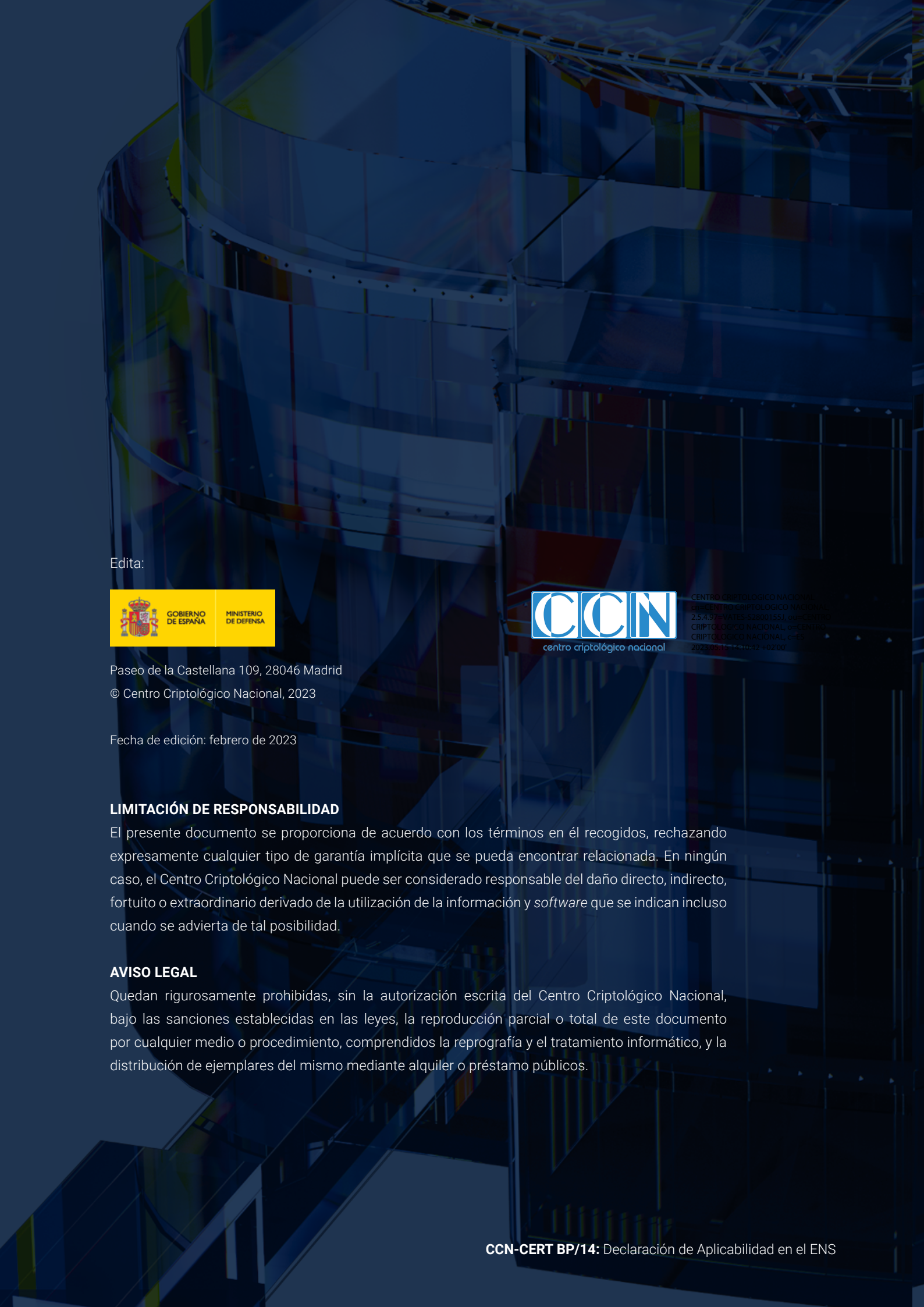
Declaración de Aplicabilidad en el ENS

INFORME DE BUENAS PRÁCTICAS

FEBRERO **2023**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional



Edita:

GOBIERNO DE ESPAÑA · MINISTERIO DE DEFENSA

centro criptológico nacional

Paseo de la Castellana 109, 28046 Madrid

Fecha de edición: febrero de 2023

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

Índice

1. Sobre el CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional Español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el Real Decreto 311/2022 de 3 de mayo.

El CCN-CERT es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y a la Ley 40/2015 de Régimen Jurídico del Sector Público, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. Introducción

La Declaración de Aplicabilidad, en el ámbito del ENS, es el documento en el que se formaliza la relación de medidas de seguridad que resultan de aplicación al sistema de información del que se trate, conforme a su categoría, y que se encuentran recogidas en el Anexo II del Real Decreto 311/2022, de 3 de mayo, que lo regula.

Como se determina en el artículo 38.3 del ENS, las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras medidas compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del Real Decreto 311/2022.

