Análisis de Riesgos y Declaración de Aplicabilidad: Perfiles de Cumplimiento

I Encuentro del ENS.
Tendencias y Políticas de Seguridad

Índice

Índice

1. Conceptos Generales del ENS

1. Conceptos Generales del ENS

¿Cómo sé las medidas de seguridad del Anexo II que son de aplicación?

¿He categorizado mi sistema?

NO

1 Proceder a realizar la **CATEGORIZACIÓN**, según el Anexo I del ENS

La **importancia** de la información que maneja y los servicios que presta

El **esfuerzo** de seguridad requerido

SI

2 De forma directa, seguir la tabla de medidas de seguridad del Anexo II del ENS

Afectadas	B	M	A	Medida
A T	aplica	=	=	[op.acc.1]
I C A T	aplica	=	=	[op.acc.4]
T	aplica	+	++	[op.exp.8]
D	n.a.	n.a.	aplica	[op.ext.9]

CCN centro criptológico nacional

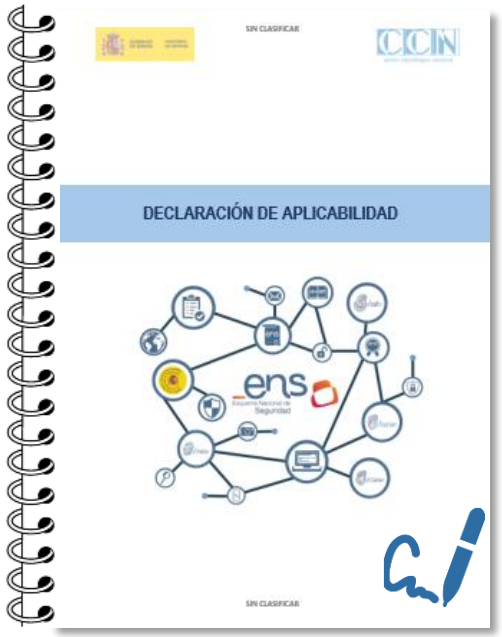
1. Conceptos Generales del ENS

CCN-STIC-819

DECLARACIÓN DE APLICABILIDAD

DEFINICIÓN

Es el documento en el que se recogen las medidas de seguridad del Anexo II del ENS que son de aplicación al Sistema y que debe estar firmado por el Responsable de Seguridad.



MEDIDAS DE SEGURIDAD DEL ANEXO II

+

MEDIDAS COMPENSATORIAS (CCN-STIC-819)

CCN centro criptológico nacional

1. Conceptos Generales del ENS

DECLARACIÓN DE APLICABILIDAD

¿Por qué es importante?

Desde el punto de vista del RESPONSABLE….

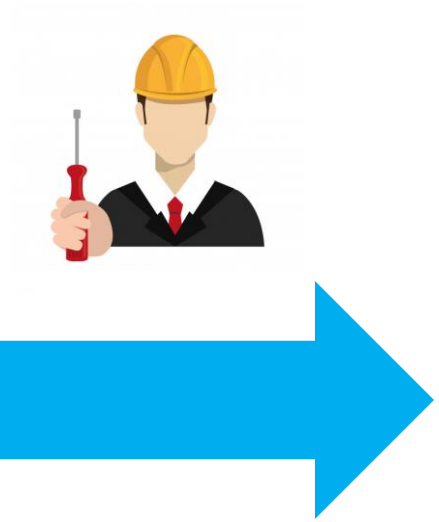
Para saber qué medidas son requeridas y, por tanto, saber qué tiene que implementar.

Desde el punto de vista del AUDITOR…

Verificar que la DdA está bien construida.

Para saber las medidas sobre las cuáles tiene que verificar su cumplimiento.

