CCN-CERT BP/14

Declaración de Aplicabilidad en el ENS (Perfil de Cumplimiento)

Junio 2019

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Fecha de Edición: julio de 2019

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 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, en adelante), modificado por el RD 951/2015 de 23 de octubre.

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 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 de que se trate, conforme a su categoría, y que se encuentran recogidas en el Anexo II del Real Decreto 3/2010, de 8 de enero, que lo regula.

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 (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del Real Decreto 3/2010.

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 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.

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, en función de los riesgos a los que está expuesto, bajo el criterio del principio de proporcionalidad.

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 3/2010.

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 la información o de los sistemas, con repercusión en la capacidad organizativa para:

a) Alcanzar sus objetivos.

b) Proteger los activos a su cargo.

c) Cumplir sus obligaciones diarias de servicio.

d) Respetar la legalidad vigente.

e) Respetar los derechos de las personas.

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, en primer lugar, realizar el inventario 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.

En función de si el activo es un servicio a prestar o información tratada, conviene centrarse en la valoración de dimensiones de seguridad concretas. Por ejemplo, se recomienda valorar las dimensiones en el siguiente orden para los activos de tipo información: *confidencialidad*, *integridad*, *autenticidad*, *trazabilidad* y, si fuera relevante, *disponibilidad* ("*conservación*", como dimensión exclusiva del Esquema Judicial de Interoperabilidad y seguridad, EJIS).

Es frecuente que la *disponibilidad* no sea un atributo relevante de la información y quede sin adscribir a ningún nivel. Sin embargo, si el activo esencial es un servicio, se recomienda valorar la dimensión de *disponibilidad*, ya que los requisitos en materia de *confidencialidad, integridad, autenticidad* y *trazabilidad* suelen venir heredados por los tipos de información que maneja el servicio, especialmente la *confidencialidad* y la *integridad*.

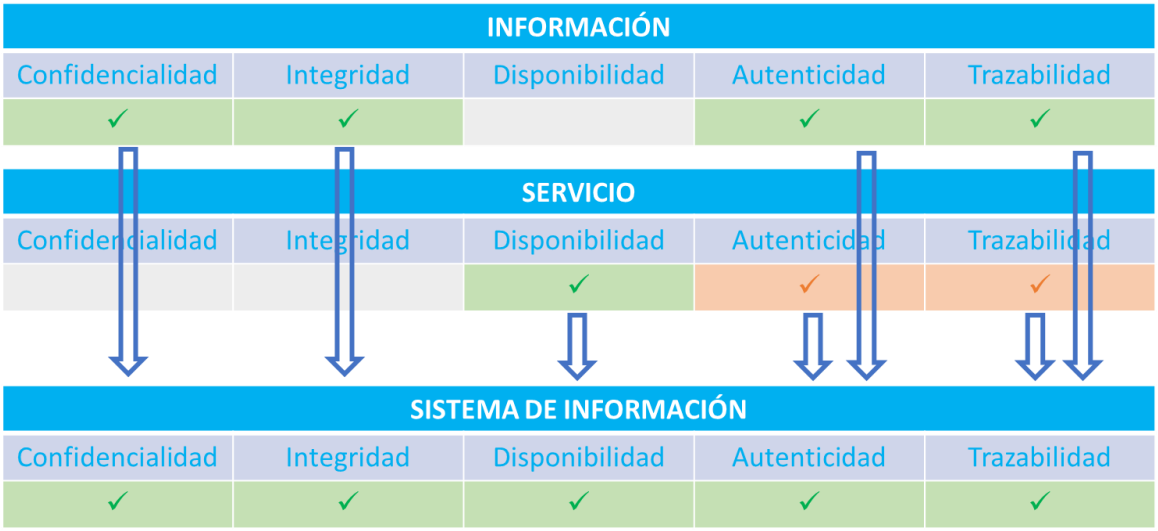


Ilustración 1.- Valoración de las dimensiones de seguridad en función del tipo de activo.

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.

CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN Y SERVICIOS					
		No Adscrito (N/A)	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, aunque subsanable al ciudadano	Grave daño, de difícil o imposible reparación al ciudadano
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 normativa de un regulador	Implica incumplimiento de normativa de un regulador	Implica sanción significativa de un regulador	Implica sanción grave de un regulador y/o pérdida de licencia de 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

CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN Y SERVICIOS					
		No Adscrito (N/A)	BAJO	MEDIO	ALTO
	Interna	No implica incumplimiento de 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.

Tabla 1.- Criterios comunes aplicables a todas las Dimensiones de Tipos de Información y Servicios.

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.

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 3/2010 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 una medida de seguridad debe ser aplicada a una o varias dimensiones de seguridad en algún nivel.
  - "**=**": indica que las exigencias de un nivel son iguales a los del nivel inferior.
  - "**+**" o "**++**": indica que el incremento de exigencias graduado en función de del nivel de la dimensión de seguridad.

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.

Afectadas	BÁSICA	MEDIA	ALTA	Medida de seguridad	
categoría	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.

Afectadas	BAJO	MEDIO	ALTO	Medida de seguridad	
D	n.a.	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 *integridad* o *confidencialidad* sea MEDIO o ALTO. El nivel de exigencia de la medida cambia si alguno de los niveles es MEDIO o ALTO. Los requisitos de cumplimiento para la medida son superiores si, al menos, uno de los niveles de seguridad asociados a las dimensiones es ALTO.

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

d) La medida [op.acc.7] aplica a todos los sistemas. El nivel de exigencia de la medida cambia si alguno de los niveles asignados a las dimensiones de integridad, *confidencialidad, autenticidad* y *trazabilidad* es BAJO o MEDIO/ALTO. Los requisitos de cumplimiento para la medida son superiores si, al menos, uno de los niveles de seguridad asociados a las dimensiones es MEDIO o ALTO. Para ambos niveles los requisitos son equivalentes pero superiores al nivel BAJO.

Afectadas	BAJO	MEDIO	ALTO	Medida de seguridad	
I C A T	aplica	+	=	[op.acc.7]	Acceso remoto

4. EJEMPLOS

4.1 CATEGORIZACIÓN

Supongamos un ejemplo sencillo de un Ayuntamiento 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:
   - 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:

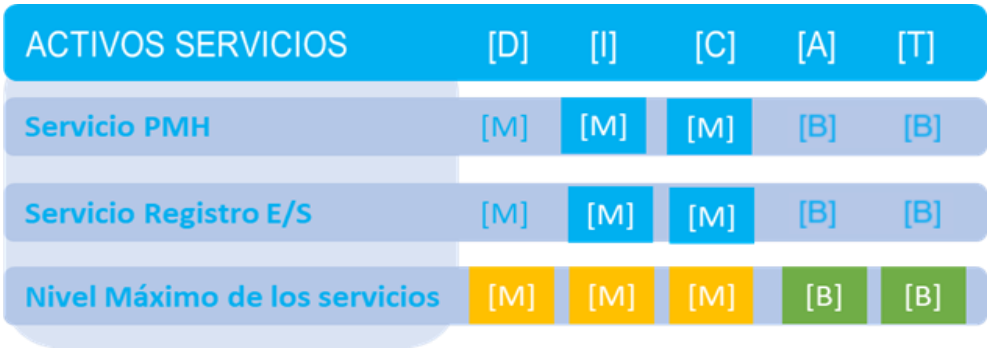
ACTIVOS INFORMACIÓN	[D]	[I]	[C]	[A]	[T]
Información PMH	n.a	[M]	[M]	[M]	[M]
Información de Registro	n.a	[M]	[M]	[M]	[M]