Asimismo, como se señala en la guía CCN-STIC-808 "Verificación del cumplimiento de las medidas en el ENS", se podrán implementar medidas complementarias de vigilancia que complementen y equilibren los requisitos exigibles que se han implementado para determinada medida de seguridad, ya sean base o de refuerzo, cuando éstos no son suficientes, a juicio de la organización, para poder alcanzar el cumplimiento del ENS para dicha medida. También pueden complementar a una medida compensatoria que no consigue igualar o mejorar el riesgo de la medida original. En ocasiones, dichas medidas serán transitorias (limitadas en el tiempo) hasta que se consiga la efectividad plena en la implantación de una medida.

La Declaración de Aplicabilidad, en el ámbito del ENS, es el documento en el que se formaliza la relación de medidas de seguridad que resultan de aplicación al sistema de información del que se trate, conforme a su categoría

Como parte integral de la Declaración de Aplicabilidad, se indicará de forma detallada la correspondencia entre las medidas compensatorias implementadas y las medidas del Anexo II que compensan, al igual que se especificarán las medidas complementarias de vigencia que se hayan podido precisar, siendo objeto de aprobación formal por parte del responsable de seguridad.

El documento formalizado de Declaración de Aplicabilidad será esencial para la elaboración del plan de adecuación y la posterior implementación de las medidas contempladas, y podrá ser analizado por la entidad certificadora y empleado como documento de apoyo durante el proceso de auditoría para la validación del cumplimiento del ENS. Para este fin, es importante que la Declaración de Aplicabilidad indique para cada una de las 73 medidas de seguridad que contempla el ENS, no solo si aplica o no aplica al sistema de información o a la organización, sino, de forma muy resumida, cómo aplica y/o la documentación donde se detalla y, en su caso, porqué no aplica.

El documento formalizado de Declaración de Aplicabilidad será esencial para la elaboración del plan de adecuación y la posterior implementación de las medidas contempladas

3. Procedimiento para definir la Declaración de Aplicabilidad

Para lograr la adecuación de un sistema de información a lo dispuesto en el ENS y poder determinar qué medidas son de aplicación, es necesario proceder a su categorización y seguir las indicaciones especificadas en el Anexo I del ENS.

El proceso de categorización tiene como objeto asignar una categoría BÁSICA, MEDIA o ALTA a los sistemas de información. La categoría de un sistema de información, en materia de seguridad, busca el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, y los riesgos a los que está expuesto, bajo el criterio del principio de proporcionalidad.

Dicho en otras palabras, las medidas de seguridad que se aplicarán al sistema de información, y así constarán en la Declaración de Aplicabilidad, procederán principalmente de la categorización del sistema con resultado de una serie de medidas tasadas (requisitos base y refuerzos obligatorios), pero, en ocasiones, también podrían ser elegibles como consecuencia de acciones de mitigación de riesgos que han sido evaluados como inaceptables (refuerzos opcionales o refuerzos obligatorios para una categoría superior).

La determinación de la categoría se efectúa en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para las dimensiones de la seguridad: **disponibilidad [D], autenticidad [A], integridad [I], confidencialidad [C]** o **trazabilidad [T],** siguiendo el procedimiento establecido en el Anexo I del Real Decreto 311/2022.

El proceso de categorización tiene como objeto asignar una categoría BÁSICA, MEDIA o ALTA a los sistemas de información

3.1. Categorización

La determinación de la categoría de un sistema (BÁSICA, MEDIA o ALTA) se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de dicho sistema de información, con repercusión en la capacidad organizativa para:

a. Alcanzar sus objetivos.
b. Proteger los activos a su cargo, incluyendo la información.
c. Cumplir sus obligaciones diarias de servicio.
d. Respetar la legalidad vigente.
e. Respetar los derechos de las personas.

La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de dicho sistema de información

La valoración de dicho impacto se realiza, además de por cada dimensión de seguridad, de forma individualizada por cada activo del sistema de información, por lo que es necesario disponer de un inventario actualizado de los mismos.

Se recomienda, en primer lugar, proceder a la valoración de los activos esenciales (información y servicios) que son los que van a exigir una valoración más exhaustiva a la hora de establecer los niveles de seguridad de acuerdo a las dimensiones, y que determinarán con ello la categoría del sistema. Los activos esenciales son aquellos que concentran el valor del sistema en materia de seguridad y son la esencia y razón de ser del sistema. El resto de activos darán soporte a los referidos activos esenciales, heredando las valoraciones de éstos en base a su relación de dependencia.

En función de si el activo es un servicio a prestar o información manejada por éstos, conviene centrarse en la valoración de dimensiones de seguridad concretas. Por ejemplo, se recomienda valorar las dimensiones de **confidencialidad** e **integridad (C, I)** para los activos de tipo información, mientras que la dimensión de **disponibilidad (D)** se asocia habitualmente a los activos de tipo servicio.

Las otras dos (2) dimensiones, como son la **autenticidad (A)** y la **trazabilidad (T)**, se asociarán indistintamente a servicios o a información, según mejor convenga a la organización; lo importante es que, de una forma u otra, se contemplen en caso de ser de aplicación.

