ángeles
Formación y Talento en Ciberseguridad

e-vens
ENTORNO DE VALIDACIÓN ENS

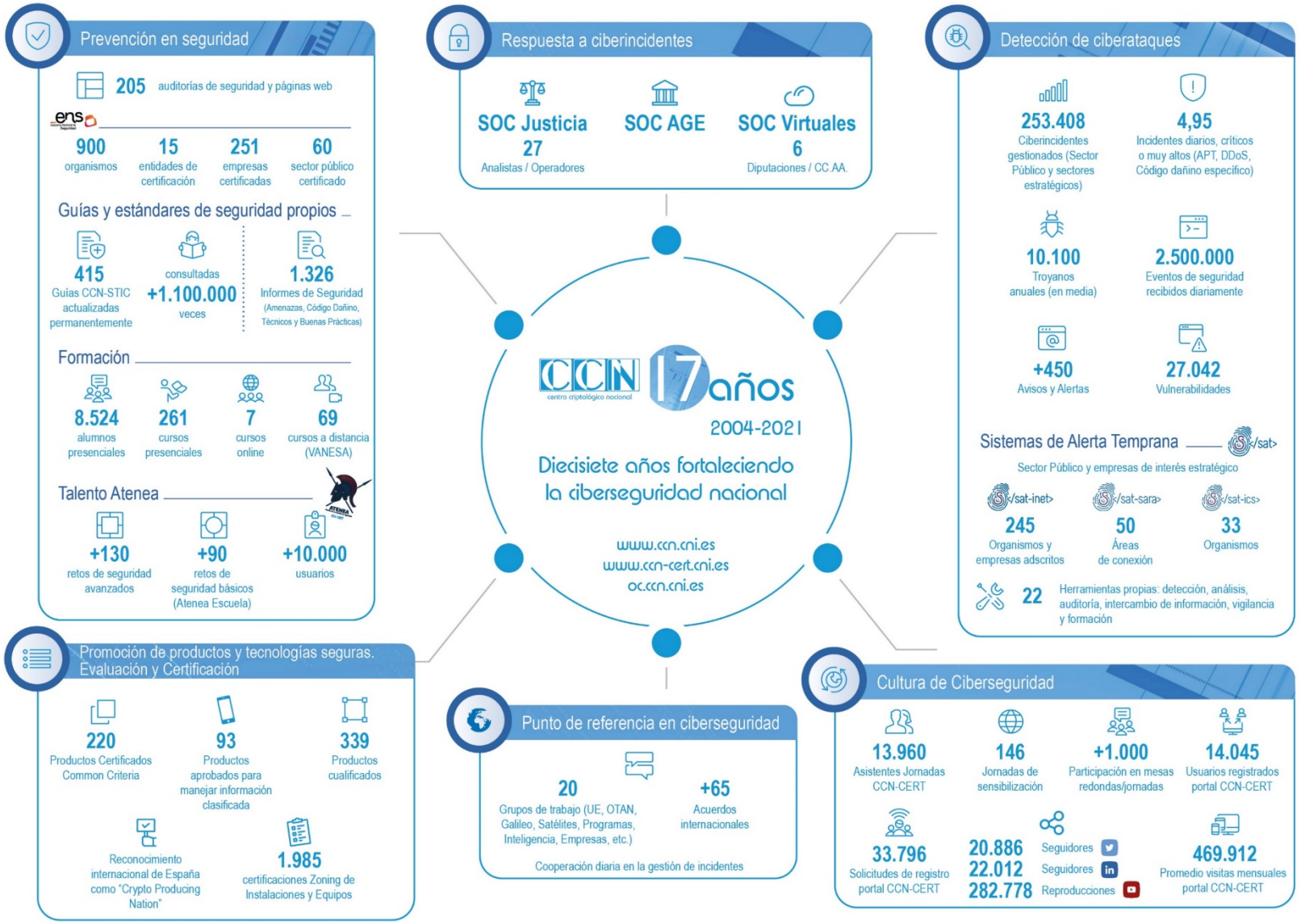
Esquema Nacional de Seguridad

Más de 10 Años de Implementación (Lecciones Aprendidas)

CCN
centro criptológico nacional

CCN
centro criptológico nacional
15 años

Centro Criptológico Nacional



CCN centro criptológico nacional

Transformación digital y ciberseguridad

Personas, procesos, tecnología, datos y ciberseguridad

Datos

- Datos para nuevos y mejores servicios, decisiones, políticas públicas, transparencia y reutilización
- Estrategia de gestión del dato, CDO,...

Personas

- Implicación de los actores (no solo TIC)
- Cambio cultural
- Competencias digitales
- Reclutamiento

Procesos

- Adecuación a la realidad digital y posibilidades
- Implementación principio de un sola vez

Ciberseguridad

Protección de datos

- Proteger sistemas de información, datos, información y servicios
- General confianza en los servicios públicos digitales

Interoperabilidad

- Facilitar el flujo de datos y servicios
- Facilitar la realización de derechos y principios (ej. OOP,...)

Tecnología

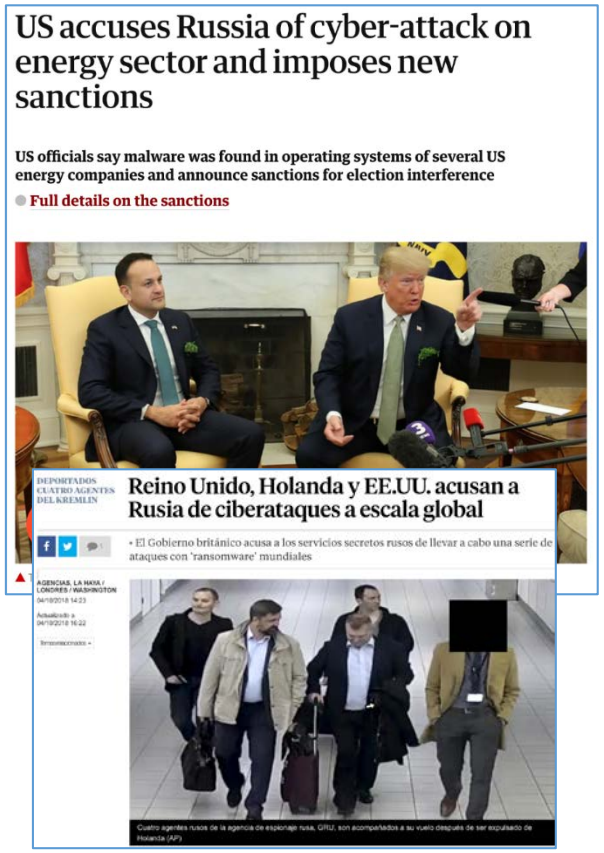
- Tecnologías habilitadoras digitales (IA, Cloud, IoT, gestión de datos, registro distribuido, lenguaje,...)
- Oportunidades y Riesgos

Lecciones aprendidas - Humildad para aprender

- **EVITAR EL PÁNICO**. Sensibilizar a la alta Dirección sin generar alarma.
- **Establecer canales de comunicación ALTERNATIVOS.**
  - Blogs, chats, mensajería instantánea, etc.
- **Boletines de ALERTA DE VULNERABILIDADES**.
  - Tiempos mínimos de actualización.
- **REEVALUACIÓN de las medidas de seguridad**. Medir la **superficie de exposición** y auditorías de seguridad.
- **Incrementar y ampliar las CAPACIDADES DE VIGILANCIA Y RESPUESTA**. Centro de Operaciones de Ciberseguridad (SoC).
- **Mejorar la NOTIFICACIÓN DE INCIDENTES e intercambio información sobre amenazas.**
  - Plataforma Común. (Notificación Incidentes)
  - Ciberinteligencia de seguridad. (Gestión Incidentes)

En el paradigma **de la respuesta**

Mientras que los **autores de ciberataques**, tanto estatales como no estatales, **solo teman al fracaso**, carecerán de motivos para dejar de intentarlo


US accuses Russia of cyber-attack on energy sector and imposes new sanctions

US officials say malware was found in operating systems of several US energy companies and announce sanctions for election interference

Full details on the sanctions

DEPORTADOS CUATRO AGENTES DEL KREMLIN

Reino Unido, Holanda y EE.UU. acusan a Rusia de ciberataques a escala global

• El Gobierno británico acusa a los servicios secretos rusos de llevar a cabo una serie de ataques con 'ransomware' mundiales

AGENCIAS. LA HAYA / LONDRES / WASHINGTON

Cuatro agentes rusos de la agencia de espionaje rusa, GRU, son acompañados a su vuelo después de ser expulsado de Holanda (AP)

- Una **respuesta más eficaz**, centrada en la **detección**, la **trazabilidad** y el emprendimiento de **acciones penales** contra los ciberdelincuentes, es fundamental **para fomentar una disuasión efectiva**.
  - Colaboración con las **Fuerzas y Cuerpos de Seguridad del Estado**.
- Una **disuasión efectiva** significa poner en marcha un **marco de medidas** que sean a la vez **creíbles** y **disuasorias** para posibles ciberdelincuentes y ciberatacantes.
  - **Identificar** a los actores maliciosos.
  - Incrementar la **vigilancia continua**.
  - Reforzar la **respuesta policial**.
  - **Cooperación** de sectores público y privado.
  - **Marco regulatorio**.

