Esquema Nacional de Seguridad e ISO 27001
¿Cómo implantar ambos en mi empresa?

Alejandro Corletti Estrada, agosto de 2018.

acorletti@darFe.es

En la actualidad, estamos viendo que el Esquema Nacional de Seguridad (*en adelante **ENS***) está en boca de muchos, y aparece la gran duda:

En mi empresa privada, ¿Necesito certificarlo?... ¡pues va a ser que sí!

Bueno, bueno … tal vez no sea tan, tan así, *puede llegar a decir alguno que otro.*

Si tu empresa guarda algún interés con las AAPP, ahí sí que **va a ser que sí,** y con toda seguridad.

¿Y qué pasa ahora con ISO-27001?, *puede preguntarse algún otro*.

Tal vez en esto esté la clave, y es lo que desarrollaremos de forma práctica en este artículo.

ÍNDICE

0. Introducción.
1. ¿Cuál certificación necesito?
2. ¿Cómo se adecúa mi empresa para obtener la misma?
3. ¿Cómo obtengo la certificación?
4. ¿Me sirve o no ISO-27001?
5. ¿Puedo obtener ambas certificaciones?
6. ¿Qué pasos debo seguir?

DESARROLLO

0. Introducción.

Durante el año **2006**, cuando comenzaron las implantaciones de ISO-27001, fui escribiendo una serie e artículos al respecto. En el **2008** al aparecer la Ley 11, también escribí algo acerca de cómo las AAPP empezaban a ponerse las pilas sobre "Ciberseguridad". En el mes de enero de **2010** se publicaron el **RD 03/2010 "Esquema Nacional de Seguridad**" (ENS) y el **RD 04/2010 "Esquema Nacional de Interoperabilidad**" de los cuáles, en su momento, también publiqué unas líneas.

Todos estos documentos, recomiendo que si estáis dándole vueltas a la idea de **ENS** y/o **ISO-27001**, les deis una leída, pues están disponibles para su libre y gratuita descarga en la sección "*Descargas → Tecnologías de la Información → Publicaciones en revistas*" de mi Web: www.darFe.es.

Hoy, estoy viendo cada vez más que a menudo, que hay incertidumbre acerca de las "certificaciones" en el ENS fuera del ámbito de las AAPP.

Tal cual he mencionado al principio, cualquier empresa que tenga proyectos en vigor, o más aún, desee participar en ofertas y licitaciones con algún Organismo Oficial, como mínimo, esta certificación le será una diferencia competitiva importante, y en breve, estimo que es muy probable que sea una cláusula mandatoria para cualquier licitación.

Por lo tanto el tema en cuestión no es una decisión acerca de si necesito la certificación del ENS, esto se responde sencillamente con lo del párrafo anterior. El tema en cuestión son varios interrogantes más:

1. ¿Cuál certificación necesito?
2. ¿Cómo se adecúa mi empresa para obtener la misma?
3. ¿Cómo obtengo la certificación?
4. ¿Me sirve o no ISO-27001?
5. ¿Puedo obtener ambas certificaciones?

Como veremos en este texto, **sí** es posible obtener ambas certificaciones y ante esta situación, describiremos paso a paso cómo hacerlo en el último punto.

1. ¿Cuál certificación necesito?

Luego de los artículos que mencioné al principio de este documento, el 23 de octubre del año 2015 se publicó el **Real Decreto 951**, que modifica al Real Decreto 3/2010, de 8 de enero. El mismo pone una fecha límite para las AAPP en cuanto al ENS y para nosotros, tal vez lo más importante, es que designa como el referente de todo este tema al Centro Criptográfico Nacional (**CCN**), a quien le encomienda la misión de velar por el ENS, por lo que en su página Web podemos encontrar todo el detalle sobre el mismo:

https://www.ccn-cert.cni.es

Dentro de está página Web, podemos ver una serie de guías de la "**familia 800**" del **CCN-STIC** (Seguridad de Tecnologías de la Información y las teleComunicaciones), las cuáles son de libre y gratuita descarga. Estas son las guías sobre las que basaremos nuestro artículo, y recomendó su detallada lectura.

El **Anexo I** del ENS define tres categorías: **BÁSICA**, **MEDIA** o **ALTA**. En su punto 1. "*Fundamentos para la determinación de la categoría de un sistema*", nos dice que la misma se basa en la valoración del impacto que tendría sobre la organización un incidente de seguridad.

En el punto 2 del mismo Anexo, sigue definiendo las "*Dimensiones de la seguridad*", a fin de poder determinar este impacto, se tendrán en cuenta las siguientes:

A: Autenticidad
C: Confidencialidad
I: Integridad
D: Disponibilidad
A: Accounting/Trazabilidad

*La vieja palabra **ACIDA** de todos mis cursos*

El punto 3. "*Determinación del nivel requerido en una dimensión de seguridad*". Establece que si las consecuencias de un incidente de seguridad afectan a alguna de las dimensiones de seguridad y suponen un determinado perjuicio sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Si el mismo es:

Impacto	Nivel
Limitado:	BAJO
Grave	MEDIO
Muy grave	ALTO

Por último el punto 4. "*Determinación de la categoría de un sistema de información*". Define que el máximo nivel determina su categoría.

Dimensiones → Impacto → Nivel → Categoría

Nos hemos detenido especialmente en estos conceptos, pues para determinar qué tipo de certificación necesito dependeremos estrictamente de la "**Categoría**" que le hayamos asignado a nuestros sistemas de información.

Comencemos ahora con la guía que nos atañe a este punto. La guía **CCN-STIC 809** "*Declaración y Certificación de conformidad con el ENS y distintivos de cumplimiento*".

Lo primero que hace esta guía es una referencia al ENS en su Artículo 41. "*Publicación de conformidad.*"

> "*Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad*".

Esta guía, en su punto 2.2. "*Procedimiento de determinación de la conformidad*" , que se desprende del **Anexo I** (del ENS) mencionado, establece que la conformidad con la norma pasa necesariamente por adoptar y manifestar que se han implantado las medidas de seguridad requeridas para tal sistema, atendiendo a su categoría (BÁSICA, MEDIA o ALTA).

Ahora, entonces, sólo nos queda aclarar cómo se obtiene esta conformidad, lo cual es bastante claro y sencillo y también se desprende del ENS, esta vez en su **Anexo III**:

Procedimiento de verificación	Categoría de los Sistemas Afectados	Manifestación de Conformidad	Resultado de la verificación
AUTOEVALUACIÓN	BÁSICA	DECLARACIÓN DE CONFORMIDAD	Documento de autoevaluación
AUDITORÍA FORMAL	MEDIA / ALTA	CERTIFICACIÓN DE CONFORMIDAD	Informe de auditoría

NOTA: Cabe aclarar que dentro del punto 3. "*Publicidad de la conformidad*" de la guía, en los apartados 20. y 42. Hace referencia a que la categoría BÁSICA, de forma voluntaria, puede pedir que se confirme por una Auditoría Formal, obteniendo entonces un "Certificado de Conformidad" emitido por la entidad correspondiente, en lugar de ser una "Declaración de conformidad de autoevaluación.

