

XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas



Certificación del ENS.
Situaciones planteadas a una
entidad de certificación



○ José Luis Colom Planas

○ Director Técnico

○ Entidad de certificación
especializada en el ENS

AUDERTIS

○ jl.colom@audertis.es



Índice

1. ¿Se certifica la organización, el sistema de información o el sistema de gestión?
2. Compatibilidad entre roles y responsabilidades en el ENS.
3. La importancia del 'alcance' en la certificación del ENS.
4. La aplicación de las medidas no solo depende de la categoría del sistema.
5. Resumen final





¿Se certifica la organización, el sistema de información o el sistema de gestión?



¿Se certifica el sistema de información, el de gestión, o la propia empresa?

SE REQUIERE

Para categorías **MEDIA** y **ALTA**



Sistema de Gestión de la Seguridad de la Información (SGSI)

SE CERTIFICA



Sistema de Información que soporta los servicios y la información que éstos tratan





Había una vez una niña muy linda que vivía en el bosque con su mama, que le había hecho una capa roja para protegerse del frio y el viento. A la niña le gustaba tanto la capuchita que la llevaba a todas horas, por lo que que todo el mundo la llamaba Caperucita Roja.

SE CERTIFICA



Sistema de Información
que soporta los servicios y
la información que éstos tratan

ALCANCE: “Sistema de información...”

ALCANCE: “Sistema de información que soporta los servicios...”

ALCANCE: “Sistema de información que soporta los servicios (...) siendo prestados por [organización certificada...”

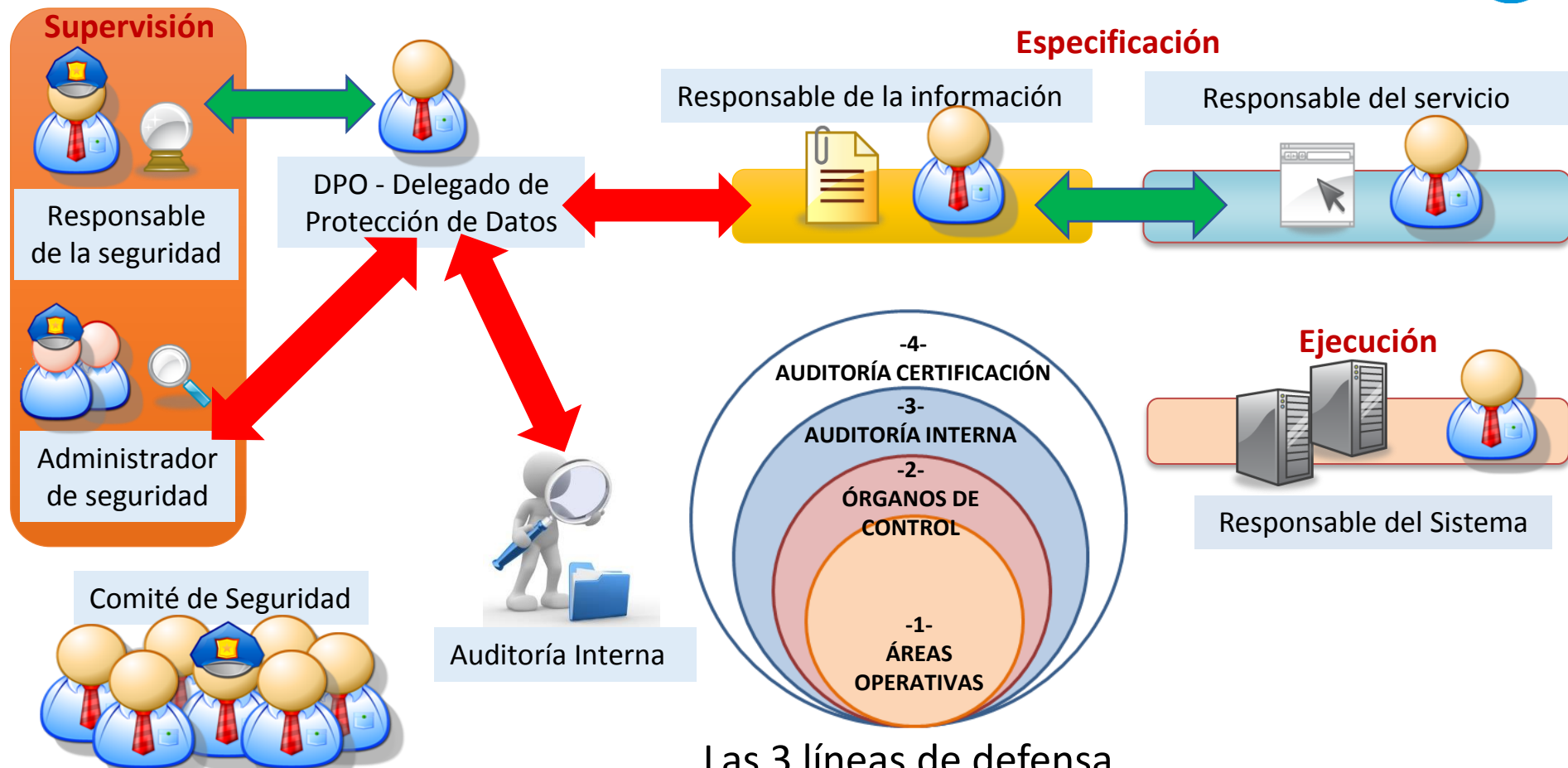
ALCANCE: “Sistema de información gestionado por [organización certificada] que soporta los servicios...”