1. Conceptos Generales del ENS



QUÉ hay que hacer
CÓMO hay que hacerlo
CUÁNDO hay que hacerlo
QUIÉN lo va a hacer
CUÁNTO nos va a costar

El **PLAN DE ADECUACIÓN** es un documento en el que se recoge cómo se va a conseguir la conformidad con el ENS: qué medidas se van a implementar, con qué recursos, los plazos, las prioridades, las responsabilidades, etc…

CCN
centro criptológico nacional

1. Categorización

PROCEDIMIENTO DEFINIDO EN ANEXO I DEL RD

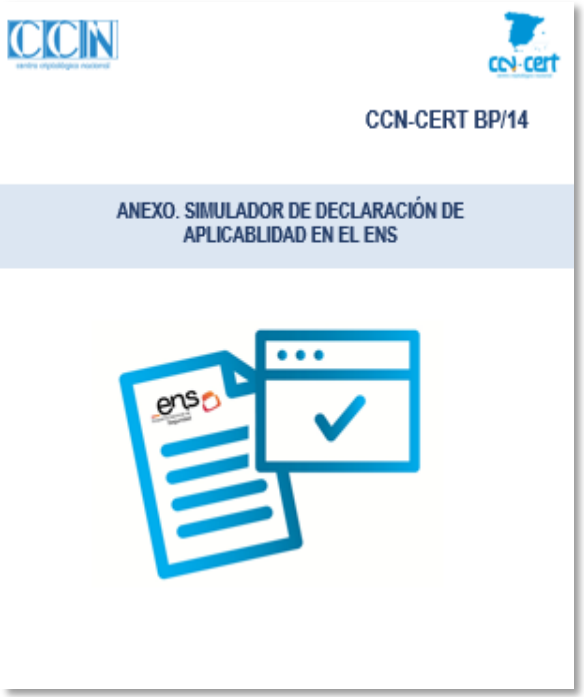
A modo de resumen, se tendrá en cuenta lo siguiente:

- Las dimensiones de la seguridad **[D]**, **[A]**, **[C]**, **[I]**, **[T]**.
- Se realizará un **inventario** de los activos del Sistema, en especial, de los **esenciales**.
- Se determinará el **nivel de seguridad** requerido para cada dimensión: NIVEL BAJO, NIVEL MEDIO o NIVEL ALTO y por cada uno de los activos esenciales identificados.
- El **nivel de seguridad global** para cada dimensión vendrá determinado por el nivel más alto asociado a cada dimensión y activo esencial.
- La **categoría** del Sistema será el mayor de los niveles de seguridad asignados.

1. Categorización

La **categorización** tiene como resultado la **Declaración de Aplicabilidad**

Determinar las medidas de seguridad que son de aplicación es un **proceso automático** derivado de seguir lo indicado en el Anexo II del RD 3/2010.



SIMULADOR DECLARACIÓN DE APLICABILIDAD

C	I	D	A	T	categoría
A	M	B	M	B	A

Se deben introducir los niveles de seguridad asociados a las dimensiones de seguridad (fila 5, desde la columna H hasta la L).

N° total de medidas: 61

ORDEN	MEDIDAS	DIMENSIONES	B	M	A	VALORES
1	[org.1]	categoría	aplica	aplica	aplica	Aplica
2	[org.2]	categoría	aplica	aplica	aplica	Aplica
3	[org.3]	categoría	aplica	aplica	aplica	Aplica
4	[org.4]	categoría	aplica	aplica	aplica	Aplica
5	[op.pl.1]	categoría	aplica	aplica	aplica	Aplica
6	[op.pl.2]	categoría	aplica	aplica	aplica	Aplica
7	[op.pl.3]	categoría	aplica	aplica	aplica	Aplica
8	[op.pl.4]	D	n.a.	aplica	aplica	
9	[op.pl.5]	categoría	n.a.	n.a.	aplica	Aplica

La Declaración de Aplicabilidad es un conjunto de medidas que puede utilizarse como **CATÁLOGO DE REFERENCIA**

1. Categorización

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

La **categoría** de este sistema es **ALTA**: [C(**A**), I(M), D(B), A(M), T(B)].

1. Categorización

ALTA: [C(**A**), I(M), D(B), A(M), T(B)]

Dimensiones	Básica	Media	Alta	Medida de seguridad	¿Aplica?	Nivel de exigencia
categoría	aplica	+	=	[op.exp.11]		
categoría	n.a.	aplica	=	[op.ext.1]		
categoría	n.a.	aplica	=	[op.ext.2]		
D	n.a.	n.a.	aplica	[op.ext.9]		
D	n.a.	aplica	=	[op.cont.1]		
categoría	n.a.	aplica	=	[op.mon.1]		
categoría	aplica	+	++	[op.mon.2]		
categoría	aplica	=	=	[mp.if.1]		
categoría	aplica	=	=	[mp.if.2]		
categoría	aplica	=	=	[mp.if.3]		
D	aplica	+	=	[mp.if.4]		
D	n.a.	aplica	=	[mp.if.6]		
D	n.a.	n.a.	aplica	[mp.if.9]		