En el punto del párrafo anterior. "*Publicidad de la conformidad*", también nos aclara que cuando se trate de sistemas de información de categoría MEDIA o ALTA, el CCN y la Entidad Nacional de Acreditación (**ENAC**), atendiendo a un procedimiento regulado, participarán en la acreditación de las Entidades de Certificación del ENS.

La Certificación de Conformidad con el ENS a la que se refiere el punto anterior deberá ser expedida por una Entidad Certificadora. El CCN mantiene en su sede electrónica una relación actualizada de las Entidades de Certificación, las mismas al día de hoy son:

Nombre	Razón social	Enlace web	Estado Acreditación ENS	Estado Acreditación STIC (DL)
AENOR Internacional S.A.U.	AENOR Internacional S.A.U.	www.aenor.com	ACREDITADA (21/04/2017)	ACREDITADA (21/04/2017)
APPLUS	APPLUS	www.applus.com/es	PRÓRROGA (HASTA 17/09/2018)	-
Audertis Audit Services, S.L.	Audertis Audit Services, S.L.	www.audertis.es	ACREDITADA (29/12/2017)	ACREDITADA (29/12/2017)
BDO Auditores, S.L.P.	BDO Auditores, S.L.P.	www.bdo.es	ACREDITADA (15/06/2018)	-
Cámara Certifica	Certificación y Confianza, Cámara S.L.U.	camaracertifica.es/	EN PROCESO (DESDE 27/10/2017)	-
Eurocertificación	Eurocert Certification Spain S.L.	Desconocida	EN PROCESO (DESDE 27/10/2017)	-
Ingeniería de Sistemas para la Defensa de España (ISDEFE)	Empresa pública de consultoría e ingeniería	www.isdefe.es	-	ACREDITADA (15/06/2018)
LEET Security, S.L.	LEET Security, S.L.	www.leetsecurity.com	ACREDITADA (23/02/2018)	-
LGAI Technological Center, S.A.	LGAI Technological Center, S.A.	www.appluscertification.com/es	ACREDITADA (27/07/2018)	-
Lloyd´s Register Quality Assurance España, S.L.	Lloyd´s Register Quality Assurance España, S.L.	www.lrqa.es	EN PROCESO (DESDE 20/10/2017)	-
Sidertia Solutions, S.L.	Sidertia Solutions, S.L.	www.sidertia.com	-	ACREDITADA (15/06/2018)

La Certificación de Conformidad con el ENS podrá representarse mediante un **Distintivo de Certificación de Conformidad**.

Cuando la provisión de las soluciones o la prestación de los servicios sujetos al cumplimiento del ENS sean realizados por organizaciones del **sector privado**, estas utilizarán los mismos modelos documentales utilizados para las Declaraciones, las Certificaciones o los Distintivos de Conformidad recogidos en la presente Guía.. Análogamente, los Distintivos de Conformidad, cuando se exhiban por parte de dichos operadores privados, deberán enlazar con las correspondientes Declaraciones o Certificaciones de Conformidad, que permanecerán siempre accesibles en la página web del operador de que se trate.

El Centro Criptológico Nacional mantiene en su página web una relación de las entidades públicas o privadas que hubieren obtenido Certificaciones de Conformidad. Podemos verlo actualizado en la siguiente URL:

https://www.ccn-cert.cni.es/ens/empresas-certificadas.html

Los distintivos de conformidad son los siguientes:

Declaración de conformidad BAJA	Certificación de conformidad BAJA	Certificación de conformidad MEDIA	Certificación de conformidad ALTA
			

2. ¿Cómo se adecúa mi empresa para obtener la misma?

Textualmente en la URL: https://www.ccn-cert.cni.es/ens/adecuacion.html del CCN se describe con máximo detalle la adecuación ordenada al ENS, la cual requiere el tratamiento de diversas cuestiones:

- Preparar y aprobar la política de seguridad, incluyendo la definición de roles y la asignación de responsabilidades. (Véase CCN-STIC 805 Política de seguridad de la información)
- Categorizar los sistemas atendiendo a la valoración de la información manejada y de los servicios prestados.(Véase CCN-STIC 803 Valoración de sistemas en el Esquema Nacional de Seguridad)
- Realizar el análisis de riesgos, incluyendo la valoración de las medidas de seguridad existentes. (Véase Magerit versión 3 y programas de apoyo –Pilar-)
- Preparar y aprobar la Declaración de aplicabilidad de las medidas del Anexo II del ENS. (Véase CCN-STIC 804 Medidas e implantación del Esquema Nacional de Seguridad)
- Elaborar un plan de adecuación para la mejora de la seguridad, sobre la base de las insuficiencias detectadas, incluyendo plazos estimados de ejecución. (Véase CCN-STIC 806 Plan de adecuación del Esquema Nacional de Seguridad)
- Implantar operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad correspondiente. (Véase serie CCN-STIC)
- Auditar la seguridad (Véase CCN-STIC 802 Auditoría del Esquema Nacional de Seguridad y CCN-STIC 808 Verificación del cumplimiento de las medidas en el Esquema Nacional de Seguridad)
- Informar sobre el estado de la seguridad (Véase CCN-STIC 815 Métricas e Indicadores en el Esquema Nacional de Seguridad y CCN-STIC 824 Informe del Estado de Seguridad)

Para ejecutar esta adecuación nos presenta el siguiente esquema.

