Marco de Certificación Específico

Caso de estudio

centro criptológico nacional

Implementación de seguridad y buenas prácticas

El SEPE sufre un ataque informático que paraliza su actividad ...

13 mar 2021 — El Servicio Público de Empleo Estatal (**SEPE**, antiguo **INEM**) confirmó el pasado martes 9 de marzo que sus sistemas habían sufrido un **ataque** ...

Ransomware llega a varios ayuntamientos españoles

... se como el principio de una oleada de **ataques** ... habían sido afectadas. ... El 4 de octubre, el ...ido atacado ...

Una veintena de ayuntamientos, atacados por ciberdelincuentes

• Los hackers bloquean todo el sist...

Otros objetivos

Hospitales y universidades también han sido blanco de ataques

El Ayuntamiento de Algeciras bloquea miles de ciberataques ...

5 dic 2020 — El **Ayuntamiento** de Algeciras está siendo víctima desde hace meses de miles de ... de datos de la ciudad y sus vecinos que gestiona la **entidad local**. ... los **ataques** ("miles, remarca") han sido en su mayoría por fuerza bruta, ...

https://www.businessinsider.es › ciberataque-castellon-fi...

El ciberataque a Castellón filtra 119 GB en datos del ...

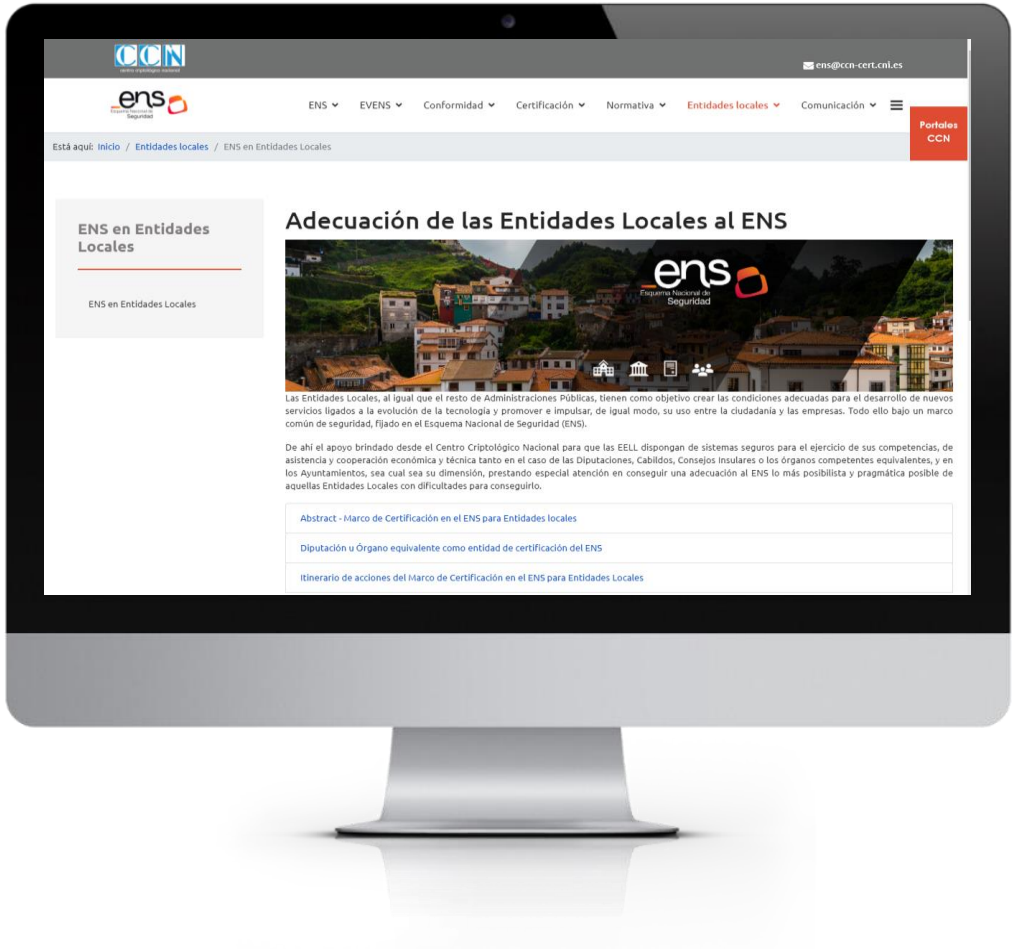
12 abr 2021 — Los atacantes del **Ayuntamiento** de Castellón reivindican la filtración de 119 gigas ... Con el **ataque** se habrían filtrado documentación de la policía **local** de ... para garantizar la continuidad de negocios y **entidades** públicas.