Aumentar la disuasión a través de la **capacidad de defensa**. Generar dudas coste/beneficio al ciberatacante

Determinación de la Superficie de Exposición

Mejora Continua

Reducción del Tiempo de Respuesta

La adaptación a las nuevas amenazas implica **MEJORAR EL CUMPLIMIENTO** y diseñar una respuesta cada vez más eficaz frente a los ataques **INCREMENTANDO LAS CAPACIDADES DE VIGILANCIA**

Prevención Proactiva: Cumplimiento y Vigilancia

Asegurar la continuidad del servicio

Para garantizar la continuidad del servicio, hay que ser consciente de que estás sufriendo un ataque, estás siendo comprometido. **Conocer/saber que te están atacando**.

- **Parametrizar la amenaza** para poderla mitigar y garantizar la prestación del servicio en condiciones adecuadas.
- Tener **mecanismos de respuesta oportuna**, la **notificación del incidente sin dilación indebida** es fundamental para asignar recursos y **aplicar planes de contingencia**.
- **Mejorando las capacidades** de monitorización, vigilancia, detección y respuesta.
- La continuidad del servicio lleva implícito atender a todas **las dimensiones de la seguridad** (confidencialidad, disponibilidad, integridad, trazabilidad y autenticidad) **sin olvidarnos de la privacidad** y las obligaciones que trae consigo el RGPD.

Implementación de seguridad y buenas prácticas

Detrás de esta aproximación está que los organismos **IMPLEMENTEN SEGURIDAD** y que no se limiten a realizar un análisis de riesgos y a documentar sus procedimientos

Se buscan los siguientes objetivos…

- Educación y **buenas prácticas**.
- **Planificación auditorías de seguridad** desde el primer momento.
- **Anticiparse** y buscar soluciones (proactividad).
- Analizar **medidas compensatorias**.
- Cumplimiento **a corto, medio y largo plazo**.
- **Gestión de expectativas** asociada a la adopción de compromisos.

Prevención

Se busca establecer un procedimiento de **MEJORA CONTINUA DE LOS NIVELES DE SEGURIDAD**, a través de una adaptación al medio y establecimiento de prioridades por parte de la entidad.

Aproximación pragmática… No resignarse

1. Estrategia de ciberseguridad.
2. Gobernanza de la ciberseguridad.
3. Desarrollo regulatorio POSIBILISTA
4. CSIRT de referencia, CSIRTs sectoriales y SOC.
5. Capacidad de detección y alerta temprana.
6. Mayor vigilancia a través del SOC.
7. Formación y certificación de personas.
8. Búsqueda de talentos.
9. Asociación público-privada. (**comunidad**)
10. Intercambio de información. (**confianza**)

Esquema Nacional de Seguridad

¿POR QUÉ EL ENS?

- Crear las **CONDICIONES NECESARIAS DE CONFIANZA** en el uso de los medios electrónicos, a través de **medidas** para garantizar la **seguridad,** que permita a los ciudadanos y a las AAPP, **el ejercicio de derechos y el cumplimiento de deberes** a través de estos medios.
- Promover la **GESTIÓN CONTINUADA DE LA SEGURIDAD**, al margen de impulsos puntuales, o de su ausencia.
- Contemplar los aspectos de **PREVENCIÓN**, **DETECCIÓN** y **RESPUESTA**.
- Promover un **TRATAMIENTO HOMOGÉNEO** de la seguridad que facilite la cooperación cuando participan diversas entidades, mediante **lenguaje y elementos comunes**, para facilitar la implementación de medidas, la interacción entre AA.PP. y la comunicación de requisitos de seguridad a la industria.
- Proporcionar **liderazgo** en materia de **BUENAS PRÁCTICAS**.

En definitiva… porque es la herramienta para IMPLEMENTAR SEGURIDAD

Esquema Nacional de Seguridad

DIMENSIONES de la seguridad: **Disponibilidad**, **Autenticidad**, **Integridad**, **Confidencialidad**, **Trazabilidad**.

C	I	D	A	T

1) Determinación del NIVEL DE SEGURIDAD requerido para cada dimensión de seguridad, teniendo en cuenta el impacto de un posible incidente de seguridad:

- **BAJO** → impacto **limitado**
- **MEDIO** → impacto **grave**
- **ALTO** → impacto **muy grave**

IMPACTO SOBRE:
- Las funciones de la organización
- Activos
- Ciudadanos
- Incumplimiento legal

2) Determinación de la CATEGORÍA del Sistema.

Importancia de la información y del servicio

El **esfuerzo** de seguridad requerido

CATEGORÍAS
BÁSICA
MEDIA
ALTA

CCN centro criptológico nacional

Seguridad basada en estándares de referencia

6 Principios básicos

a) Seguridad integral
b) Gestión de riesgos
c) Prevención, reacción y recuperación
d) Líneas de defensa
e) Reevaluación periódica
f) La seguridad como función diferenciada

75 Medidas de seguridad

a) Marco organizativo
b) Marco operacional
c) Medidas de protección

15 Requisitos mínimos

a) Organización e implantación del proceso de seguridad
b) Análisis y gestión de riesgos
c) Gestión del personal
d) Profesionalidad
e) Autorización y control de accesos
f) Protección de las instalaciones
g) Adquisición de productos
h) Seguridad por defecto
i) Integridad y actualización del sistema
j) Protección de la información almacenada y en tránsito
k) Prevención ante otros sistemas de información interconectados
l) Registro de actividad
m) Incidentes de Seguridad
n) Continuidad de la actividad
o) Mejora continua del proceso de seguridad

Consejo de Certificación del Esquema Nacional de Seguridad

CCN-CERT centro criptológico nacional

1. Los **principios básicos**, que sirven de guía.
2. Los **requisitos mínimos** de obligado cumplimiento.
3. La **Categorización de los sistemas** para la adopción de medidas de seguridad proporcionadas.
4. La **auditoría de la seguridad** que verifique el cumplimiento del ENS. **Sellos de conformidad.**
5. La **respuesta a incidentes de seguridad**. Papel del CCN-CERT. Notificación.
6. El uso de **productos certificados**. Papel del OC-CCN.
7. La **formación y concienciación.**
8. Serie 800 Guías CCN-STIC.

CCN centro criptológico nacional

Seguridad basada en estándares de referencia

Esquema Nacional de Seguridad

ANEXO II
Medidas de seguridad

1. Marco organizativo [org]

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

3.1 Política de seguridad [org.1].

dimensiones	Todas			
categoría	DL	confidencial	reservado	secreto
	aplica	=	=	=

La política de seguridad será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el artículo 11, y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:

a) Los objetivos o misión de la organización.
b) El marco legal y regulatorio en el que se desarrollarán las actividades.
c) Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
d) La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

La política de seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, en lo que corresponda.

3.2 Normativa de seguridad [org.2].

dimensiones	Todas			
categoría	DL	confidencial	reservado	secreto
	aplica	=	=	=

Se dispondrá de una serie de documentos que describan:

a) [org.2.a] Tal y como se indica en la CCN-STIC 101 todo sistema que maneje información clasificada deberá tener actualizada la documentación de seguridad que se relaciona en la norma específica correspondiente al acuerdo de protección suscrito.