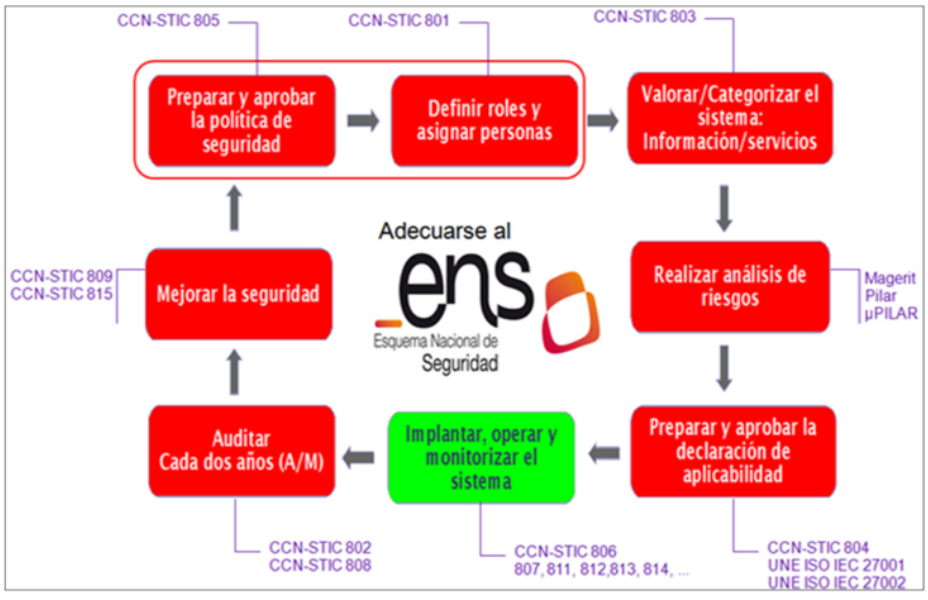


Imagen tomada de la página Web del CCN-CERT

Sobre el mismo, entraremos en detalle en nuestro punto 6. *¿Qué pasos debo seguir*?

3. ¿Cómo obtengo la certificación?

Lo más importante, como punto de partida y metodología concreta a seguir para obtener esta certificación es nuevamente recurrir al CCN y considerar los "Instrumentos para la adecuación" que pone a nuestra disposición en la URL:

https://www.ccn-cert.cni.es/ens/instrumentos-para-la-adecuacion.html

Desde esta página podemos descargar todas las guías que nos hacen falta:

- CCN-STIC 802 Guía de Auditoría
- CCN-STIC 804 Guía de Implantación
- CCN-STIC 808 Verificación cumplimiento medidas del ENS
- CCN-STIC 815 Métricas e Indicadores
- CCN-STIC 809 Declaración y Certificación Conformidad ENS. Distintivos Cumplimiento.
- CCN-STIC 824 Informe Estado Seguridad
- CCN-STIC 844 INES
- CCN-STIC 47X Manual de uso PILAR

4. ¿Me sirve o no ISO-27001?

Para resolver esta duda, nada mejor que la guía **CCN-STIC 825** "*Esquema Nacional de Seguridad - Certificaciones 27001*" de Noviembre 2013 Noviembre 2013, cuya URL es:

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/543-ccn-stic-825-ens-iso27001/file.html

Punto 2. "*Objeto*" de esta guía, nos indica claramente:

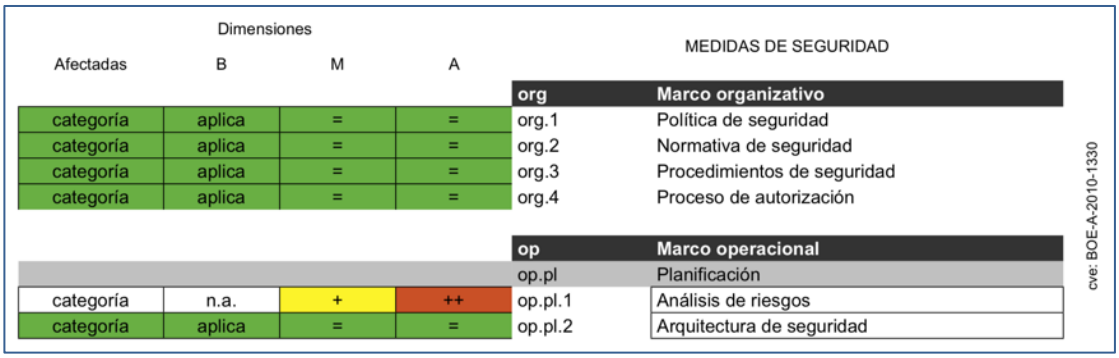
> "*Nótese que la correspondencia no es una relación matemática de equivalencia. Lo que se busca en esta guía es, en primer lugar, explicar la utilización de una certificación 27001 como soporte de cumplimiento del ENS y, en segundo lugar, determinar qué controles de la norma 27002 son necesarios para el cumplimiento de cada medida del Anexo II y, en su caso, qué elementos adicionales son requeridos".*

El punto 5. "*Cumplimiento del ENS a través de una Certificación 27001*" es de sumo interés para nosotros pues nos da una premisa fundamental:

> *El primer requisito para poder utilizar una certificación 27001 como soporte de cumplimiento del ENS es que el alcance de la certificación 27001* ***cubra*** *lo exigido por la Ley 40/2015, tanto desde el punto de vista de los activos esenciales (Anexo I) como del equipamiento empleado.*

Por lo tanto es fundamental considerar el "Alcance" que definiremos para nuestro SGSI (Sistema de Gestión de la Seguridad de la Información), para que desde el inicio, podamos tener una analogía entre ambos.

El **Anexo II** del ENS define cada uno de los requisitos en función de la categoría del sistema de información. Un ejemplo de ello es la imagen que figura a continuación:



Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
				org	**Marco organizativo**
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización
				op	**Marco operacional**
				op.pl	Planificación
categoría	n.a.	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	=	=	op.pl.2	Arquitectura de seguridad

cve: BOE-A-2010-1330

Imagen tomada del Real Decreto 3/2010, de 8 de enero

Esta misma guía 825 en su punto 5.1. "*Cuadro resumen*", presenta tabla que resume las diferencias que cabe esperar entre una certificación 27001 y el cumplimiento del ENS, que para nuestro trabajo es una excelente aportación, abajo podemos apreciar una imagen de algunas líneas de la misma.

MEDIDAS DE SEGURIDAD

org	Marco organizativo	
org.1	Política de seguridad	1
org.2	Normativa de seguridad	1
org.3	Procedimientos de seguridad	1
org.4	Proceso de autorización	1

op	Marco operacional	
op.pl	Planificación	
op.pl.1	Análisis de riesgos	1
op.pl.2	Arquitectura de seguridad	1
op.pl.3	Adquisición de nuevos componentes	2
op.pl.4	Dimensionamiento / Gestión de capacidades	1
op.pl.5	Componentes certificados	3

Imagen tomada de la guía CCN-STIC 825

En la imagen anterior, podemos apreciar justamente algunos de los puntos de los requisitos del ENS (*presentados en la imagen previa: org 1, org 2,…)* respecto al grado de cobertura o esfuerzo (1, 2, 3…) para asociarlo con los controles de ISO-27001.

Como resumen final de este punto, podemos afirmar que una certificación ISO 27001, cubre bastante más que el ENS. Si tenemos la opción de **adecuar nuestra organización a ambos en paralelo es lo ideal**, si ya tengo ISO-27001, tendré gran parte del camino recorrido, sólo nos quedará analizar en detalle el ámbito y "ajustar" lo que esta tabla nos indica.

