

**XIII
JORNADAS
STIC
CCN-CERT**



**La incidencia del ENS
en la contratación de
servicios con
operadores del sector
privado**

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



Miguel A. Lubián

Grupo CIES (Instituto CIES y AliSEC)

miguel.lubian@institutocies.es

En los 2 años anteriores...

2017



CCN-cert
centro criptológico nacional

XI JORNADAS STIC CCN-CERT

Ciberamenazas_ El reto de compartir
#XIJornadasCCNCERT

MADRID. 13 Y 14 DE DICIEMBRE 2017

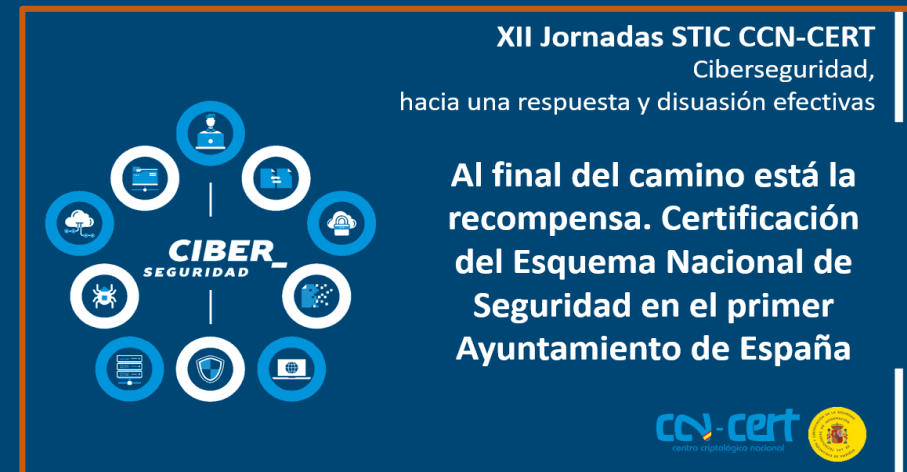
"La aplicación el Esquema Nacional de Seguridad en las Administraciones Públicas bajo un enfoque práctico"

Menos es Más
- ES +

CCN
Centro Criptológico Nacional

Logo of the Spanish Government

2018



XII Jornadas STIC CCN-CERT
Ciberseguridad,
hacia una respuesta y disuasión efectivas

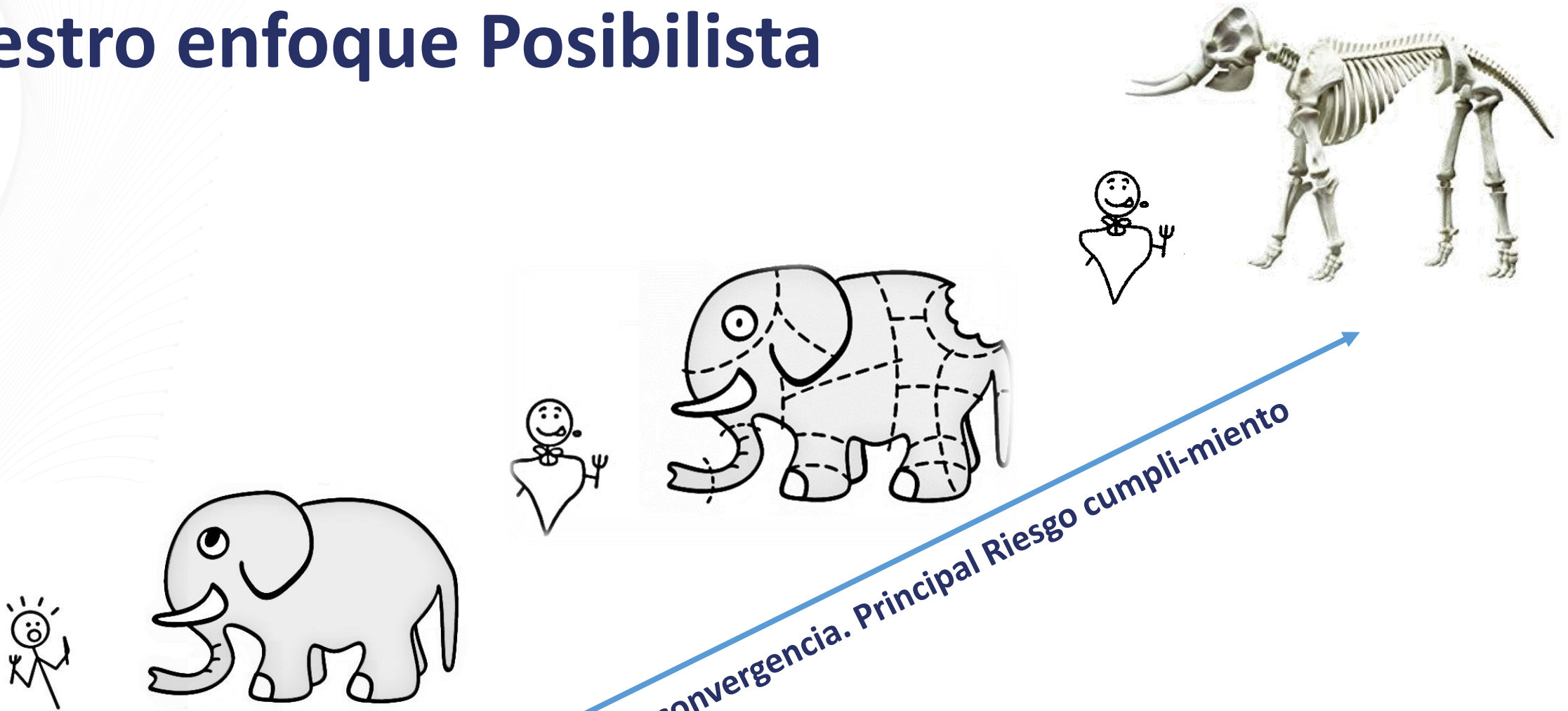
CIBER-SEGURIDAD

Al final del camino está la recompensa. Certificación del Esquema Nacional de Seguridad en el primer Ayuntamiento de España

CCN-cert
centro criptológico nacional

Logo of the Spanish Government

Nuestro enfoque Posibilista



Índice

1. ¿Quién es quién?
2. La Ley de la Oferta y la Demanda del ENS
 1. ¿Qué debo solicitar a mis proveedores?
 2. ¿Qué debo ofrecer a mis clientes?
3. La conformidad de Mi Nube
4. El perfil de cumplimiento específico: Presente y Futuro
5. CONCLUSIONES



Exposición de motivos de
la presentación

Ciberamenazas y Tendencias 2019

2.3. Ataques a la cadena de suministro



A la vista de la efectividad y los beneficios que comporta para los atacantes, es previsible que este tipo de acciones se mantenga en los próximos años, pues este método presenta dos ventajas para el atacante: puede utilizar un proveedor de confianza como origen de la distribución dañina y acota la superficie del ataque, sin que sea fácil determinar cuáles son, exactamente, los objetivos perseguidos.