1

2

1

3

2

CCN centro criptológico nacional

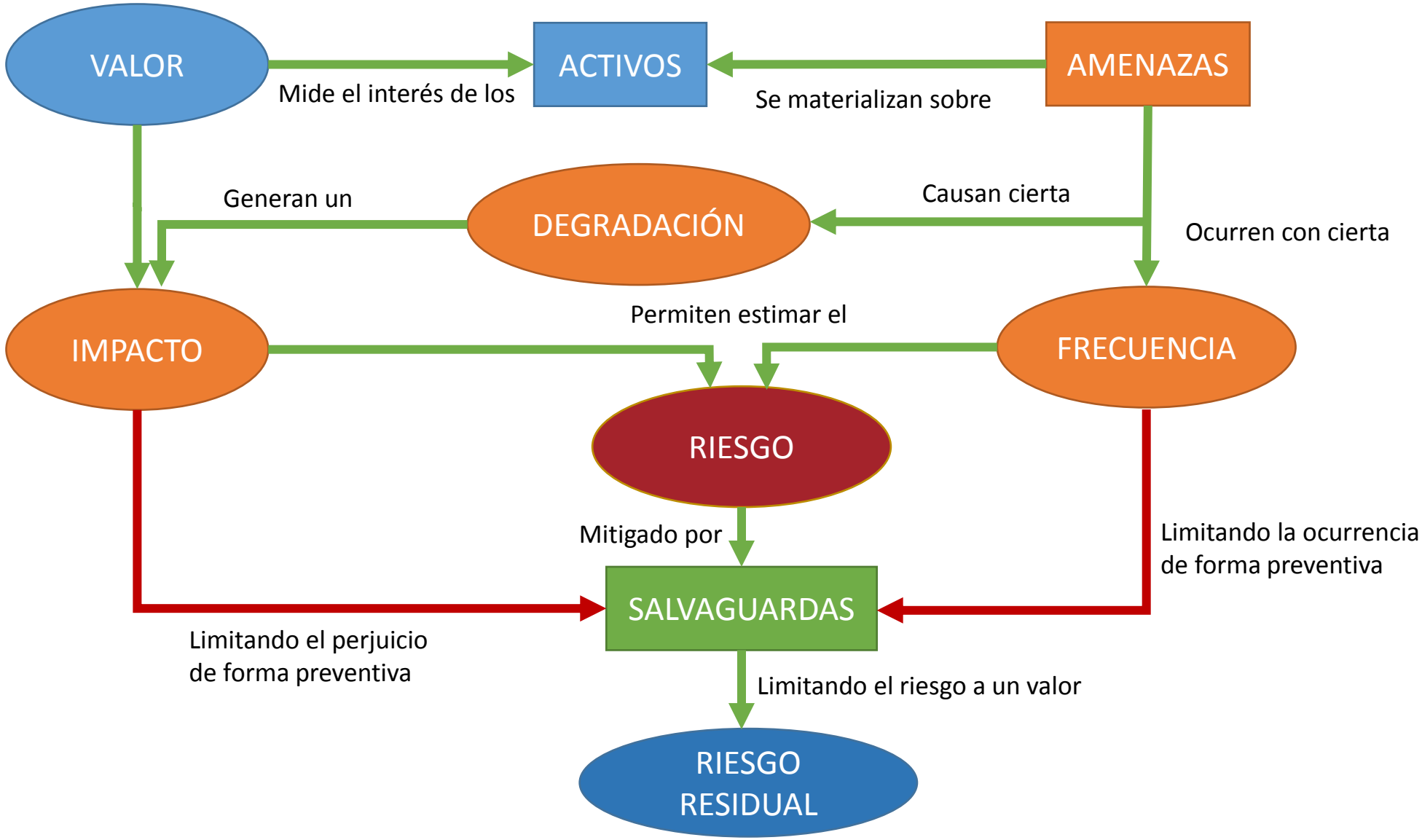
Índice

2. Análisis de Riesgos

DEFINICIÓN

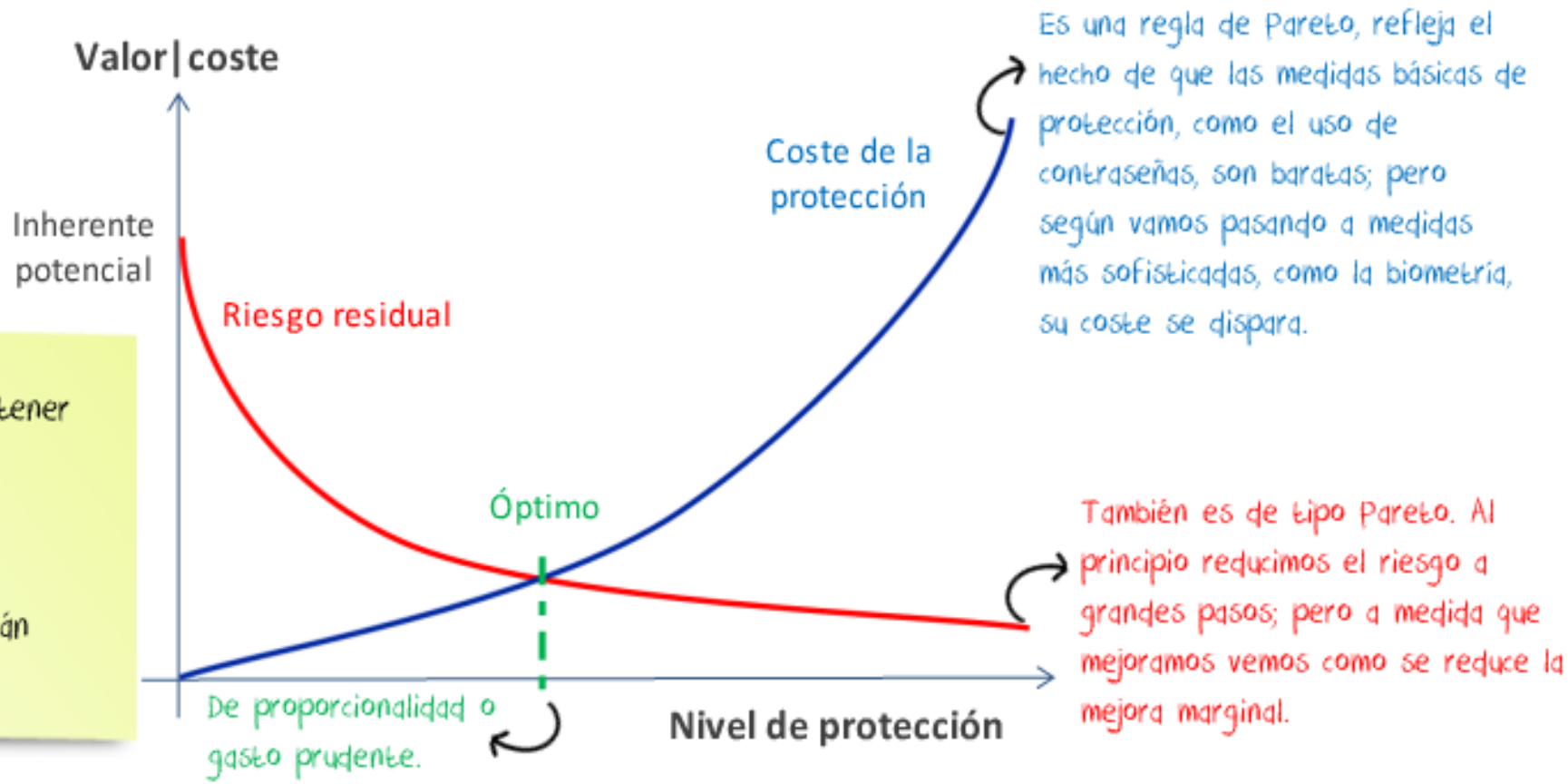
El **análisis de riesgos** informáticos es un **proceso** que comprende la identificación de **activos** informáticos, las **vulnerabilidades** y **amenazas** a los que se encuentran expuestos, su **probabilidad** de ocurrencia y el **impacto** de su materialización, a fin de determinar los **controles** adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