5. ¿Puedo obtener ambas certificaciones?

Por supuesto que **sí**, y tal cual lo expresamos en el punto anterior, si está en nuestro alcance lanzar ambos en paralelo, nos ahorraremos mucho trabajo, y en definitiva nuestro SGSI será bastante más sólido.

Un importante consejo aquí, es preparar ambos de forma "sincrónica" para poder solicitar las dos certificaciones al unísono, y de ser posible con la misma entidad de certificación. Si lo logramos, todo será más sencillo, tanto para nuestra empresa, como para los auditores externos.

Este tema ha sido tratado en los puntos anteriores y se terminará de desarrollar en el siguiente.

6. ¿Qué pasos debo seguir?

Ahora sí desarrollemos con mayor detalle el cuadro que presentamos al principio que propone el CCN-CERT:

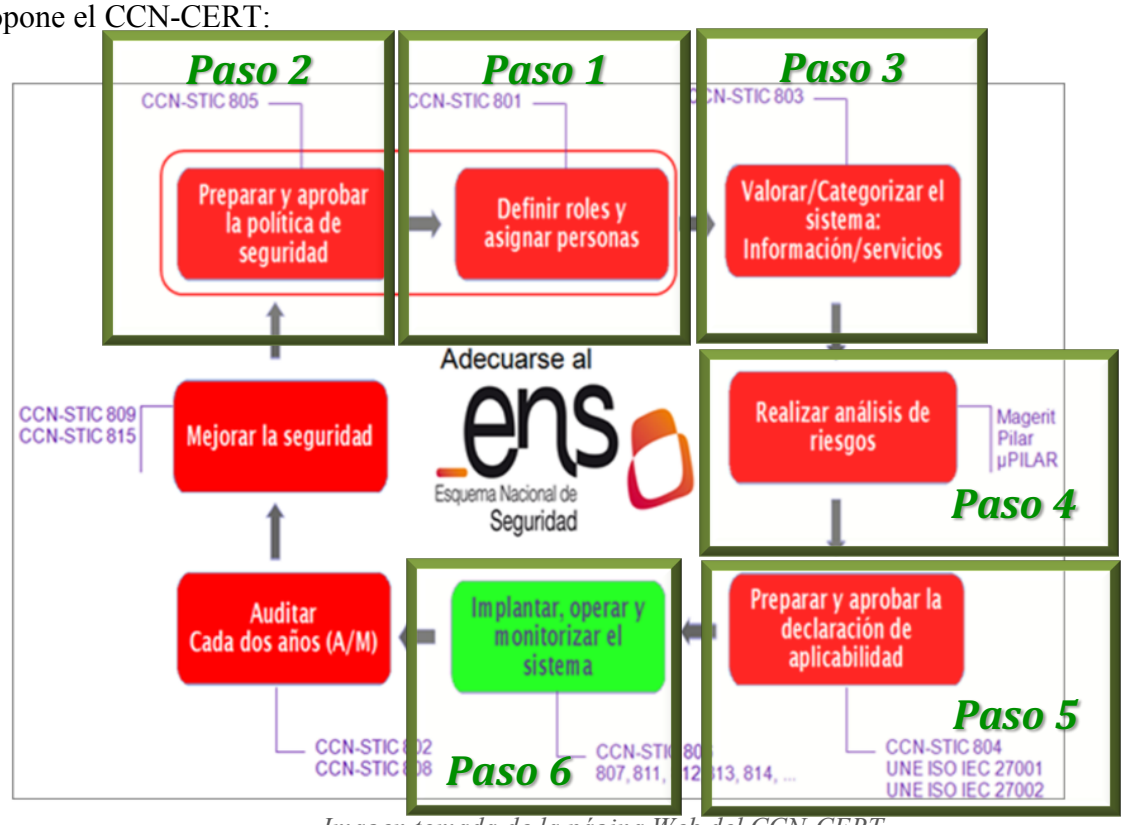


Imagen tomada de la página Web del CCN-CERT

Sobre la imagen anterior y **remarcados en verde** podemos ver los pasos que iremos desarrollando en este punto, en el orden que creemos más práctico de ser abordado.

Paso 1: Definir roles y asignar personas.

Para esta tarea, tal cual nos lo indica la imagen, tomaremos como referencia la guía **CCN_STIC 801**, la descarga de la misma, no está clara en la Web desde, así que aquí abajo figura el enlace correspondiente:

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html

Sobre esta guía, nos centraremos únicamente en los aspectos que consideramos "mandatorios" o que al menos no podemos dejar de lado para ir organizando nuestro SGSI con el objetivo de una futura certificación en ambas normas. El primer punto sobre el que nos detendremos es el punto 2. "*Objeto*", que textualmente nos indica en el apartado 7.

"*El objeto de esta guía es crear un marco de referencia que establezca las responsabilidades generales en la gestión de la seguridad de los sistemas de información, así como proponer unas figuras o roles de seguridad que asuman dichas responsabilidades*".

El punto 3. Nos define su "*Alcance*".

Apartado 9.

"La estructura propuesta en este documento sirve como guía, pudiendo ser la implantación final diferente en cada Organización. No obstante, las responsabilidades definidas en esta norma ***deben ser cubiertas sea cual fuere la solución final adoptada****".*

En pocas palabras: "**Deben** ser cubiertas"… no nos hace falta más datos (mandatorio).

A medida que avanzamos en la guía nos va presentando cómo se organiza la seguridad. Punto 4. "*Organización de la Seguridad*"

Apartado 11.

"*La estructura propuesta diferencia 3 grandes bloques de responsabilidad:*

- *la* ***especificación*** *de las necesidades o requisitos,*
- *la* ***operación*** *del sistema de información*
- *la función de* ***supervisión***"

Los siguientes apartados, nos siguen ampliando la misma:

"*12. Puede que exista por encima de todos ellos un Comité de Seguridad Corporativa.*

13. Puede que exista un Comité de Seguridad de la Información.

14. A menudo pueden distinguirse 3 niveles en el organigrama de una organización:

Nivel 1 – Órganos de Gobierno: alta dirección, que entiende la misión de la organización, determina los objetivos que se propone alcanzar y responde de que se alcancen.

Nivel 2 – Dirección Ejecutiva: gerencias, que entienden qué hace cada departamento y cómo los departamentos se coordinan entre sí para alcanzar los objetivos marcados por la Dirección.

Nivel 3: Operacional, que se centra en una actividad concreta y controla cómo se hacen las cosas.