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



https://www.boe.es/diario_boe/txt.php?id=BOE-A-2016-10109

VII. Soluciones y servicios prestados por el sector privado

VII.1 Cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de **exhibir la correspondiente Conformidad con el Esquema Nacional de Seguridad**

VIII.2 Es responsabilidad de las entidades públicas contratantes notificar a los operadores del sector privado que **participen** en la provisión de soluciones tecnológicas o la prestación de servicios, **la obligación de que tales soluciones o servicios sean conformes** con lo dispuesto en el Esquema Nacional de Seguridad



RGPD

#XIIIJORNADASCCNCERT

Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento.



<https://www.boe.es/doue/2016/119/L00001-00088.pdf>

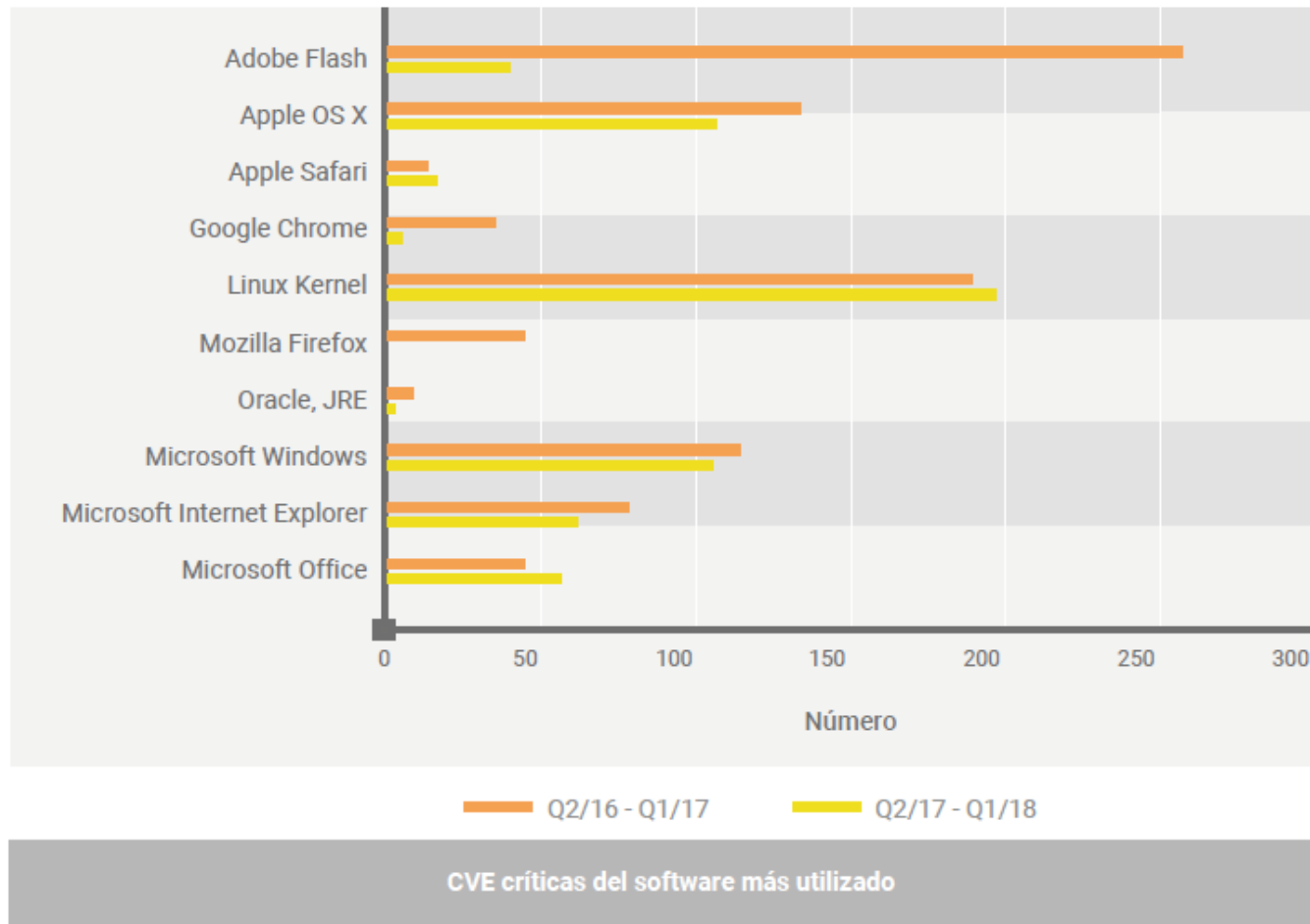
CONSIDERANDO 81: “In Eligendo, In Vigilando”

Las entidades públicas sólo encomendaremos actividades de tratamiento a un encargado que le ofrezcan suficientes garantías.

Que se propaga, de forma
proporcional, a lo largo de la
cadena de suministro ...

Sabiendo que el mundo
IT no es sencillo ...

0 Day de fabricantes, Vulnerabilidades ...



Fuente: CCN

Prevención de Riesgos Digitales, es un concepto que transita sobre los modelos tradicionales a los nuevos modelos de negocio

Algo que no es nuevo, pues sucede igual en el mundo tradicional, no?

Prevención de Riesgos Laborales Digitales

BIENVENIDOS

EN ESTE MOMENTO CUMPLIMOS

242 29 : 59 : 54

DÍAS HORAS MINUTOS SEGUNDOS

SIN ACCIDENTES

Nuestro record: **244** días sin accidentes

La Seguridad es un Valor que Crece ... *segundo a segundo*

El reto de Dormir tranquilo en la contratación con terceros

(Qué exijo | Que ofrezco)



Las Administraciones serán más exigentes en los requisitos de contratación.

El nivel de concurencia del mercado empieza a ser aceptable (Solvencia ENS). Aceptable en LCSP.

Reciente RDL 14/2019 establece el foco en la contratación de servicios, limitando ubicación de información y siendo clausula esencial. (PCA)

Pero antes de llegar a este punto, necesitamos ver una serie de pasos ...

Índice

1. ¿Quién es quién?
2. La Ley de la Oferta y la Demanda del ENS
 1. ¿Qué debo solicitar a mis proveedores?
 2. ¿Qué debo ofrecer a mis clientes?
3. La conformidad de Mi Nube
4. El perfil de cumplimiento específico: Presente y Futuro
5. CONCLUSIONES



Índice

1. ¿Quién es quién?

2. La Ley de la Oferta y la Demanda del ENS

1. ¿Qué debo solicitar a mis proveedores?

2. ¿Qué debo ofrecer a mis clientes?