	SECRETO/ RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Concepto de Operación (CO)	SI	SI	SI
Análisis o Valoración de Riesgos	FORMAL	FORMAL	NO FORMAL
Declaración de Requisitos de Seguridad (DRS)	SI	SI	OPCIONAL
Procedimientos Operativos de Seguridad (POS)	SI	SI	SI
Declaración de Acreditación de Seguridad	SI	SI	SI

3.3 Procedimientos de seguridad [org.3].

dimensiones	Todas			
categoría	DL	confidencial	reservado	secreto
	aplica	=	=	=

[org.3.a] La normativa de Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC) exige que el manejo de información nacional clasificada en un Sistema de las Tecnologías de la Información y las Comunicaciones (Sistema) sea llevado a cabo de acuerdo con unos Procedimientos Operativos de Seguridad (POS).

Para ello, se deberá disponer de la guía CCN-STIC 203 siguiendo las instrucciones necesarias para el desarrollo de los procedimientos de seguridad necesarios en el sistema.
En este conjunto de procedimientos deberán estar incluidos aspectos de seguridad como por ejemplo los métodos de identificación y autenticación, de manera que cubran la fortaleza requerida según el nivel de clasificación del sistema.

3.4 Proceso de autorización [org.4].

dimensiones	Todas			
categoría	DL	confidencial	reservado	secreto
	aplica	=	=	=

[org.4.l] La validación de los procedimientos operativos de seguridad (POS) por la AAS, antes de recibir una autorización para manejar información clasificada (acreditación).

3. Marco operacional [op]

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

4.1 Planificación [op.pl].

4.1.1 Análisis de riesgos [op.pl.1].

dimensiones	Todas			
categoría	DL	confidencial	reservado	secreto
	aplica	+	=	=

Categoría DIFUSIÓN LIMITADA
Se deberá realizar un análisis semi-formal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que describa los siguientes aspectos:
[op.pl.1.a] Identifique y valore cualitativamente los activos más valiosos del sistema.
[op.pl.1.b] Identifique y cuantifique las amenazas más probables.
[op.pl.1.c] Identifique y valore las salvaguardas que protegen de dichas amenazas.
[op.pl.1.d] Identifique y valore el riesgo residual.

Categoría CONFIDENCIAL O SUPERIOR
Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente.
El análisis deberá cubrir los siguientes aspectos:
Identifique y valore cualitativamente los activos más valiosos del sistema.
[op.pl.1.a] Identifique y cuantifique las amenazas posibles.
[op.pl.1.b] Identifique las vulnerabilidades habilitantes de dichas amenazas.
[op.pl.1.c] Identifique y valore las salvaguardas adecuadas.
[op.pl.1.d] Identifique y valore el riesgo residual.

4.1.2 Arquitectura de seguridad [op.pl.2].

dimensiones	Todas		
categoría	DL	confidencial	reservad
	aplica	=	

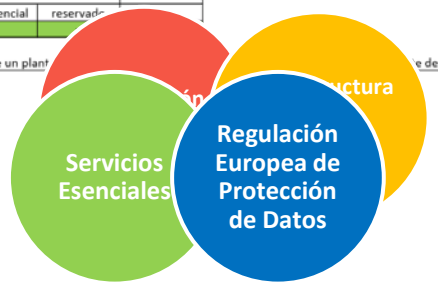
La seguridad del sistema será objeto de un plant… e de al menos,

Consejo de Certificación del Esquema Nacional de Seguridad

+

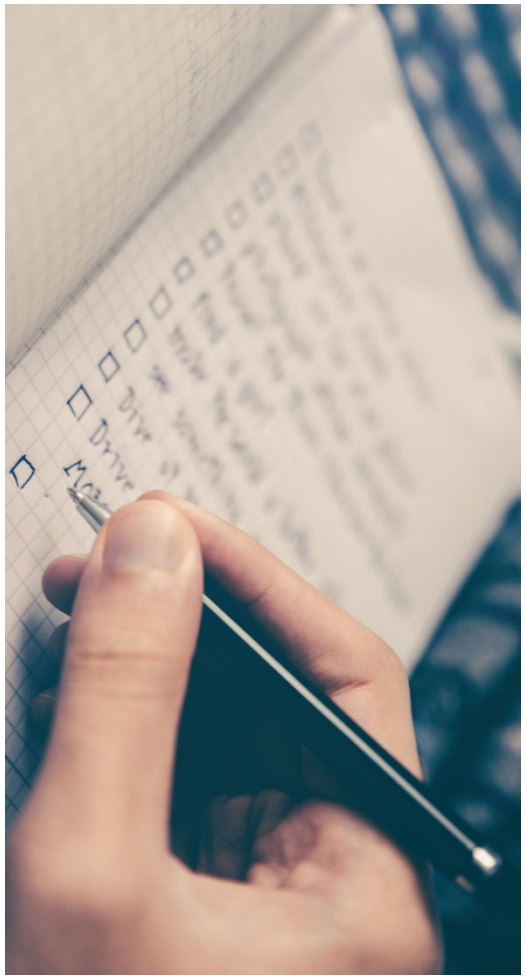
INCREMENTALES

=



centro criptológico nacional

Medidas Compensatorias y Complementaria de Vigilancia



- El **conjunto de medidas aplicables** se formalizará en la Declaración de Aplicabilidad, firmada por el Responsable de Seguridad.
- Las medidas (Anexo II) pueden ser reemplazadas por otras medidas compensatorias, siempre que justifiquen la **misma o mejor protección** de los activos (Anexo I) y cumplan con los principios básicos y los requisitos mínimos.
- La Declaración de aplicabilidad indica la **correspondencia** entre las medidas compensatorias implementadas y las medidas en el Anexo II que están compensadas.
- Es necesario **evaluar el riesgo adicional** que la implementación de la medida compensatoria podría acarrear por la no implementación de las medidas originales (Anexo II).
- Durante la autoevaluación o auditoría (bienal o extraordinaria), el Equipo de Auditoría debe analizar en profundidad las medidas compensatorias adoptadas.

Guía CCN-STIC-819 Medidas compensatorias

Certificación de Conformidad

Los organismos y las Entidades de Derecho Público **PUBLICARÁN** en sus sedes electrónicas correspondientes **LAS DECLARACIONES DE CONFORMIDAD Y LOS CERTIFICADOS DE CUMPLIMIENTO** obtenidos con respecto al cumplimiento del Esquema Nacional de Seguridad.

Según la **CATEGORÍA DEL SISTEMA**, se hace una distinción entre:

- Declaración de conformidad: aplicable a los sistemas de información de categoría básica.
- Certificación de cumplimiento: obligatorio para sistemas de categoría Media o Alta y voluntario en el caso de sistemas de categoría Básica


CERTIFICADO DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD


DECLARACIÓN DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

centro criptológico nacional

10 años del ens Esquema Nacional de Seguridad

Actualizado en 2015

- ✓ Experiencia de aplicación
- ✓ Marco europeo (eIDAS)
- ✓ Escenario de ciberseguridad

Referente de medidas de seguridad para otros .ámbitos /RGPD; …)

Ámbito de aplicación

Extendido a todo el Sector Público

(leyes 39 y 40 de 2015)

4 ITS publicadas

- ✓ Informe
- ✓ Conformidad
- ✓ Auditoría
- ✓ Notificación de incidentes

Conformidad

- ✓ Acreditación y certificación con ENAC
- ✓ Certificadores acreditados por ENAC (>8)
- ✓ Entidades certificadas (públicas/privadas; >160)
- ✓ Consejo de Certificación del ENS (CoCENS)

Monitorización - INES

- ✓ 6 ediciones del informe INES
- ✓ 768 entidades en 2018, 30% más que en 2017
- ✓ 1080 en 2019, 22 % más que en 2018
- ✓ La campaña permanece abierta todo el año

Soporte

- ✓ > 80 **guías** CCN- STIC de la serie 800.
- ✓ 21 **soluciones** de ciberseguridad

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

PERFIL DE CUMPLIMIENTO

Entidades Locales

Facilitar su adecuación al ENS con un perfil de cumplimiento específico, de forma que la adecuación sea factible, dados los recursos humanos y económicos disponibles en la entidad.