ALCANCE: “Sistema de información propiedad de [organización certificada] para la prestación de los servicios...”



Compatibilidad entre Roles y responsabilidades en el ENS







Noviembre de 2018

Gabinete Jurídico

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, sobre la posible compatibilidad entre la figura del delegado de protección de datos del Reglamento general de protección de datos y el responsable de seguridad de la información del Esquema Nacional de Seguridad, cúmpleme informarle lo siguiente:

(...)

Solo excepcionalmente, en aquellas organizaciones que, por su tamaño y recursos, no pudieran observar dicha separación, sería admisible la designación como delegado de protección de datos de la persona que ejerciera las funciones de responsable de seguridad del ENS, siempre que en la misma concurren los requisitos de formación y capacitación previstos en el RGPD.

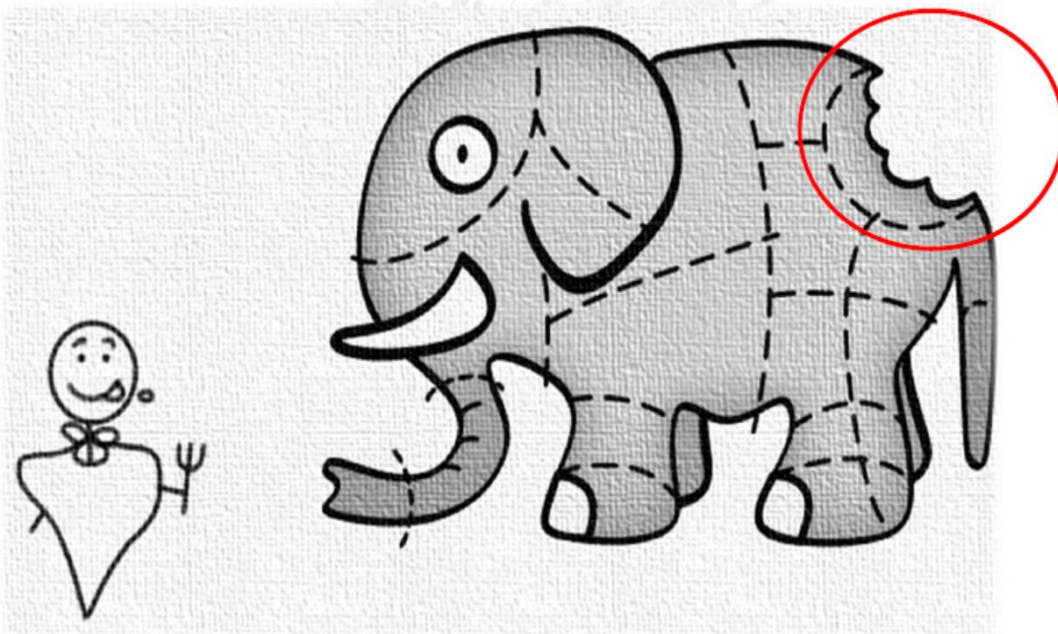
Además, resultaría imprescindible adoptar todas las medidas organizativas, debidamente reflejadas en su Política de seguridad de la información, que garantice la necesaria independencia y la ausencia de conflicto de intereses, por lo que no podría recibir instrucciones respecto al desempeño de sus funciones como delegado de protección de datos, deberá responder directamente al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios del tratamiento. En todo caso, esta circunstancia, que como decíamos, tiene carácter excepcional, deberá evaluarse caso por caso, y deberá dejarse documentada dicha designación haciendo constar los motivos por lo que el organismo correspondiente no ha podido observar dicha separación de funciones así como las medidas que garantizan la necesaria independencia del delegado de protección de datos.