3. La conformidad de Mi Nube

4. El perfil de cumplimiento específico: Presente y Futuro



5. CONCLUSIONES

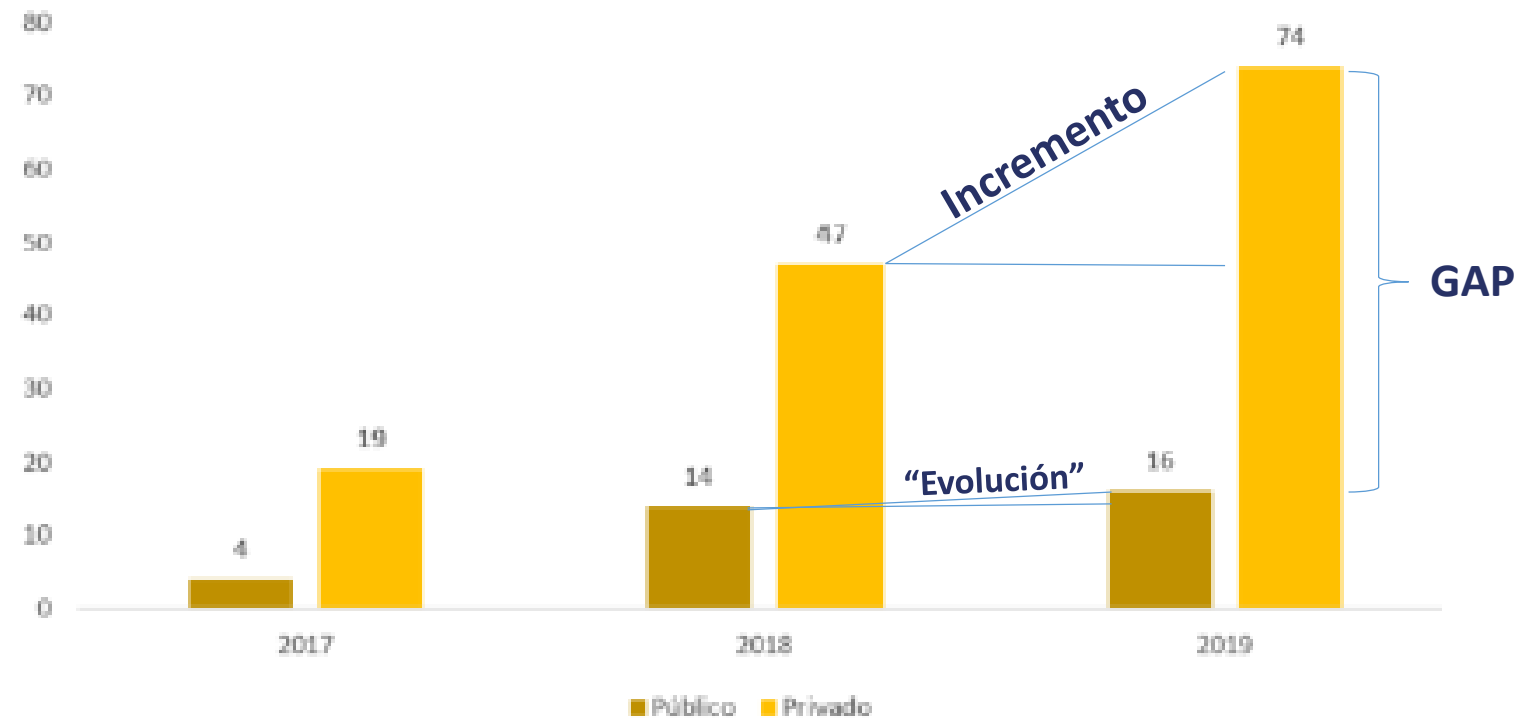
Principalmente, tenemos 2 actores:

A) Responsable (Sector Público)

B) Operador Privado (Prestador)