15. El Responsable de la Información estará en el nivel 1.

16. El Responsable de la Seguridad estará en el nivel 2.

17. El Responsable del Sistema estará en el nivel 3.

18. El Responsable del Servicio, cuando sea diferente del Responsable de la Información, estará en el nivel 1 o en el nivel 2 dependiendo del organigrama de la organización.

19. Cuando exista un Comité de Seguridad Corporativa, estará en el nivel 1.

20. Cuando existe un Comité de Seguridad de la Información, estará en el nivel 1."

En el punto 4.1. "*Segregación*", nos interesa prestar atención al apartado 24. Que dice:

El artículo 10 del Esquema Nacional de Seguridad recoge el principio de "La seguridad como función diferenciada". Este principio exige que el Responsable de la Seguridad sea independiente del Responsable del Sistema.

Otro punto a considerar es el 5. "*Responsables esenciales*"

Apartado 27.

"*La responsabilidad del éxito de una Organización recae, en última instancia, en su Dirección. La Dirección es responsable de organizar las funciones y responsabilidades, la política de seguridad del Organismo, y de facilitar los recursos adecuados para alcanzar los objetivos propuestos*".

Apartado 29.

"*En una organización pueden coexistir diferentes informaciones y servicios, debiendo identificarse al responsable (o propietario) de cada uno de ellos. Una misma persona puede aunar varias responsabilidades*".

Luego, como podemos ver en los puntos que siguen, se definen los siguientes cargos (mandatorios):

"5.1. EL RESPONSABLE DE LA INFORMACIÓN

5.2. EL RESPONSABLE DEL SERVICIO

6. EL RESPONSABLE DE LA SEGURIDAD

41. Persona designada por la Dirección, según procedimiento descrito en su Política de Seguridad".

7. ESTRUCTURA OPERACIONAL DEL SISTEMA

Otros cargos mandatorios que se designan:

"7.1. EL RESPONSABLE DEL SISTEMA

54. Persona designada por la Dirección. La persona designada figurará en la documentación de seguridad del sistema de información.

7.2. SEGURIDAD FÍSICA

61. Cuando la seguridad física (de las instalaciones) esté segregada de la seguridad lógica, esta se ajustará a lo establecido por el ENS en materia de seguridad física de forma análoga a lo establecido en los puntos anteriores.

8. EL ADMINISTRADOR DE LA SEGURIDAD DEL SISTEMA (ASS)

65. La persona designada figurará en la documentación de seguridad del Sistema de información. Según las circunstancias, el ASS puede depender del Responsable del Sistema o del Responsable de la Seguridad.

9. COMITÉS

81. Algunas responsabilidades pueden instrumentarse por medio de comités, que se articularán y funcionarán como órganos colegiados de acuerdo con la normativa administrativa. Estos comités facilitan la armonía de las diferentes partes de la organización.

82. Son habituales los siguientes:

- *Comité de Seguridad de la Información, que se responsabiliza de alinear las actividades de la organización en materia de seguridad de la información.*
- *Comité de Seguridad Corporativa, que se responsabiliza de alinear todas las actividades de la organización en materia de seguridad, cabiendo destacar los aspectos de seguridad patrimonial (seguridad de las instalaciones) y planes de contingencia".*

A continuación, se presenta este anexo de la guía, pues es importante, considerar las tareas que deben ser redactadas y asignadas en el documento de "Organización de la seguridad".

"*ANEXO A. TAREAS*

En la tabla se usan las siguientes abreviaturas:

***CSI** – Comité de Seguridad de la Información*

***RINFO** – Responsable de la Información*

***RSERV** – Responsable del Servicio*

***RSEG** – Responsable de la Seguridad*

***RSIS** – Responsable del Sistema*

***ASS** – Administrador de la Seguridad del Sistema*

A.1. MATRIZ RACI (Responsible, Accountable, Consulted, Informed)"

En Español, la llamaremos **AECI**: Ejecutar (Ejecución) - Aprobación - Consultor - Informar

Tarea	Dirección	RINFO	RSERV	RSEG	RSIS	ASS
niveles de seguridad requeridos por la información		A	I	R	C	
niveles de seguridad requeridos por el servicio		I	A	R	C	
determinación de la categoría del sistema		I	I	A/R	I	
análisis de riesgos		I	I	A/R	C	
declaración de aplicabilidad		I	I	A/R	C	
medidas de seguridad adicionales				A/R	C	
configuración de seguridad		I	I	A	C	R
aceptación del riesgo residual (1)		A	A	R	I	
documentación de seguridad (3)				A	C	I
política de seguridad	A			R	C	
normativa de seguridad (3)				A	C	I
procedimientos de seguridad (3)				C	A	I
implantación de las medidas de seguridad		I	I	C	A	R
supervisión de las medidas de seguridad				(2)	(2)	R
estado de seguridad del sistema	I	I	I	A	I	R
planes de mejora de la seguridad (3)				A	C	
planes de concienciación y formación (3)				A	C	
planes de continuidad (3)				C	A	
suspensión temporal del servicio	A	C	C	C	R	
seguridad en el ciclo de vida (3)				C	A	

Imagen tomada de la guía CCN_STIC 801

Es muy importante detenerse el tiempo suficiente en el cuadro anterior y verificar que estamos adjudicando y cumpliendo al detalle con cada una de las responsabilidades que se expresan en la matriz. Este tipo de detalles, tal vez sean uno de los factores más importantes que suelen tener en cuenta los auditores.

Paso 2: Preparar y aprobar la política de seguridad.

Para esta tarea, tal cual nos lo indica la imagen, tomaremos como referencia la guía **CCN_STIC 805** "Política de Seguridad de la Información". Aquí abajo figura el enlace correspondiente:

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/508-ccn-stic-805-politica-de-seguridad-de-la-informacion/file.html

Esta guía es sumamente concreta y sencilla de aplicar, en particular porque hasta nos ofrece una ejemplo de ella en el **ANEXO C**. "EJEMPLO DE POLÍTICA".

El único punto que presentaremos a continuación es el 3. "Contenido", que nos presenta con total precisión qué debemos incluir en la misma (cada punto está desarrollado también a continuación en la misma guía), su esquema es:

Apartado 11.

"*Secciones típicas de una Política de Seguridad de la Información:*

1. Misión u objetivos del organismo

2. Marco normativo

3. Organización de seguridad

- *Definición de comités y roles unipersonales ! Funciones*
- *Responsabilidades*
- *Mecanismos de coordinación*
- *Procedimientos de designación de personas*

4. *Concienciación y formación*
5. *Postura para la gestión de riesgos*
   - *Plan de análisis*
   - *Criterios de evaluación de riesgos*
   - *Directrices de tratamiento*
   - *Proceso de aceptación del riesgo residual*
6. *Proceso de revisión de la política de seguridad*"

No merece la pena detenernos más en la misma, el consejo es que llegado el momento, la leáis en detalle y la cumplimentéis en su totalidad, tomando como referencia el modelo del ANEXO C.