La importancia del 'alcance' en la certificación del ENS



Menos es Más (- es +) XI JORNADAS STIC CCN-CERT



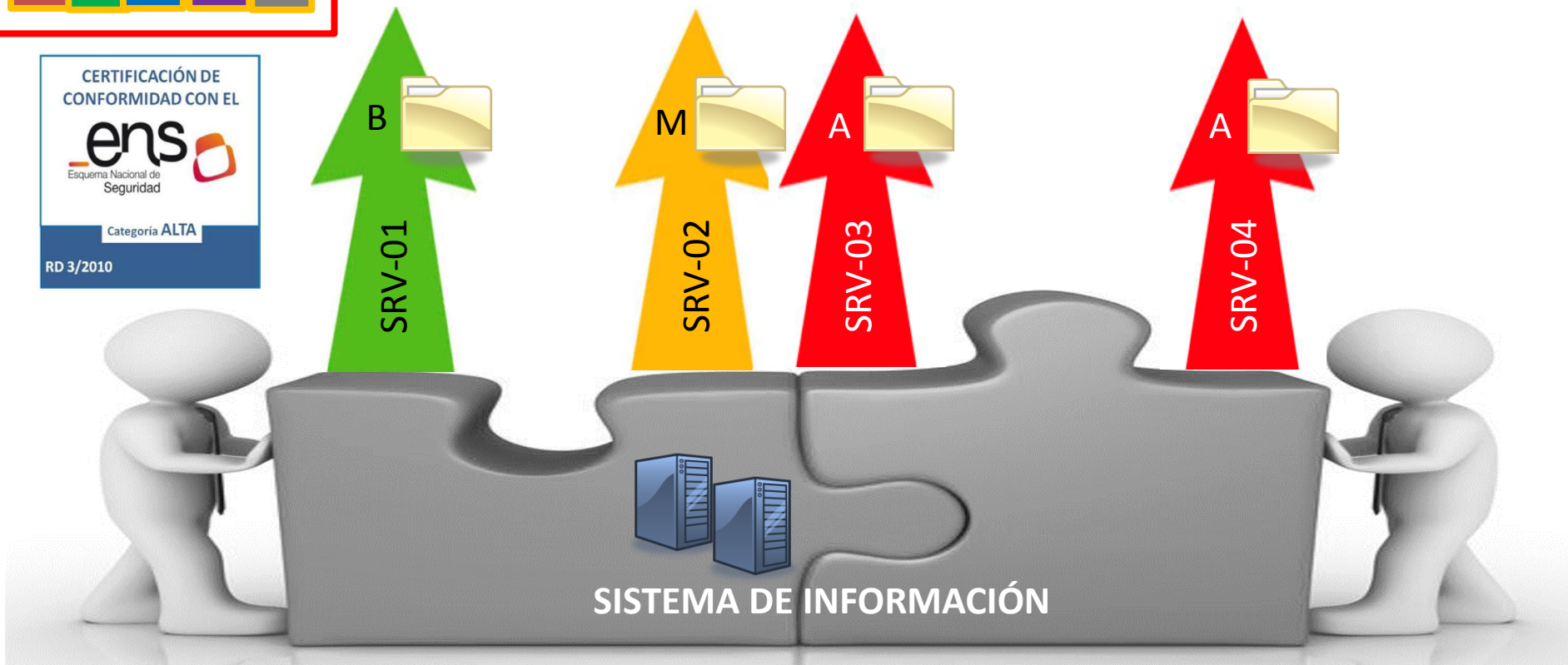