Evolución en la conformidad ENS Sector Público vs Operador Privado

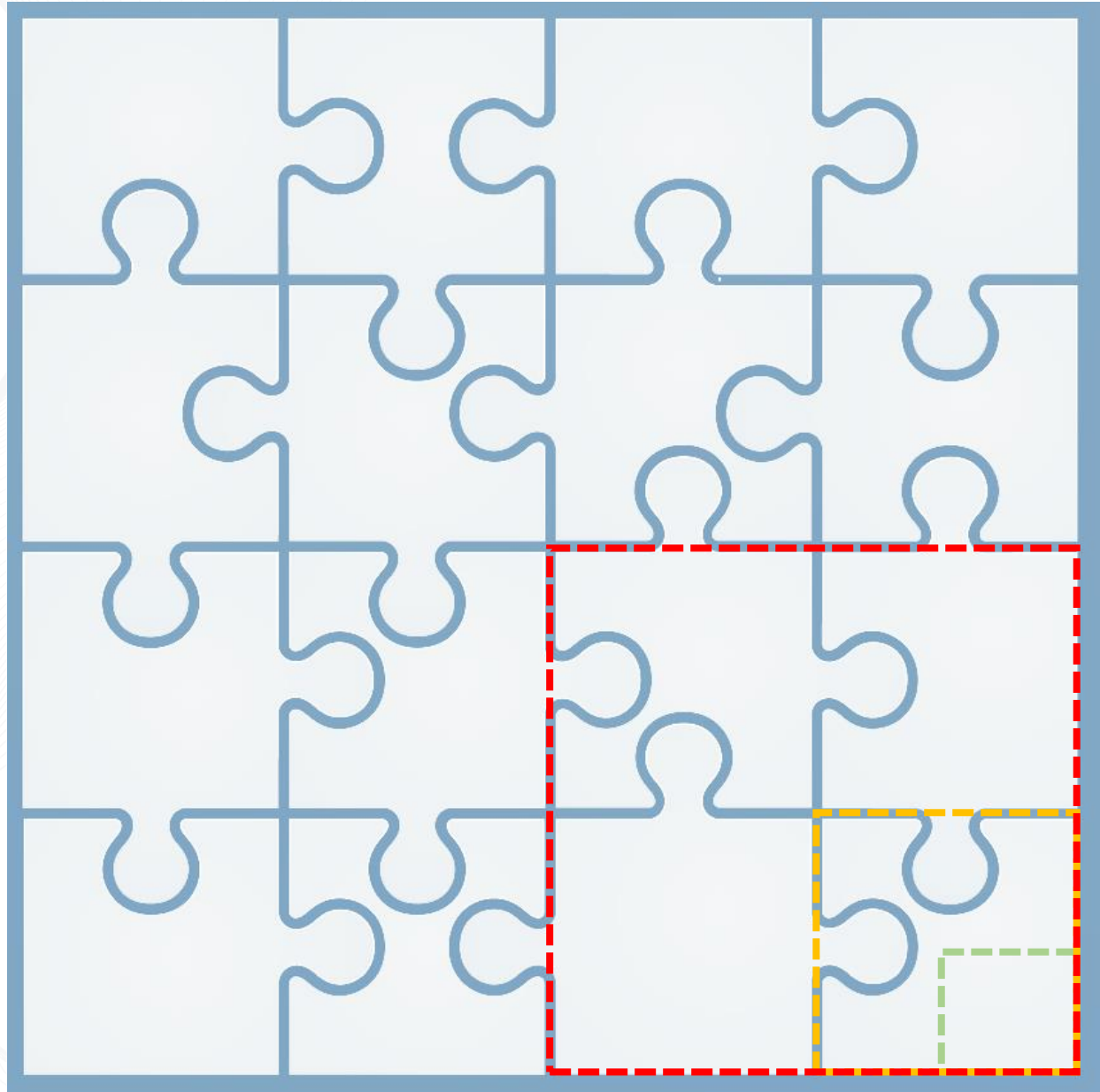


**Aunque, a veces, no es trivial
determinar el papel que juega cada
una de las partes...**



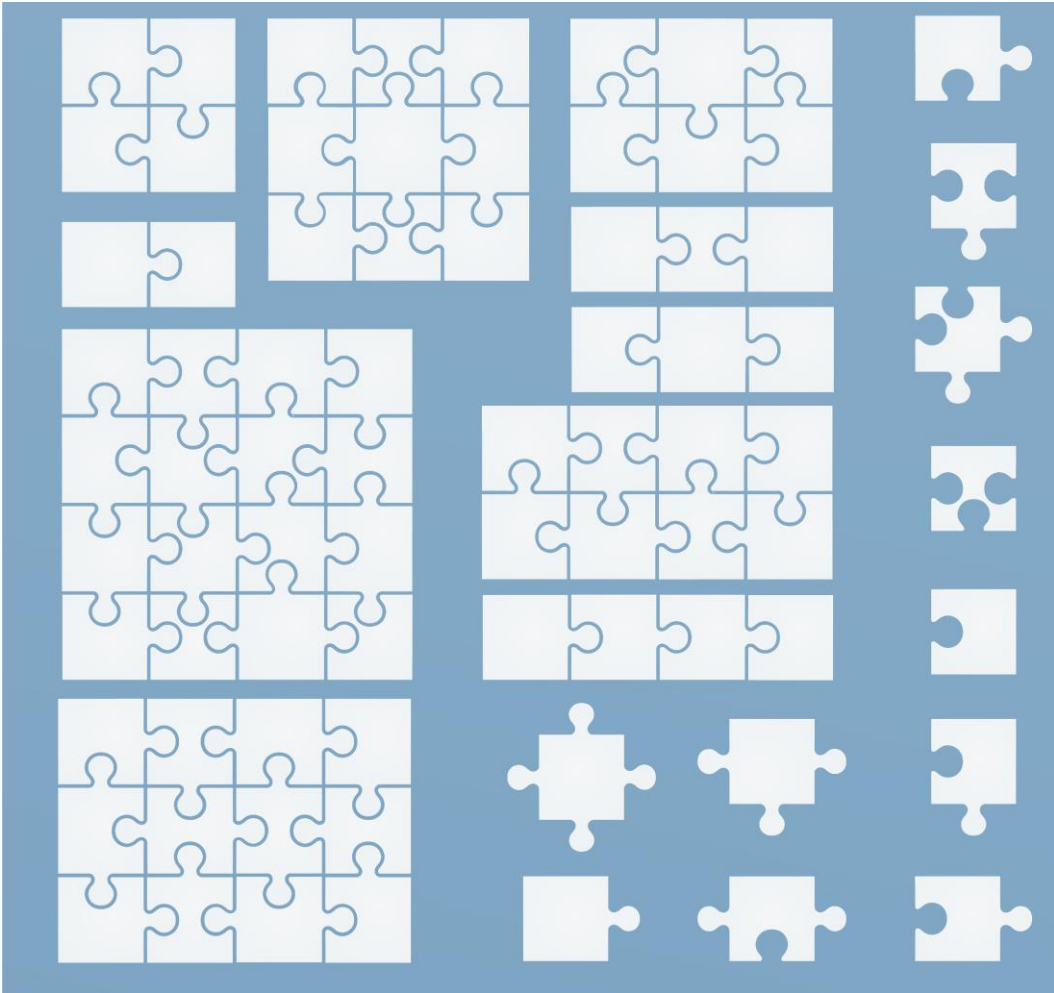


Determinación del Alcance Material del ENS “El problema del Puzzle”

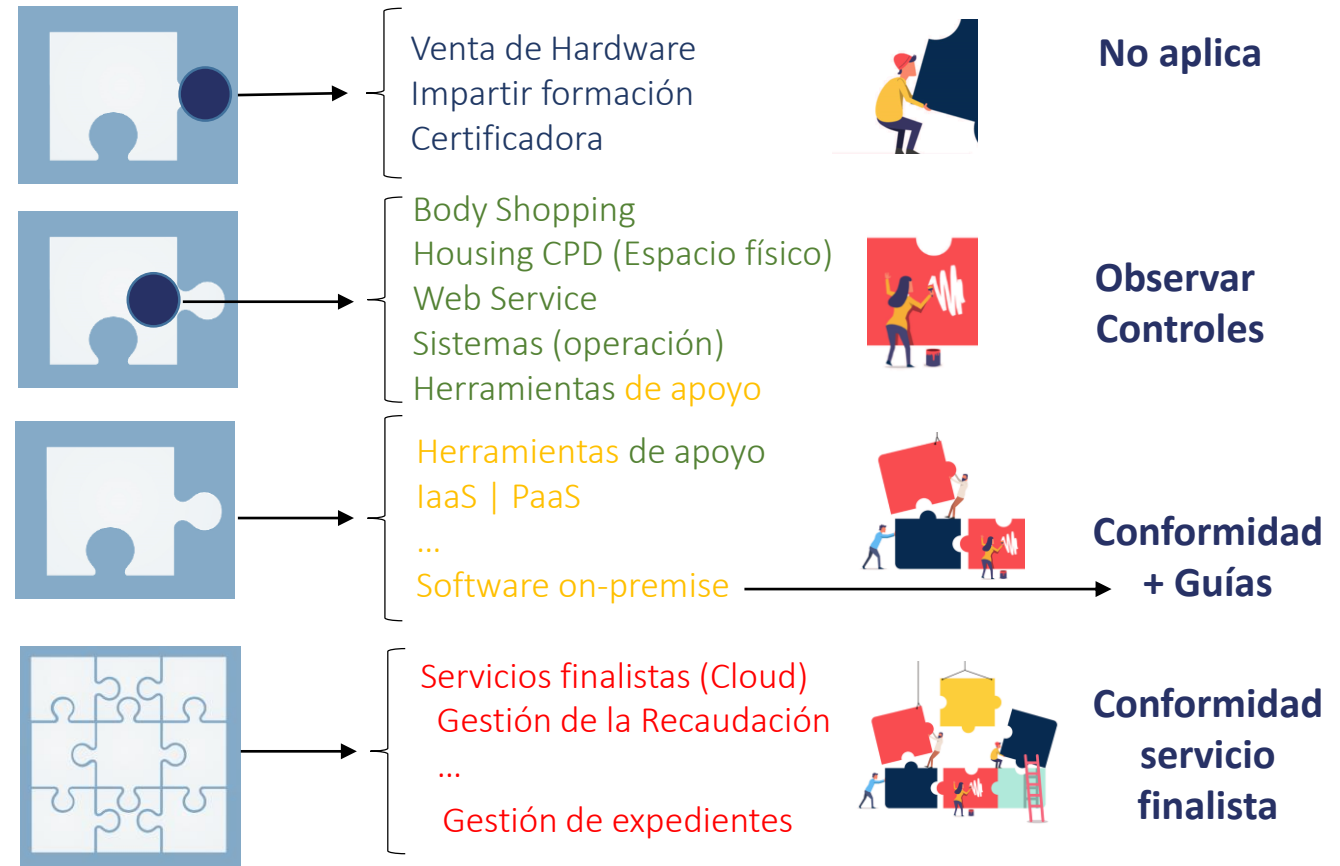


**Sistema de
información que
soporta los
servicios....**

“El problema del Puzzle”



Como prestador, ¿En qué medida me afecta el ENS?