Catálogo de medidas/salvaguardas

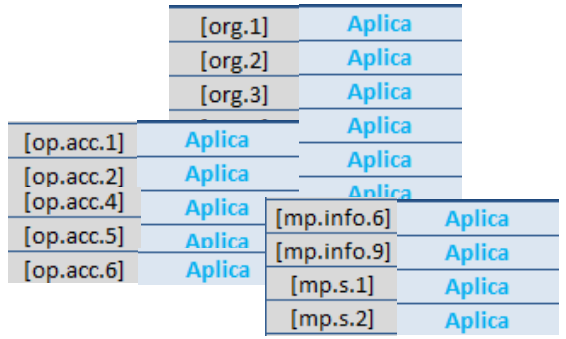
reco...	control	ENS
	[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)	L2-L3
5	[org] Marco organizativo	L2-L3
5	[org.1] Política de Seguridad	L2-L3
5	[org.2] Normativa de seguridad	L2-L3 (L2)
5	[org.3] Procedimientos de seguridad	L2-L3 (L2)
5	[org.4] Proceso de autorización	L2-L3
8	[op] Marco operacional	L2-L3
5	[op.pl] Planificación	L2-L3
3	[op.pl.1] Análisis de riesgos	L3
5	[op.pl.2] Arquitectura de seguridad	L2-L3
5	[op.pl.3] Adquisición de nuevos componentes	L2-L3 (L
3	[op.pl.4] Dimensionamiento / Gestión de capacidades	L2
3	[op.pl.5] Componentes certificados	
7	[op.acc] Control de acceso	L
5	[op.acc.1] Identificación	L2-

Análisis del riesgo residual

Selección de aquellas medidas cuyo aplicación se considera obligatoria porque el riesgo residual resultante de no aplicarlas no sería asumible

- ✓ Algunas medidas que, por defecto aplicarían, podrían no ser exigidas.
- ✓ Podrían exigirse otras que, según el Anexo II, no aplicarían.

Perfil de cumplimiento



- ✓ Recogerá un número de medidas que podrían no ser las 45 medidas que son de aplicación para categoría BÁSICA.

PERFIL DE CUMPLIMIENTO

Declaración de Aplicabilidad Inicial

Medida de seguridad	Aplica	Nivel de exigencia
[op.exp.11]	Aplica	Alto
[op.ext.1]	Aplica	Alto
[op.ext.2]	Aplica	Alto
[op.ext.9]	No Aplica	No aplica
[op.cont.1]	Aplica	Alto
[op.mon.1]	No Aplica	No Aplica
[mp.if.4]	Aplica	Bajo
[mp.if.6]	No Aplica	No aplica
[mp.if.7]	No Aplica	No Aplica
[mp.if.8]	Aplica	Alto
[mp.if.9]	Aplica	Alto
[mp.exp.1]	Aplica	Alto

Perfil de Cumplimiento

Medida de seguridad	Aplica	Nivel de exigencia
[op.exp.11]	Aplica	Alto
[op.ext.1]	Aplica	Alto
[op.ext.2]	Aplica	Medio
[op.ext.9]	No Aplica	No aplica
[op.cont.1]	No Aplica	No aplica
[op.mon.1]	No Aplica	Alto
[mp.if.4]	Aplica	Alto
[mp.if.6]	No Aplica	No aplica
[mp.if.7]	Aplica	Alto
[mp.if.8]	Aplica	Alto
[mp.if.9]	Aplica	Compensada
[mp.exp.1]	Aplica	Alto

Implicaciones de un Perfil de Cumplimiento

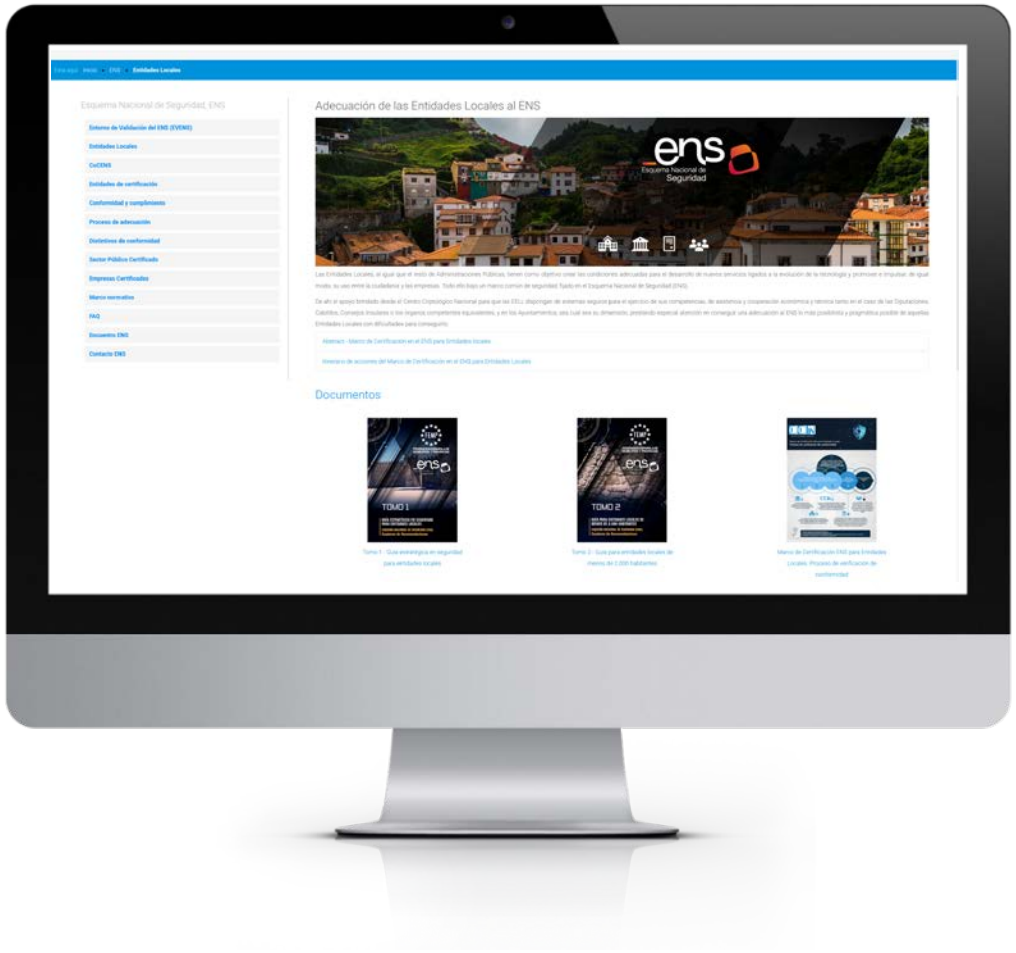
- Reducir el nivel incremental de una medida
- Suprimir la aplicación de una medida
- Aumentar el nivel incremental de una medida
- Incluir la aplicación de una medida
- Proponer medida compensatoria

Prevención Proactiva: cumplimiento y vigilancia

Las Entidades Locales, al igual que el resto de Administraciones Públicas, tienen como objetivo crear las condiciones adecuadas para el desarrollo de nuevos servicios ligados a la evolución de la tecnología y promover e impulsar, de igual modo, su uso entre la ciudadanía y las empresas. Todo ello bajo un marco común de seguridad, fijado en el Esquema Nacional de Seguridad (ENS).

De ahí el apoyo brindado desde el Centro Criptológico Nacional para que las EELL dispongan de sistemas seguros para el ejercicio de sus competencias, de asistencia y cooperación económica y técnica tanto en el caso de las Diputaciones, Cabildos, Consejos Insulares o los órganos competentes equivalentes, y en los Ayuntamientos, sea cual sea su dimensión, prestando especial atención en conseguir una adecuación al ENS lo más posibilista y pragmática posible de aquellas Entidades Locales con dificultades para conseguirlo.