www.ccn-cert.cni.es

34

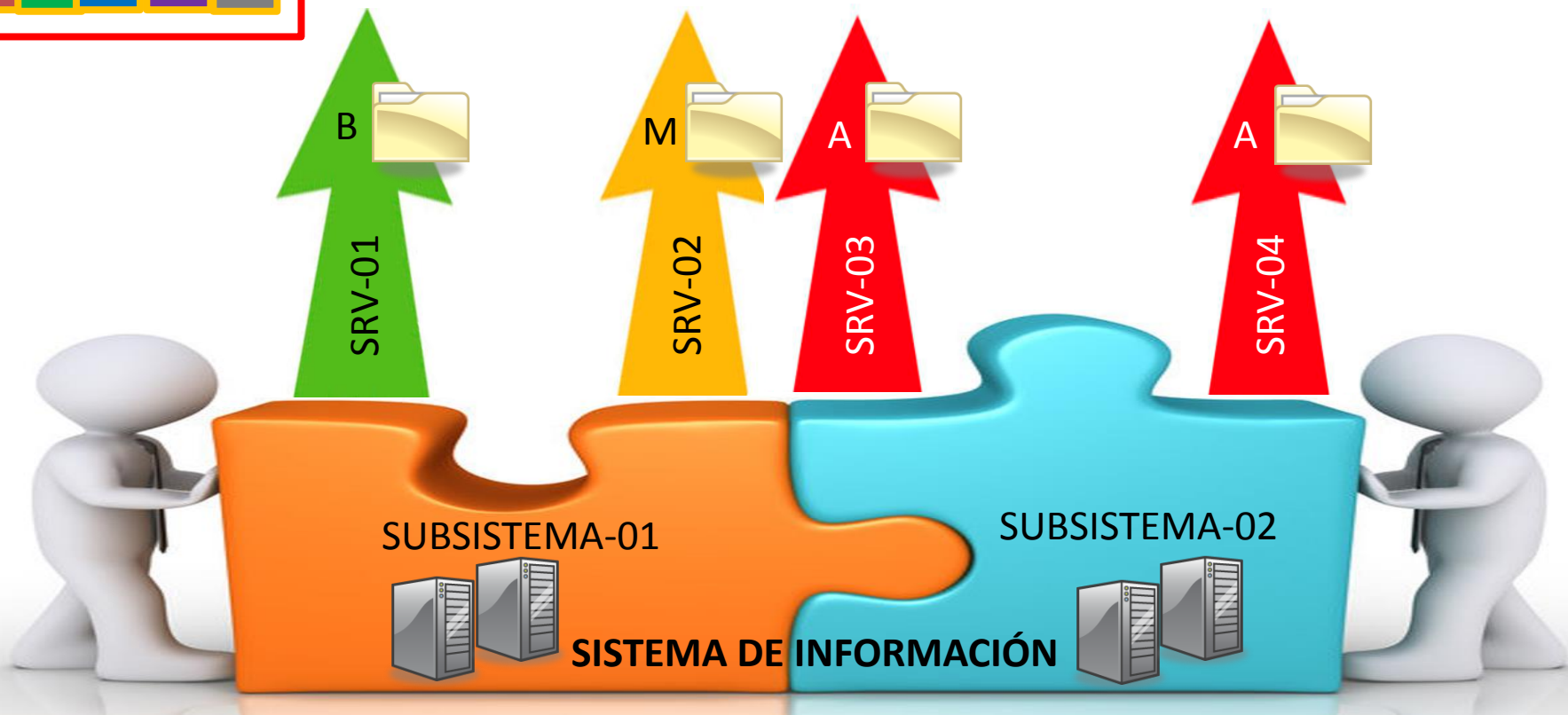
"Nada es especialmente difícil si lo dividimos en tareas pequeñas."