Sector Privado

Como Administración, ¿Qué debo requerir o dónde debo fijarme?

Gestión de expedientes on-premise
Servicios de soporte y mantenimiento
Gestión de expedientes en la nube
Monitorización como Servicio
Sistemas de Backup Remoto
Correo electrónico en la nube
Antivirus con consola centralizada de logs



Conformidad (En el S.I. que fabrica) + Guía
para administradores / usuarios



Sector Privado

Como Administración, ¿Qué debo requerir o dónde debo fijarme?

Gestión de expedientes on-premise
Servicios de soporte y mantenimiento
Gestión de expedientes en la nube
Monitorización como Servicio
Sistemas de Backup Remoto
Correo electrónico en la nube
Antivirus con consola centralizada de logs

Certificación de producto (de seguridad)

A) Catálogo de Productos CCN STIC105

B) LINCE

C) Common Criteria



1: De quién

3: Restricción



Sistema de Información **propiedad** de XXXXXX, para ser implantado en instalaciones de cliente final (on-premise) y también en **modalidad** de Software como Servicio (SaaS) **siempre que** se apoye en una infraestructura Cloud también certificada de la misma categoría: <**Servicios de XXXXXX**>

2: Tipo de servicio

4: Servicios afectados

Alcances “peculiares”



A) Sistema de Información asociado a la prestación de servicios de: Venta, instalación y mantenimiento de sistema de información tanto físicos como en la nube.

B) Los sistemas de información que dan soporte a los servicios gestionados:

1. Instalación y configuración de hardware, sistemas operativos y ofimática.
2. Mantenimiento de hardware



Al alcance si importa

Tiene que proporcionar de forma concisa la cobertura del servicio requerido / prestado.

En el caso de que el software se instale on-premise, el fabricante deberá de suministrar obligatoriamente 2 guías para el correcto despliegue y utilización, donde se deberán delimitar la responsabilidad de cada una de las partes (reparto de controles ENS)



Guía de Seguridad CCN-STIC CCN-CERT IC-01/19

ENS: Criterios adicionales de Auditoría y Certificación

3.9 EN RELACIÓN CON LA CERTIFICACIÓN DE SISTEMAS DE INFORMACIÓN

38. El Centro Criptológico Nacional ha analizado la adecuación y certificación de sistemas de información on-premise que originariamente hubieren sido desplegados en modo Cloud, debido a que su casuística no encaja con la certificación de conformidad del ENS al uso (más enfocado a sistemas y servicios) y tampoco se ajusta al tipo de producto cualificado que se incluye en el catálogo (CPSTIC) para su utilización en el ENS, al no tratarse específicamente de un producto cuyas funciones principales están asociadas a la seguridad. Ante esta situación, parece necesario definir los requisitos para certificar el mencionado sistema de información.
39. Las Entidades de Certificación deben evaluar la adecuada adopción de las medidas del Anexo II del RD 3/2010, de 8 de enero, que sean de aplicación, dadas las características particulares del objeto de la certificación. En estos casos, habrá que determinar qué medidas (o controles dentro de ellas) son responsabilidad de una configuración correcta del sistema de información on-premise y qué medidas (o controles dentro de ellas) son parte de un correcto despliegue y uso por parte del usuario.
40. El fabricante del sistema de información debe disponer de los siguientes documentos, que serán verificados por la Entidad de Certificación:
- Guía de instalación de la aplicación, de forma compatible y alineada con el ENS.
 - Procedimiento de “cliente-usuario” para utilizar el sistema instalado de forma compatible y alineado con el ENS.

Requisitos de Seguridad Adicionales para Servicios en la Nube prestados desde instalaciones en modo local (Versión Preliminar)

Abstract: *Dadas las especiales características de seguridad que deben contemplarse en los sistemas de información instalados en modo local por entidades proveedoras, que originalmente hubieran sido desplegados como soluciones en la nube, se hace necesario establecer unos requisitos adicionales para garantizar la seguridad de los sistemas implicados y velar por el cumplimiento de los requisitos establecidos en el Esquema Nacional de Seguridad (ENS).*

De esta manera y para minimizar el riesgo, se elaborarán los documentos que se determinen y que comprenderán como mínimo:

- 1 • **Una Guía de Instalación y Configuración Segura del Sistema destinada a administradores**, donde se explicarán todas las acciones que deben realizar los administradores y los aspectos a tener en cuenta a la hora de instalar la aplicación, establecer una configuración inicial, actualizar el sistema y realizar pruebas de integridad del mismo, así como cualquier otro aspecto que se estime relevante para la seguridad del sistema, todo ello alineado con los requisitos del ENS.
- 2 • **Una Guía de Uso Seguro del Sistema destinada a usuarios finales**, donde se detallarán la Normativa de Uso del sistema, el Manual de Usuario (resaltando las implicaciones de seguridad en las acciones que puedan realizar los usuarios) y todas aquellas configuraciones y procedimientos de seguridad que deban ser realizados por los usuarios finales para el uso seguro del sistema, todo ello alineado con los requisitos del ENS.

Igualmente, será responsabilidad de la entidad contratante adoptar estos documentos como propios del organismo, incluyéndolos en las medidas de seguridad propias de la entidad (las configuraciones de seguridad, normativas de seguridad y procedimientos de seguridad) en el grado y circunstancia que se estime apropiado.

Con independencia de lo ya indicado, se aconseja disponer de un documento que analice en todo su conjunto las obligaciones directas de cumplimiento del ENS. Es decir, una guía que persiga aclarar la relación entre un proveedor de software y un cliente contratante, en modo compatible con el ENS:

- [3] • **Una Guía de Recomendaciones para la gestión de la relación entre proveedor y cliente contratante**, donde se identificará la relación entre el cliente contratante y un proveedor de software y establecerá la carga de responsabilidad de cada parte respecto a los controles de seguridad del ENS que aplican.