MUESTRA REPRESENTATIVA	APROBACIÓN PROVISIONAL DE CONFORMIDAD	CERTIFICACIÓN DE CONFORMIDAD
¿Cómo seleccionar la muestra representativa? Si todos los Ayuntamientos adheridos al Marco de Certificación poseen una infraestructura tecnológica similar, la selección de la muestra representativa podría ser aleatoria entre todos los Ayuntamientos adheridos.	**Obtención de la aprobación provisional de conformidad (APC)** [paso 8] La obtención de la APC exige que TODAS las entidades de la muestra representativa superen favorablemente la Auditoría de Conformidad con el ENS.	**Obtención de la certificación de conformidad (categoría BÁSICA)** Las entidades con APC disponen de dos años para alcanzar la Certificación de Conformidad con el ENS (categoría Básica), previa Auditoría de Certificación del Órgano de Auditoría Técnica de la Diputación u órgano equivalente



CCN
centro criptológico nacional

PERFIL DE CUMPLIMIENTO

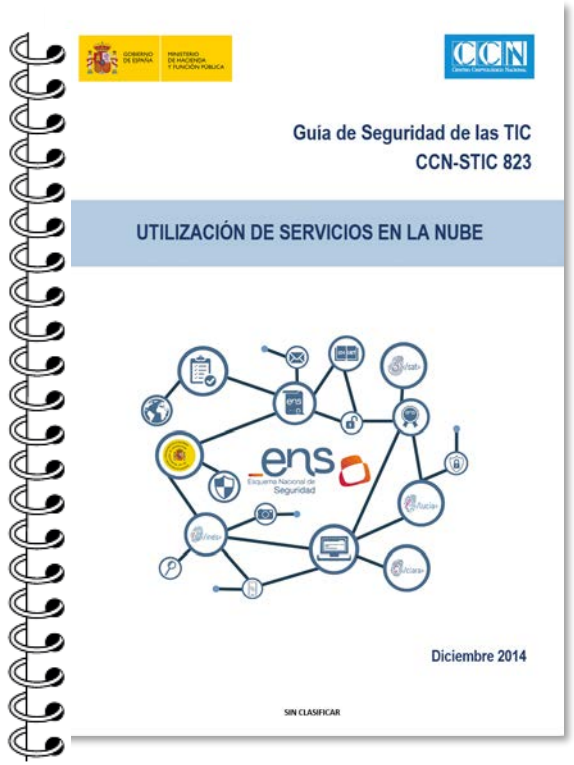
Servicios *cloud*

Facilitar su adecuación al ENS con un perfil de cumplimiento específico, de forma que las Administraciones Públicas sepan qué deben exigir a sus proveedores de servicios en la nube.

Una vez que se analizan las dimensiones de seguridad, el siguiente paso es una Evaluación de riesgos, una declaración de aplicabilidad (las medidas que se deberán tener en cuenta) y el **PERFIL DE CUMPLIMIENTO** que especificará la configuración de seguridad de las medidas incluidas en la declaración de aplicabilidad.

Servicios en Nube

La próxima guía CCN-STIC-823 incluye los **aspectos de seguridad** (metodología y elementos) necesarios que deben considerarse para la adopción de la nube como paradigma tecnológico.



Metodología y elementos a conseguir para adoptar servicios en la nube, según el ENS:

Análisis de riesgos (AR).

Declaración de aplicabilidad (el conjunto de medidas que son de aplicación)

Un PERFIL DE CUMPLIMIENTO que incluya las configuraciones de seguridad de las medidas incluidas en la declaración de aplicabilidad.

Certificación de conformidad con el ENS (categoría ALTA).

Evolución

Esquema Nacional de Seguridad

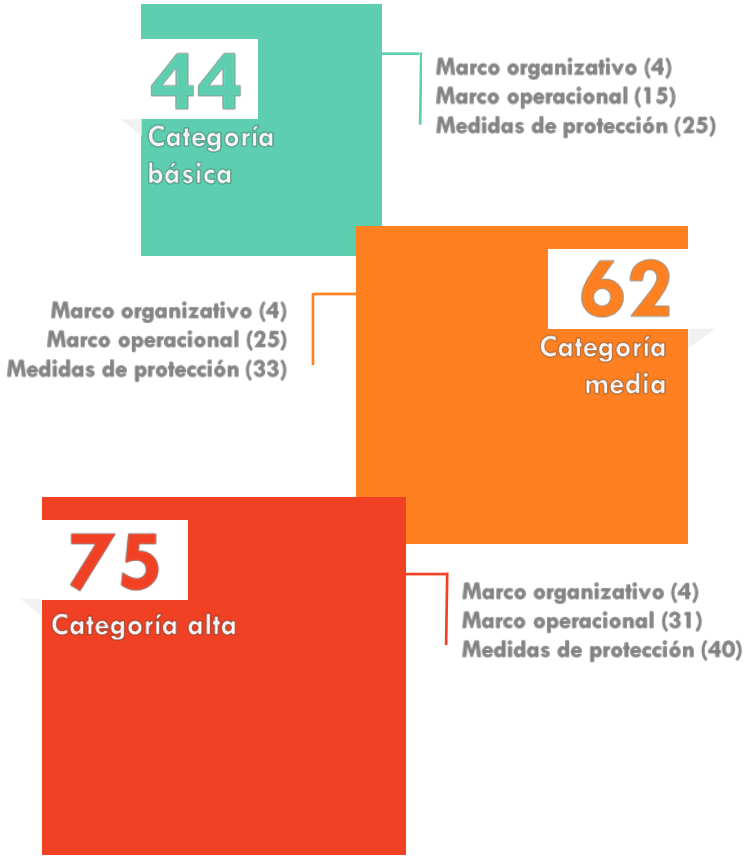
RD 2015

Nuevo RD

Evolución

Esquema Nacional de Seguridad

RD 2015



Nuevo RD

Medidas por Categoría

centro criptológico nacional

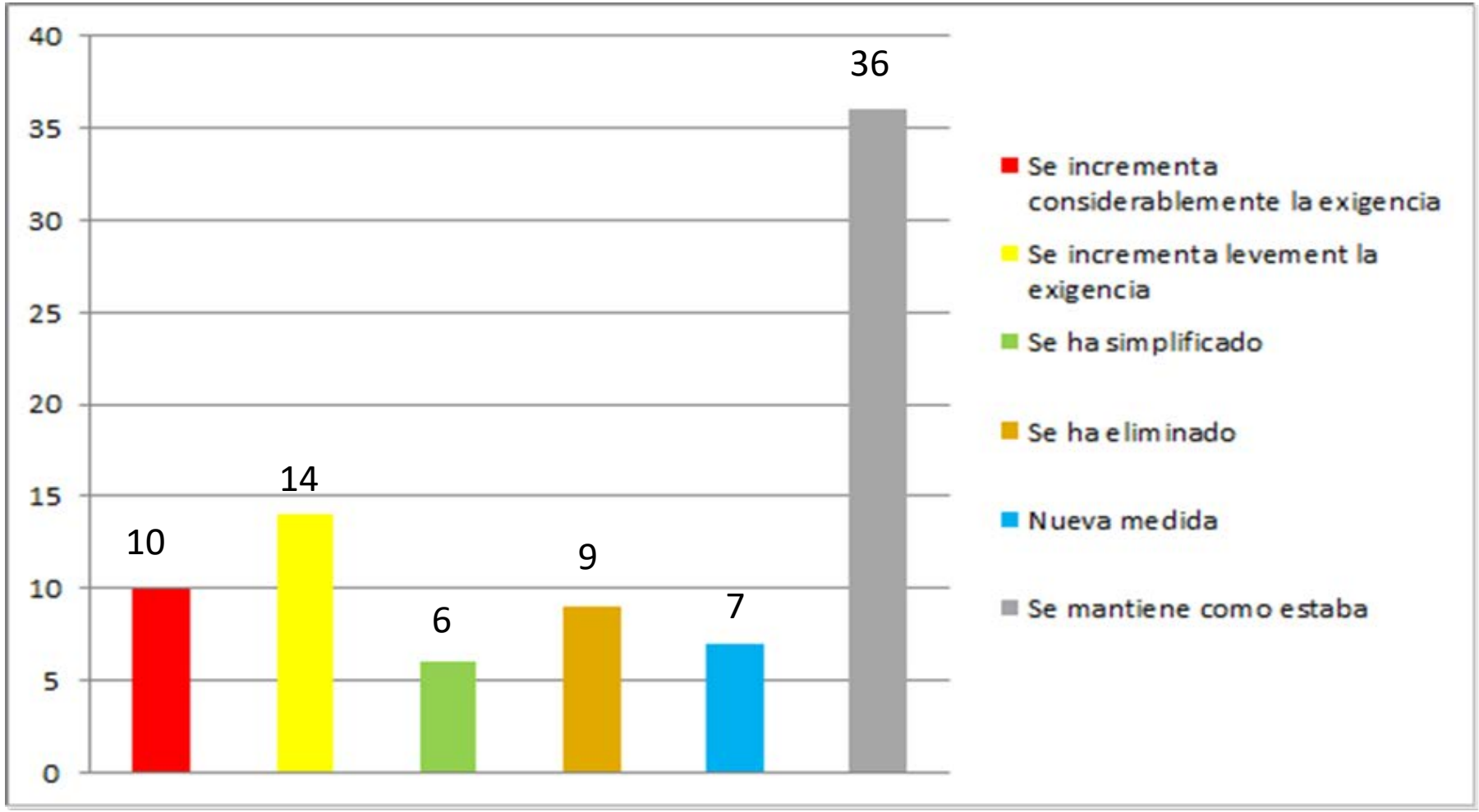
Seguridad basada en estándares de referencia