Henry Ford





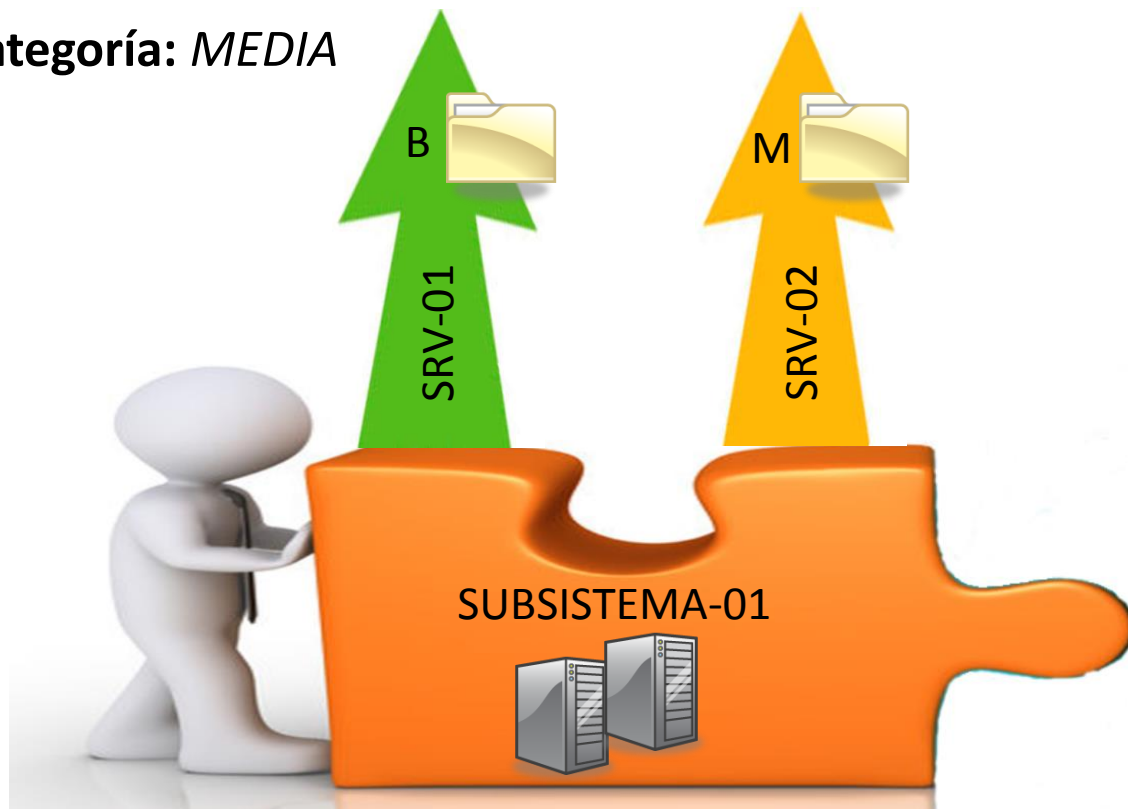
C I D A T





Alcance: *Sistema de información que soporta los servicios SRV-01 y SRV-02...*

Categoría: *MEDIA*



La aplicación de las medidas no solo depende de la categoría del sistema.



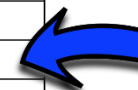


Caso 1: Afectación del nivel, en cada dimensión de seguridad del sistema, respecto a las medidas de seguridad del Anexo II.





				op	Marco operacional
	B	M	A	op.pl	Planificación
categoría	aplica	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	+	++	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento/Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
I C A T	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local (<i>local logon</i>)
I C A T	aplica	+	=	op.acc.7	Acceso remoto (<i>remote login</i>)



SISTEMA DE CATEGORÍA MEDIA



				op	Marco operacional
	B	M	A	op.pl	Planificación
categoría	aplica	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	+	++	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento/Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
AT	aplica	=	=	op.acc.1	Identificación
ICAT	aplica	=	=	op.acc.2	Requisitos de acceso
ICAT	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
ICAT	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
ICAT	aplica	+	++	op.acc.5	Mecanismo de autenticación
ICAT	aplica	+	++	op.acc.6	Acceso local (<i>local logon</i>)
ICAT	aplica	+	=	op.acc.7	Acceso remoto (<i>remote login</i>)

CATEGORÍA BÁSICA: [C(N/A), I(B), D(B), A(B), T(B)]

CATEGORÍA MEDIA: [C(N/A), I(B), D(B), A(M), T(B)]

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



Sector Público:

- ☐ Se nombran **Responsables del Servicio y de la Información**.
- ☐ Dichos responsables valoran los servicios y la información, categorizando el sistema el **Responsable del Sistema** a partir de dichas valoraciones.
- ☐ Son importantes los valores de los niveles en sus cinco dimensiones.



Sector Privado:

- ☐ No es necesario nombrar responsables del Servicio y de la Información.
- ☐ No es necesario valorar servicios ni información.
- ☐ Se adscribe a determinada categoría del sistema.
- ☐ Debe cumplir en todas las dimensiones para determinada categoría, inexorablemente, al desconocer con que AAPP colaborarán.



Sector Privado:

- ☐ (...).
- ☐ Deben cumplir en todas las dimensiones para determinada categoría, inexorablemente, al desconocer con que AAPP colaborarán, **excepto si lo detallan en el alcance.**

Everis

Everis, S.L.U.

www.everis.com/spain/es

06/09/2018 MEDIA

Detalle ▼

Sistema de información propiedad de EVERIS que soporta los servicios de monitorización y operación del Centro de Servicios Gestionados (iCenter) al Ministerio de Asuntos Exteriores y Cooperación (MAEC).