Un ejemplo de una guía

1.1.	Cumplimiento del Esquema Nacional de Seguridad.....	5
1.2.	Referencias	6
2.	Resumen.....	6
2.1.	Objeto	6
3.	Requisitos	6
3.1.	Requisitos previos.....	6
3.1.1	Requisitos de Despliegue o Arquitectura	7
3.2.	Requisitos del sistema para utilizar el sistema de manera compatible con el Esquema Nacional de Seguridad	7
4.	Aplicación de medidas en la aplicación.....	7
4.1.	MARCO OPERACIONAL	9
4.1.1	CONTROL DE ACCESO	9
4.1.2	EXPLOTACIÓN	27
4.1.3	DESARROLLO.....	29
5.	Configuración de la aplicación para adecuarla al Esquema Nacional de Seguridad	32
5.1.	Guía de implementación segura.....	32
5.1.1	Instalación de Administrador	32
5.1.2	Instalación de	49
5.1.3	Pruebas de acceso	78
6.	Implementación en supuestos diferentes a los recomendados.	80
6.1.	Credenciales para el registro de dlls.....	80
7.	Gestión de tareas diferentes	83
7.1.	Soportes y tareas de mantenimiento	83
7.2.	Actualizaciones de la aplicación	83
7.2.1	Actualización de	83
7.2.2	Actualización de	85
7.3.	Desinstalación de la aplicación	87
7.4.	Limpieza de metadatos de documentos.....	87
7.5.	Protección de fichero con contraseña	88

DIMENSIONES				MEDIDA DE SEGURIDAD		APLICABILIDAD			
Afecta	Básico	Medio	Alto			Alcance de Implantación		Nivel de Madurez	Implementación
						AAPP	Proveedor		
todas	n.a.	aplica	=	op.mon.1	Detección de intrusión	SI	SI	L2	En el Apartado 14 se identifican los registros generados por el componen que podrán ser integrados en la plataforma de recolección y correlación de eventos SIEM La AAPP determinará la infraestructura TIC donde se implantará el componente necesario para diseñar la recopilación y correlación de eventos asociados al componente a través de la plataforma SIEM

4.1.1.1.1. Responsabilidad

4.1.1.1.1.1. Cliente

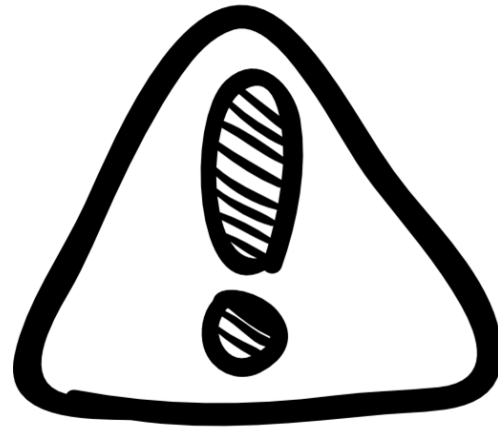
Será responsabilidad de la Entidad definir los criterios por los que se le habilitarán los derechos de acceso a los recursos requeridos por la aplicación, así como su protección y monitorización.

4.1.1.1.1.2. Proveedor

La aplicación permite usuarios diferenciados y los requerimientos de seguridad pueden cumplirse con la correcta configuración. El cumplimiento de las políticas asociadas a este control recae única y exclusivamente en el cliente.

Pero el alcance sólo, no es suficiente.

Existen parámetros adicionales a considerar (**Previo al lanzamiento, durante la ejecución y en la finalización**), como por ejemplo: Responsabilidad de cada una de las partes, ubicación de la información, requisitos legales, etc.



Índice

1. ¿Quién es quién?

2. La Ley de la Oferta y la Demanda del ENS

1. ¿Qué debo solicitar a mis proveedores?

2. ¿Qué debo ofrecer a mis clientes?

3. La conformidad de Mi Nube

4. El perfil de cumplimiento específico: Presente y Futuro



5. CONCLUSIONES

Supuesto práctico:

La organización en la que trabajo quiere

- A) [AAPP] Localizar información en Cloud (Interna o Externa)
- B) [Privado] Proporcionar servicios Cloud a nuestros clientes



¿Por dónde empiezo?



Lo primero, tener clara las piezas que conforman tu Puzzle

DÓNDE: ¿Nube “privada on premise” o nube “externa”?

QUIÉN: ¿Administrada por recursos tuyos o por recursos externos?

NEW !

Guía de Seguridad de las TIC CCN-STIC 823

UTILIZACIÓN DE SERVICIOS EN LA NUBE

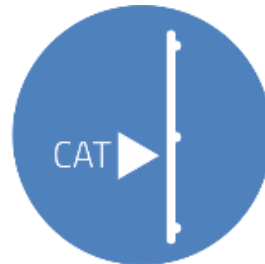


#XIIIJORNADASCCNCERT

1. INTRODUCCIÓN	5
1.1 CONCEPTOS PREVIOS.....	5
1.2 CARACTERÍSTICAS DE LOS SERVICIOS EN LA NUBE	6
1.3 MODELOS DE DESPLIEGUE.....	7
1.4 CATEGORÍAS DE SERVICIO	7
1.5 ASPECTOS RELATIVOS A LA SEGURIDAD DE LA INFORMACIÓN	8
2. REQUISITOS DE SEGURIDAD	9
2.1 PRIMEROS PASOS.....	9
2.2 CONSIDERACIONES PARA IMPLANTAR SEGURIDAD	10
2.2.1 ASPECTOS ORGANIZATIVOS	10
2.2.2 ASPECTOS OPERACIONALES DE SEGURIDAD.....	11
2.2.2.1 PLANIFICACIÓN DEL SISTEMA.....	11
2.2.2.2 CONTROL DE ACCESO	12
2.2.2.3 EXPLOTACIÓN	12
2.2.2.4 CONTRATACIÓN UN PROVEEDOR DE SERVICIOS EN LA NUBE	14
2.2.2.5 CONTINUIDAD	17
2.2.2.6 MONITORIZACIÓN DEL SISTEMA	18
2.2.3 MEDIDAS DE PROTECCIÓN DE LOS ACTIVOS.....	18
2.2.3.1 PROTECCIÓN DE LOS SERVICIOS.....	20
3. CONCLUSIONES.....	21
4. DECÁLOGO.....	22



Determinación de los niveles de seguridad (bajo, medio, alto, sin valorar)



Determinación de la categoría del sistema (básica, media y alta)



Elaboración de la declaración de aplicabilidad



Realización de un análisis de riesgos



Acogerse a un Perfil de Cumplimiento Específico (opcional)



¿Qué tipo de información
voy a poner en esta nube?



Debemos analizar que requisitos inciden sobre la información. Puede estar afectada por diferentes leyes (Leyes 39/40, Transparencia, GDPR, etc.) o simplemente, normativa interna.





Tengo que analizar la
modalidad....

¿Y si me hago una matriz de
requerimientos generales?



Criticidad (5 dimensiones)

MENOS

MAS

Requisitos y parámetros (Modalidad)	NIVEL 1 (Ej. Contabilidad)	NIVEL 2 (Ej. Intercambio de archivos)	NIVEL 3 (Ej. Exámenes pruebas selectivas)	NIVEL 4 (Ej. Voto Electrónico)
UBICACIÓN	Externa	Externa	Externa	Interna
TIPO NUBE	Pública	Pública	Nube “dedicada”	On Premise
CONTROL	SaaS	IaaS	IaaS Housing	N/A
UBICACIÓN (TID)	UE + EEUU (Privacy S.)	UE	UE (Biometría España)	N/A
...	...	...	...	...