La **CIBERSEGURIDAD** es clave en el reto de la **TRANSFORMACIÓN DIGITAL** de los organismos

Marco de Certificación Específico con el ENS (MCE-ENS)

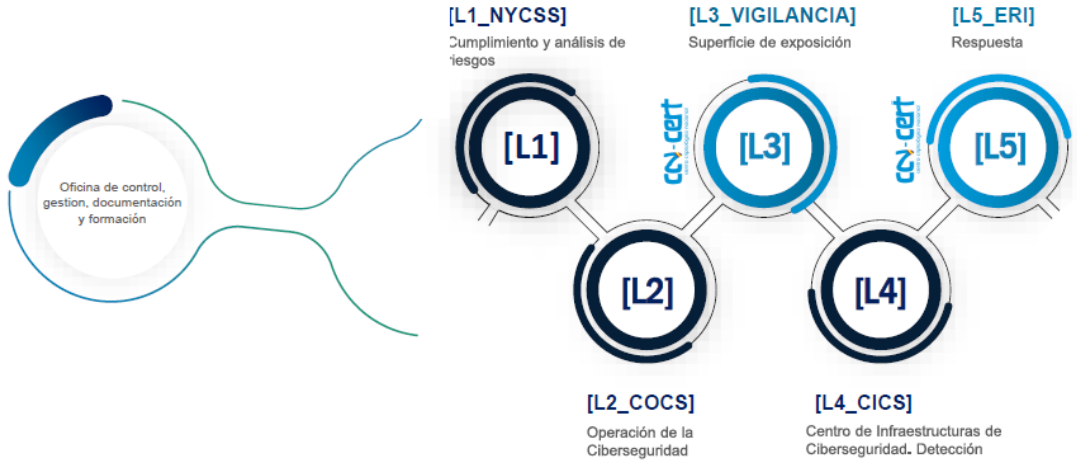
- EELL pequeñas y limitados recursos
- Obligaciones de difícil cumplimiento de manera individualizada

- Adecuación e implantación multi-organismo (grupos homogéneos)
- Procedimiento de auditoría y certificación para optimizar recursos



Centro de Operaciones de Ciberseguridad

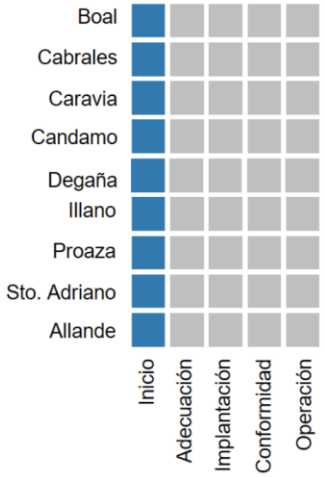
- Mejorar las capacidades de despliegue, actuación y protección de las entidades
  - Cumplimiento y análisis de riesgos
  - Operación de ciberseguridad
  - Superficie de exposición
  - Centro de infraestructuras de Ciberseguridad
  - Respuesta



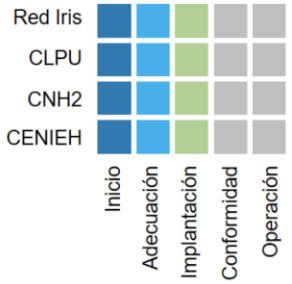
Iniciativas

Tras el diseño e implantación del ENS para EELL, han surgido iniciativas para su aplicación directa en diferentes proyectos pilotos, como organismos superiores de los que dependen los diferentes órganos.

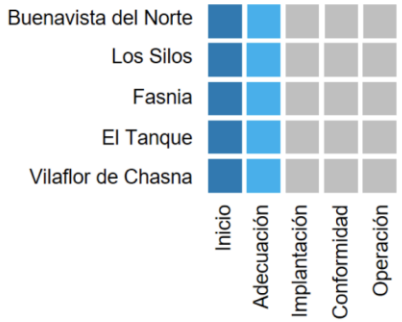
CAST (EE.LL. Asturias)
Total entidades: 78 | Muestra: 9 EE.LL.



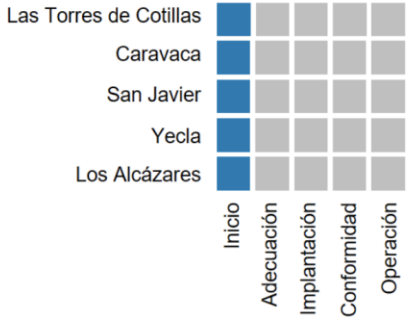
Infraestructuras y Técnicas Singulares (ICTS)
Total entidades: 65



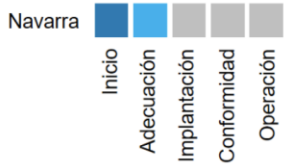
Cabildo de Tenerife
Total entidades: 31

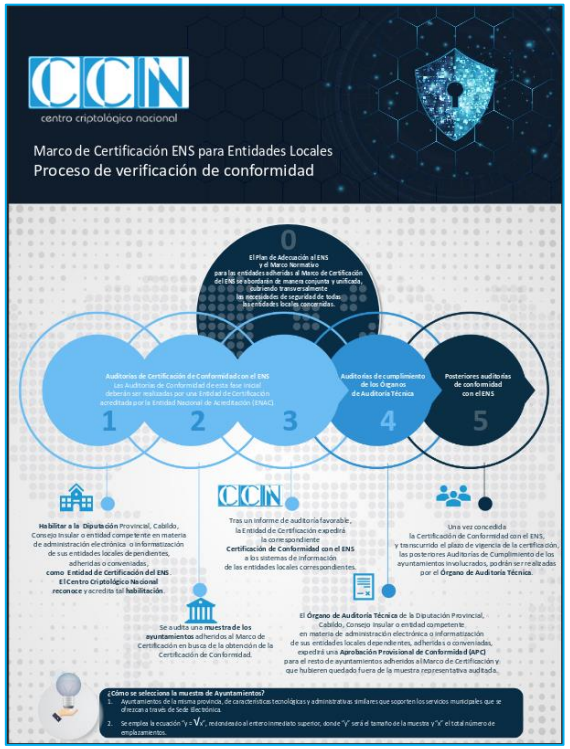


CARM (EE.LL. Murcia)
Total entidades: 27



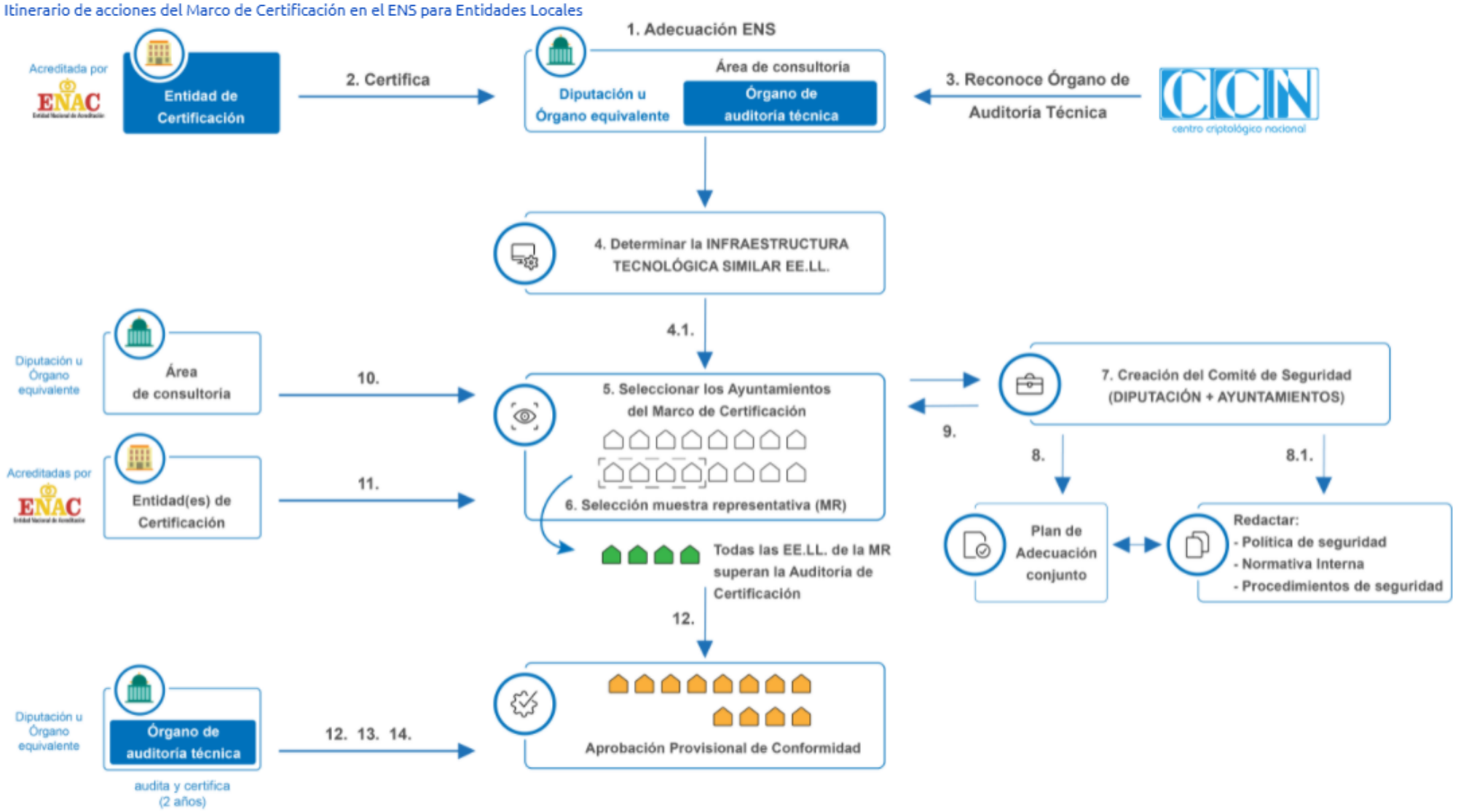
ANIMSA (EE.LL. Navarra)
Total entidades: 57
Muestra: 7 EE.LL.





Consorcio Asturiano de Servicios Tecnológicos
PRINCIPADO DE ASTURIAS
Infraestructuras Científicas y Técnicas Singulares
MINISTERIO DE DEFENSA
ISFAS
INSTITUTO SOCIAL DE LAS FUERZAS ARMADAS
GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
Metro
animsa
AJUNTAMENT XABIA
CABILDO DE TENERIFE
CCN
centro criptológico nacional

Prevención Proactiva: cumplimiento y vigilancia



Prevención Proactiva: cumplimiento y vigilancia

1. Adecuación al ENS – Diputación u Órgano equivalente

2. Certificación del ENS – Diputación u Órgano equivalente

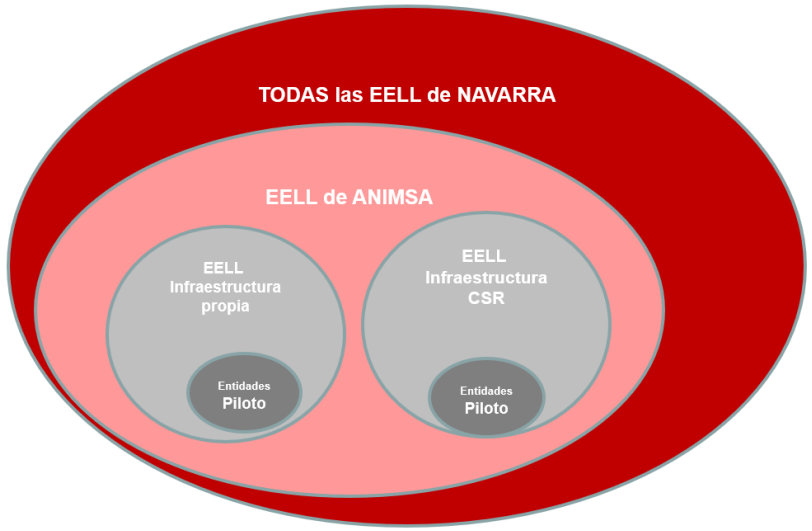
animsa **OK**

3. Reconocimiento del Órgano de Auditoría Técnica

animsa **EN CURSO**

4. Infraestructura Tecnológica EE.LL.

5. Selección de las EE.LL. del MCE-ENS



6 Selección muestra representativa (MR)

- Grupo 1: centros de servicios remoto (CSR) - 6
  - AYUNTAMIENTO DE DICASTILLO
  - (AGRUPACIÓN DE SERVICIOS ADMINISTRATIVOS VALDEMAÑERU): AYUNTAMIENTO DE ARTAZU, AYUNTAMIENTO DE CIRAUQUI, AYUNTAMIENTO DE GUIRGUILLANO, AYUNTAMIENTO DE MAÑERU
  - AYUNTAMIENTO DEL VALLE DE YERRI
- Grupo 2: infraestructuras propias en local - 9
  - AYUNTAMIENTO DE ANSOÁIN
  - AYUNTAMIENTO DE ARANGUREN
  - AYUNTAMIENTO DE BARAÑAIN
  - AYUNTAMIENTO DE BERIÁIN
  - AYUNTAMIENTO DE BURLADA
  - AYUNTAMIENTO DEL VALLE DE EGÜÉS
  - AYUNTAMIENTO DE LA CENDEA DE GALAR
  - AYUNTAMIENTO DE LOS ARCOS
  - AYUNTAMIENTO DE VILLAVA

7 Creación COMSEG

Jueves 13 de Mayo

Prevención Proactiva: cumplimiento y vigilancia

1. Adecuación al ENS – Diputación u Órgano equivalente
2. Certificación del ENS – Diputación u Órgano equivalente

Región de Murcia **OK**

3. Reconocimiento del Órgano de Auditoría Técnica

Región de Murcia **EN CURSO**

4. Infraestructura Tecnológica EE.LL.
5. Selección de las EE.LL. del MCE-ENS
6. Selección muestra representativa (MR)

- LOS ALCÁCERES
- YECLA
- SAN JAVIER
- CARAVACA

CCN centro criptológico nacional

Prevención Proactiva: cumplimiento y vigilancia

8 Plan de Adecuación Conjunto

Guía CCN-STIC 806
Contenido del Plan de Adecuación

1 Alcance del Sistema

Guía CCN-STIC 803
Valoración de Sistemas

1.1 Información que se maneja, y su valoración

1.2 Servicios que se prestan, y su valoración

2 Categoría del Sistema

CCN-CERT BP/14
Declaración de Aplicabilidad en el ENS

3 Declaración de Aplicabilidad Provisional

Guía CCN-STIC 470
MAGERIT v.3

4 Análisis de Riesgos

CCN-CERT BP/14
Declaración de Aplicabilidad en el ENS

5.1 Declaración de Aplicabilidad

5.2 Perfil de Cumplimiento

Guía CCN-STIC 805
Modelo de Política de Seguridad

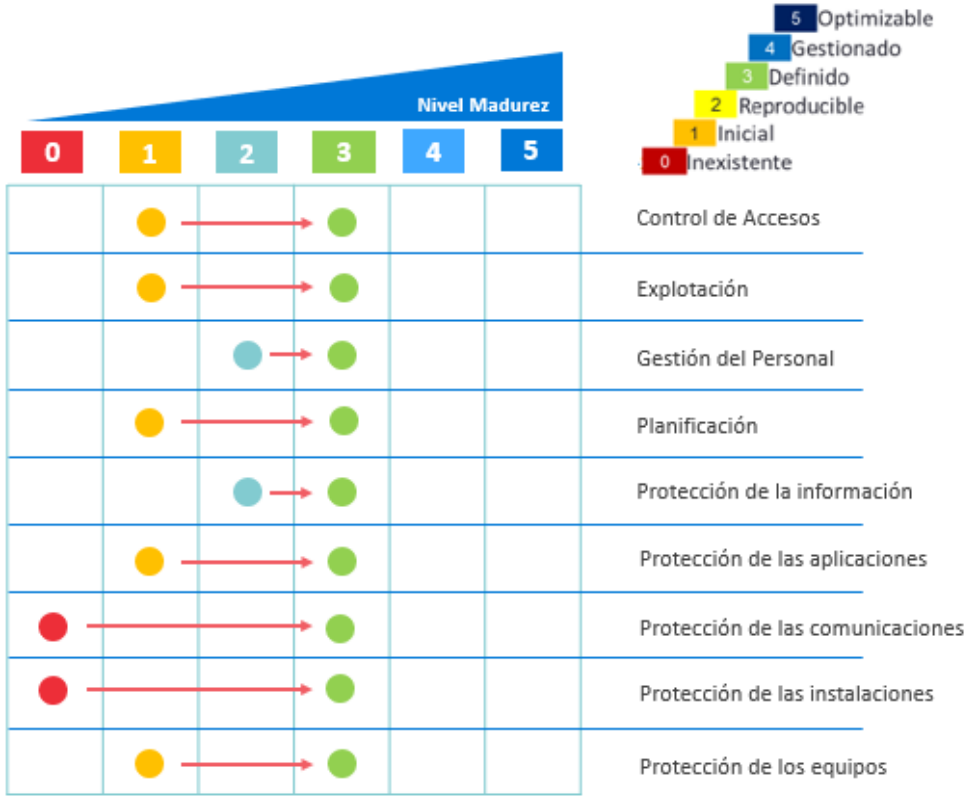
Guía CCN-STIC 801
Responsabilidades en el ENS

6 Política de Seguridad

centro criptológico nacional

Plan de adecuación

- Entrega de valor desde el principio
- Hoja de ruta a seguir



Cumplimentar **INFORME INES**

</inés> ccn-cert

CCN centro criptológico nacional

Elementos entregables – Plan de Adecuación

Identificación de Alcance

1. Catálogo de Servicios Identificados y valoración (Documento)
2. Fichas de Servicios (Varios Documentos)

Categorización

3. Procedimiento de Categorización del Sistema (Documento)

Análisis de Riesgos

4. Fichero de Análisis de Riesgos (Fichero .mgr)
5. Informe Ejecutivo de Análisis de Riesgos (Documento)

6. Declaración de Aplicabilidad (Documento)

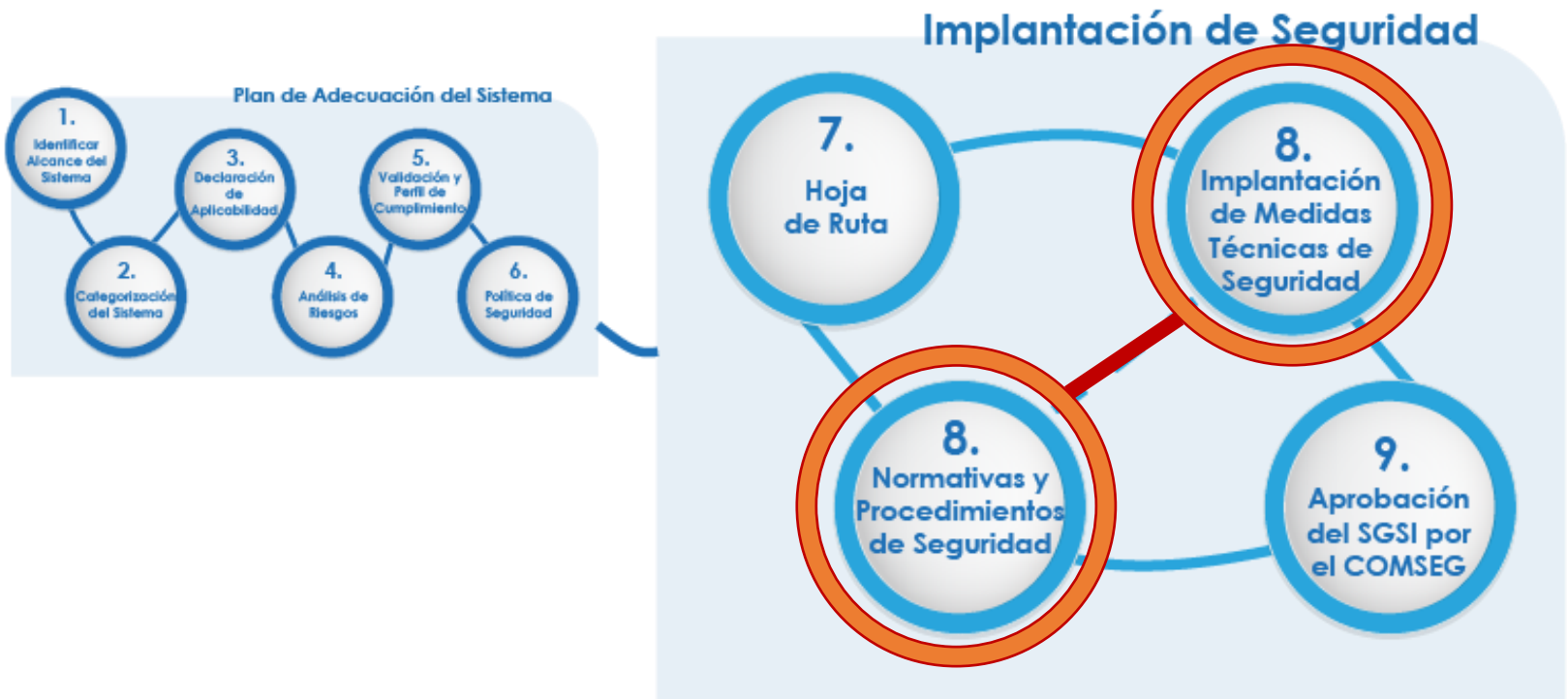
7. Política de Seguridad (Documento)

Previsión de ejecución del Plan de Adecuación – 8-10 semanas

Documentos y Fases – Plan de Adecuación	Semana 1-2	Semana 3-4	Semana 5-6	Semana 7-8	Ejecución
1. Identificación de Alcance (Fichas de Servicio)	Borrador	Borrador	Final		Organismo – Asesoría CCN
Identificar Servicios (Sede Electrónica)	Borrador	Final	Final		Organismo – Asesoría CCN
Identificar Infraestructura tecnológica (servidores propios?, Gestiona?)	Borrador	Final	Final		Organismo – Asesoría CCN
Valorar servicios	Borrador	Final	Final		Organismo – Asesoría CCN
2. Categorización del Sistema (cat. BASICA)		Borrador	Final		CCN – Aprobación Organismo
3. Declaración Aplicabilidad (BORRADOR)		Borrador	Final		CCN – Aprobación Organismo
4. Análisis de Riesgos (PILAR)		Borrador	Final	Final	CCN – Aprobación Organismo
5. Declaración de Aplicabilidad (FINAL)		Borrador	Borrador	Final	CCN – Aprobación Organismo
Perfil de Cumplimiento (Sí aplica)		Borrador	Final	Final	CCN – Aprobación Organismo
Medidas adicionales (ej. Monitorización)		Borrador	Borrador	Final	CCN – Aprobación Organismo
6. Política de Seguridad	Borrador	Borrador	Borrador	Final	-
Definir Estructura de Gobernanza (COMSEG)	Borrador	Borrador	Final	Final	Propuesta Organismo - CCN
Redactar Política de Seguridad			Borrador	Final	CCN – Aprobación Organismo
Aprobación de Política de Seguridad y celebración de COMSEG			Planificación	Aprobación	Organismo

Prevención Proactiva: cumplimiento y vigilancia

9 Adecuación al ENS de la MR



4 Marco organizativo

- Política de seguridad
- Normativa de seguridad
- Procedimientos de seguridad
- Proceso de autorización

31 Marco operacional

- Planificación
- Control de acceso
- Explotación
- Servicios externos
- Continuidad del servicio
- Monitorización del sistema

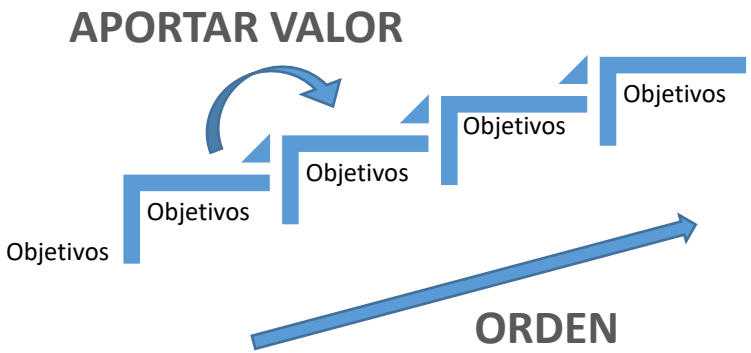
40 Medidas de protección

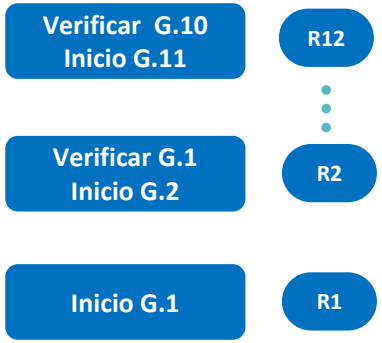
- Instalaciones e infraestructuras
- Gestión del personal
- Protección de los equipos
- Protección de las comunicaciones
- Protección soportes de informanción
- Protección aplicaciones informáticas
- Protección de la información
- Protección de los servicios

CCN centro criptológico nacional

Implantación de Seguridad

- Entrega de valor en cada grupo
- Desarrollo iterativo e incremental
- Formación progresiva
- Priorización de actuaciones





Apoyo en herramientas **LORETO** y **AMPARO**

Seguimiento de la implantación

PACM

GRUPO	TEMÁTICA	TIPO TAREA	DESCRIPCIÓN	FECHA INICIO	FECHA VENCIMIENTO	PRIORIDAD	ESTADO NORMATIVA	VERSION NORMATIVA	ESTADO TAREA	OBSERVACIONES/DIARIO	MEDIDA ENS	CATEGORÍA
5	Inicio grupo 5	REUNIÓN	Reunión inicio Grupo de prioridad	24/03/2021	24/03/2021	ALTA			Completada			
5	Gestión de Ciberincidentes	NORMATIVA	Procedimiento de gestión de incidentes de seguridad	24/03/2021	07/04/2021	ALTA	Elaboración		En curso		OP.EXP.7, OP.EXP.9	Medida nueva (OP.EXP.7, OP.EXP.9)
5	Gestión de Ciberincidentes	ACTUACIÓN	Evidencia de registro de incidentes	24/03/2021	07/04/2021	MEDIA			No iniciada		OP.EXP.9	Medida nueva (OP.EXP.9)

Ejemplo de tareas para gestión de Ciberincidentes

TIPO_TAREA
- REUNIÓN
- ACTUACIÓN
- NORMATIVA

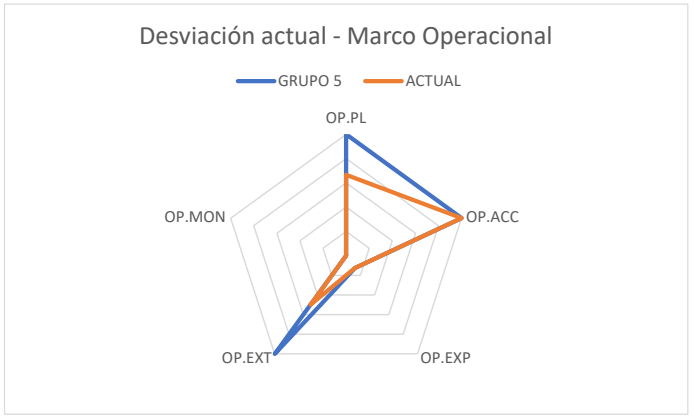
PRIORIDAD
- ALTA
- MEDIA
- BAJA

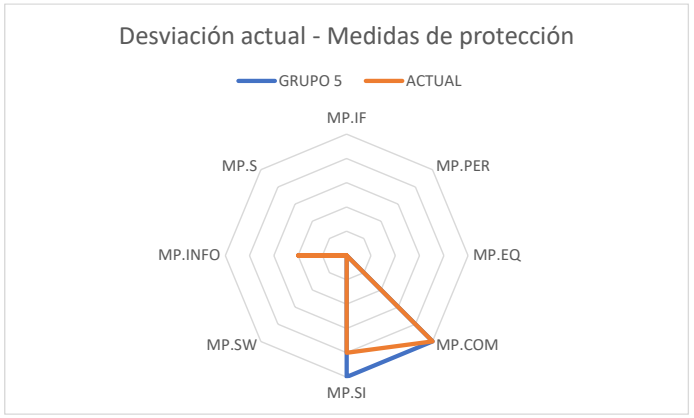
ESTADO_TAREA
- NO INICIADA
- EN CURSO
- COMPLETADA
- APLAZADA
- ANULADA

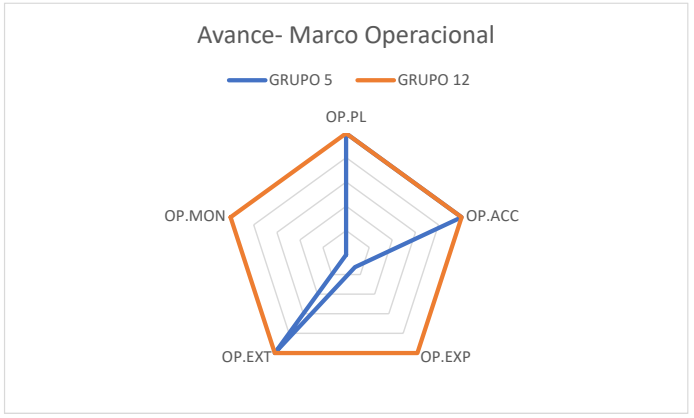
ESTADO_NORMATIVA
- APROBADO
- ELABORACIÓN
- REVISIÓN
- REVISIÓN CLIENTE

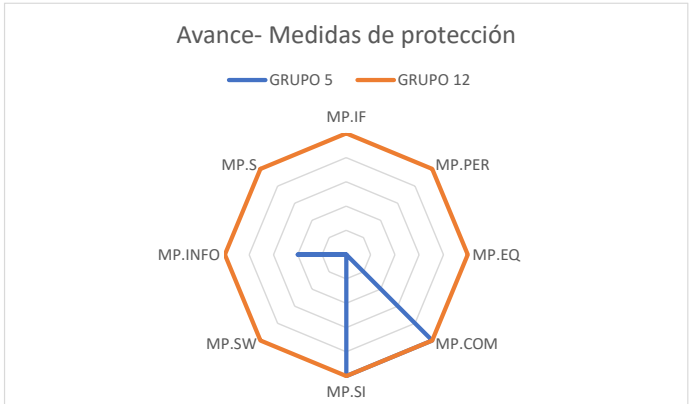
SI ES NECESARIO, TAMBIÉN SE ENCUENTRA LA **SOLUCIÓN TECNÓLOGICA** QUE MEJOR SE ADAPTE A LAS NECESIDADES

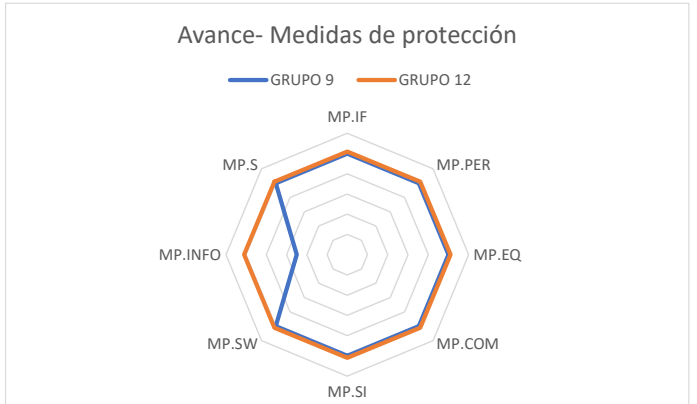
Avance de la implantación











Elementos entregables – Implantación ENS

Plan de Adecuación

Análisis de Riesgos

Marco Normativo del Sistema

30-35 Normativas y Procedimientos

Registros y evidencias de las medidas de seguridad implantadas

Informe de Evaluación/Auditoría Interna

Certificación

Previsión de Implantación de medidas – 24-30 semanas

Documentos y Medidas - IMPLANTACIÓN	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1. Preparación de Implantación																														
Presentación de AMPARO																														
Definición de Mapa Normativo																														
2. Uso de Medios Electrónicos		B																									F	C		
3. Marco normativo Grupo 1			B		F									C																
4. Marco normativo Grupo 2					B		F							C																
5. Marco normativo Grupo 3							B		F					C																
6. Marco normativo Grupo 4									B		F			C																
7. Marco normativo Grupo 5											B		F	C																
8. Marco normativo Grupo 6															B		F											C		
9. Marco normativo Grupo 7																	B		F									C		
10. Marco normativo Grupo 8																			B		F							C		
11. Marco normativo Grupo 9																					B		F					C		
12. Marco normativo Grupo 10																							B		F			C		
13. Marco normativo Grupo 11																									B		F	C		
14. Evaluación/Auditoría Interna																														

B Versión Borrador

F Versión Final

C COMSEG

Total Implantación

(Aproximado)

35 Documentos

24-30 semanas

Asesoría puntual

Prevención Proactiva: cumplimiento y vigilancia

10 Auditoría interna

11 Auditoría de Certificación

12 Expedición de las APC

13 Adecuación definitiva de las EE.LL. adheridas al Marco de Certificación

14 Auditoría(s) de Certificación

Oficina de Seguridad-vSOC

- Adecuación definitiva de las Entidades vinculadas o dependientes y nuevas entidades
- Mantenimiento y gestión de la seguridad de las Entidades certificadas

Órgano de Auditoría Técnica (OAT)

- Verificación de seguridad de las entidades cada 2 años
- Gestión de la certificación de conformidad

Total planificación tiempos de Adecuación ENS

[01] Plan de Adecuación del Sistema

8-10 semanas

- Identificar el Alcance del Sistema
- Categorizar el sistema
- Declaración de aplicabilidad
- Análisis de riesgos
- Perfiles de cumplimiento | Validación
- Política de Seguridad

[02] Implantación de medidas de seguridad

24-30 semanas

- Hoja de Ruta de implantación (priorización de medidas)
- Elaboración del Marco Normativo
- Implantación de medidas Técnicas de Seguridad

[03] Conformidad

Dependiendo disponibilidad Entidad de Certificación (2-3 semanas)

- Preauditoría interna (validación)
- Auditoría de Certificación
- Certificación ENS

CCN centro criptológico nacional

Seguridad de la Información

La seguridad de la información es un asunto de **PERSONAS**, **PROCESOS** y **TECNOLOGÍA**

¡ENSECURIZATE!

María Elvira García Bernal
Responsable Consultoría en seguridad de la información en Inycom
mariaelvira.garcia@inycom.es
www.inycom.es

Muchas

Gracias

Web sites:

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es