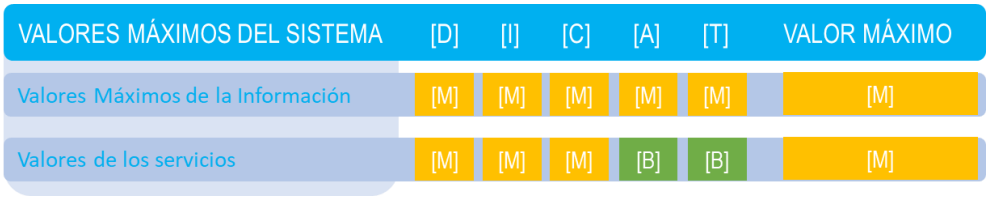
ACTIVOS SERVICIOS	[D]	[I]	[C]	[A]	[T]
Servicio PMH	[M]	n.a	n.a	[B]	[B]
Servicio Registro E/S	[M]	n.a	n.a	[B]	[B]

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]





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

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 3/2010. 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)	A
	INTEGRIDAD (I)	A
	DISPONIBILDAD (D)	A
	AUTENTICIDAD (A)	A
	TRAZABILIDAD (T)	B

Su categoría corresponde con el nivel más elevado asociado a alguna de las dimensiones. Por tanto, la **categoría de este sistema es Alta: [C(A), I(A), D(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). Es decir, no se tendrán en cuenta para el cálculo del Índice de cumplimiento las medidas, [op.exp.10: Protección de los registros de actividad] y [mp.info.5: Sellos de tiempo], pero si se tendrá en cuenta la medida [op.exp.8: Registro de la actividad de los usuarios] correspondiente a un nivel de Trazabilidad Bajo, pero **solo la parte de la medida exigible a dicho nivel BAJO**.

La declaración de aplicabilidad, por tanto, será la siguiente:

Dimensiones afectadas	Básica	Media	Alta	Medida de seguridad	Nivel de aplicación
categoría	aplica	=	=	[org.1]	Alto
categoría	aplica	=	=	[org.2]	Alto
categoría	aplica	=	=	[org.3]	Alto
categoría	aplica	=	=	[org.4]	Alto
categoría	aplica	+	++	[op.pl.1]	Alto
categoría	aplica	+	++	[op.pl.2]	Alto
categoría	aplica	=	=	[op.pl.3]	Alto
D	n.a.	aplica	=	[op.pl.4]	Alto
categoría	n.a.	n.a.	aplica	[op.pl.5]	Alto
A T	aplica	=	=	[op.acc.1]	Alto
I C A T	aplica	=	=	[op.acc.2]	Alto
I C A T	n.a.	aplica	=	[op.acc.3]	Alto
I C A T	aplica	=	=	[op.acc.4]	Alto
I C A T	aplica	+	++	[op.acc.5]	Alto
I C A T	aplica	+	++	[op.acc.6]	Alto
I C A T	aplica	+	=	[op.acc.7]	Alto
categoría	aplica	=	=	[op.exp.1]	Alto
categoría	aplica	=	=	[op.exp.2]	Alto
categoría	n.a.	aplica	=	[op.exp.3]	Alto
categoría	aplica	=	=	[op.exp.4]	Alto
categoría	n.a.	aplica	=	[op.exp.5]	Alto
categoría	aplica	=	=	[op.exp.6]	Alto
categoría	n.a.	aplica	=	[op.exp.7]	Alto