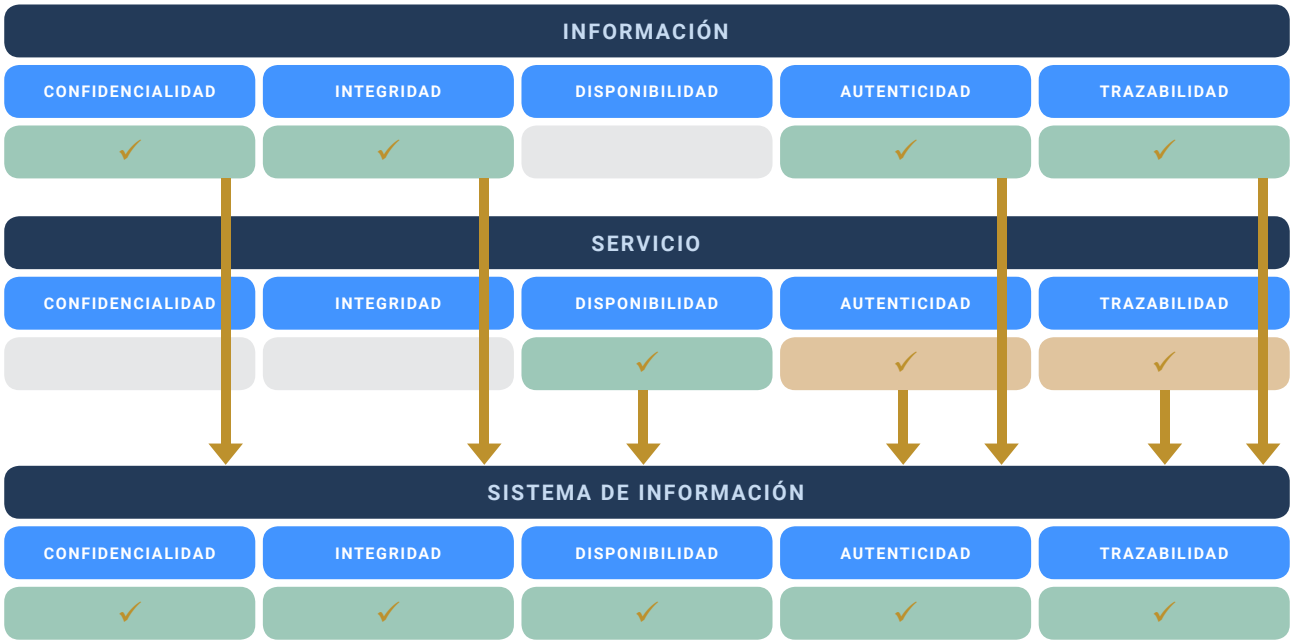


Ilustración 1. Valoración de las dimensiones de seguridad en función del tipo de activo.

3.1.1 Determinación de los niveles de Seguridad por Dimensión

El Esquema Nacional de Seguridad establece tres (3) niveles de seguridad a asignar a las diferentes dimensiones: **Bajo [B], Medio [M]** y **Alto [A]**.

La determinación del nivel de seguridad (en cada dimensión) se obtendrá en base a la evaluación del impacto que tuviera para la entidad la materialización de los riesgos siguientes:

- **Disposición legal:** existencia de una disposición legal o administrativa que condicione el nivel de la dimensión.
- **Perjuicio directo:** existencia de un perjuicio directo para el ciudadano.
- **Incumplimiento de una norma:** implica el incumplimiento de una norma (legal, regulatoria, contractual o interna).
- **Pérdidas económicas:** implica pérdidas económicas para la entidad.
- **Reputación:** implica daño reputacional para la entidad.
- **Protestas:** previsión de que pueda desembocar en protestas.
- **Delitos:** facilitaría la comisión de delitos o dificultaría su investigación.

TABLA 1. CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE LOS TIPOS DE INFORMACIÓN Y SERVICIOS

CRITICIDAD		NO ADSCRITO	BAJO	MEDIO	ALTO
Disposición legal o administrativa		No existe ninguna disposición legal que condicione su nivel	Por disposición legal o administrativa: ley, decreto, orden, reglamento…	Por disposición legal o administrativa: ley, decreto, orden, reglamento…	Por disposición legal o administrativa: ley, decreto, orden, reglamento…
Perjuicio directo al ciudadano		No supone ningún perjuicio directo al ciudadano	Algún perjuicio al ciudadano	Daño importante al ciudadano, aunque subsanable	Grave daño al ciudadano, de difícil o imposible reparación
Incumplimiento de una Norma	Legal	No implica incumplimiento de una norma jurídica	Incumplimiento formal leve de una norma jurídica, de carácter subsanable	Incumplimiento material de una norma jurídica o incumplimiento formal no subsanable	Incumplimiento grave de una norma jurídica
	Regulatoria	No implica incumplimiento de la normativa de un regulador	Implica incumplimiento de la normativa de un regulador	Implica sanción significativa de un regulador	Implica sanción grave de un regulador y/o pérdida de licencia para operar
	Contractual	No implica incumplimiento de una obligación contractual	Incumplimiento leve de una obligación contractual	Incumplimiento material o formal de una obligación contractual	Incumplimiento grave de una obligación contractual
	Interna	No implica incumplimiento de la normativa interna	Incumplimiento leve de una norma interna	Incumplimiento material o formal de una norma interna	Incumplimiento grave de una norma interna
Pérdidas económicas		No implica pérdidas económicas	Pérdidas económicas apreciables (inferior a un 4% del presupuesto anual de la organización)	Pérdidas económicas importantes (igual o superior a un 4% e inferior a un 10% del presupuesto anual de la organización)	Pérdidas económicas o alteraciones financieras significativas (igual o superior a un 10% del presupuesto anual de la organización)
Reputación		No implica daño reputacional	Daño reputacional apreciable con los ciudadanos o con otras organizaciones	Daño reputacional importante con los ciudadanos o con otras organizaciones	Daño reputacional grave con los ciudadanos o con otras organizaciones
Protestas		No se prevé que pueda desembocar en protestas	Múltiples protestas individuales	Protestas públicas (alteración del orden público)	Protestas masivas (alteración seria del orden público)
Delitos		No facilitaría la comisión de delitos ni dificultaría su investigación	Favorecería la comisión de delitos	Favorecería significativamente la comisión de delitos o dificultaría su investigación	Incitaría a la comisión de delitos, constituiría en sí un delito, o dificultaría enormemente su investigación