2. Análisis de Riesgos



2. Análisis de Riesgos

Implantación de salvaguardas / medidas de seguridad



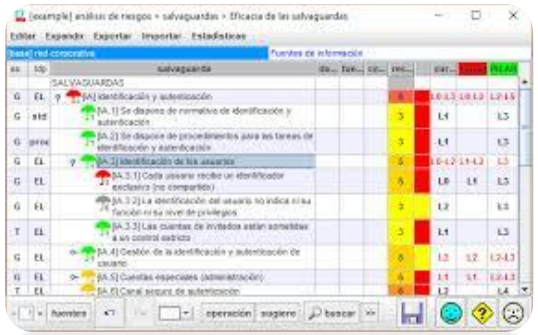
En la práctica no es posible tener un cálculo tan fino, con líneas continua, de gasto y riesgo residual. Tendremos algunas opciones concretas que estarán situadas sobre estas líneas.

2. Análisis de Riesgos

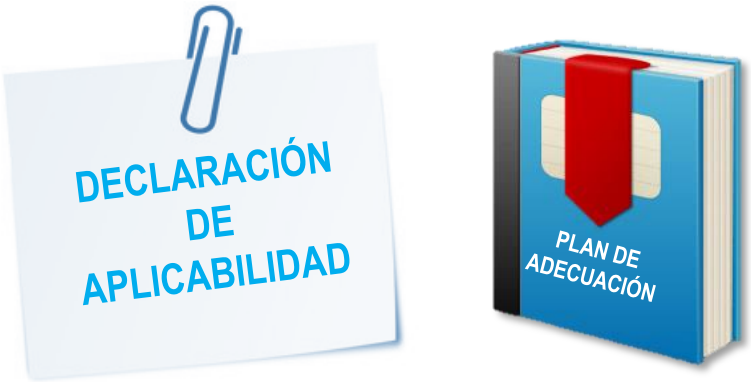
Pero… **¿qué relación existe entre la Declaración de Aplicabilidad y el AR?**

Versión Inicial

Análisis de Riesgos



Versión Final



Ajuste medidas de aplicación

Priorización

centro criptológico nacional

2. Análisis de Riesgos

¿Qué implica la realización de un Análisis de Riesgos?

El resultado del Análisis del Riesgo es un **Riesgo Residual,** que debe ser asumido por los Responsables del Sistema

Riesgo Residual

Es el nivel de riesgo que permanece en la organización **tras mitigar/reducir o eliminar los riesgos** con la implementación de medidas

Si el Riesgo Residual no es aceptado

Las medidas a aplicar serán las derivadas del Análisis de Riesgos realizado

Si el Riesgo Residual es aceptado

Las medidas a aplicar serán las definidas en el Anexo II del RD (la Declaración de Aplicabilidad)

CCN centro criptológico nacional

Índice

3. Perfiles de cumplimiento

Pero… **¿qué relación existe entre la Declaración de Aplicabilidad y el AR?**

Tras realizar el AR…

a) **PRIORIZACIÓN** en la implementación de medidas: actualización del Plan de Adecuación

b) **DETERMINACIÓN** de las medidas incluidas en la Declaración de Aplicabilidad en función del **RIESGO RESIDUAL** a aceptar:

- Medidas compensatorias que sustituye a una de aplicación.
- Medidas excepcionales, a aplicar con independencia de la aplicabilidad que determina el Anexo 2 RD 3/2010. (Perfil de Cumplimiento validado)
  - Sistemas Clasificados.
  - Entidades Locales.
  - Servicios en nube.

La inclusión del Análisis de Riesgos en el proceso de determinación de la Declaración de Aplicabilidad deriva en un **PERFIL DE CUMPLIMIENTO**

3. Perfiles de cumplimiento

PERFIL DE CUMPLIMIENTO

La inclusión del Análisis de Riesgos en el proceso de determinación Declaración de Aplicabilidad resulta en un **PERFIL DE CUMPLIMIENTO**

Un **PERFIL DE CUMPLIMIENTO** implica:

1) Un conjunto de medidas de seguridad.
2) La implementación concreta y detallada de cada medida de seguridad.
3) Aceptación del riesgo residual obtenido tras la implementación de las medidas de seguridad.