- **Medidas eliminadas.**
- **Nuevas medidas.**
- **Medidas que refuerzan significativamente la exigencia**
- **Medidas que incrementan levemente la exigencia**
- **Medidas que se simplifican.**

Nuevo sistema de referencia

- Más **moderno**
- Más adecuado, para **facilitar** de manera proporcionada **la seguridad** de los sistemas de información, su **implantación** y su **auditoría**
- **Medidas del Anexo II**
  - Se han codificado los requisitos de las medidas
  - Se han organizado de la siguiente forma:
    - **Requisitos base**
    - Posibles **refuerzos** de seguridad (R), alineados con el nivel de seguridad perseguido, que se suman (+) a los requisitos base de la medida, pero que no siempre son incrementales entre sí; de forma que, en ciertos casos, se puede elegir entre aplicar un refuerzo u otro
  - Especial foco en Marco Operacional y Medidas de Protección

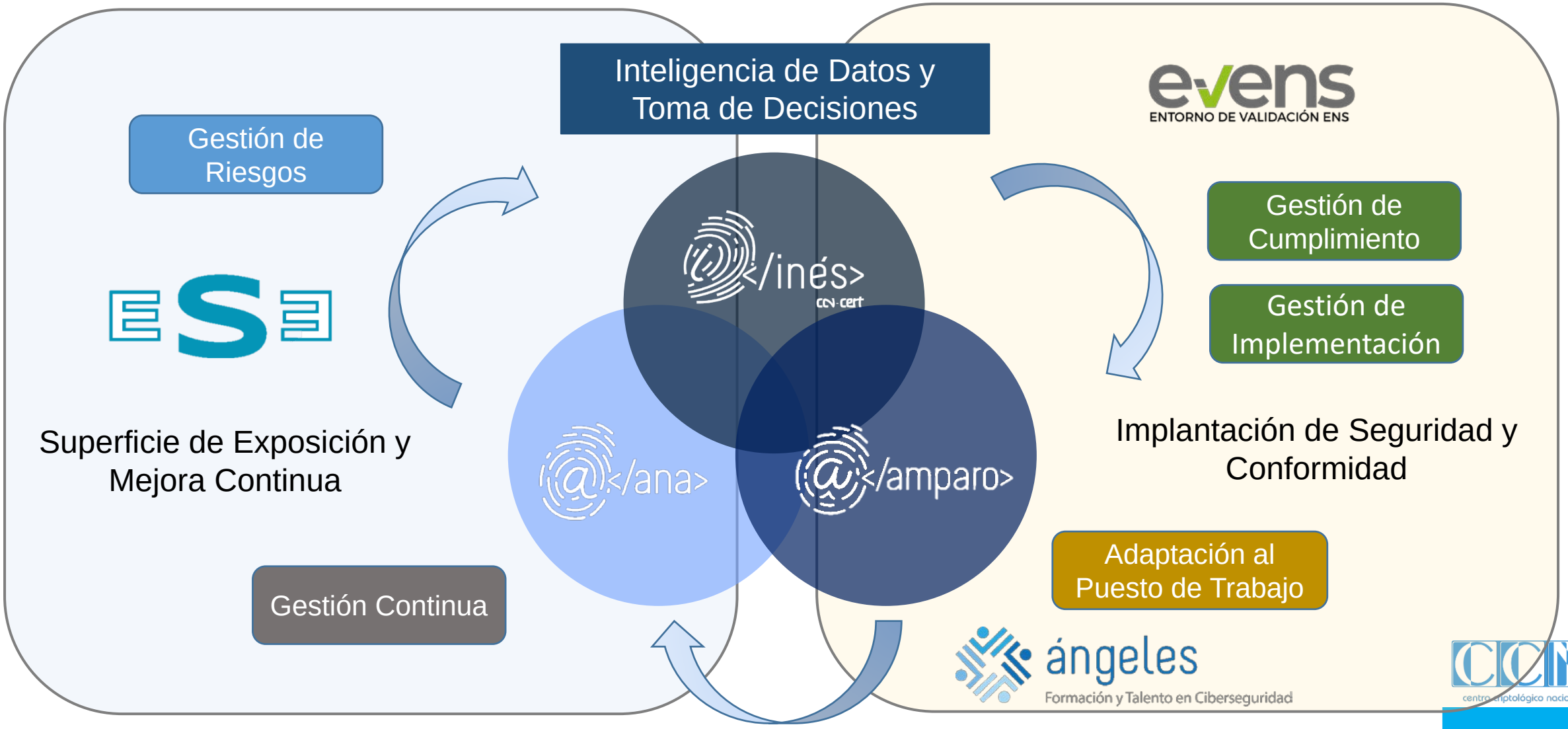
Evolución


40
35
30
25
20
15
10
5
0
10
14
6
9
7
36
Se incrementa considerablemente la exigencia
Se incrementa levement la exigencia
Se ha simplificado
Se ha eliminado
Nueva medida
Se mantiene como estaba

Prevención Proactiva: **Cumplimiento** y **Vigilancia**

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

Gestión continua de la seguridad



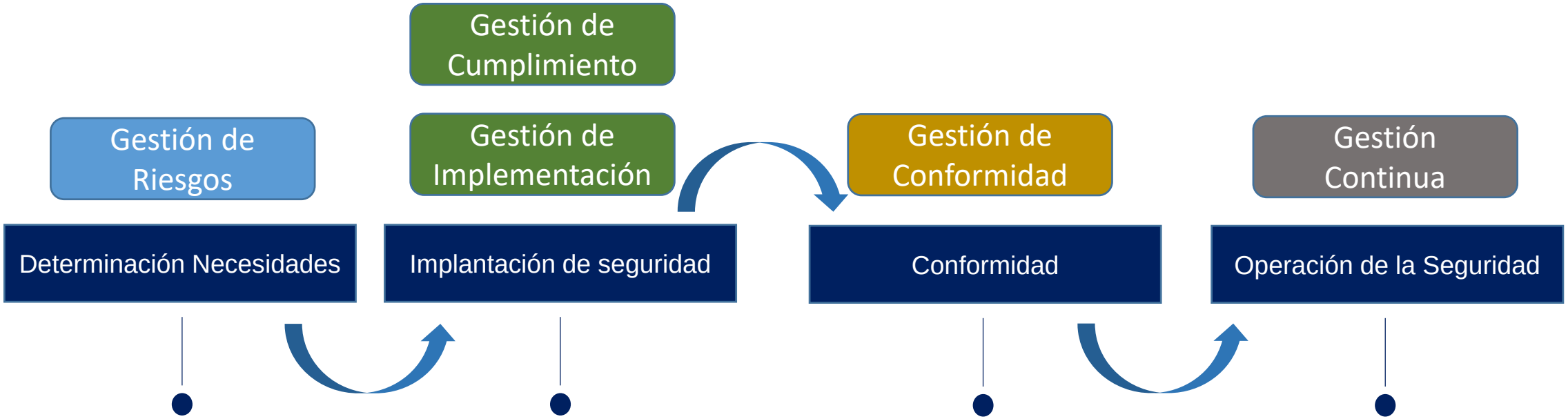
Prevención Proactiva: **Cumplimiento** y **Vigilancia**

- **Establecer una hoja de ruta** que permita adelantarse al problema y, lo que es más importante, cómo poder **gestionarlo a priori** ante el menor indicio de materialización…
- Construir modelos, analizar el problema y elaborar una hipótesis fundamentada de cara a **optimizar los recursos** disponibles y **priorizar la asignación** de los mismos.
- **Predecir** el potencial ataque y **la materialización de la amenaza**… *podemos anticiparnos porque conocemos y conocemos porque medimos y medimos porque tenemos capacidades de vigilancia.*
- Al final la **mejora continua** se convierte en el elemento de **apoyo a la decisión**.