3.1.2 Determinación de la Categoría

El Esquema Nacional de Seguridad establece tres (3) **categorías de seguridad** para los sistemas de información: BÁSICA, MEDIA y ALTA:

- Un sistema de información será de **categoría ALTA** si alguna de sus dimensiones de seguridad alcanza el Nivel Alto.
- Un sistema de información será de **categoría MEDIA** si alguna de sus dimensiones de seguridad alcanza el Nivel Medio y ninguna alcanza un nivel superior.
- Un sistema de información será de **categoría BÁSICA** si alguna de sus dimensiones de seguridad alcanza el Nivel Bajo y ninguna alcanza un nivel superior.

La determinación de la categoría de un sistema no implica que se altere, por este hecho, el nivel de las dimensiones de seguridad que no han influido en la determinación de la categoría del mismo. Sin embargo, se debe tener en cuenta que la asignación de una categoría al sistema requiere fijar el nivel de madurez de las medidas que resulten de aplicación.

La determinación de la categoría de un sistema no implica que se altere, por este hecho, el nivel de las dimensiones de seguridad que no han influido en la determinación de la categoría del mismo

3.2. Determinación de las medidas de aplicación

Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos en el Esquema Nacional de Seguridad, se debe aplicar un conjunto de medidas de seguridad, que serán proporcionales a las dimensiones de seguridad relevantes en el sistema a proteger y su categoría.

El Anexo II del Real Decreto 311/2022 recoge la correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad aplicables.

En concreto, por cada medida de seguridad se indica:

- Si se determina su aplicación en función de la categoría del sistema o en función del nivel de seguridad asignado a una o varias dimensiones de seguridad.
- Si es de aplicación o no para un determinado nivel de seguridad. En caso de que la aplicación de la medida no sea necesaria para obtener la adecuación con el ENS, en la tabla del Anexo II se recoge el valor **"n.a."**.

Por otro lado, en caso de sí ser necesaria su aplicación, aparecerá alguno de los siguientes valores:

- **"aplica":** indica que los **requisitos base** de una medida de seguridad deben ser aplicados a una o varias dimensiones de la seguridad en algún nivel.
- **"+Rn":** Pudiendo adoptar 'n' los valores del '1' al '9', indica que dicho r**efuerzo obligatorio** debe ser aplicado a una o varias dimensiones de la seguridad en algún nivel.

Pueden ser de aplicación simultánea varios refuerzos obligatorios a una o varias dimensiones de la seguridad en algún nivel, por ejemplo, 'R1 + R2 + R5'. Asimismo, puede requerirse escoger determinado refuerzo obli-

Se debe aplicar un conjunto de medidas de seguridad, que serán proporcionales a las dimensiones de seguridad relevantes en el sistema a proteger y su categoría

gatorio de un subconjunto de ellos, por ejemplo, 'R1 o R2 o R3'. Ambas casuísticas pueden combinarse, por ejemplo, '[R1 o R2 o R3] + R9'.

A continuación, se recogen algunos ejemplos de lo indicado anteriormente:

a • La medida [org.1] aplica a los sistemas de cualquier categoría. El nivel de exigencia de la medida no varía en función de categoría asociada al sistema; en cualquiera de ellas únicamente aplican los **requisitos base**.

Afectadas	BÁSICA	MEDIA	ALTA	Medida de seguridad	
Categoría	aplica	aplica	aplica	[org.1]	Política de seguridad

b • La medida [mp.if.6] aplica a los sistemas cuyo nivel de seguridad asociado a la dimensión de *disponibilidad* sea Medio o Alto. El nivel de exigencia de la medida no varía en función de si el Nivel es Medio o Alto; en cualquiera de ambos casos únicamente aplican los **requisitos base**.

Afectadas	BAJO	MEDIO	ALTO	Medida de seguridad	
D	n.a.	aplica	aplica	[mp.if.6]	Protección frente a inundaciones

c • La medida [mp.si.2] aplica a los sistemas cuyo nivel de seguridad asociado a las dimensiones de *confidencialidad* o *integridad* sea Medio o Alto. El nivel de exigencia de la medida cambia si alguno de los niveles es Medio o Alto. Los **requisitos base** son los mismos para Nivel Medio y Alto, mientras que los refuerzos opcionales únicamente aplican para Nivel Alto en esas dos (2) dimensiones.