Dimensiones afectadas	Básica	Media	Alta	Medida de seguridad	Nivel de aplicación
T	aplica	+	++	[op.exp.8]	Bajo
categoría	n.a.	aplica	=	[op.exp.9]	Alto
T	n.a.	n.a.	aplica	[op.exp.10]	No aplica
categoría	aplica	+	=	[op.exp.11]	Alto
categoría	n.a.	aplica	=	[op.ext.1]	Alto
categoría	n.a.	aplica	=	[op.ext.2]	Alto
D	n.a.	n.a.	aplica	[op.ext.9]	Alto
D	n.a.	aplica	=	[op.cont.1]	Alto
D	n.a.	n.a.	aplica	[op.cont.2]	Alto
D	n.a.	n.a.	aplica	[op.cont.3]	Alto
categoría	n.a.	aplica	=	[op.mon.1]	Alto
categoría	aplica	+	++	[op.mon.2]	Alto
categoría	aplica	=	=	[mp.if.1]	Alto
categoría	aplica	=	=	[mp.if.2]	Alto
categoría	aplica	=	=	[mp.if.3]	Alto
D	aplica	+	=	[mp.if.4]	Alto
D	aplica	=	=	[mp.if.5]	Alto
D	n.a.	aplica	=	[mp.if.6]	Alto
categoría	aplica	=	=	[mp.if.7]	Alto
D	n.a.	n.a.	aplica	[mp.if.9]	Alto
categoría	n.a.	aplica	=	[mp.per.1]	Alto
categoría	aplica	=	=	[mp.per.2]	Alto
categoría	aplica	=	=	[mp.per.3]	Alto
categoría	aplica	=	=	[mp.per.4]	Alto
D	n.a.	n.a.	aplica	[mp.per.9]	Alto
categoría	aplica	+	=	[mp.eq.1]	Alto
A	n.a.	aplica	+	[mp.eq.2]	Alto
categoría	aplica	=	+	[mp.eq.3]	Alto
D	n.a.	aplica	=	[mp.eq.9]	Alto
categoría	aplica	=	+	[mp.com.1]	Alto
C	n.a.	aplica	+	[mp.com.2]	Alto
I A	aplica	+	++	[mp.com.3]	Alto
categoría	n.a.	n.a.	aplica	[mp.com.4]	Alto
D	n.a.	n.a.	aplica	[mp.com.9]	Alto
C	aplica	=	=	[mp.si.1]	Alto
I C	n.a.	aplica	+	[mp.si.2]	Alto
categoría	aplica	=	=	[mp.si.3]	Alto
categoría	aplica	=	=	[mp.si.4]	Alto
C	aplica	+	=	[mp.si.5]	Alto
categoría	n.a.	aplica	=	[mp.sw.1]	Alto
categoría	aplica	+	++	[mp.sw.2]	Alto

Dimensiones afectadas	Básica	Media	Alta	Medida de seguridad	Nivel de aplicación
categoría	aplica	=	=	[mp.info.1]	Alto
C	aplica	+	=	[mp.info.2]	Alto
C	n.a.	n.a.	aplica	[mp.info.3]	Alto
I A	aplica	+	++	[mp.info.4]	Alto
T	n.a.	n.a.	aplica	[mp.info.5]	No aplica
C	aplica	=	=	[mp.info.6]	Alto
D	aplica	=	=	[mp.info.9]	Alto
categoría	aplica	=	=	[mp.s.1]	Alto
categoría	aplica	=	+	[mp.s.2]	Alto
D	n.a.	aplica	+	[mp.s.8]	Alto
D	n.a.	n.a.	aplica	[mp.s.9]	Alto

En resumen, de las 75 medidas definidas en el Anexo II del Real Decreto 3/2010, solo 73 son de aplicación/exigidas para el sistema del ejemplo:

- 72 son de aplicación con un nivel de exigencia ALTO.
- 1 es de aplicación con un nivel de exigencia BAJO.
- 2 No aplican.

Ejemplo 2:

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

Sistema 2		
NIVELES DE LAS DIMENSIONES DE SEGURIDAD	CONFIDENCIALIDAD (C)	M
	INTEGRIDAD (I)	A
	DISPONIBILDAD (D)	A
	AUTENTICIDAD (A)	M
	TRAZABILIDAD (T)	B

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

En general, para conseguir la declaración de aplicabilidad se ha tenido en cuenta lo siguiente:

- Se han seleccionado todas las medidas que afectan a las dimensiones de Integridad y Disponibilidad de nivel Alto.
- Se han seleccionado todas las medidas que afectan a las dimensiones de Confidencialidad y Autenticidad de nivel Medio (sin afectar a las dimensiones de Integridad y Disponibilidad).

- Se han seleccionado aquellas medidas que sólo afecta a la dimensión de Trazabilidad de nivel Bajo. Es decir, no aplican las medidas [op.exp.10 Protección de los registros de actividad], la medida [mp.info.5 Sellos de tiempo] ni la medida [mp.info.3 Cifrado de la Información].