Es decir, los datos que ubicaré en esta nube tienen una serie de **condicionantes** (Desde el Diseño), que marcaran mi elección.

En realidad, si lo alineamos con el ENS, simplemente estamos calificando la información, y **determinando la CATEGORIA del sistema que soportará la solución en la NUBE.**



Empezamos a implantar
medidas de seguridad

Tendré que realizar mi propia política de seguridad y normativa de uso para las personas usuarias de esta nube



(Ej. Si es una nube de intercambio de archivos, qué puedo colocar, si hay que cifrar los archivos subidos, plazo de cancelación, limpieza de metadatos, acceso a través de link público o un código de descarga, etc.)

Y así con todas las medidas en los 3 marcos. Por ejemplo, en relación a las medidas operacionales ...

2.2.2.1 Planificación del sistema

Para la realización del **análisis riesgos**, el organismo reflejará los activos en función de la modalidad de nube:

- En el caso de un servicio SaaS, la solución en la nube se reflejará como un activo de “servicios externos”, del que dependerán los servicios e información soportados por esta.
- En el caso de un servicio PaaS y IaaS, se reflejarán los activos sobre los que se tiene control.

En el caso de que la provisión de los servicios se realice desde una nube privada “on premise”, el organismo reflejará en el análisis de riesgos todos los activos involucrados en la prestación de los servicios.

Este mismo criterio se seguirá, para detallar los elementos (equipos, redes, cortafuegos, etc.) que definen la **arquitectura de seguridad**.



¿Sabías que te podrás
acoger a un Perfil de
Cumplimiento
Específico?



El nuevo ENS del 2020 te permitirá certificar sobre un conjunto específico de medidas (comprendidas o no en el Anexo 2)

Artículo xx: Perfiles de cumplimiento específicos

En virtud del principio de proporcionalidad y para facilitar la conformidad con el ENS a una entidad singular o sector de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que contemplen un conjunto de medidas de seguridad, comprendidas o no el Anexo 2 del presente real decreto, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación para una determinada categoría de seguridad.

El CCN validará y publicará los correspondientes perfiles de cumplimiento específicos determinados para el Sector Público.



Acogerse a un Perfil de
Cumplimiento Específico
(opcional)

Un adelanto ...

Perfil de Cumplimiento Especifico para Sistemas Cloud Privados y Comunitarios

De las 75 medidas de seguridad definidas en el Anexo II del RD 3/2010, aplican un total de **56* medidas**. Son las siguientes:

4.1 [OP.ACC.5] Mecanismos de Autenticación

Serán exigibles los requisitos de nivel MEDIO para esta medida, con las siguientes particularidades:

- En el caso de utilizarse como factor “algo que se sabe”, no será requerido que:
 - Las credenciales se activen una vez estén bajo el control efectivo del usuario.
 - Las credenciales estarán bajo el control exclusivo del usuario.

El cambio de las credenciales en el primer acceso será responsabilidad de los usuarios finales de la plataforma, por lo que deberá incluirse en las normas de uso de la misma, haciendo mención expresa a que se deberá cambiar la contraseña en el primer acceso.

- No será requerido el uso de doble factor de autenticación para los usuarios finales de la plataforma.
- El uso de doble factor de autenticación sí será requerido para:
 - Los usuarios finales con privilegios de administrador, así como otros usuarios finales
 - de la plataforma a criterio del Responsable de Seguridad.
 - Los usuarios que realicen tareas de configuración y mantenimiento de la plataforma.

NO

SI



En este punto, ya podemos
concretar más particularidades
en la contratación...



Con carácter previo a la contratación, en la solicitud de ofertas o en los pliegos, deberemos contemplar:

- Modalidad de nube seleccionada: Tipo de servicio e infraestructura
- Descripción de Servicio: Detalle concreto de la prestación del servicio
- Riesgos: de la contratación del tipo de nube seleccionada (Justificación de su elección)
- Solvencia técnica y económica: Viabilidad económica de la compañía y certificaciones en función de la modalidad (TIER, ENS, Continuidad, etc.)
- ANS / SLA: Definir parámetros para comprobar la adecuada prestación del servicio
 - **Responsabilidades**: quién recoge y facilita los datos necesarios para realizar los cálculos
 - **Fórmula**: descripción del cálculo para la obtención del SLA.
 - **Tiempo**: Periodicidad de la captura de datos, del cálculo de las métricas derivadas y de la verificación de umbrales de aviso y de alarma.
 - **Umbrales**: valores mínimos en la prestación del servicio que disparan situaciones de aviso (hay que monitorizar) y de alarma (hay que corregir).
 - **Penalización**: procedimiento para determinar y cuantificar las consecuencias derivadas del incumplimiento de SLA.
 - ...

Con carácter previo a la contratación, en la solicitud de ofertas o en los pliegos, deberemos contemplar:

- Delimitación de responsabilidades de las partes: ¿Quién actualiza el servidor de aplicaciones? ¿Quién bastiona? En GDPR: Encargado + [Responsable]
- Registros de actividad: Trazabilidad de los usuarios y posible integración en un SIEM
- Gestión de incidentes de seguridad: Plazo y mecanismos de coordinación para los procesos de investigación y comunicación (Alineamiento brechas seguridad GDPR)
- Copias de seguridad y mecanismos de recuperación: Diferente a la tolerancia a fallos
- Continuidad del servicio: Alineamiento BIA – SLA (Medios alternativos, plan de pruebas, etc.)
- Finalización del contrato: Devolución “portable”, bloqueo y eliminación certificada
- Subcontratación: Limitación y gestión de transferencias ulteriores. Otros prestadores que intervengan en la prestación (operación, almacenamiento, etc.)
- Ubicación de la información: Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega).
- Requisitos legales: ENS, RGPD, Real Decreto-ley 14/2019, etc.

Un operador privado, estará alineado, contemplando requisitos como los siguientes:

- Describe de forma clara la tipología de servicios y su modalidad.
- Ofrece información de la arquitectura de seguridad para facilitar el Análisis de Riesgos.
- Su solvencia se acredita a través de un tercero: Conformidad ENS + [Certificaciones]
- Tiene un punto de contacto con la Administración (Ej. DPD)
- Detalla las medidas de seguridad, facilitando información (Algoritmo de cifrado)
- Dispone de guías técnicas de configuración de medidas de seguridad (parametrizar)
- Facilita el seguimiento de los SLA con herramientas de monitorización o informes periódicos
- Articula mecanismos para facilitar controles periódicos (localización de evidencias)
- Informa y permite localizar la ubicación de la información
- Detalle claramente la cadena de subcontratación y sus cambios
- Dispone de mecanismos que garanticen la portabilidad de la información

Índice

1. ¿Quién es quién?

2. La Ley de la Oferta y la Demanda del ENS

1. ¿Qué debo solicitar a mis proveedores?

2. ¿Qué debo ofrecer a mis clientes?