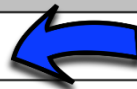
Caso 2: Afectación del alcance en las medidas de seguridad del Anexo II.



Una organización perteneciente al sector privado ha categorizado su sistema de información de categoría **MEDIA**. En consecuencia, en su Declaración de Aplicabilidad para la continuidad del servicio queda:



	BÁSICA	MEDIA	ALTA	op.cont	Continuidad del servicio
D	n.a.	aplica	=	op.cont.1	Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas



En base a ella, únicamente debe hacerse un Análisis de Impacto (BIA) [op.cont.1], pero no el Plan de Continuidad [op.cont.2] ni las pruebas del mismo [op.cont.3], ya que no aplican para categoría MEDIA.

ALCANCE: Sistema de Información propiedad de [Organización], necesario para la correcta prestación de servicios profesionales de instalación, configuración y migración de soluciones de (...), **servicio de replicación y continuidad de negocio**, (...), conforme a los requisitos de seguridad establecidos en el Real Decreto 3/2010, de acuerdo con la Declaración de Aplicabilidad vigente.




	BÁSICA	MEDIA	ALTA	op.cont	Continuidad del servicio
D	n.a.	aplica	=	op.cont.1	Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas







(Activo-Amenaza)

$$R = P \times I \times \text{Valor}$$

categoria	aplica	n	n	cp.exp.	Explotación
categoria	aplica	n	n	cp.exp.1	inventario de activos
categoria	n.a.	aplica	n	cp.exp.2	Configuración de seguridad
categoria	aplica	n	n	cp.exp.3	Gestión de la configuración
categoria	n.a.	aplica	n	cp.exp.4	Mantenimiento
categoria	n.a.	aplica	n	cp.exp.5	Gestión de cambios
categoria	aplica	n	n	cp.exp.6	Protección frente a código dañino
categoria	n.a.	aplica	n	cp.exp.7	Gestión de incidentes
categoria	aplica	n	n.a.	cp.exp.8	Registro de la actividad de los usuarios
categoria	n.a.	aplica	n	cp.exp.9	Registro de la gestión de incidentes
categoria	n.a.	n.a.	aplica	cp.exp.10	Protección de los registros de actividad
categoria	aplica	n	n	cp.exp.11	Protección de claves criptográficas
categoria	n.a.	aplica	n	cp.exp.	Servicios externos
categoria	n.a.	aplica	n	cp.exp.1	Contratación y acuerdos de nivel de servicio
categoria	n.a.	aplica	n	cp.exp.2	Gestión de datos
categoria	n.a.	n.a.	aplica	cp.exp.9	Medios alternativos

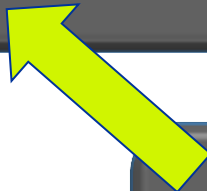
GESTIÓN DE RIESGOS
(Apreciación +
Tratamiento)



**DECLARACIÓN DE
APLICABILIDAD**
(SOA)



**VALORACIÓN y
CATEGORIZACIÓN**





Resumen final





- ❑ Lo que **se certifica del ENS es el Sistema de Información**, debiendo quedar reflejado en el alcance: *“Sistema de información...”*.
- ❑ El **modelo de las 3 líneas de defensa** puede ayudarnos a determinar incompatibilidades entre roles.
- ❑ A veces *“lo mejor es enemigo de lo bueno”*. **Es preferible reducir el alcance inicialmente para conseguir antes la certificación** comprobando así la seguridad del sistema, que esperar 4 años más para poder certificar un alcance total, sin tener nada mientras.
- ❑ Especialmente las organizaciones pertenecientes al Sector Público, deben **tener en cuenta la valoración del sistema en cada una de las cinco dimensiones** de la seguridad, dado que hay medidas que puede no sean de aplicación para determinadas combinaciones dimensión/valor.
- ❑ Lo que indiquemos en **el alcance nos puede ocasionar la aplicación de otras medidas de seguridad**, más allá de las que correspondan según la categoría del sistema.



José Luis Colom Planas

jl.colom@audertis.es

www.audertis.es AUDERTIS

www.aspectosprofesionales.info

<https://www.linkedin.com/in/joseluiscolom/>

<https://twitter.com/JLColomPlanas>

MUCHAS GRACIAS



XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- oc.ccn.cni.es

➤ Síguenos en