La declaración de aplicabilidad, por tanto, será la siguiente:

Dimensiones Afectadas	B	M	A	Medida	Nivel de aplicación
categoría	aplica	=	=	[org.1]	Alto
categoría	aplica	=	=	[org.2]	Alto
categoría	aplica	=	=	[org.3]	Alto
categoría	aplica	=	=	[org.4]	Alto
categoría	aplica	+	++	[op.pl.1]	Alto
categoría	aplica	+	++	[op.pl.2]	Alto
categoría	aplica	=	=	[op.pl.3]	Alto
D	n.a.	aplica	=	[op.pl.4]	Alto
categoría	n.a.	n.a.	aplica	[op.pl.5]	Alto
A T	aplica	=	=	[op.acc.1]	Medio
I C A T	aplica	=	=	[op.acc.2]	Alto
I C A T	n.a.	aplica	=	[op.acc.3]	Alto
I C A T	aplica	=	=	[op.acc.4]	Alto
I C A T	aplica	+	++	[op.acc.5]	Alto
I C A T	aplica	+	++	[op.acc.6]	Alto
I C A T	aplica	+	=	[op.acc.7]	Alto
categoría	aplica	=	=	[op.exp.1]	Alto
categoría	aplica	=	=	[op.exp.2]	Alto
categoría	n.a.	aplica	=	[op.exp.3]	Alto
categoría	aplica	=	=	[op.exp.4]	Alto
categoría	n.a.	aplica	=	[op.exp.5]	Alto
categoría	aplica	=	=	[op.exp.6]	Alto
categoría	n.a.	aplica	=	[op.exp.7]	Alto
T	aplica	+	++	[op.exp.8]	Bajo
categoría	n.a.	aplica	=	[op.exp.9]	Alto
T	n.a.	n.a.	aplica	[op.exp.10]	No Aplica
categoría	aplica	+	=	[op.exp.11]	Alto
categoría	n.a.	Aplica	=	[op.ext.1]	Alto
categoría	n.a.	Aplica	=	[op.ext.2]	Alto
D	n.a.	n.a.	aplica	[op.ext.9]	Alto
D	n.a.	Aplica	=	[op.cont.1]	Alto
D	n.a.	n.a.	aplica	[op.cont.2]	Alto
D	n.a.	n.a.	aplica	[op.cont.3]	Alto
categoría	n.a.	Aplica	=	[op.mon.1]	Alto
categoría	aplica	+	++	[op.mon.2]	Alto

categoría	aplica	=	=	[mp.if.1]	Alto
categoría	aplica	=	=	[mp.if.2]	Alto
categoría	aplica	=	=	[mp.if.3]	Alto
D	aplica	+	=	[mp.if.4]	Alto
D	aplica	=	=	[mp.if.5]	Alto
D	n.a.	Aplica	=	[mp.if.6]	Alto
categoría	aplica	=	=	[mp.if.7]	Alto
D	n.a.	n.a.	aplica	[mp.if.9]	Alto
categoría	n.a.	Aplica	=	[mp.per.1]	Alto
categoría	aplica	=	=	[mp.per.2]	Alto
categoría	aplica	=	=	[mp.per.3]	Alto
categoría	aplica	=	=	[mp.per.4]	Alto
D	n.a.	n.a.	aplica	[mp.per.9]	Alto
categoría	aplica	+	=	[mp.eq.1]	Alto
A	n.a.	Aplica	+	[mp.eq.2]	Medio
categoría	aplica	=	+	[mp.eq.3]	Alto
D	n.a.	Aplica	=	[mp.eq.9]	Alto
categoría	aplica	=	+	[mp.com.1]	Alto
C	n.a.	Aplica	+	[mp.com.2]	Medio
I A	aplica	+	++	[mp.com.3]	Alto
categoría	n.a.	n.a.	aplica	[mp.com.4]	Alto
D	n.a.	n.a.	aplica	[mp.com.9]	Alto
C	aplica	=	=	[mp.si.1]	Medio
I C	n.a.	Aplica	+	[mp.si.2]	Alto
categoría	aplica	=	=	[mp.si.3]	Alto
categoría	aplica	=	=	[mp.si.4]	Alto
C	aplica	+	=	[mp.si.5]	Medio
categoría	n.a.	Aplica	=	[mp.sw.1]	Alto
categoría	aplica	+	++	[mp.sw.2]	Alto
categoría	aplica	=	=	[mp.info.1]	Alto
C	aplica	+	=	[mp.info.2]	Medio
C	n.a.	n.a.	aplica	[mp.info.3]	No Aplica
I A	aplica	+	++	[mp.info.4]	Alto
T	n.a.	n.a.	aplica	[mp.info.5]	No Aplica
C	aplica	=	=	[mp.info.6]	Medio
D	aplica	=	=	[mp.info.9]	Alto
categoría	aplica	=	=	[mp.s.1]	Alto
categoría	aplica	=	+	[mp.s.2]	Alto
D	n.a.	Aplica	+	[mp.s.8]	Alto
D	n.a.	n.a.	aplica	[mp.s.9]	Alto