3. Perfiles de cumplimiento

riesgo
{4,5}
{4,5}
{4,5}
{4,5}
{4,5}
{4,5}
{4,2}

Análisis de Riesgos

</pilar>

Categorización

Declaración de Aplicabilidad Inicial

Medida de seguridad	Aplica	Nivel de exigencia
[op.exp.11]	Aplica	Alto
[op.ext.1]	Aplica	Alto
[op.ext.2]	Aplica	Alto
[op.ext.9]	No Aplica	No aplica
[op.cont.1]	No Aplica	No aplica
[op.mon.1]	Aplica	Alto
[mp.if.4]	Aplica	Bajo
[mp.if.6]	No Aplica	No aplica

Perfil de Cumplimiento

VALIDADO

Medida de seguridad	Aplica	Nivel de exigencia
[op.exp.11]	Aplica	Alto
[op.ext.1]	Aplica	Medio
[op.ext.2]	Aplica	Alto
[op.ext.9]	No Aplica	No aplica
[op.cont.1]	No Aplica	No aplica
[op.mon.1]	No Aplica	No Aplica
[mp.if.4]	Aplica	Alto
[mp.if.6]	No Aplica	No aplica

</pilar>

Aceptación Riesgo Residual

Versión Final

DECLARACIÓN DE APLICABILIDAD

PLAN DE ADECUACIÓN

ALTA: [C(**A**), I(M), D(B), A(M), T(B)]

3. Perfiles de cumplimiento

Declaración de Aplicabilidad Inicial

Medida de seguridad	Aplica	Nivel de exigencia
[op.exp.11]	Aplica	Alto
[op.ext.1]	Aplica	Alto
[op.ext.2]	Aplica	Alto
[op.ext.9]	No Aplica	No aplica
[op.cont.1]	Aplica	Alto
[op.mon.1]	No Aplica	No Aplica
[mp.if.4]	Aplica	Bajo
[mp.if.6]	No Aplica	No aplica
[mp.if.7]	No Aplica	No Aplica
[mp.if.8]	Aplica	Alto
[mp.if.9]	Aplica	Alto
[mp.exp.1]	Aplica	Alto

Perfil de Cumplimiento

Medida de seguridad	Aplica	Nivel de exigencia
[op.exp.11]	Aplica	Alto
[op.ext.1]	Aplica	Alto
[op.ext.2]	Aplica	Medio
[op.ext.9]	No Aplica	No aplica
[op.cont.1]	No Aplica	No aplica
[op.mon.1]	No Aplica	Alto
[mp.if.4]	Aplica	Alto
[mp.if.6]	No Aplica	No aplica
[mp.if.7]	Aplica	Alto
[mp.if.8]	Aplica	Alto
[mp.if.9]	Aplica	Compensada
[mp.exp.1]	Aplica	Alto

Que encontramos en un Perfil de Cumplimiento

- Reducir el nivel incremental de una medida
- Suprimir la aplicación de una medida
- Aumentar el nivel incremental de una medida
- Incluir la aplicación de una medida
- Proponer medida compensatoria

CCN centro criptológico nacional

3. Perfiles de cumplimiento

PERFIL DE CUMPLIMIENTO

Entidades Locales

Facilitar su adecuación al ENS con un perfil de cumplimiento específico, de forma que la adecuación sea factible, dados los recursos humanos y económicos disponibles en la entidad.

Aunque la categoría del sistema sea BÁSICA, si aplicamos el Anexo II del RD 3/2010, se deberían adoptar 45 medidas. Si embargo, si realizamos un **Análisis de Riesgos** podrían darse los siguientes escenarios:

ESCENARIO 1

La modificación de una o varias medidas de seguridad aplicables NO afecta al riesgo residual.

?	Valorar si tiene sentido la exigencia de dicha medida

ESCENARIO 2

La modificación de una o varias medidas de seguridad aplicables AUMENTA el riesgo residual

?	Valorar si el aumento del riesgo residual puede todavía ser asumible

CCN centro criptológico nacional

3. Perfiles de cumplimiento

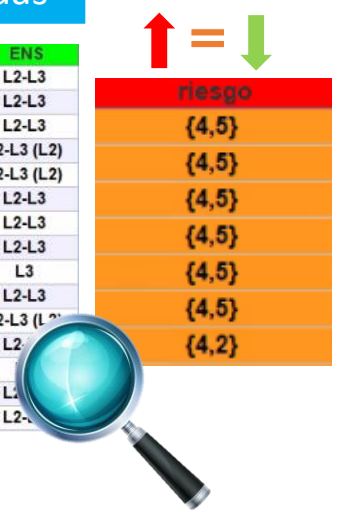
PERFIL DE CUMPLIMIENTO

Entidades Locales

Facilitar su adecuación al ENS con un perfil de cumplimiento específico, de forma que la adecuación sea factible, dados los recursos humanos y económicos disponibles en la entidad.