3. La conformidad de Mi Nube

| 4. El perfil de cumplimiento específico: Presente y Futuro |



5. CONCLUSIONES

Perfil de Cumplimiento Especifico para Sistemas Cloud Privados y Comunitarios



1. INTRODUCCIÓN	5
2. APLICACIÓN DEL PERFIL DE CUMPLIMIENTO	6
3. DECLARACIÓN DE APLICABILIDAD	6
3.1 MEDIDAS DE APLICACIÓN	9
4. CRITERIOS DE APLICACIÓN DE MEDIDAS	12
4.1 [OP.ACC.5] MECANISMOS DE AUTENTICACIÓN	12
4.2 [OP.ACC.6] ACCESO LOCAL (LOCAL LOGON)	12
4.3 [OP.EXP.6] PROTECCIÓN FRENTE A CÓDIGO DAÑINO	12
4.4 [MP.IF] MEDIDAS DE PROTECCIÓN DE INSTALACIONES E INFRAESTRUCTURAS..	13
4.5 [MP.SI] PROTECCIÓN DE SOPORTES DE INFORMACIÓN	13
4.6 [MP.SW.1] DESARROLLO DE APLICACIONES	13
4.7 [MP.INFO.2] CALIFICACIÓN DE LA INFORMACIÓN	13
4.8 [MP.INFO.4] FIRMA ELECTRÓNICA.....	14
4.9 [MP.INFO.6] LIMPIEZA DE DOCUMENTOS	14
4.10 [MP.S.1] PROTECCIÓN DEL CORREO ELECTRÓNICO	14
5. CONFIGURACIÓN DE SEGURIDAD.....	14

Microsoft Cloud: de la Certificación frente al Esquema Nacional de Seguridad (2016) a la automatización y documentación de la configuración de nivel alto STIC-823 (2019)

Guías STIC-823 para Servicios Cloud

1. Microsoft Azure
2. Microsoft Office 365
3. Microsoft Teams
4. Microsoft Sharepoint Online
5. Microsoft Exchange Online
6. Microsoft Azure SQL
7. Microsoft Kubernetes
8. Microsoft Cognitive Services



Microsoft

Sala Microsoft – 20

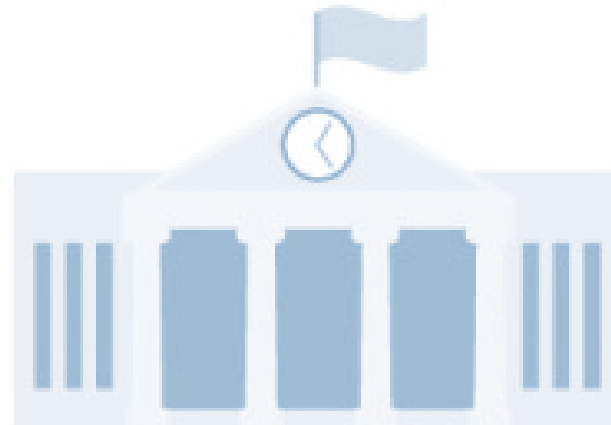
Miércoles, 11 Diciembre, 2019 – 17:00-17:20

Lanzamiento oficial de guías de Cumplimiento del ENS en Azure y Office 365: guías técnicas y scripts oficiales para aplicación de la guía STIC-823

Héctor Sánchez Montenegro, Microsoft

Iván González, Plain Concepts

En 2020 se publicará un perfil de
cumplimiento específico para
Ayuntamientos



Índice

1. ¿Quién es quién?

2. La Ley de la Oferta y la Demanda del ENS

1. ¿Qué debo solicitar a mis proveedores?

2. ¿Qué debo ofrecer a mis clientes?

3. La conformidad de Mi Nube

4. El perfil de cumplimiento específico: Presente y Futuro



5. CONCLUSIONES

1

IDENTIFICA al tercero de
forma adecuada en tu
Puzzle



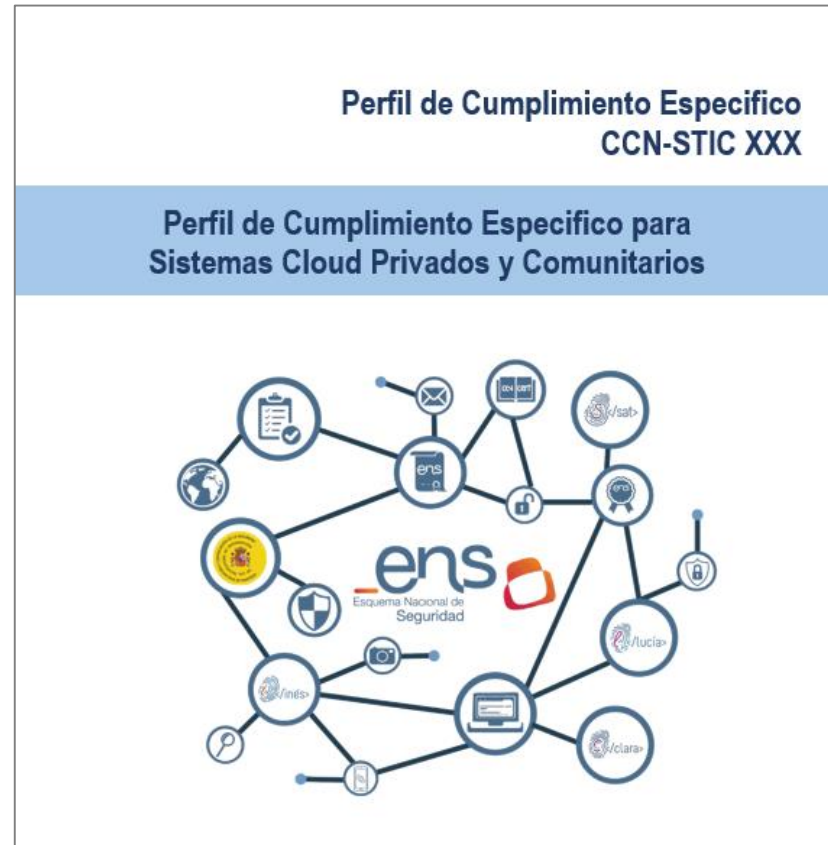
2

EVALUA el impacto normativo en información y determina la categoría que soportará la nube (calificación información)



3

FIJA EL OBJETIVO. Aplicabilidad, riesgos y, si es posible, acógete a un perfil de cumplimiento específico (cuando sea de aplicación)



4

ESTABLECE las condiciones contractuales, con carácter previo, cubriendo todo el ciclo de vida (Desde tu diseño)



5

SUPERVISA del cumplimiento por parte del CSP, establecidos con anterioridad en las condiciones de contratación.



6

EVIDENCIA (Accountability). Revisión periódica de los acuerdos de nivel de servicio establecidos (SLA), controles, etc. El CSP deberá disponer de este tipo de funcionalidades (plataforma, informe periódico, etc.)



7

DEFINE, con carácter previo, las “reglas del juego” para las personas usuarias de tu nube.



One more thing...

Y no te olvides, que el mejor contrato de Cloud, se empieza negociando por el divorcio.



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional