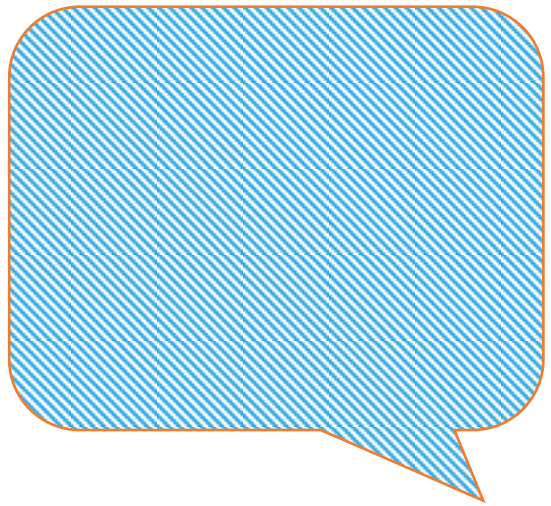
Stand by me. Cuenta Conmigo

Caso Práctico de Implantación del ENS. La CHJ



- José Manuel Leal García
- Antonio Grimaltos Vidal

- **Confederación Hidrográfica del Júcar. Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente.**

- josemanuel.leal@chj.es
- antonio.grimaltos@chj.es

Caso Práctico del Plan de Adecuación e Implantación del ENS

Índice

Caso Práctico del Plan de Adecuación e Implantación del ENS

¿Quiénes Somos?

Normativa y funciones

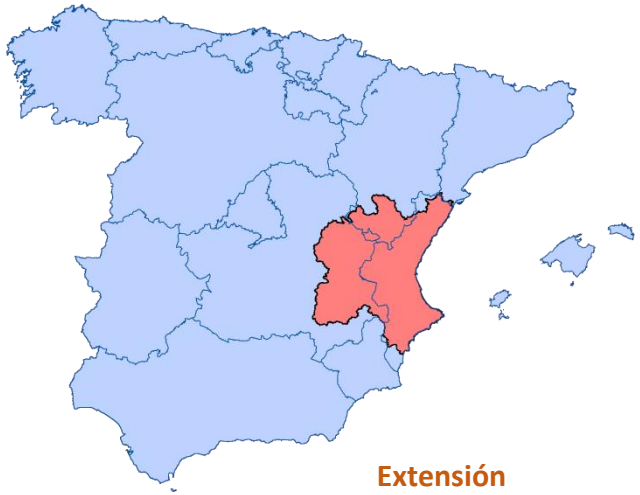
Las Confederaciones Hidrográficas, son organismos autónomos de los previstos en el artículo 43.1.ª) de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, adscritos, a efectos administrativos, al **Ministerio de Medio de Agricultura y Pesca, Alimentación y Medio Ambiente**

El texto refundido de la Ley de Aguas determina en su artículo 21 y siguientes la naturaleza y régimen jurídico, así como sus funciones y atribuciones. Siendo su principales funciones:

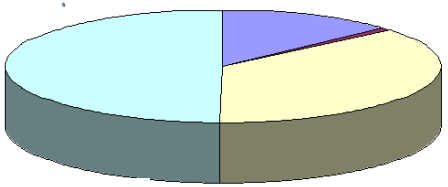
La elaboración del plan hidrológico de cuenca, así como su seguimiento y revisión.
La administración y control del Dominio Público Hidráulico.
La administración y el control de los aprovechamientos de interés general o que afecten a más de una comunidad autónoma.
El proyecto, construcción y explotación de las obras realizadas con cargo a los fondos propios de Organismo y las que les sean encomendadas por el Estado.
Las que se deriven de los convenios con comunidades autónomas, corporaciones locales y otras entidades públicas o privadas, o de los suscritos con los particulares.

Caso Práctico del Plan de Adecuación e Implantación del ENS

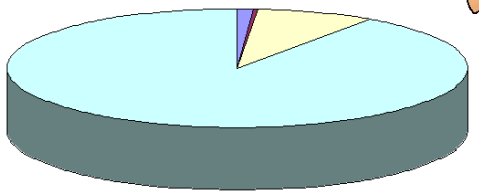
¿Quiénes Somos?



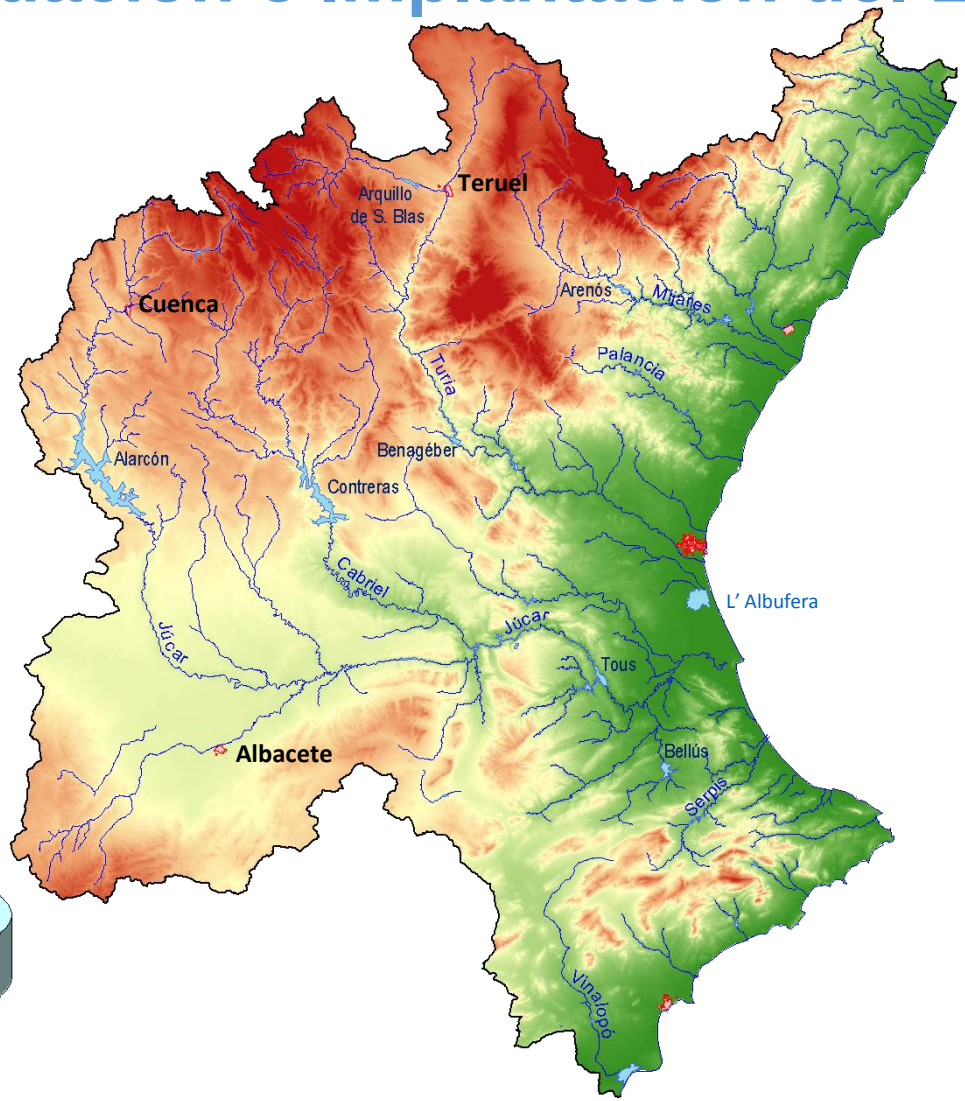
Extensión



Población



- Aragón
- Cataluña
- Castilla – La Mancha
- Comunidad Valenciana
- Región de Murcia



Caso Práctico del Plan de Adecuación e Implantación del ENS

¿Quiénes Somos?

Datos Generales de la CHJ

- Superficie de la cuenca del Júcar: 42.735 km^2
- Número de habitantes: 5.348.000
- Comunidades autónomas
  - Aragón
  - Cataluña
  - Castilla – La Mancha
  - Comunidad Valenciana
  - Región de Murcia
- Recursos hídricos: 3.900 hm^3/año
- Superficie de regadío: 390.000 ha

Caso Práctico del Plan de Adecuación e Implantación del ENS

¿Quiénes Somos?

Organización de la CHJ

Presidencia

- **Dirección Técnica**
- **Comisaría de Aguas**
- **Secretaria General**
- **Oficina de Planificación Hidrológica**

Caso Práctico del Plan de Adecuación e Implantación del ENS

¿Quiénes Somos?

De acuerdo con el art. 6 del Real Decreto 984/1989, de 28 de julio, por el que se determina la estructura orgánica dependiente de la Presidencia de las Confederaciones Hidrográficas, **una de las funciones de la Secretaría General, como unidad integrada en el organismo de cuenca es:**

Servicio de Informática de la CHJ

La supervisión y coordinación de la informática en materia administrativa

El Servicio de informática debe atender las necesidades de:

- Equipamiento informático
- Aplicaciones y sistemas de información
- Comunicaciones
- Bases de datos
- Portales web e Intranet
- Administración electrónica
- **Seguridad**
- …

Caso Práctico del Plan de Adecuación e Implantación del ENS

¿Quiénes Somos?

De acuerdo con el art. 6 del Real Decreto 984/1989, de 28 de julio, por el que se determina la estructura orgánica dependiente de la Presidencia de las Confederaciones Hidrográficas, **una de las funciones de la Secretaría General, como unidad integrada en el organismo de cuenca es:**

Servicio de Informática de la CHJ

La supervisión y coordinación de la informática en materia administrativa

El Servicio de informática debe atender las necesidades de:

- Equipamiento informático
- Aplicaciones y sistemas de información
- Comunicaciones
- Bases de datos
- Portales web e Intranet
- Administración electrónica
- …
- **Seguridad**

Elemento integral

Caso Práctico del Plan de Adecuación e Implantación del ENS

¿Quiénes Somos?

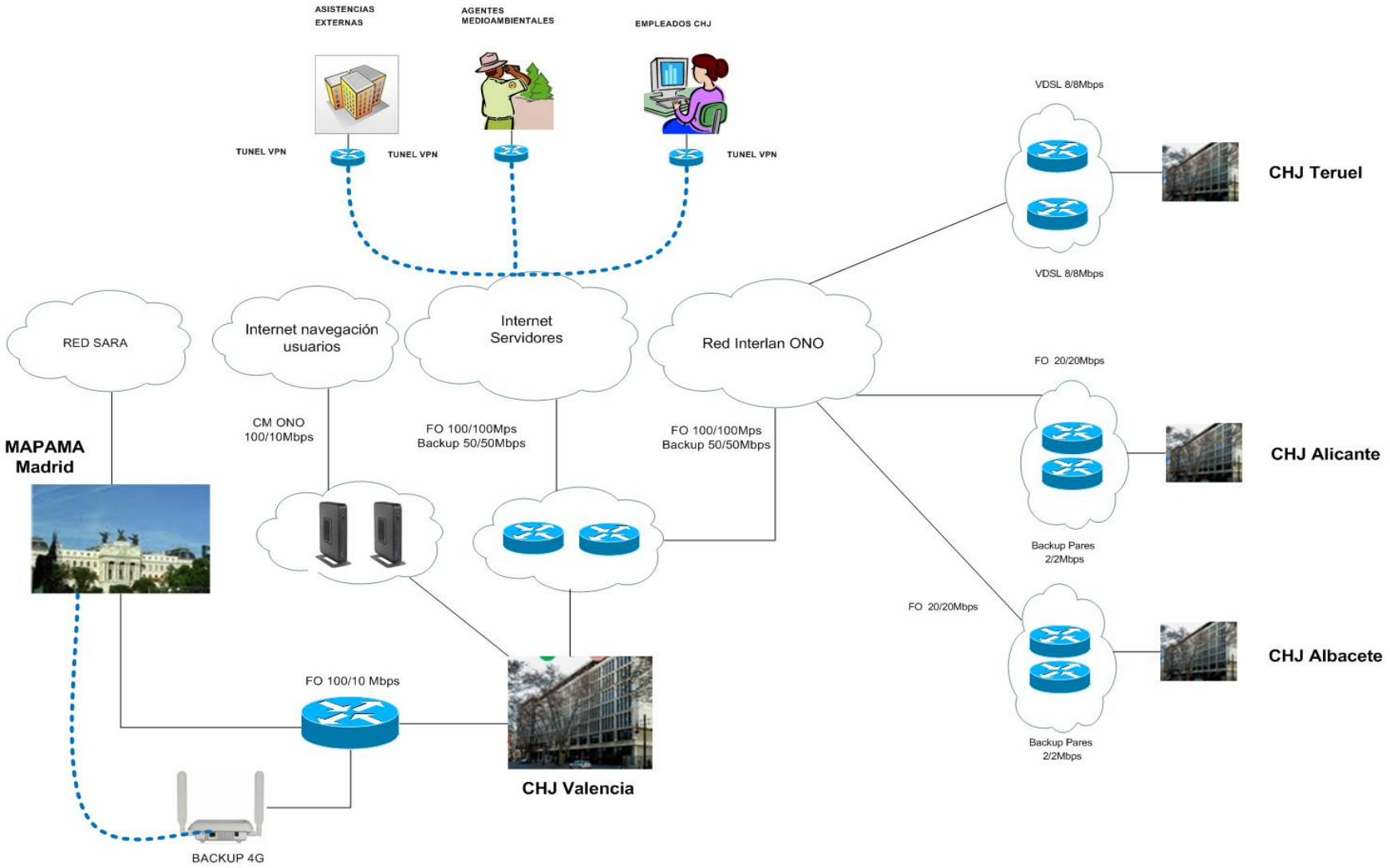
Organización de la CHJ

- **Presidencia**
  - → **Dirección Técnica**
  - → **Comisaría de Aguas**
  - → **Secretaria General** → **Servicio de Informática de la CHJ**
  - → **Oficina de Planificación Hidrológica**

Caso Práctico del Plan de Adecuación e Implantación del ENS

¿Quiénes Somos?

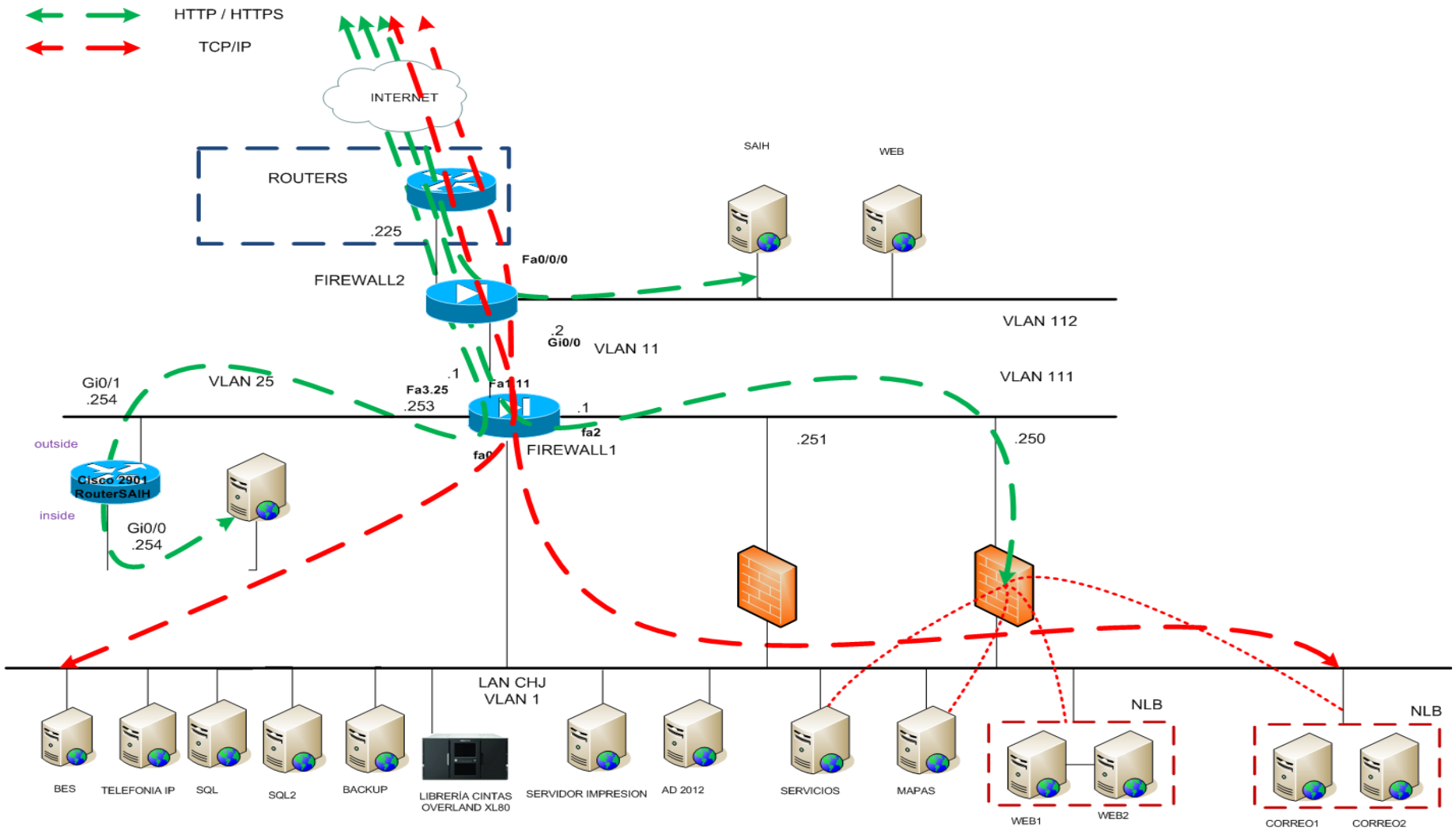
Esquema de comunicaciones externo



Caso Práctico del Plan de Adecuación e Implantación del ENS

¿Quiénes Somos?

Esquema de comunicaciones interno



Caso Práctico del Plan de Adecuación e Implantación del ENS

Imperativo Legal

El artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, crea el Esquema Nacional de Seguridad.

El art. 156.2 de Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece *que "tiene por **objeto** establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada."*

Caso Práctico del Plan de Adecuación e Implantación del ENS

Imperativo Legal

Real decreto 3/2010 de 8 de Enero regula el ENS (Esquema nacional de Seguridad). ***Boe del 29 de enero de 2010***

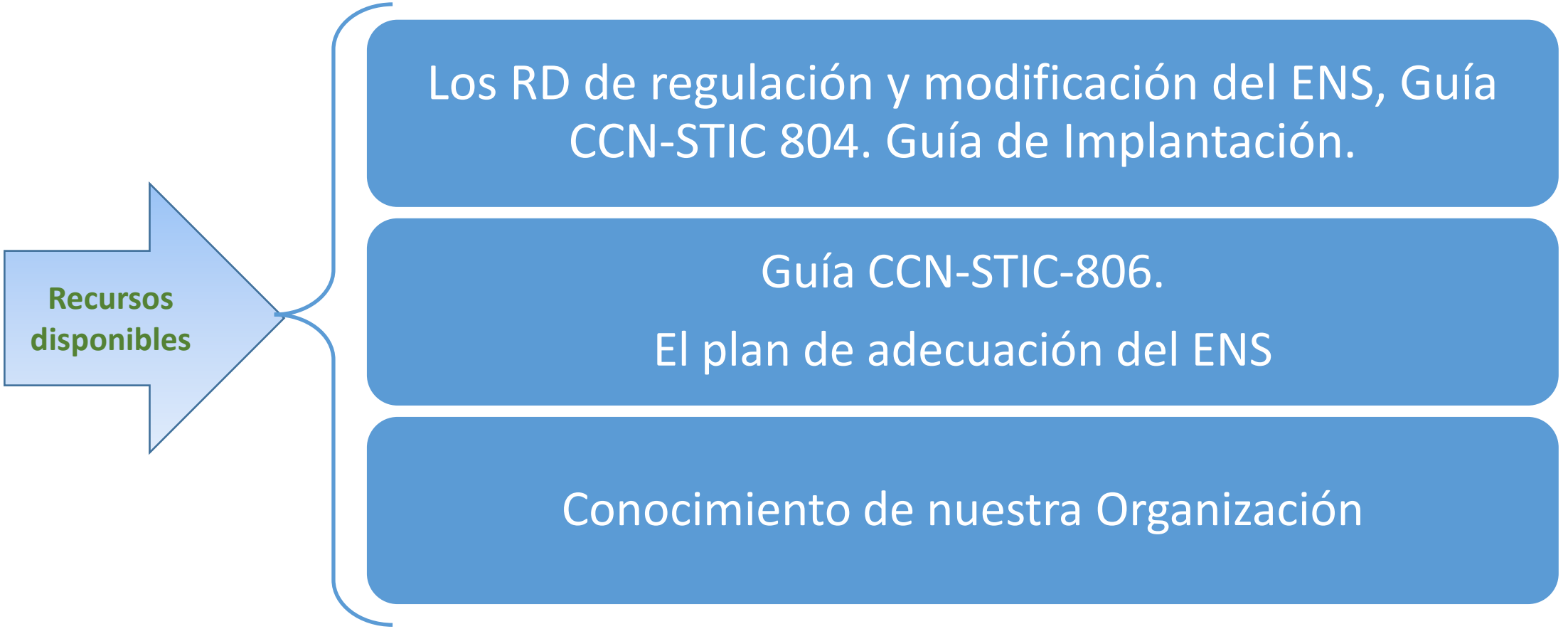
Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. ***Boe, Del 4 de Noviembre de 2015***

Finalidad del ENS

… crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios

Caso Práctico del Plan de Adecuación e Implantación del ENS

¿Por donde empezar?

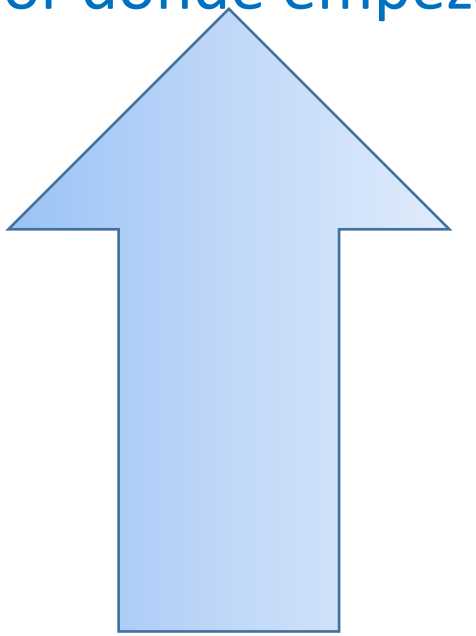


Caso Práctico del Plan de Adecuación e Implantación del ENS

¿Por donde empezar?

Caso Práctico del Plan de Adecuación e Implantación del ENS

¿Por donde empezar?



Usamos esos recursos disponibles

- El BOE y los RD de regulación y modificación del ENS, Guía CCN-STIC 804. Guía de Implantación
- Conocer nuestra Organización
- Guía CCN-STIC-806.
  El plan de adecuación del ENS

Encontramos el 1er Problema. EXCESO DE DOCUMENTACIÓN

Al Final la pregunta sigue sin Respuesta…….

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

Según la guía CCN-STIC-806, el PLAN DE ADECUACIÓN al ENS debe contener al menos los siguientes elementos:

- La política de seguridad
- Información que se maneja, con su valoración
- Servicios que se prestan, con su valoración
- Datos de carácter personal
- Categoría del sistema
- Análisis de riesgos
- Declaración de aplicabilidad de las medidas del Anexo II del ENS y las requeridas por el tratamiento de datos de carácter personal, si los hubiera
- Insuficiencias del sistema (gap analysis)
- Plan de mejora seguridad, incluyendo plazos estimados de ejecución

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

Según la guía CCN-STIC-806, el PLAN DE ADECUACIÓN al ENS debe contener al menos los siguientes elementos:

- La política de seguridad
- Información que se maneja, con su valoración
- Servicios que se prestan, con su valoración
- Datos de carácter personal
- Categoría del sistema
- Análisis de riesgos
- Declaración de aplicabilidad de las medidas del Anexo II del ENS y las requeridas por el tratamiento de datos de carácter personal, si los hubiera
- Insuficiencias del sistema (gap analysis)
- Plan de mejora seguridad, incluyendo plazos estimados de ejecución

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

PLAN DE ADECUACIÓN
Aprobado por el Órgano Superior Competente…¿?

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

Órgano Superior Competente

- La guía CCN-STIC-402 Organización de la Seguridad.
- Comité de Seguridad de la Información……

La guía CCN-STIC-402 establece una serie de modelos que podemos tomar como referencia, pero son solamente eso, modelos de una guía de referencia.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

0

Fomentar la creación del Comité de Seguridad de la Información, que será el órgano decisivo en materia de seguridad y estableciendo su funcionamiento.
Comité de Seguridad de la Información (STIC).

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

0

Fomentar la creación del Comité de Seguridad de la Información, que será el órgano decisivo en materia de seguridad y estableciendo su funcionamiento.
Comité de Seguridad de la Información (STIC).

¿Cómo?

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

0

Fomentaremos la creación del Comité de Seguridad de la Información, que será el órgano decisivo en materia de seguridad y estableciendo su funcionamiento.
Comité de Seguridad de la Información (STIC)

Preparando la documentación necesaria para que se ponga en funcionamiento dicho comité.

- **Convocatoria**
- **Reglamento de régimen interior**
- **Nombramiento Miembros comité**
- **Etc. …**

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

0

Comité de Seguridad

Decisiones

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

0

Comité de Seguridad

Decisiones

Problemas:

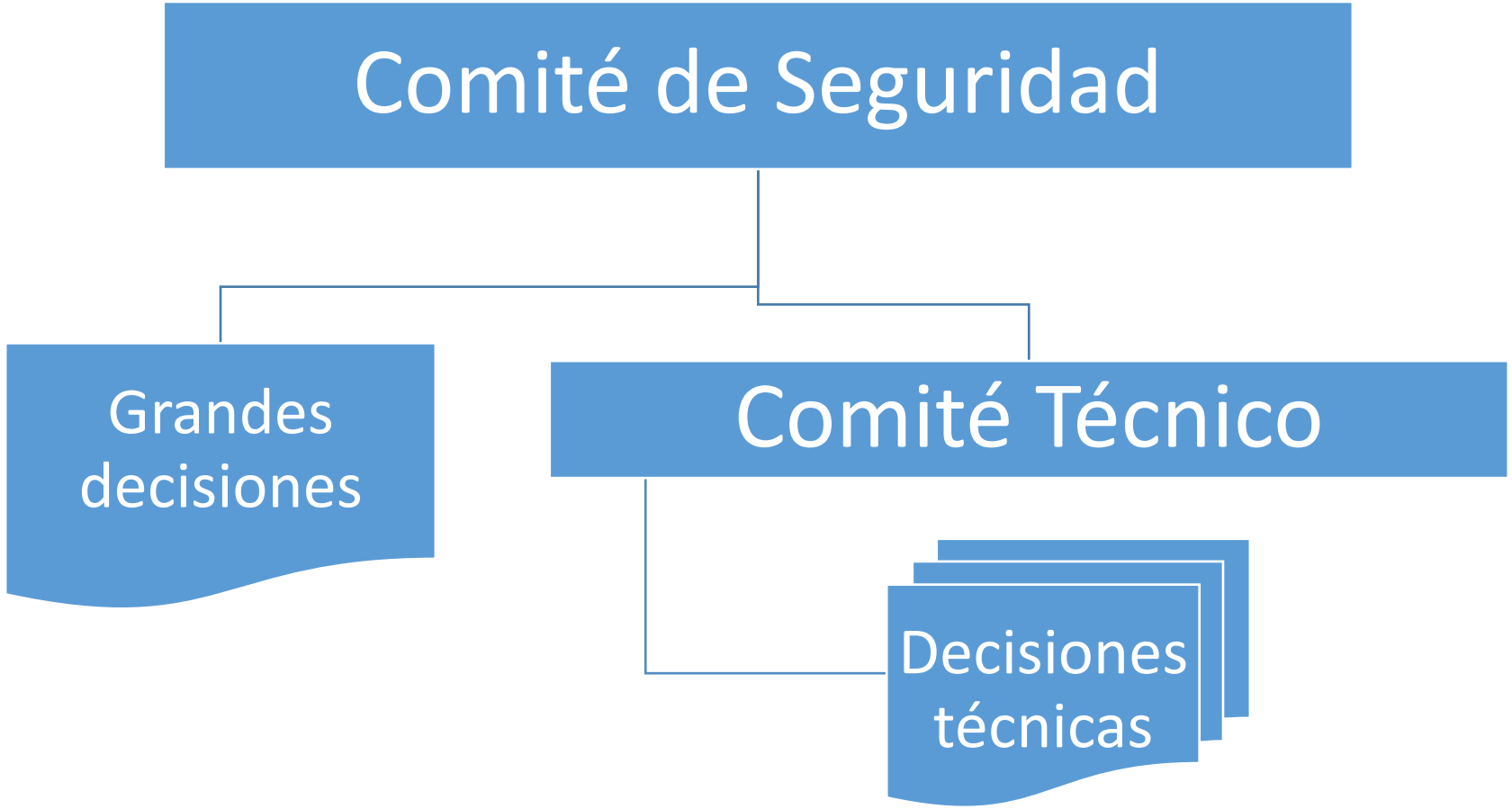
El comité lo componen los miembros de la "Alta dirección" , no podemos reunirlos continuamente.
Normalmente la mayoría de miembros de ese comité no tiene conocimientos ni en materia de seguridad ni técnicos.

ESTO NO ES OPERATIVO

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

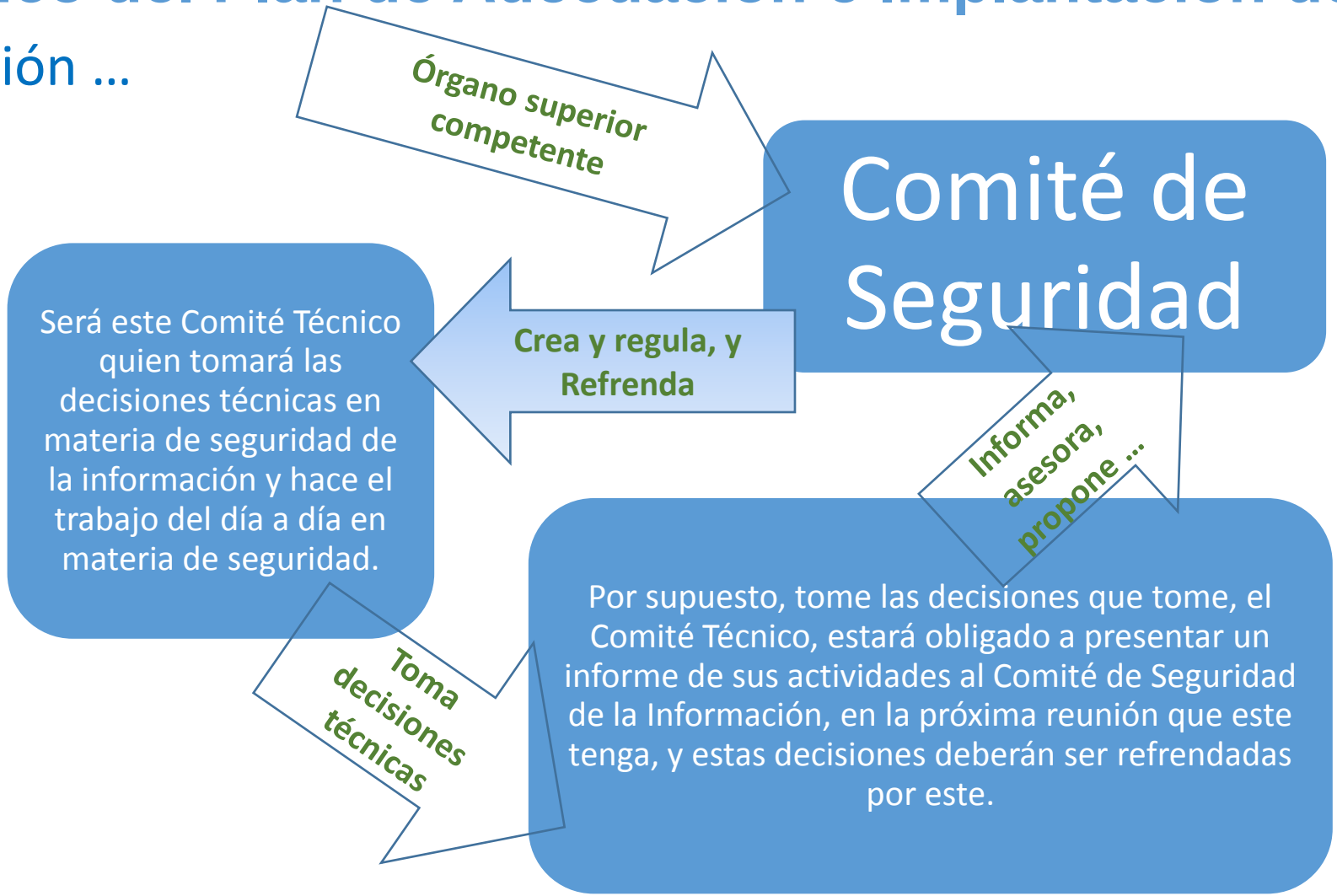
0



Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

0



Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

0

A modo de ejemplo:

Será el **Comité Técnico** quien redacte, consensuado con el departamento de sistemas, la política de copias de seguridad de la organización, será el **Comité Técnico**, quien redacte el procedimiento para llevar a cabo la comprobación de que las copias son correctas y el procedimiento funciona.

El **Comité de Seguridad de la información** (Comité STIC), refrendará, a informe del **Comité Técnico** (Comité TIC), dicha política de copias, y el procedimiento,

Pero será el **Comité Técnico** el encargado de velar por el cumplimiento de esa política o procedimiento de copias y solo informará al Comité de Seguridad de la información **en caso de incumplimiento o de un incidente** derivado de él.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

Con esto ya teníamos el órgano superior competente que aprobara nuestro plan de adecuación al ENS

Y un modelo de plan de adecuación….

- La política de seguridad
- Información que se maneja, con su valoración
- Servicios que se prestan, con su valoración
- Datos de carácter personal
- Categoría del sistema
- Análisis de riesgos
- Declaración de aplicabilidad de las medidas del Anexo II del ENS y las requeridas por el tratamiento de datos de carácter personal, si los hubiera
- Insuficiencias del sistema (gap analysis)
- Plan de mejora seguridad, incluyendo plazos estimados de ejecución

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

Pero…….

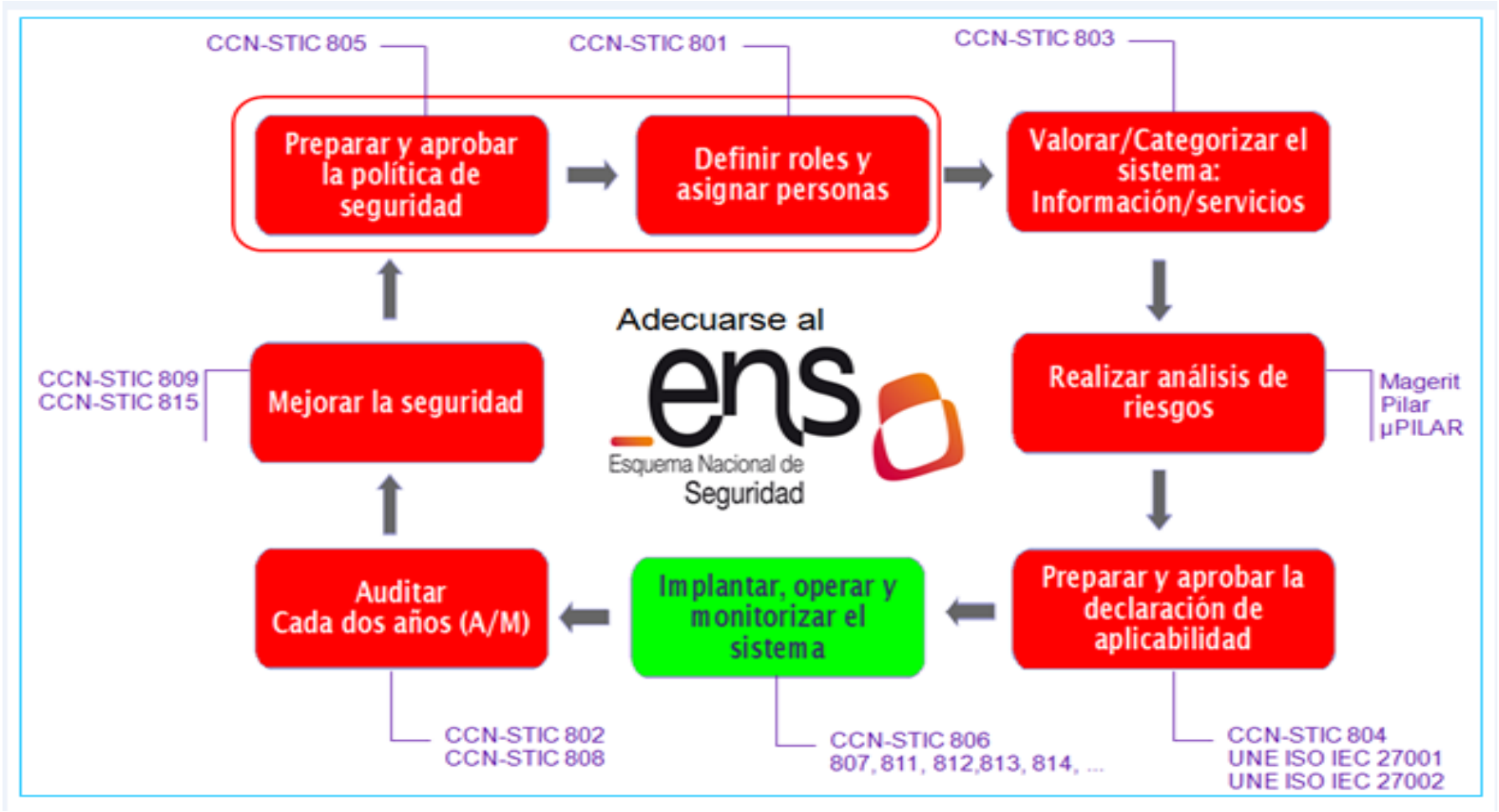
Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

Pero adecuarse al ENS, **no sólo significa establecer en un documento los apartados** que provee la guía 806, supone también que **esos contenidos deben ser concebidos como un proceso integral y de mejora continua.**

Caso Práctico del Plan de Adecuación e Implantación del ENS

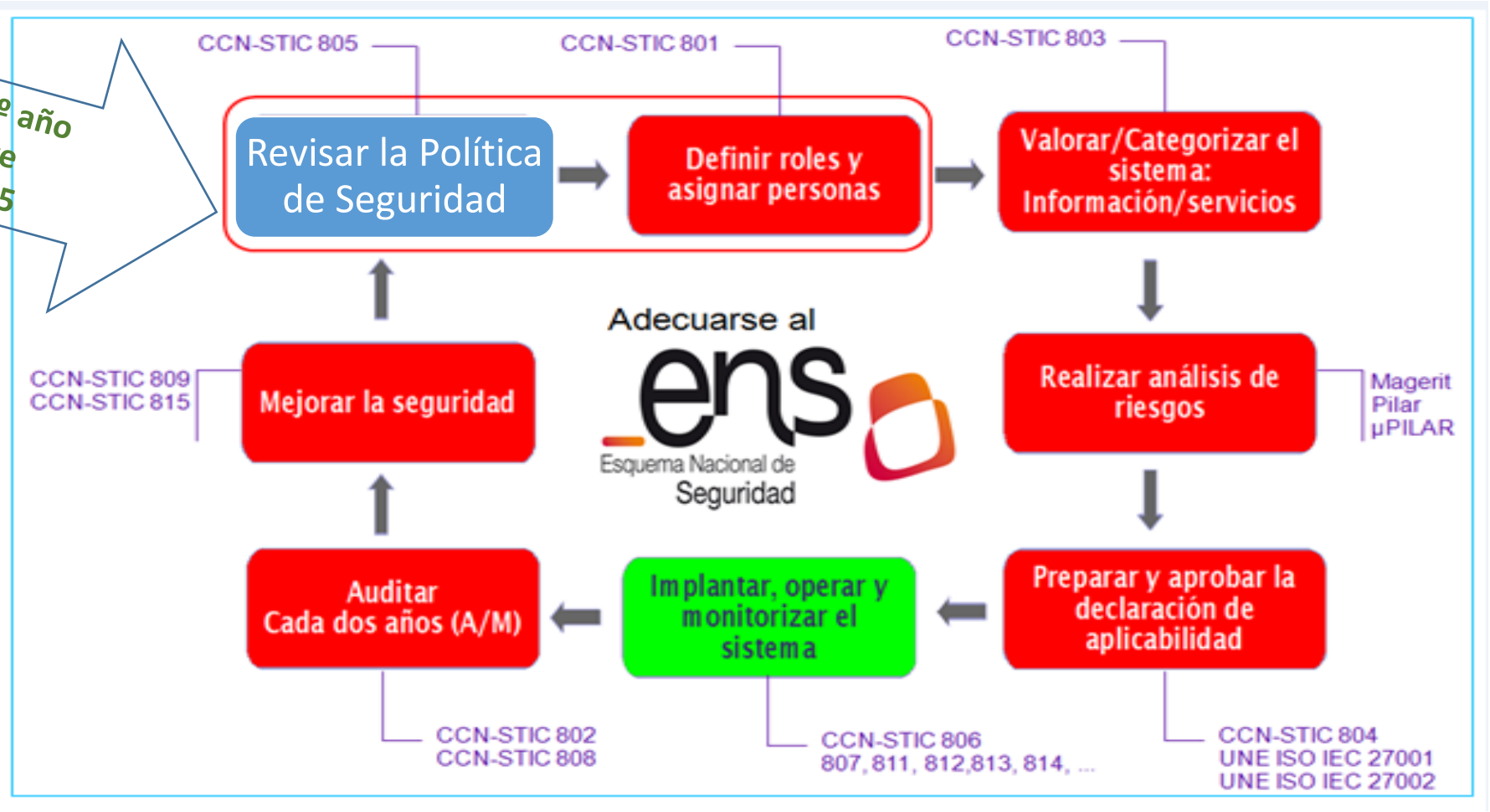
Nuestra Solución …



Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

A partir del 2º año
Se convierte
RD.951/2015



Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestra Solución …

Y así establecimos nuestro plan de adecuación….