Catálogo de medidas/salvaguardas

reco...	control	ENS
	[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)	L2-L3
5	[org] Marco organizativo	L2-L3
5	[org.1] Política de Seguridad	L2-L3
5	[org.2] Normativa de seguridad	L2-L3 (L2)
5	[org.3] Procedimientos de seguridad	L2-L3 (L2)
5	[org.4] Proceso de autorización	L2-L3
8	[op] Marco operacional	L2-L3
5	[op.pl] Planificación	L2-L3
3	[op.pl.1] Análisis de riesgos	L3
5	[op.pl.2] Arquitectura de seguridad	L2-L3
5	[op.pl.3] Adquisición de nuevos componentes	L2-L3 (L2)
3	[op.pl.4] Dimensionamiento / Gestión de capacidades	L2
3	[op.pl.5] Componentes certificados	
7	[op.acc] Control de acceso	L2
5	[op.acc.1] Identificación	L2-



Análisis del riesgo residual

Selección de aquellas medidas cuyo aplicación se considera obligatoria porque el riesgo residual resultante de no aplicarlas no sería asumible

- ✓ Algunas medidas que, por defecto aplicarían, podrían no ser exigidas.
- ✓ Podrían exigirse otras que, según el Anexo II, no aplicarían.

Perfil de cumplimiento

[org.1]	Aplica
[org.2]	Aplica
[org.3]	Aplica
[op.acc.1]	Aplica
[op.acc.2]	Aplica
[op.acc.4]	Aplica
[op.acc.5]	Aplica
[op.acc.6]	Aplica
[mp.info.6]	Aplica
[mp.info.9]	Aplica
[mp.s.1]	Aplica
[mp.s.2]	Aplica

- ✓ Recogerá un número de medidas que podrían no ser las 45 medidas que son de aplicación para categoría BÁSICA.

centro criptológico nacional

3. Perfiles de cumplimiento

PERFIL DE CUMPLIMIENTO

Servicios *cloud*

Facilitar su adecuación al ENS con un perfil de cumplimiento específico, de forma que las Administraciones Públicas sepan qué deben exigir a sus proveedores de servicios en la nube.

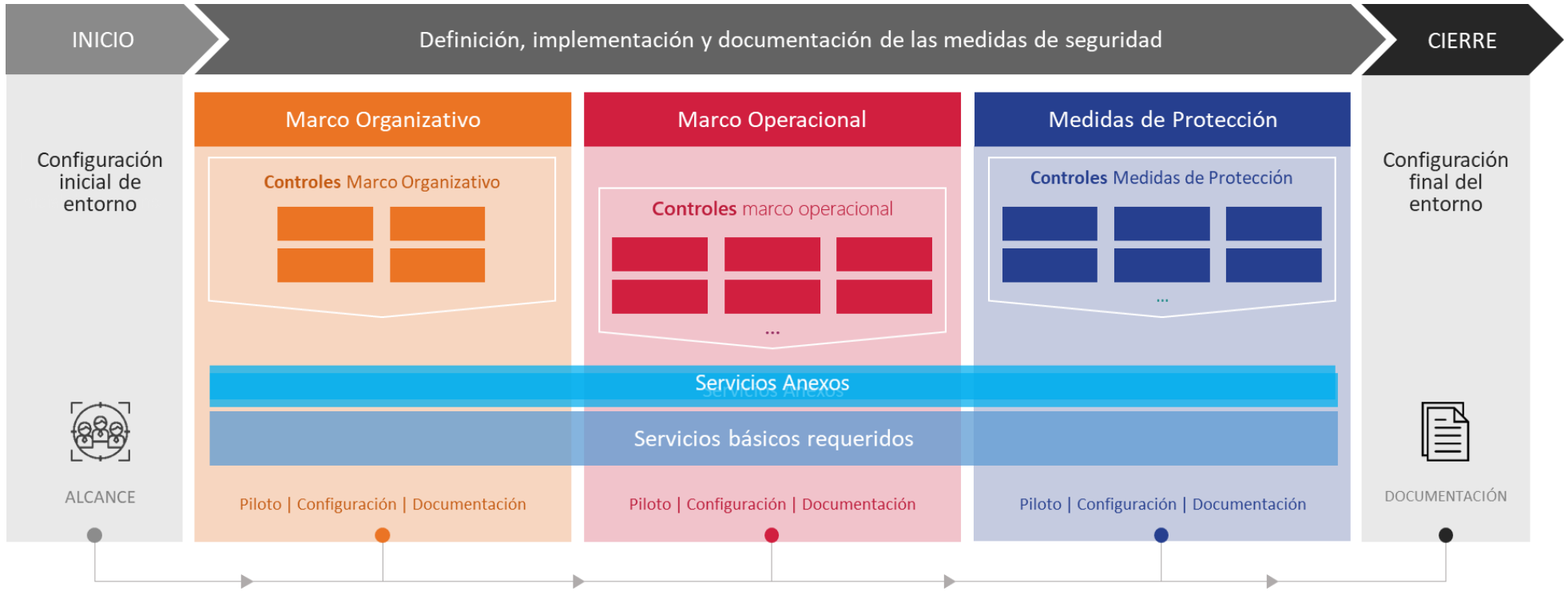
Una vez que se analizan las dimensiones de seguridad, el siguiente paso es una Evaluación de riesgos, una declaración de aplicabilidad (las medidas que se deberán tener en cuenta) y el **PERFIL DE CUMPLIMIENTO** que especificará la configuración de seguridad de las medidas incluidas en la declaración de aplicabilidad.