Paso 3: Valorar/Categorizar el sistema.

Para esta tarea, tal cual nos lo indica la imagen, tomaremos como referencia la guía **CCN_STIC 803** "ENS. Valoración de los sistemas". Aquí abajo figura el enlace correspondiente

Algo importante que hace referencia en el punto 1. "*Introducción*" es que también hace mención al **RGPD** (Reglamento General Europeo de Protección de Datos), el cual, si nuestros sistemas tratan datos personales, impone también la realización de un Análisis de Riesgo.

Este detalle para nosotros es de suma importancia, pues es casi seguro que nuestros SSII traten estos datos, y lo que acabamos de leer implica que si "hacemos las cosas bien", es el mismo análisis de riesgo el que nos servirá para ENS, ISO-27001 y RGPD.

El apartado 7. de esta Introducción nos define que:

"*Esta guía pretende definir los criterios para determinar el nivel de seguridad requerido en cada dimensión*".

Del punto 2. "*Criterios de Valoración*", nos detenemos en el Apartado 30.

"*Los criterios de impacto considerados son los 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."*

Luego de ello viene una tabla (*que no pegamos por su tamaño*) que DEBEMOS tener en cuenta cuando realicemos esta actividad.

En relación con el **RGPD**, el Apartado 35 nos deja claro que:

"*Es función del Responsable de la Seguridad determinar el conjunto de medidas requerido, uniendo los que se requieren por una y otra norma, e imponiendo la exigencia superior*".

Luego más abajo presenta también una tabla a considerar en el tratamiento de datos personales (¡TENEDLA EN CUENTA!)

El resto de la guía, son un conjunto de criterios, que es necesario tener en cuenta en esta actividad.

Por último, es importante que consideremos los puntos:

"5. DETERMINACIÓN DE LOS NIVELES Y CATEGORÍA DEL SISTEMA

5.1. VALORACIÓN DE LAS DIMENSIONES DE LOS ACTIVOS ESENCIALES

96. Por cada activo esencial, sea de tipo información o de tipo servicio, se solicita la valoración de su nivel (bajo, medio o alto) en cada dimensión de seguridad".

Denominación del Activo esencial	tipo[8]	C[9]	I	D	A	T
Valor máximo del nivel registrado en las dimensiones de seguridad						

Imagen tomada de la guía 803 - Categorización de un Sistema a partir de los Niveles en cada Dimensión de sus Activos Esenciales.

Otro punto sobre el que también debemos centrar nuestra atención es:

"*5.3. FORMULACIÓN DE LA CATEGORÍA DE UN SISTEMA*

106. La forma de representar la categoría de un sistema será la siguiente, explicitando el nivel en cada dimensión para ayudar a determinar las medidas de seguridad exactas que han sido de aplicación:

CATEGORÍA (BÁSICA-MEDIA-ALTA): [C=(N/A-B-M-A), I= (N/A-B-M-A), D=(N/A-B- M-A), A=(N/A-B-M-A), T= (N/A-B-M-A)]"

Categoría que se ha asignado al/los sistema(s) de << Nombre de la entidad>> es:
(Categoría): [C(Nivel), I(Nivel), D(Nivel), A(Nivel), T(Nivel)]

Imagen tomada de la guía 803 - Categorización de un Sistema junto a los Niveles en sus Dimensiones de Seguridad.

Y a continuación de la tabla la misma guía nos pone los siguientes ejemplos:

"Ejemplos:

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)]".*

Prestad mucha atención a estos ejemplos de la guía, pues nos indican claramente que con **UNA SOLO** dimensión superior, el sistema adopta esa Categoría Superior (*Jamás hacia abajo, o minimizando la Categoría*).

Paso 4: Realizar el análisis de riesgo.

Si prestamos atención al cuadro que nos ofrece el CCN (*sobre el que hemos remarcadoen verde los pasos)*, podemos apreciar claramente que hacer referencia a Magerit.

Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), es la metodología, que fue creada por **José Mañas** e incorporada desde su *versión 1* en las AAPP Españolas. Como metodología es suficientemente completa. Existen dos herramientas que no son obligatorias, pero facilitan el trabajo a la hora de trabajar con esta metodología, en nuestro caso, para empresas privadas la que corresponde es **EAR** (Entorno de Análisis de Riesgos) que está desarrollada y financiada parcialmente por el CCN.

Pero esto es una recomendación, NO es mandatorio. En ninguno de los Reales Decretos se menciona Magerit.

Consideremos qué nos dice sobre esta actividad el **ENS**.

En su Artículo 13. "*Análisis y gestión de los riesgos*".

"1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.

2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.

3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos".

Vayamos a la última actualización del ENS: El **Real Decreto 951**, que modifica al Real Decreto 3/2010, en su Artículo único y Punto Quince.

Apartados 1. "Objeto de la auditoría" y 1.1. expresa:

"La seguridad de los sistemas de información de una organización será auditada en los siguientes términos

d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual".

¿Por qué se recalca esta situación?, pues porque nuestra metodología a aplicar, lo que de verdad importa es que sea "Completa", es decir que el Auditor pueda evaluar que hemos realizado un trabajo serio, robusto y contundente que nos lleva a determinar con toda claridad el impacto final y el riesgo que deberemos tratar.

La metodología Magerit, es "Completa", por lo tanto tomarla como referencia o guía es una sabia decisión, pero lo importante en definitiva es que sigamos los pasos que el mismo CCN en su Web nos propone, los cuáles son:

- tipos de activos (Identificación, cuantificación, interrelaciones)
- dimensiones de valoración de los activos
- criterios de valoración de los activos
- amenazas típicas sobre los sistemas de información
- salvaguardas a considerar para proteger sistemas de información

Paso 5: Preparar y aprobar la Declaración de Aplicabilidad.

Este es un paso "Clave" para integrar todas nuestras normas, pues justamente

Tal cual nos indica la imagen del CCN, esta vez emplearemos la Guía **CCN-STIC 804** "*ENS. Guía de implantación*" (Junio 2017)

Esta sí que la podemos encontrar en la URL del ENS:

https://www.ccn-cert.cni.es/ens/instrumentos-para-la-adecuacion.html

Comencemos con un tema importante, el punto 2. "*Niveles de madurez*"

Apartado 6.

"Es habitual el empleo de niveles de madurez para caracterizar la implementación de un proceso. El modelo de madurez permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad".