Afectadas	BAJO	MEDIO	ALTO	Medida de seguridad	
C I	n.a.	aplica	+R1 +R2	[mp.si.2]	Criptografía

d • La medida [mp.com.4] no aplica a categoría BÁSICA, siendo el nivel de exigencia de la medida distinto en función de si la categoría es MEDIA o ALTA. Los **requisitos base** aplican a ambas categorías; para categoría MEDIA se elegirá entre aplicar el **refuerzo obligatorio** R1, R2 o R3, mientras que para categoría ALTA siempre se aplicará el **refuerzo obligatorio** R4, junto al que se considere elegido entre R2 o R3.

Afectadas	BÁSICA	MEDIA	ALTA	Medida de seguridad	
Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	[mp.com.4]	Separación flujos de información en red

4. Ejemplo

4.1. Categorización

Supongamos un ejemplo sencillo de una Entidad Local que, debido a su naturaleza pública, está bajo el alcance del ENS.

Seguimos los siguientes pasos:

1 · **Inventario de activos**
En lugar de realizar el inventario completo, nos centramos en aquellos activos que son esenciales para el Sistema de Información en el alcance definido:

- Información asociada al Padrón Municipal de Habitantes (PMH).
- Información asociada al Registro.
- Servicio de Padrón Municipal de Habitantes (PMH).
- Servicio de Registro.

2 · **Valoración de activos**
Tras analizar el impacto que un incidente podría tener sobre los activos esenciales, los niveles de seguridad asignados, por dimensión, son los siguientes:

ACTIVOS INFORMACIÓN	[D]	[I]	[C]	[A]	[T]
Información PMH	n.a.	[M]	[M]	[M]	[M]
Información de Registro	n.a.	[M]	[M]	[M]	[M]

ACTIVOS SERVICIOS	[D]	[I]	[C]	[A]	[T]
Servicio PMH	[M]	n.a.	n.a.	[B]	[B]
Servicio Registro E/S	[M]	n.a.	n.a.	[B]	[B]

No se han valorado los niveles de seguridad de la *integridad* y *confidencialidad* en los activos de tipo "Servicio" (valor fijado a "n.a.") ya que se ha considerado que los hereden de los asignados a los activos de tipo "Información". De igual forma, se ha considerado en los activos de tipo "Información" que el nivel de seguridad asociado a la *disponibilidad* esté determinado por el nivel asociado a los servicios.

3 · Agrupación y herencia de valores

ACTIVOS INFORMACIÓN	[D]	[I]	[C]	[A]	[T]
Información PMH	[M]	[M]	[M]	[M]	[M]
Información de Registro	[M]	[M]	[M]	[M]	[M]
Nivel máximo de la Información	[M]	[M]	[M]	[M]	[M]

ACTIVOS SERVICIOS	[D]	[I]	[C]	[A]	[T]
Servicio PMH	[M]	[M]	[M]	[B]	[B]
Servicio Registro E/S	[M]	[M]	[M]	[B]	[B]
Nivel máximo de los Servicios	[M]	[M]	[M]	[B]	[B]

Los niveles del sistema serán: [D] = M, [I] = M, [C] = M, [A] = M y [T] = M.

VALORES MÁXIMOS DEL SISTEMA	[D]	[I]	[C]	[A]	[T]	VALOR MÁXIMO
Información PMH	[M]	[M]	[M]	[M]	[M]	[M]
Información de Registro	[M]	[M]	[M]	[M]	[M]	[M]

4 · Determinación de la categoría

La categoría del sistema de información viene determinada por el nivel de seguridad más alto asignado a alguna dimensión, para algún activo en concreto.

Analizando los niveles asignados, se determina que la categoría del sistema de información es MEDIA.

VALORES MÁXIMOS DEL SISTEMA	[D]	[I]	[C]	[A]	[T]	VALOR MÁXIMO
Valores máximos de la Información	[M]	[M]	[M]	[M]	[M]	[M]
Valores de los Servicios	[M]	[M]	[M]	[B]	[B]	[M]
Categoría del Sistema						[M]

Se debe tener en cuenta que la determinación de la categoría del sistema de información no altera el nivel de seguridad de las dimensiones individuales, siendo estas dimensiones individuales relevantes a la hora de determinar la aplicabilidad de ciertas medidas del Anexo II del Real Decreto 311/2022. Esta casuística se ejemplarizará en las siguientes secciones de esta guía.

4.2. Determinación de la Declaración de Aplicabilidad

Ejemplo 1. Sea un sistema de información con los siguientes niveles en cada dimensión de seguridad:

SISTEMA 1		
NIVELES DE LAS DIMENSIONES DE SEGURIDAD	CONFIDENCIALIDAD **(C)**	**Alto**
	INTEGRIDAD **(I)**	**Alto**
	DISPONIBILDAD **(D)**	**Medio**
	AUTENTICIDAD **(A)**	**Alto**
	TRAZABILIDAD **(T)**	**Bajo**

Su categoría corresponde con el nivel más elevado asociado a alguna de las dimensiones. Por tanto, la **categoría de este sistema es ALTA: [D(M), I(A), C(A), A(A), T(B)].**

Las medidas que serán de aplicación son aquellas exigidas para Nivel Alto, exceptuando aquellas que sólo apliquen a *trazabilidad* (Nivel Medio o Alto) y a *disponibilidad* (Nivel Alto).