3. Perfiles de cumplimiento

PERFIL DE CUMPLIMIENTO

Servicios *cloud*

El **VALOR AÑADIDO** comprenderá suministrar una guía y una configuración de seguridad de las medidas de seguridad incluidas en la Declaración de Aplicabilidad (Perfil de Cumplimiento).



3. Perfiles de cumplimiento

PERFIL DE CUMPLIMIENTO

Servicios *cloud*

El **VALOR AÑADIDO** consiste en proporcionar una guía de configuración segura/bastionado de acuerdo a las medidas de seguridad incluidas en perfil de cumplimiento.

 *Workshop*

 Configuración

 Documentación

Para cada medida, revisar las **responsabilidades** del **proveedor**, las responsabilidades del **cliente** y los elementos a incluir para cubrir estas responsabilidades

Para todos los elementos identificados como responsabilidad del proveedor, incluir los **mecanismos necesarios** para trazar que están **cubiertos** por las diferentes auditorías y certificaciones.

Dentro del perfil de cumplimiento es necesario detallar **cómo se cubren** las diferentes responsabilidades.

CCN centro criptológico nacional

3. Perfiles de cumplimiento

PERFIL DE CUMPLIMIENTO

Servicios *cloud*

Adecuación al ENS con un perfil de cumplimiento específico, de forma que las Administraciones Públicas sepan qué deben exigir a sus proveedores de servicios.

Metodología y elementos a conseguir para adoptar servicios en la nube, según el ENS:

Análisis de riesgos (AR).

Declaración de aplicabilidad (el conjunto de medidas que son de aplicación)

Certificación de conformidad con el ENS (categoría ALTA).

Un PERFIL DE CUMPLIMIENTO que incluya las configuraciones de seguridad de las medidas incluidas en la declaración de aplicabilidad.

Índice

4. Conclusiones

La elaboración de **PERFILES DE CUMPLIMIENTO** tienen como objetivo facilitar el cumplimiento del ENS y que los servicios de los que hacen uso las Administraciones Públicas se presten de acuerdo a unos niveles mínimos de confianza.

- Las medidas derivadas de la aplicación del Anexo II del RD 3/2010 es una referencia a tener en cuenta que, tras el oportuno Análisis de Riesgos, y en casos puntuales, podrían permitir el ajuste del riesgo residual en función de los recursos disponibles y la adopción de medidas compensatorias.
- El riesgo residual resultante de no aplicar alguna medida debe ser asumido, controlado y monitorizado por la entidad.
- Los perfiles de cumplimiento serán validados por el Centro Criptológico Nacional.
- Se persigue que el cumplimiento del ENS tenga un mayor enfoque en los riesgos del sistema (flexibilidad). El resultado del Análisis de Riesgos determinará, a priori, las medidas a cumplir para conseguir la adecuación con el ENS.

Muchas gracias