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan.

Pasos a seguir en nuestro PDCA para implantación de la seguridad como un proceso integral de mejora continua.	Según la guía CCN-STIC-806, el plan de adecuación del ENS debe contener al menos los siguientes elementos
1. Preparar y aprobar la política de seguridad. 2. Definir Roles y asignar personas. 3. Valorar/Categorizar el sistema: Información / Servicios. 4. Realizar el análisis de riesgos. 5. Preparar y aprobar la declaración de aplicabilidad. **6. Implantar Operar y monitorizar el sistema.** **7. Auditar cada dos años .** 8. Mejora de la seguridad. Y volveríamos a empezar, pero en esta ocasión no sería "Preparar y aprobar la política de Seguridad", sino REVISAR. Esa REVISIÓN, incluiría que anualmente se repetirían los 3 primeros pasos y volveríamos a empezar el ciclo.	1. La política de seguridad 2. Información que se maneja, con su valoración 3. Servicios que se prestan, con su valoración 4. Datos de carácter personal 5. Categoría del sistema 6. Análisis de riesgos 7. Declaración de aplicabilidad de las medidas del Anexo II del ENS y las requeridas por el tratamiento de datos de carácter personal, si los hubiera 8. insuficiencias del sistema (gap analysis) 9. plan de mejora seguridad, incluyendo plazos estimados de ejecución

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan.

6. **Implantar, Operar y monitorizar el sistema.**

7. **Auditar cada dos años .**

8. Mejora de la seguridad.

Y volveríamos a empezar, pero en esta ocasión no sería "Preparar y aprobar la política de Seguridad", sino REVISAR.

Esa REVISIÓN, incluiría **que anualmente** se repetirían los 3 primeros pasos y volveríamos a empezar el ciclo.

Los pasos 6 y 7 son los que realmente establecen el funcionamiento de nuestro Sistema de Gestión de la Seguridad de la Información, y junto al, 8 le dan ese carácter cíclico.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

Nuestro Plan de Adecuación, y las fechas probables de Implantación

Pasos a seguir en nuestro esquema para implantación del ENS	Fecha de Implantación
1.- Preparar y aprobar la política de seguridad.	Se opta por la del MAGRAMA. Debe aprobarlo el Comité
2.- Definir Roles y asignar personas.	Junto a Auditoria LOPD de julio a noviembre 2016
3.- Valorar/Categorizar el sistema: Información / Servicios.	Junto a Auditoria LOPD de julio a noviembre 2016
4.- Realizar el análisis de riesgos.	Enero 2017
5.- Preparar y aprobar la declaración de aplicabilidad.	Enero 2017
6.- Implantar Operar y monitorizar el sistema.	De julio 2016 a Noviembre de 2017
7.- Auditar cada dos años .	
7.a.- LOPD	Noviembre 2016
7.b.- ENS	Noviembre 2017
8.- Mejora de la seguridad.	El ciclo empieza cada año en enero.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan.

1

PREPARAR Y APROBAR LA POLÍTICA DE SEGURIDAD

- **Nos adheriremos a la política de seguridad de Ministerio (MAPAMA)**, hasta que si es necesario, tengamos una propia.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan.

1. Preparar y aprobar la Política de Seguridad.
2. Definir Roles y asignar personas.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan.

1

2

MINISTERIO
DE AGRICULTURA, ALIMENTACIÓN
Y MEDIO AMBIENTE

CONFEDERACIÓN
HIDROGRÁFICA
DEL JÚCAR

La presidenta de la Confederación Hidrográfica del Júcar,

Fundamentándose en el Esquema Nacional de Seguridad (RD 3/2010 de 9 de enero, y posterior modificación de 4 de noviembre de 2015), la política de seguridad que ha establecido el MAGRAMA (Orden AAA/991/2015 de 21 de mayo), y consultadas la pertinentes guías de seguridad que el Centro Criptológico Nacional (CCN) elabora para dar cumplimiento a sus cometidos y a lo reflejado en el Esquema Nacional de Seguridad,

Y consciente de la importancia que tiene **el establecimiento de la organización de la seguridad** y que esta organización de la seguridad sirva de apoyo para que el personal de la Administración encargado a tal efecto lleve a cabo su tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad,

Convoca para el día _____, a las _____ horas, a las siguientes personas, dada la relevancia que los cargos que ocupan tiene para la organización de la seguridad.

-
-
-
-

Informa que el orden del día de dicha reunión será:

1. Acto de presentación del comité.
2. Presentación de los miembros del comité y nombramiento de los mismos.
3. Adhesión a la Política de Seguridad del MAGRAMA.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan.

1

2

Puntos del Orden del día FUNDAMENTALES

MINISTERIO DE AGRICULTURA, ALIMENTACIÓN Y MEDIO AMBIENTE

CONFEDERACIÓN HIDROGRÁFICA DEL JÚCAR

La presidenta de la Confederación Hidrográfica del Júcar,

Fundamentándose en el Esquema Nacional de Seguridad (RD 3/2010 de 9 de enero, y posterior modificación de 4 de noviembre de 2015), la política de seguridad que ha establecido el MAGRAMA (Orden AAA/991/2015 de 21 de mayo), y consultadas la pertinentes guías de seguridad que el Centro Criptológico Nacional (CCN) elabora para dar cumplimiento a sus cometidos y a lo reflejado en el Esquema Nacional de Seguridad,

Y consciente de la importancia que tiene **el establecimiento de la organización de la seguridad** y que esta organización de la seguridad sirva de apoyo para que el personal de la Administración encargado a tal efecto lleve a cabo su tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad,

2. Presentación de los miembros del comité y nombramiento de los mismos.

3. Adhesión a la Política de Seguridad del MAGRAMA.

Informa que el orden del día de dicha reunión será:

1. Acto de presentación del comité.
2. Presentación de los miembros del comité y nombramiento de los mismos.
3. Adhesión a la Política de Seguridad del MAGRAMA.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan.

1

2

Definir Roles y asignar personas.

Nombramientos de los miembros del comité de Seguridad

Incluyen:

- Nombres
- Cargos en la Organización
- Cargo en el Comité
- Información sobre el Comité

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan.

1

2

MINISTERIO
DE AGRICULTURA, ALIMENTACIÓN
Y MEDIO AMBIENTE

CONFEDERACIÓN
HIDROGRÁFICA
DEL JÚCAR

El Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y adaptándonos a la política de seguridad del MAGRAMA, (Orden AAA/991/2015 de 21 de mayo), y consultadas la pertinentes guías de seguridad que el Centro Criptológico Nacional (CCN) elabora para dar cumplimiento a sus cometidos y a lo reflejado en el Esquema Nacional de Seguridad:

Mediante el presente escrito se nombra a

_____(persona)_____,
_____(cargo)_____,

Miembro del Comité de Seguridad de la Información de la Confederación Hidrográfica del Júcar, en calidad de

_____(función en el comité)_____, en dicho comité.

La principal función de este comité será la de Gestionar la seguridad de la información ya que:

- Es conveniente coordinarla para racionalizar el gasto.
- Es necesario coordinarla para evitar disfunciones que permitan fallas de seguridad al ofrecer el Sistema puntos débiles donde pudieran ocurrir accidentes o se pudieran perpetrar ataques.

En Valencia, a _____

La Presidenta de la Confederación Hidrográfica del Júcar

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan.

1

2

Preparar y aprobar la Política de Seguridad.

BOLETÍN OFICIAL DEL ESTADO
Núm. 128 Viernes 29 de mayo de 2015 Sec. III. Pág

III. OTRAS DISPOSICIONES

MINISTERIO DE AGRICULTURA, ALIMENTACIÓN Y MEDIO AMBIENTE

5937 *Orden AAA/991/2015, de 21 de mayo, por la que se aprueba la política de seguridad de la información en el ámbito de la Administración Electrónica del Ministerio de Agricultura, Alimentación y Medio Ambiente.*

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, establece la relación entre la Administración Pública y los ciudadanos a través de la Administración Electrónica, compuesta principalmente tanto por los sistemas de tecnologías de la información y comunicaciones como por el tratamiento y almacenamiento automatizado de la información que reside en los mismos, y determina, de acuerdo con su artículo 42, la aprobación del Esquema Nacional de Seguridad (ENS).