En resumen, de las 75 medidas definidas en el Anexo II del Real Decreto 3/2010, solo 72 son de aplicación/exigidas para el sistema del ejemplo:

- 64 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.
- 3 No aplican.

5. PERFIL DE CUMPLIMIENTO

El Anexo II del Real Decreto 3/2010 determina las medidas de seguridad a implementar en función de un riesgo residual identificado según los niveles de seguridad asociados a las dimensiones y la categoría del Sistema. De esta manera, se constituye e identifica una línea base a asumir por el responsable del sistema para que este sea considerado conforme con el Esquema Nacional de Seguridad.

Por consiguiente, categorizando el sistema y a partir de un catálogo de referencia concretado en setenta y cinco (75) medidas de seguridad, la Declaración de Aplicabilidad determina, a priori, las medidas de seguridad que el sistema está obligado a implementar para conseguir su adecuación. El Esquema Nacional de Seguridad también considera la inclusión de medidas compensatorias.

Este catálogo de medidas a implementar no deja de ser una referencia, ya que, en casos muy concretos y excepcionales, se podría asumir un riesgo residual mayor o menor en función de los recursos disponibles por la entidad titular del sistema de información objeto de la adecuación o el servicio que se vaya a prestar.

En algunos casos, incluso, podría determinarse que no fuera obligatoria la implementación de alguna de las medidas de seguridad a las que compromete el Anexo II del Real Decreto 3/2010, en función de un perfil de cumplimiento validado.

Un perfil de cumplimiento estará conformado por un conjunto de medidas de seguridad y su implementación concreta resultado de un análisis de riesgos (riesgo residual asumible).

El Centro Criptológico Nacional, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento que se determinen para garantizar la seguridad de los sistemas de tecnologías de la información en las entidades del Sector Público, de acuerdo con lo establecido en el Artículo 29 del Real Decreto 3/2010 sobre instrucciones técnicas de seguridad y guías de seguridad.

6. DECÁLOGO DE RECOMENDACIONES

A continuación, se muestra un decálogo de recomendaciones a tener en cuenta para determinar una Declaración de Aplicabilidad en el ámbito 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 del tipo “Servicio”, se recomienda valorar en primer lugar la dimensión de disponibilidad [D], pues los requisitos en materia de confidencialidad, integridad, autenticidad y trazabilidad suelen venir heredados por la valoración de los activos del 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 el nivel de madurez 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 40 medidas.
6	Seleccionar las medidas que aplican al sistema en función de sus niveles de seguridad, de un total de 35 medidas.
7	Emplear el simulador elaborado por el CCN-CERT, que determina 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. 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 la Declaración de Aplicabilidad, hacer uso de la plantilla elaborada por el CCN-CERT y tener en cuenta los perfiles de cumplimiento validados por el CCN en las correspondientes guías CCN-STIC.