Es decir, debido a la *trazabilidad* de Nivel Bajo, no será de aplicación la medida [mp.info.4], marcada como 'NO APLICA'. Por otro lado, debido a la *disponibilidad* de Nivel Medio, no serán de aplicación las medidas [op.cont.2], [op.cont.3] y [op.cont.4], mientras que en [mp.s.4] aplica únicamente el **requisito base** y en [mp.info.6] aplica únicamente el **refuerzo obligatorio** R1.

Las medidas que serán de aplicación son aquellas exigidas para Nivel Alto, exceptuando aquellas que sólo apliquen a *trazabilidad* (Nivel Medio o Alto) y a *disponibilidad* (Nivel Alto)

CÓDIGO	DESCRIPCIÓN	DIMENSIONES	CATEGORÍA DEL SISTEMA
ORG	MARCO ORGANIZATIVO		
org.1	Política de seguridad	D I C A T	aplica
org.2	Normativa de seguridad	D I C A T	aplica
org.3	Procedimientos de seguridad	D I C A T	aplica
org.4	Proceso de autorización	D I C A T	aplica
	MARCO OPERACIONAL		
op.pl	Planificación		
op.pl.1	Análisis de riesgos	D I C A T	+R2
op.pl.2	Arquitectura de Seguridad	D I C A T	+R1 +R2 +R3
op.pl.3	Adquisición de nuevos componentes	D I C A T	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D _ _ _ _	+R1
op.pl.5	Componentes certificados	D I C A T	aplica
op.acc	Control de acceso		
op.acc.1	Identificación	_ _ _ A T	+R1
op.acc.2	Requisitos de acceso	_ I C A T	+R1
op.acc.3	Segregación de funciones y tareas	_ I C A T	+R1
op.acc.4	Proceso de gestión de derechos de acceso	_ I C A T	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	_ I C A T	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	_ I C A T	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp	Explotación		
op.exp.1	Inventario de activos	D I C A T	aplica
op.exp.2	Configuración de seguridad	D I C A T	aplica
op.exp.3	Gestión de la configuración de seguridad	D I C A T	+R1 +R2 +R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	D I C A T	+R1 +R2
op.exp.5	Gestión de cambios	D I C A T	+R1
op.exp.6	Protección frente a código dañino	D I C A T	+R1 +R2 +R3 +R4
op.exp.7	Gestión de incidentes	D I C A T	+R1 +R2 +R3
op.exp.8	Registro de la actividad	_ _ _ _ T	aplica
op.exp.9	Registro de la gestión de incidentes	D I C A T	aplica
op.exp.10	Protección de claves criptográficas	D I C A T	+R1
op.ext	Recursos externos		
op.ext.1	Contratación y acuerdos de nivel de servicio	D I C A T	aplica
op.ext.2	Gestión diaria	D I C A T	aplica
op.ext.3	Protección de la cadena de suministro	D I C A T	aplica
op.ext.4	Interconexión de sistemas	D I C A T	+R1

CÓDIGO	DESCRIPCIÓN	DIMENSIONES	CATEGORÍA DEL SISTEMA
ORG	MARCO ORGANIZATIVO		
op.nub	Servicios en la nube		
op.nub.1	Protección de servicios en la nube	D I C A T	+R1 +R2
op.cont	Continuidad del servicio		
op.cont.1	Análisis de impacto	D _ _ _ _	aplica
op.cont.2	Plan de continuidad	D _ _ _ _	n.a.
op.cont.3	Pruebas periódicas	D _ _ _ _	n.a.
op.cont.4	Medios alternativos	D _ _ _ _	n.a.
op.mon	Monitorización del sistema		
op.mon.1	Detección de intrusión	D I C A T	+R1 +R2
op.mon.2	Sistema de métricas	D I C A T	+R1 +R2
op.mon.3	Vigilancia	D I C A T	+R1 +R2 +R3 +R4 +R5 +R6
	MEDIDAS DE PROTECCIÓN		
mp.if	Protección de las instalaciones e infraestructuras		
mp.if.1	Áreas separadas y con control de acceso	D I C A T	aplica
mp.if.2	Identificación de las personas	D I C A T	aplica
mp.if.3	Acondicionamiento de los locales	D I C A T	aplica
mp.if.4	Energía eléctrica	D _ _ _ _	+R1
mp.if.5	Protección frente a incendios	D _ _ _ _	aplica
mp.if.6	Protección frente a inundaciones	D _ _ _ _	aplica
mp.if.7	Registro de entrada y salida de equipamiento	D I C A T	aplica
mp.per	Gestión del personal		
mp.per.1	Caracterización del puesto de trabajo	D I C A T	aplica
mp.per.2	Deberes y obligaciones	D I C A T	+R1
mp.per.3	Concienciación	D I C A T	aplica
mp.per.4	Formación	D I C A T	aplica
mp.eq	Protección de los equipos		
mp.eq.1	Puesto de trabajo despejado	D I C A T	+R1
mp.eq.2	Bloqueo de puesto de trabajo	_ _ _ A _	+R1
mp.eq.3	Protección de dispositivos portátiles	D I C A T	+R1 +R2
mp.eq.4	Otros dispositivos conectados a la red	_ _ C _ _	+R1
mp.com	Protección de las comunicaciones		
mp.com.1	Perímetro seguro	D I C A T	aplica
mp.com.2	Protección de la confidencialidad	_ _ C _ _	+R1 +R2 +R3
mp.com.3	Protección de la integridad y de la autenticidad	_ I _ A _	+R1 +R2 +R3 +R4
mp.com.4	Separación de flujos de información en la red	D I C A T	+[R2 o R3] +R4