Si se conoce el problema (vulnerabilidades, deficiencias y mala praxis), las carencias y potenciales amenazas se pueden **predecir y hacer prospectiva**

Si medimos, gestionamos y si gestionamos, avanzamos…

Gobernanza de la Ciberseguridad



- Identificar Alcance del Sistema
- Categorización del Sistema
- Declaración de Aplicabilidad
- Análisis de Riesgos
- Validación y Perfil de Cumplimiento
- Política de Seguridad

- Auditoría Interna de Verificación
- Normativas y Procedimientos de Seguridad
- Implantación de Medidas Técnicas de Seguridad
- Aprobación del SGSI por el COMSEG

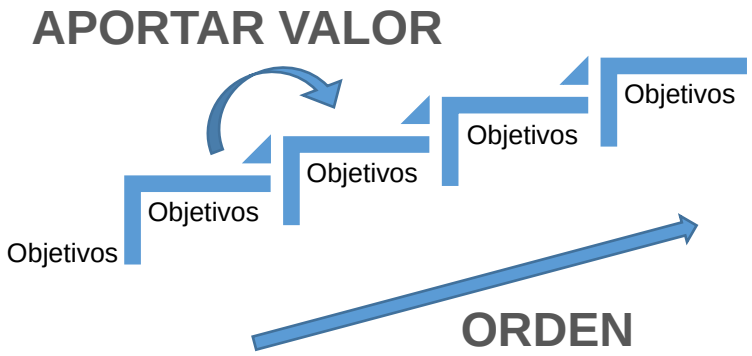
- Auditoría Interna de Verificación
- Auditoría de Certificación
- Certificación de Conformidad

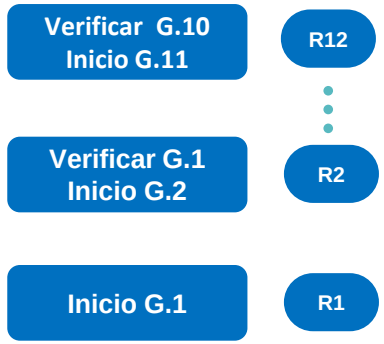
- Operación de la seguridad
  - Prevención
  - Operación
  - Detección
  - Respuesta
  - Formación
  - Mejora continua

Seguridad en base a **Criterio y Orden**

- Metodología basada en mejora continua
- Entrega de valor en cada grupo
- Desarrollo iterativo e incremental

- Formación progresiva
- Priorización de actuaciones
- Aproximación posibilista





Apoyo en herramientas **INES** y **AMPARO**

</inés> ccn-cert </amparo> </pilar> </loreto> ángeles Formación y Talento en Ciberseguridad

CCN centro criptológico nacional

Plan de _Adecuación

El proceso de Certificación/Conformidad con el ENS exige la elaboración de un **Plan de Adecuación**.

El **PLAN DE ADECUACIÓN** es un documento que contendrá la siguiente información: el alcance de los sistemas que se van a someter al proceso de certificación en el ENS, la categoría los mismos, qué medidas del Anexo II se van a implementar (Declaración de Aplicabilidad), qué riesgos se asumen, la Política de Seguridad del Organismo con su organización de la seguridad...

Para abordar de forma eficiente el Plan de Adecuación es necesario realizar los siguientes pasos:

Estado del cumplimiento del ENS

- [1] Identificar Alcance del Sistema
- [2] Categorización del Sistema
- [3] Declaración de Aplicabilidad
- [4] Análisis de Riesgos
- [5] Validación y Perfil de Cumplimiento
- [6] Política de Seguridad

PROPUESTA

Plan de _Adecuación

Prevención Proactiva: cumplimiento y vigilancia

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

CCN
centro criptológico nacional

Seguridad en base a **Gobernanza**

Creación de Oficina Técnica de Ciberseguridad y Cumplimiento Normativo

Garantiza la planificación, coordinación y puesta en marcha de los planes diseñados para la protección y cumplimiento normativo de entidades

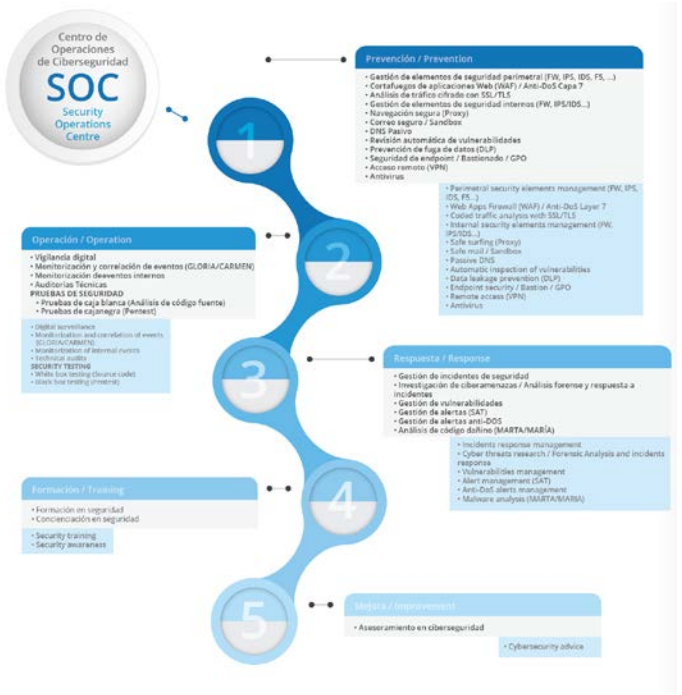
Funciones

Oficina Técnica de Ciberseguridad y Cumplimiento Normativo

- Coordinación entre los diferentes agentes del proyecto
- Apoyo en las reuniones de seguimiento y al plan de gobernanza
- Definición de los proyectos de Ciberseguridad, Adecuación y Cumplimiento Normativo a abordar
- Seguimiento de los proyectos puestos en marcha
- Supervisión y seguimiento de los proyectos ejecutados
- Soporte a las instituciones en materia de Ciberseguridad

Oficina de control, gestión, documentación y formación

En aquellas organizaciones dónde por tamaño de administración (muy grande) o por falta de recursos internos (menos de los necesarios) no se pueda llevar un control efectivo de todas las Acciones de Ciberseguridad, es necesario incorporar una Oficina de Control, Gestión y Formación. Entre otras funciones, destacan:



Enlace
Hacer de enlace entre los diferentes pilares.

Comunicación
Comunicar a los responsables de las APP cualquier incidencia, problema o hecho destacado.

Seguimiento
Hacer el seguimiento del cumplimiento de cada pilar.

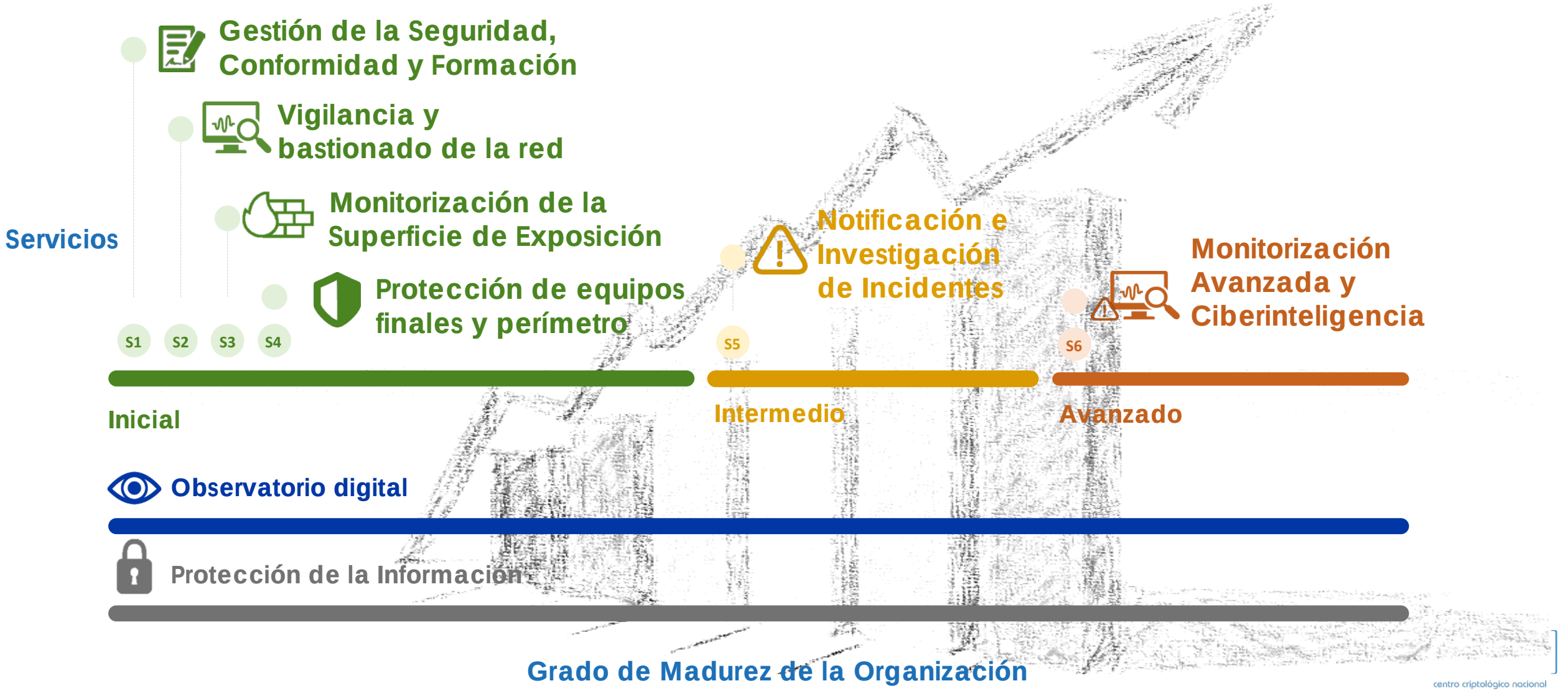
Documentación
Documentar el sistema completo, desde el alto nivel hasta el nivel de detalle, usando para ello la información suministrada por el COCS, el CICS y el NYCCS.