Los clasifica desde "**L0**"(Inexistente), hasta "**L5**" (optimizado)

El apartado 8. nos dice:

"Como regla general, se exigirá un nivel de madurez en las medidas de seguridad en proporción al nivel de las dimensiones afectadas o de la categoría del sistema":

Nivel de madurez medidas de seguridad	Categoría del sistema de las tecnologías de la información y la comunicación	Nivel de madurez mínimo exigido
Bajo	Básica	L2 - Repetible, pero intuitivo
Medio	Media	L3 - Proceso definido
Alto	Alta	L4 - Gestionado y medible

Imagen tomada de la guía 803 - Niveles de madurez exigidos en función de la categoría del sistema o nivel de la dimensión de seguridad

Luego esta guía nos desarrolla al completo todos los puntos que debemos considerar, haciendo referencia también a ISO 27001 y 27002.

Sobre estas dos últimas, merece la pena tener en cuenta que si bien la que se certifica es la 27001, que la llamaremos "cuerpo de la norma", la que detalla los controles es la 27002. Es decir la "Declaración de Aplicabilidad" (o **SoA** en Inglés), muchas veces se piensa que está referida a los 116 controles de la 27002, pero NO deben ser dejados de lado varios puntos específicos que son mandatorios del cuerpo de la orden (es decir de la ISO 27001).

Es aquí donde está la "clave" que hemos mencionado al principio de este paso 5, pues debemos hacer el máximo esfuerzo para que esta "Declaración de Aplicabilidad" cubra ambos estándares… y de paso, así como por las dudas, controlemos también en detalle lo que corresponde a **RGPD**, para no dejar nada librado al azar.

Paso 6: Implantar, operar y monitorizar el sistema.

En este punto vamos a tratar los aspectos fundamentales de las guías que nos propone el CCN, la primera es la guía **CCN-STIC 807** "Criptología de empleo en el Esquema Nacional de Seguridad" (Abril 2017)

Como su nombre lo indica, en ella se redactan todas las consideraciones necesarias a tener en cuenta, por lo tanto, a la hora de decidir emplear cualquier herramienta o algoritmo, recomendamos sea leída en detalle la guía, pues muchas de estas recomendaciones son mandatorias para el sistema que estemos tratando.

Los puntos fundamentales son:

2. OBJETIVO
8. En la presente guía se presentan los algoritmos criptográficos que han sido acreditados nominalmente para su uso en el Esquema Nacional de Seguridad, cuando sus características y requerimientos se consideren necesarios.

3. ALGORITMOS ACREDITADOS
9. Se recomienda el uso de los algoritmos listados en el documento "SOGIS Agreed cryptographic Mechanisms" publicado por el Senior Officials Group Information Systems Security (SOG-IS). Este documento se encuentra disponible digitalmente en el apartado "Supporting documents" del grupo de trabajo de criptografía (Crypto WG) de SOG-IS en su página web www.sogis.org.

10. Además de los algoritmos listados en el documento de SOG-IS, la siguiente relación de algoritmos y protocolos criptográficos se consideran acreditados por el CCN para su uso dentro del Esquema Nacional de Seguridad (ENS), siempre que se realice una implementación correcta de los mismos según las especificaciones adjuntas:

3.1 CIFRADO SIMÉTRICO

11. TDEA (Triple Data Encryption Algorithm, Triple Algoritmo de Cifrado de Datos): SP 800-20, SP800-38B y SP 800-67 del NIST ([NIST, SP800-20], [NIST, SP800- 38B], [NIST, SP800-67]).
12. AES (Advanced Encryption Standard, Cifrado de Datos Avanzado): FIPS 197 y SP800-38B del NIST ([NIST, FIPS197], [NIST, SP800-38B]).

3.2 PROTOCOLOS DE ACUERDO DE CLAVE

13. DH o DHKA (Diffie-Hellman Key Agreement, Acuerdo de Clave de Diffie- Hellman): ANSI X9.42 ([ANSI, X9.42]) y PKCS #3 de los laboratorios RSA ([RSALab, 1993]).
14. MQV (Menezes-Qu-Vanstone Key Agreement, Acuerdo de Clave de Menezes- Qu-Vanstone): ANSI X9.42 ([ANSI, X9.42]), ANSI X9.63 ([ANSI, X9.63]) e IEEE 1363 [IEEE, 1363].
15. ECDH (Elliptic Curve Diffie-Hellman, Acuerdo de Clave de Diffie-Hellman con Curvas Elípticas): ANSI X9.63 ([ANSI, X9.63]), IEEE1363 ([IEEE, 1363]), IEEE1363a ([IEEE, 1363a]) y la Suite B de la NSA ([NSA, SuiteB]).
16. ECMQV (Elliptic Curve Menezes-Qu-Vanstone, Acuerdo de Clave de Menezes- Qu-Vanstone con Curvas Elípticas): SEC 1 del SECG ([SECG, SEC1]).

3.3 ALGORITMOS ASIMÉTRICOS

17. DSA (Digital Signature Algorithm, Algoritmo de Firma Digital): ANSI X9.30 ([ANSI, X9.30-1]), FIPS 186-4 ([NIST, FIPS186-4]).
18. ECDSA (Elliptic Curve Digital Signature Algorithm, Algoritmo de Firma Digital con Curvas Elípticas): ANSI X9.62 ([ANSI, X9.62]), FIPS 186-4 ([NIST, FIPS186-4]), SP 800-57A del NIST ([NIST, SP800-57A])y SEC 1 del SECG ([SECG, SEC1]).
19. RSA (Criptosistema RSA): ANSI X9.44 ([ANSI, X9.44]), ANSI X9.31 ([ANSI, X9.44]), FIPS 186-4 ([NIST, FIPS186-4]) y PKCS #1 de los laboratorios RSA ([RSALab, 2002]).
20. ECIES (Elliptic Curve Integrated Encryption Scheme, Esquema de Cifrado Integrado con Curvas Elípticas): ANSI X9.63 ([ANSI, X9.63]), IEEE1363a ([IEEE, 1363a]), ISO 11770-3 ([ISOIEC, 11770-3]) e ISO 18033-2 ([ISOIEC, 18033-2]).

3.4 FUNCIONES RESUMEN

21. SHA-2 (Secure Hash Algorithm, Algoritmo Resumen Seguro): FIPS180-4 ([NIST, FIPS180-4]).
22. SHA-3 (Secure Hash Algorithm, Algoritmo Resumen Seguro): FIPS202 ([NIST, FIPS202]).
23. HMAC (Hash Message Authentication Code, Código de Autenticación de Mensaje con Resumen): ANSI X9.71 ([ANSI, X9.71]) y FIPS 198-1 ([NIST, FIPS198- 1]).