CÓDIGO	DESCRIPCIÓN	DIMENSIONES	CATEGORÍA DEL SISTEMA
ORG	MARCO ORGANIZATIVO		
mp.si	Protección de los soportes de información		
mp.si.1	Marcado de soportes	_ _ C _ _	aplica
mp.si.2	Criptografía	_ I C _ _	+R1 +R2
mp.si.3	Custodia	D I C A T	aplica
mp.si.4	Transporte	D I C A T	aplica
mp.si.5	Borrado y destrucción	_ _ C _ _	+R1
mp.sw	Protección de las aplicaciones informáticas		
mp.sw.1	Desarrollo de aplicaciones	D I C A T	+R1 +R2 +R3 +R4
mp.sw.2	Aceptación y puesta en servicio	D I C A T	+R1
mp.info	Protección de la información		
mp.info.1	Datos personales	D I C A T	aplica
mp.info.2	Calificación de la información	_ _ C _ _	aplica
mp.info.3	Firma electrónica	_ I _ A _	+R1 +R2 +R3 +R4
mp.info.4	Sellos de tiempo	_ _ _ _ T	n.a.
mp.info.5	Limpieza de documentos	_ _ C _ _	aplica
mp.info.6	Copias de seguridad	D _ _ _ _	+R1
mp.s	Protección de los servicios		
mp.s.1	Protección del correo electrónico	D I C A T	aplica
mp.s.2	Protección de servicios y aplicaciones web	D I C A T	+R2 +R3
mp.s.3	Protección de la navegación web	D I C A T	+R1
mp.s.4	Protección frente a denegación de servicio	D _ _ _ _	aplica

A modo de resumen, de las 73 medidas definidas en el Anexo II del Real Decreto 311/2022, solo 69 son de aplicación/exigidas para el sistema del ejemplo:

- 61 son de aplicación con un Nivel de exigencia Alto.
- 7 son de aplicación con un Nivel de exigencia Medio.
- 1 es de aplicación con un Nivel de exigencia Bajo.
- 4 no aplican.

5. Perfil de cumplimiento específico

Podemos definir un Perfil de Cumplimiento Específico (PCE) como el conjunto de medidas de seguridad, comprendidas o no en el Anexo II del RD 311/2022, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad.

El CCN, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan, junto a los esquemas de acreditación y validación correspondientes, de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda del ENS.

En consecuencia, una organización al elaborar la Declaración de Aplicabilidad para determinado Sistema de Información, deberá evaluar si puede optar a un PCE y, en su caso, adaptar la Declaración de Aplicabilidad al mismo.

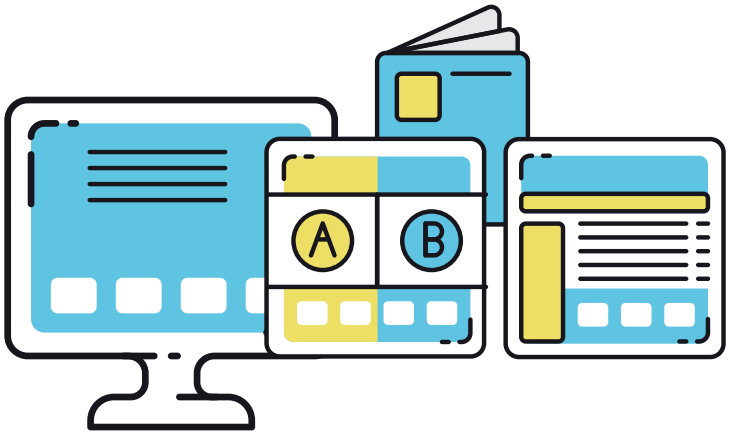
Una organización al elaborar la Declaración de Aplicabilidad para determinado Sistema de Información, deberá evaluar si puede optar a un PCE y, en su caso, adaptar la Declaración de Aplicabilidad al mismo

6. Recomendaciones

6.1. Respecto al formato de la Declaración de Aplicabilidad

Para mayor claridad y utilidad de la Declaración de Aplicabilidad, es una buena práctica añadir dos (2) columnas adicionales: el **grado de implementación** de cada una de las medidas que apliquen (CCN-STIC-808), así como el **nivel de madurez** con una breve descripción de cómo aplica cada medida en el Sistema de Información de la Organización.

En esa descripción, en el caso de que se haya sustituido alguna medida de seguridad (ya sea completa o de su refuerzo base o posible refuerzo obligatorio) mediante una **medida compensatoria**, deberá constar una referencia a la misma. Igual sucederá si se emplean **medidas complementarias de vigilancia** para determinada medida de seguridad.