En efecto, esta consagración del derecho a comunicarse a través de medios electrónicos comporta la correlativa obligación de las Administraciones de atender a cuantas necesidades se adviertan para garantizar una aplicación segura de estas tecnologías sobre la base de los mandatos constitucionales de promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas y de remoción de los obstáculos que impidan o dificulten su plenitud.

En su desarrollo, se aprobaría el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, que tiene por objeto el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan.

1

2

Preparar y aprobar la Política de Seguridad.

Artículo 1. *Objeto y ámbito de aplicación.*

1. Constituye el objeto de la presente orden la aprobación de la Política de Seguridad de la Información (PSI) en el ámbito de la Administración Electrónica del Ministerio de Agricultura, Alimentación y Medio Ambiente.

2. La PSI será de obligado cumplimiento para todos los órganos superiores y directivos del Ministerio de Agricultura, Alimentación y Medio Ambiente, incluidos los organismos públicos vinculados o dependientes del Departamento, que no tengan establecida su propia política de seguridad. En aquellos organismos que tengan su propia política de seguridad, prevalecerá en caso de discrepancia la definida en esta orden ministerial.

3. La PSI será de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la propia información que sea gestionada por el Departamento, con independencia de cuál sea su destino, adscripción o relación con el mismo.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan.

1

2

Preparar y aprobar la Política de Seguridad.

Artículo 2. *Principios de la seguridad de la información.*

1. Principios básicos.

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Además de los previstos en el artículo 4 Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, se establecen los siguientes:

a) Alcance estratégico: la seguridad de la información cuenta con el compromiso y apoyo de todos los niveles directivos de forma que está coordinada e integrada con el resto de iniciativas estratégicas del Departamento para conformar un todo coherente y eficaz.

b) Proporcionalidad: el establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

c) Mejora continua: las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

d) Seguridad por defecto: los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

3

¿Cómo?

VALORAR Y CATEGORIZAR EL SISTEMA DE INFORMACIÓN Y LOS SERVICIOS

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

3

VALORAR Y CATEGORIZAR EL SISTEMA DE INFORMACIÓN Y LOS SERVICIOS

- Este es el apartado que compete a ese Comité Técnico (que opera de forma independiente bajo la tutela del comité de seguridad)
- En esta fase serán de vital importancia los resultados que se obtengan de la auditoria de la LOPD.

Caso Práctico del Plan de Adecuación e Implantación del ENS

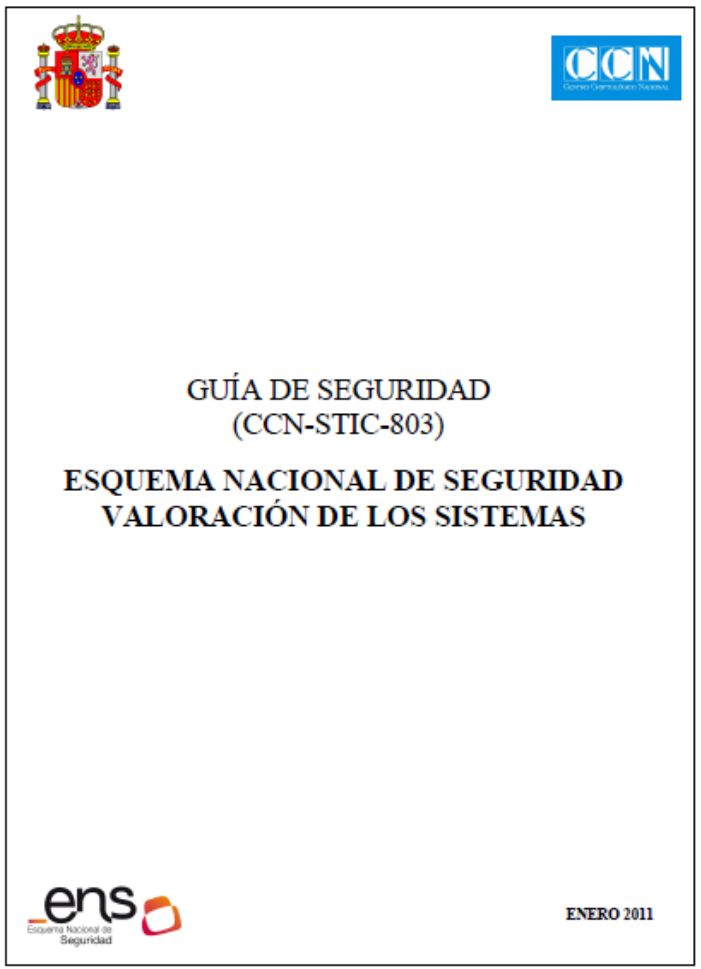
Nuestro Plan

3

Anexo I. RD 3/2010

Fundamentos para la determinación de la categoría de un sistema.
La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:

Alcanzar sus objetivos.
b) Proteger los activos a su cargo.
c) Cumplir sus obligaciones diarias de servicio.
d) Respetar la legalidad vigente.
e) Respetar los derechos de las personas.



Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

3

Creamos nuestra propia guía, basándonos en los tres documentos anteriores un documento que resume todo y nos permitía hacer una categorización FÁCIL del sistema.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

3

Creamos nuestra propia guía,

Ejemplos:

CONFIDENCIALIDAD:
Qué se conocieran los datos de una determinada información, produciría un daño:

- Irreparable? → Alto
- Reparable? → Medio
- Fácilmente reparable? → Bajo

DISPONIBILIDAD:
Si por un incidente se para un determinado Servicio, este debería Volver a funcionar:

- En menos de 4 horas. → Alto
- En un periodo de entre 4 horas y un día. → Medio
- Puede estar parado Más de 1día. → Bajo

Y así iríamos llenando la anterior tabla, al final tenemos categorizado el sistema.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

4

REALIZAR EL ANÁLISIS DE RIESGOS

- Compete también al Comité Técnico, y más concretamente al responsable de seguridad.
- Su cometido no sólo consiste en realizarlo (siguiendo las directivas que establece PILAR para el ENS), sino además mantenerlo actualizado constantemente, para que en todo momento ese análisis de riesgos sea lo más real posible, y de verdad sea útil.
- Y Presentar los resultados al comité de Seguridad.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

4

REALIZAR EL ANÁLISIS DE RIESGOS

- Realizamos un primer análisis con **Micropilar.**
- Método del “Activo Gordo”. (La idea nos la dio el Profesor Mañas).
- Así obtuvimos datos de un primer análisis que presentamos en la 1ª Reunión del comité.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

5

PREPARAR Y APROBAR LA DECLARACIÓN DE APLICABILIDAD

- Es un documento en el que se establecen los controles del ENS que aplican a este organismo, donde además se refleja el nivel de implantación y los plazos para que esta implantación se lleve a cabo.
- Se debe justificar porque aplica un control o por qué NO

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

6

IMPLANTAR, OPERAR Y MONITORIZAR EL SISTEMA

- En este apartado es donde definimos los diferentes procedimientos cuya suma final será la implantación del ENS, hemos optado por hacer uno para cada apartado del ENS
- Estos procedimientos llevan a que nos aparezcan tareas de dos tipos:
  - Periódicas (revisión semestral de los log de conexión)
  - Bajo demanda (dar de alta un usuario)
- Son los que llevan a que existan las ITT (Instrucciones técnicas de trabajo, para realizar determinadas tareas (instrucciones para dar acceso a una VPN)
- Y en los que se hace referencia a manuales de operación (apagado del CPD, inclusión de un PC en dominio)
- Llevan aparejado un documento de Planificación de tareas, en donde dejamos reflejo de las tareas tanto periódicas como bajo demanda y donde haces referencia a como y donde has guardado las evidencias de que lo que has establecido en los procedimientos se ha llevado a cabo.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

6

IMPLANTAR, OPERAR Y MONITORIZAR EL SISTEMA

- Pusimos en marcha la 1ª sonda.
- Creamos un servidor con Clara y auditamos nuestros sistemas para saber que teníamos que mejorar.
- Empezamos a categorizar las incidencias. (Gestión de la vulnerabilidad, Continuidad del negocio…)
- Hicimos una prueba (Básica) de continuidad del negocio (simplemente apagar y re-arrancar el CPD, y establecimos el procedimiento).
- Creamos nuestro servidor CLOUD, para poder quitar Dropbox, Drive, ONE, y en ello estamos.
- Empezamos a usar Lucia para la gestión de Incidentes.
- Elaboramos la Normativa de buenas prácticas.
- Pusimos en marcha la 2ª sonda para el SAIH.
- Empezamos a consultar Reyes para la investigación de incidentes.
- EN PARALELO HEMOS IDO REDACTANDO LOS PROCEDIMIENTOS, Y LAS ITT.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

6

Lo que obtenemos con LUCIA…

[OP.EXP.7]. Gestión de incidencias.

[OP.EXP.9]. Registro de la Gestión de Incidencias.

[OP.EXP.10] Protección de los Registros.

Compartimos información sobre los incidentes de nuestra organización y obtenemos información de otros incidentes que te ayudan.

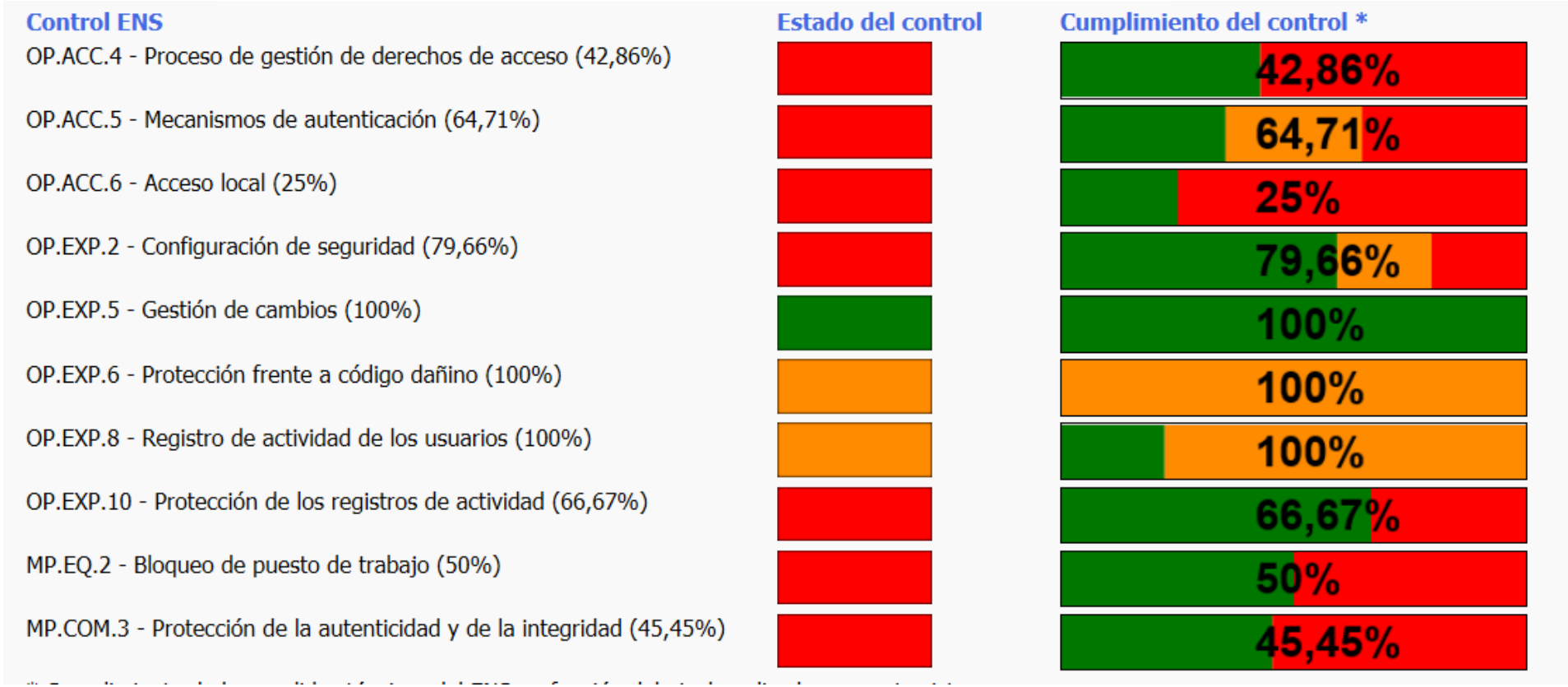
Y la información sobre incidentes que hay que poner en INES, se puede volcar Automáticamente.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

6

Lo que obtenemos con CLARA…



Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

6

Lo que obtenemos con CLARA…

OP.ACC.5 - Mecanismos de autenticación (64,71%)

Nombre	Valor actual	Valor esperado	Resultado
Vigencia máxima de la contraseña	180	90	Incorrecto
Vigencia mínima de la contraseña	1	2	Incorrecto
Exigir historial de contraseñas	3	24	Incorrecto
Longitud mínima de la contraseña	8	8	Correcto
La contraseña debe cumplir los requisitos de complejidad	Verdadero	Verdadero	Correcto
Almacenar contraseñas con cifrado reversible	0	0	Correcto
Cuentas: estado de la cuenta de invitado	0	0	Correcto
Vigencia máxima del vale de usuario	No configurado	8	No aplica, el sistema no es DC
Vigencia máxima de renovación de vales de usuario	No configurado	4	No aplica, el sistema no es DC
Vigencia máxima del vale de servicio	No configurado	480	No aplica, el sistema no es DC
Tolerancia máxima para la sincronización de los relojes de los equipos	No configurado	10	No aplica, el sistema no es DC

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

7

AUDITAR CADA 2 AÑOS

- ENS
- LOPD

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

8

MEJORA DE LA SEGURIDAD

- De los resultados de esas auditorias y del resultado del análisis de riesgos es de donde saldría el documento fundamental que daría anualmente continuidad a esa Gestión de la seguridad
  - El PTR o Plan de tratamiento de riesgos
- Y volveríamos a empezar, pero en esta ocasión no sería “Preparar y aprobar la política de Seguridad”, sino REVISAR dicha política y esto convertiría el PTR, en **el Plan de Acciones Correctoras**, que es el documento que base para volver a empezar el ciclo.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

Nuestro Plan de Adecuación.

A día de hoy

Pasos a seguir en nuestro esquema para implantación del ENS	Fecha de Implantación
1.- Preparar y aprobar la política de seguridad.	Se opta por la del MAGRAMA. Debe aprobarlo el Comité
2.- Definir Roles y asignar personas.	Junto a Auditoria LOPD de julio a noviembre 2016
3.- Valorar/Categorizar el sistema: Información / Servicios.	Junto a Auditoria LOPD de julio a noviembre 2016
4.- Realizar el análisis de riesgos.	Enero 2017
5.- Preparar y aprobar la declaración de aplicabilidad.	Enero 2017
6.- Implantar Operar y monitorizar el sistema.	De julio 2016 a Noviembre de 2017
7.- Auditar cada dos años .	
7.a.- LOPD	Noviembre 2016
7.b.- ENS	Noviembre 2017
8.- Mejora de la seguridad.	El ciclo empieza cada año en enero.

Caso Práctico del Plan de Adecuación e Implantación del ENS

Nuestro Plan

Nuestro Plan de Adecuación.

A día de hoy

Pasos a seguir en nuestro esquema para implantación del ENS	Fecha de Implantación
1.- Preparar y aprobar la política de seguridad. HECHO	Se opta por la del MAGRAMA. Debe aprobarlo el Comité
2.- Definir Roles y asignar personas. HECHO	Junto a Auditoria LOPD de julio a noviembre 2016
3.- Valorar/Categorizar el sistema: Información / Servicios. En proceso (80%)	Auditoria LOPD de julio a noviembre 2016
4.- Realizar el análisis de riesgos. HECHO un primer análisis inicial	Enero 2017
5.- Preparar y aprobar la declaración de aplicabilidad. En Proceso (20%)	Enero 2017
6.- Implantar Operar y monitorizar el sistema. En proceso (40%)	2016 a Noviembre de 2017
7.- Auditar cada dos años .	
7.a.- LOPD En Proceso (90%)	Noviembre 2016
7.b.- ENS	Noviembre 2017 En Fecha
8.- Mejora de la seguridad.	El ciclo empieza cada año en enero. Primera revisión Enero 2018. En Fecha

Caso Práctico del Plan de Adecuación e Implantación del ENS

En Resumen

Adecuar nuestra organización al ENS, NO ES FACIL, pero NO ES IMPOSIBLE.

NO ESTAMOS SOLOS. Cuenta Conmigo, y con el CCN.

CUMPLIR **solamente** CON LA LEGALIDAD, NO TE PROTEGE.

Una vez implantado el ENS, con su ciclo de mejora continua, hay que seguir aplicándolo y trabajando en él.

Muchas Gracias por su atención.

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

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

Síguenos en