A título de ejemplo, se presenta a continuación, como esta guía especifica cada una de las medidas criptográficas a aplicar, siempre basándose en la "Categoría" y lo desarrolla, dimensión por dimensión.

4.2 MECANISMOS DE AUTENTICACIÓN.

4.2.1. NIVEL BAJO
34. Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor.

4.2.2. NIVEL MEDIO
38. Para nivel medio se exigirá el uso de al menos dos factores de autenticación.

4.2.3. NIVEL ALTO
41. Para el nivel alto, se exigirá el uso de al menos dos factores de autenticación.

Luego en sus anexos, que ocupan más de cien hojas presenta un verdadero "curso de criptografía" pues describe detalladamente cada uno de los algoritmos.

La segunda es la guía **CCN-STIC 811** "Interconexión en el ENS" (Octubre 2017). Su URL es:

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/521-ccn-stic-811-interconexion-en-el-ens/file.html

Los puntos más importantes de ella son:
"3. ALCANCE
13. Esta guía tratará las interconexiones basadas en protocolos estándares de comunicaciones cuando uno de los sistemas esté afectado por el Esquema Nacional de Seguridad.

7. ARQUITECTURA DE PROTECCIÓN PERIMETRAL (APP)
25. Se deberá constituir una arquitectura de protección perimetral, utilizando para ello dispositivos que permitan proteger los flujos de información.
26. Dentro de las posibilidades tecnológicas que podemos adquirir, para cumplir ese objetivo, nos centraremos en los siguientes dispositivos.
- Enrutadores (routers)
- Cortafuegos (firewalls)
- Intermediarios (proxies)
- Pasarelas de intercambio seguro
- Diodos de datos

8. TIPOS DE ARQUITECTURAS DE PROTECCIÓN DE PERÍMETRO
Este punto describe y clasifica varias opciones de arquitecturas a considerar.

10. REQUISITOS DEL ENS SOBRE ARQUITECTURAS DE PROTECCIÓN DE PERÍMETRO
105.Para sistemas de las tecnologías de la información sujetos al Esquema Nacional de Seguridad, se autorizan las siguientes

arquitecturas de protección del perímetro.

Categoría del sistema	Arquitectura de Protección de Perímetro
Básica	APP-3 o superior
Media	APP-4 o superior
Alta	APP-5 o superior

Imagen tomada de la guía 811 - Arquitectura de protección de perímetro mínima a implantar por categoría del sistema

12. REQUISITOS DEL ENS SOBRE HERRAMIENTAS DE SEGURIDAD

130.El despliegue de herramientas de seguridad en el sistema de protección del perímetro se atendrá a los siguientes parámetros no funcionales en función de la categoría del sistema protegido por dicho perímetro.

Categoría del sistema	Básica	Media	Alta
Detección de código dañino	Aplica	=	+
• La base de datos se mantiene actualizada	< 4 días	< 48 horas	< 24 horas
• Se aplican las actualizaciones (parches) de seguridad	< 7 días	< 7 días	< 4 días
Análisis de vulnerabilidades	Aplica	=	=
• El software se mantiene actualizado	< 7 días	< 7 días	< 7 dias
• Frecuencia mínima de escaneo	3meses	1mes	1semana
Análisis de registros de actividad	Recomendado	Aplica	=
• Frecuencia mínima de revisión	1 mes-	1semana	3 día
Detección y prevención de intrusos	Opcional	Aplica	+
• El software se mantiene actualizado	< 7 días	< 7 días	< 7 días
Monitorización de tráfico	Opcional	Recomendado	Aplica
Verificación de la configuración	Opcional	Recomendado	Aplica
• Frecuencia mínima de verificación	1 año	6 meses	2 meses
Prevención de fuga de datos (DLP)	Opcional	Opcional	Recomendado
• El software se mantiene actualizado	< 7dias	< 7dias	< 7dias

Imagen tomada de la guía 811 - Requisitos del ENS sobre herramientas de seguridad

Hemos querido poner de manifiesto las dos tablas anteriores, pues estas son las típicas medidas que **sí o sí** debemos considerar para demostrar que hemos trabajado para implantar adecuadamente lo que indica el ENS

Luego siguen el resto de ellas:

Guía CCN-STIC 812 SEGURIDAD EN ENTORNOS Y APLICACIONES WEB

Guía CCN-STIC 813 Componentes certificados en el ENS

Guía CCN-STIC 814 SEGURIDAD EN CORREO ELECTRÓNICO

……..

Sobre las cuáles no merece la pena detenernos más, pues básicamente lo que hay que hacer es leerlas cada una de ellas para poder "bastionar" estos servicios cumpliendo como mínimo con lo que en ellas se establece.

Un tema adicional que no debemos olvidar es la "**FORMACIÓN**", pues es parte de esta Certificación, por lo que debemos haber impartido desde uno a "n" cursos a TODO el personal de nuestra organización, y dejar constancia (por escrito) de su asistencia.

El consejo final, que siempre me ha dado resultado, es preparar un documento de "**Presentación del SGSI**" (al menos yo lo he denominado de esta forma en todas las implantaciones que he participado…).

Un viejo refrán dice "El que pega primero, pega dos veces".

La idea del mismo es justamente la del refrán.

Lo primero a lograr es una Robusta "Estructura Documental". Luego, este documento, debe comenzar con un cuadro muy detallado de **qué punto** y **de qué documento** de nuestra "Estructura Documental" está cubriendo absolutamente TODO lo que en las guías que acabamos de presentar puede ser interpretado como "mandatorio", por supuesto incluyendo sin lugar a dudas, TODOS los puntos de la "Declaración de Aplicabilidad" (que en nuestro caso recordad que estamos hablando de ENS, ISO 27001, ISO 27002 y RGPD).

Lo segundo a incluir en este documento, es una bitácora de las acciones que fuimos llevando a cabo hasta llegar a la fecha de la Auditoría externa. Esta bitácora cobra importancia, pues demuestra que el SGSI viene rodando desde hace tiempo.

Una vez que este documento este finalizado, deberá ser lo primero que haremos cuando llegue el Auditor, solicitándole que por favor, nos permita robarle quince minutos para presentarle (muy brevemente) lo que se ha hecho, luego le dejamos este documento como guía a seguir en su búsqueda de cualquier tipo de acción o documento dentro de nuestro SGSI.

Con estas tareas bien hechas, sólo nos queda tener "Fe" en que todo saldrá bien, y como el nombre de mi empresa indica, si trabajamos bien este artículo puedo "**DarFE**" que lograrás estas certificaciones.