DECLARACIÓN DE APLICABILIDAD RD 311/2022									
DIMENSIÓN	**B**	**M**	**A**	**Medida**	**Descripción**	**Aplica**	**Grado Implemen.**	**Nivel madurez**	**DETALLE DE CÓMO APLICA, O POR QUÉ APLICA**
MARCO ORGANIZATIVO									
Categoría	APL	APL	APL	org.1	Política de seguridad	Si	G2	L3	Se dispone del documento "**POL-001 Política de Seguridad**" que en el control de versiones está referenciado como última versión la V1.1 de fecha 24/10/2022. Se ha comunicado internamente en la organización a través de la Intranet.
Categoría	APL	APL	APL	org.2	Normativa de seguridad	Si	G2	L3	Se dispone del documento "**NOR-001 Normativa de Uso de los sistemas**" que desarrolla la Política de Seguridad. La normativa de uso de los sistemas ha sido suscrita por los empleados de la organización, firmando el apartado final.
Categoría	APL	APL	=	org.3	Procedimiento de seguridad	Si	G2	L1	
Categoría	APL	APL	APL	org.4	Proceso de autorización	Si	G2	L1	
MARCO OPERACIONAL									
				op.pl.	**PLANIFICACIÓN**				
Categoría	APL	+R1	+R2	op.pl.1	Análisis de riesgos	Si	G2	L2	
Categoría	APL	+R1	+R1 +R2 +R3	op.pl.2	Arquitectura de seguridad	Si	G2	L2	
Categoría	APL	APL	APL	op.pl.3	Adquisición nuevos componentes	Si	G2	L2	
D	APL	+R1	+R1	op.pl.4	Gestión de capacidad	Si	G0	L0	
Categoría	N/A	APL	APL	op.pl.5	Componentes certificados	NO			NO APLICA AL SER UNA MEDIDA PARA SISTEMAS DE CATEGORÍA MEDIA Y ALTA

Se aprecia en el extracto ejemplo de la figura superior, que representa un sistema de categoría BÁSICA, cómo se describe la aplicabilidad concreta para las medidas [org.1] y [org.2]. En la columna 'Grado de implementación', G0 significa que la medida no está implementada, G1 que está en proceso de implementación y G2 que está implementada.

Ilustración 2. Extracto de una posible Declaración de Aplicabilidad.

6.2. Decálogo de recomendaciones generales

A continuación, se muestra un decálogo de recomendaciones a tener en cuenta para determinar una Declaración de Aplicabilidad en el ámbi to del Esquema Nacional de Seguridad.

DECÁLOGO DE RECOMENDACIONES PARA LA DECLARACIÓN DE APLICABILIDAD (ENS)	
1	Valorar, en primer lugar, los activos esenciales (de los tipos “Información” y “Servicio”).
2	Para valorar los activos, determinar el nivel de seguridad por cada una de las dimensiones: confidencialidad [C], integridad [I], disponibilidad [D], autenticidad [A] y trazabilidad [T]. Dicho nivel se determinará en función de las consecuencias de un incidente de seguridad sobre alguna de las dimensiones.
3	Si el activo esencial es de tipo “Servicio”, se recomienda valorar en primer lugar la dimensión de disponibilidad [D], pues los requisitos en materia de confiden- cialidad, integridad, autenticidad y trazabilidad suelen venir heredados por la valoración de los activos de tipo “Información”.
4	Establecer la categoría del sistema (BÁSICA, MEDIA o ALTA) en función de los niveles de seguridad asignados a las distintas dimensiones, teniendo en cuenta que la asignación de una categoría al sistema requiere fijar un grado de im- plementación de las medidas que resulten de aplicación y que la categoría del sistema será el mayor de los niveles de seguridad asignados.
5	Seleccionar las medidas que aplican al sistema en función de su categoría, de un total de 45 medidas.
6	Seleccionar las medidas que aplican al sistema en función de sus niveles de seguridad, de un total de 28 medidas.

7	Emplear el simulador elaborado por el CCN-CERT, que ayuda a determinar la Declaración de Aplicabilidad de forma automática, introduciendo los niveles de seguridad para cada una de las dimensiones del activo.
8	Indicar de forma detallada la correspondencia entre las medidas compensatorias implementadas y las medidas del Anexo II que compensan; de manera análoga, respecto a las posibles medidas complementarias de vigilancia. El conjunto será objeto de la aprobación formal por parte del Responsable de Seguridad.
9	En caso de que en la Declaración de Aplicabilidad se incluya alguna medida compensatoria, detallar, por cada una de ellas, los siguientes parámetros: ámbito de aplicación, limitaciones o restricciones, objetivo, riesgo identificado, definición de la compensatoria, validación de la medida compensatoria y mantenimiento. El contenido de dichos parámetros es recogido en la Guía CCN-STIC-819 “Medidas Compensatorias”.
10	Para la redacción del documento de Declaración de Aplicabilidad, hacer uso de un documento de elaboración propia o de la plantilla desarollada por el CCN-CERT, debiendo tener en cuenta los perfiles de cumplimiento validados por el CCN en las correspondientes guías CCN-STIC.

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es