REDUCIR SUPERFICIE DE EXPOSICIÓN

MEJORA CONTINUA

Identificar / Valorar RESPUESTA EFICIENTE a los riesgos

Hoja de Ruta – Prevención Proactiva



Prevención Proactiva: Cumplimiento y Vigilancia

Marco Operacional

Medidas de Operación

Marco Organizativo

Medidas de Gestión

Medidas de Protección

Infraestructura de Seguridad

Prevención Proactiva: cumplimiento y vigilancia

1. Adecuación al ENS – Diputación u Órgano equivalente
2. Certificación del ENS – Diputación u Órgano equivalente
3. Reconocimiento del Órgano de Auditoría Técnica
4. Infraestructura Tecnológica EE.LL.
5. Selección de las EE.LL. del MCE-ENS
6. Selección muestra representativa (MR)
7. Creación COMSEG
8. Plan de Adecuación Conjunto
9. Adecuación al ENS de la MR
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

Ciclo de mejora continua de la seguridad

Las actividades 13 y 14 comprenden el Ciclo de mejora continua de la seguridad, y abarcan las siguientes tareas por parte de la **Oficina de Seguridad-vSoC** y el **Órgano de Auditoría Técnica (OAT)**:

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

Servicios de **Ciberseguridad**

Creación de Centro de Operaciones de Ciberseguridad

Gestión y coordinación de **servicios de ciberseguridad**

Implantación y operación de herramientas

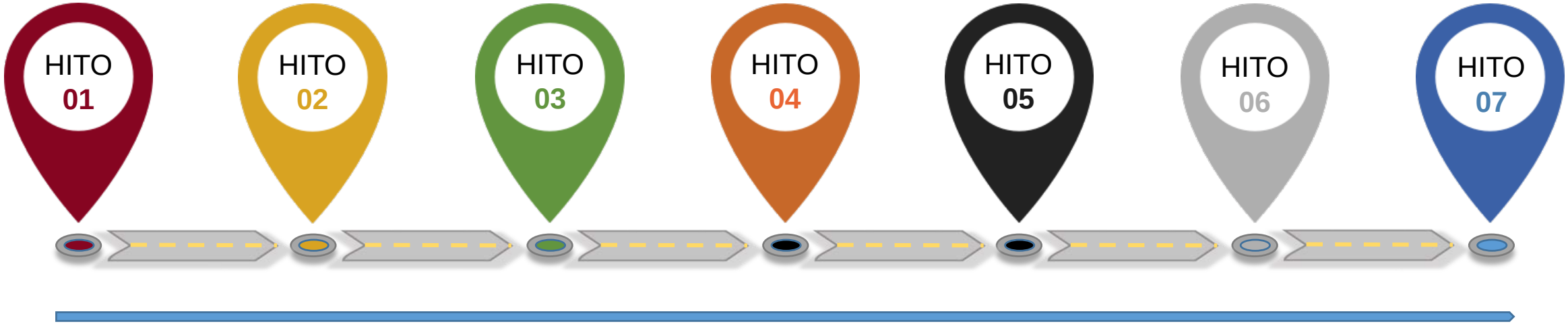
Se responsabilizará de la operación Centralizada de Servicios de Ciberseguridad (**herramientas comunes y compartidas**)

Instalación, configuración, parametrización y personalización de una serie de soluciones, que den apoyo y soporte al cumplimiento normativo y adecuación al ENS y contribuyan a una vigilancia continua:

- Cumplimiento de **Esquema Nacional de Seguridad**
- Monitorización de la **superficie de exposición**
- **Mejora continua**
- Trazabilidad y protección del **dato**
- Contexto de **incidentes**
- Identificación de **Amenazas** (comportamientos anómalos)
- Correlación compleja de **eventos** (SIEM)
- **Detección temprana**

CCN centro criptológico nacional

Prevención Proactiva: Cumplimiento y Vigilancia



Determinación Activos Esenciales

Salvaguardas (AR Residual)

Superficie de Exposición

Adaptación al Puesto de Trabajo

Contexto de la Amenaza (Incidentes)

Protección y Trazabilidad del Dato

Evolución Dinámica (Mejora Continua)

/inés> CCN-CERT

/pilar>

/clara>

ángeles
Formación, capacitación y talento en ciberseguridad

/lucía> CCN-CERT

/carla>

/ana>

/amparo>

/emma>

/rocío>

centro criptológico nacional

Pragmatismo y **Contextualización**

Triaje

- Apoyo a la entidad para generar un plan de remediación abordable.
- Mecanismos correctores de criticidad de acuerdo a los niveles de peligrosidad:
  - **Riesgos identificados** durante los procesos de inspección.
  - Debilidades asociadas a **vectores de ataques actualmente utilizados** o muy “de moda”.
  - **Vulnerabilidades** asociadas a productos software innecesarios o **ampliamente explotados**.
  - Vulnerabilidades **fácilmente explotables**.
  - Vulnerabilidades cuya subsanación **no impacte en servicios esenciales**.
  - Vulnerabilidades **expuestas a Internet**.
  - …
- Aplicación de mediadas complementarias de vigilancia para minimizar el impacto de vulnerabilidades difíciles de corregir.

Hoja de Ruta – Prevención Proactiva

Servicios

Gestión de la Seguridad, Conformidad y Formación

Vigilancia y bastionado de la red

Monitorización de la Superficie de Exposición

Protección de equipos finales y perímetro

S1 S2 S3 S4

Inicial

ángeles Formación y Talento en Ciberseguridad

e-vens ENTORNO DE VALIDACIÓN ENS

ES

Notificación e Investigación de Incidentes

S5

Intermedio

Monitorización Avanzada y Ciberinteligencia

S6

Avanzado

Observatorio digital

Protección de la Información

Grado de Madurez de la Organización

CCN centro criptológico nacional

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)

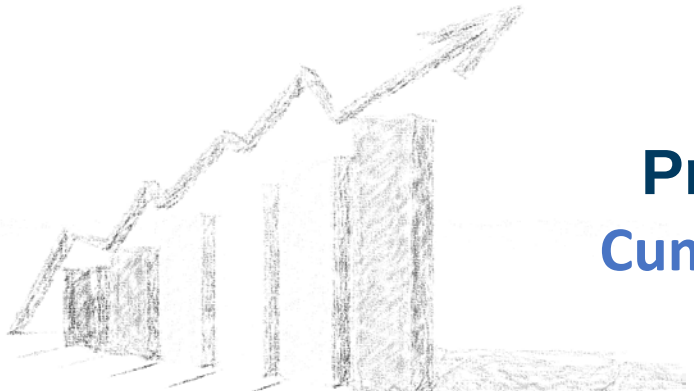
- Preauditoría interna (validación)
- Auditoría de Certificación
- Certificación ENS

Hoja de Ruta – Adaptación de la Amenaza

Madurez	Coste Preventivo	Coste Reactivo	Coste Cumplimiento	Total
Inicial	20-25 €/usuario	2 horas/usuario	1 hora/usuario	20-25 €/usuario 3 horas/usuario
Intermedio	50-60 €/usuario	6 horas/usuario	2 horas/usuario	50-60 €/usuario 8 horas/usuario
Avanzado	100-200 €/usuario	12-20 horas/usuario	4-12 horas/usuario	100-200 €/usuario 4-12 horas/usuario

Madurez: - a +

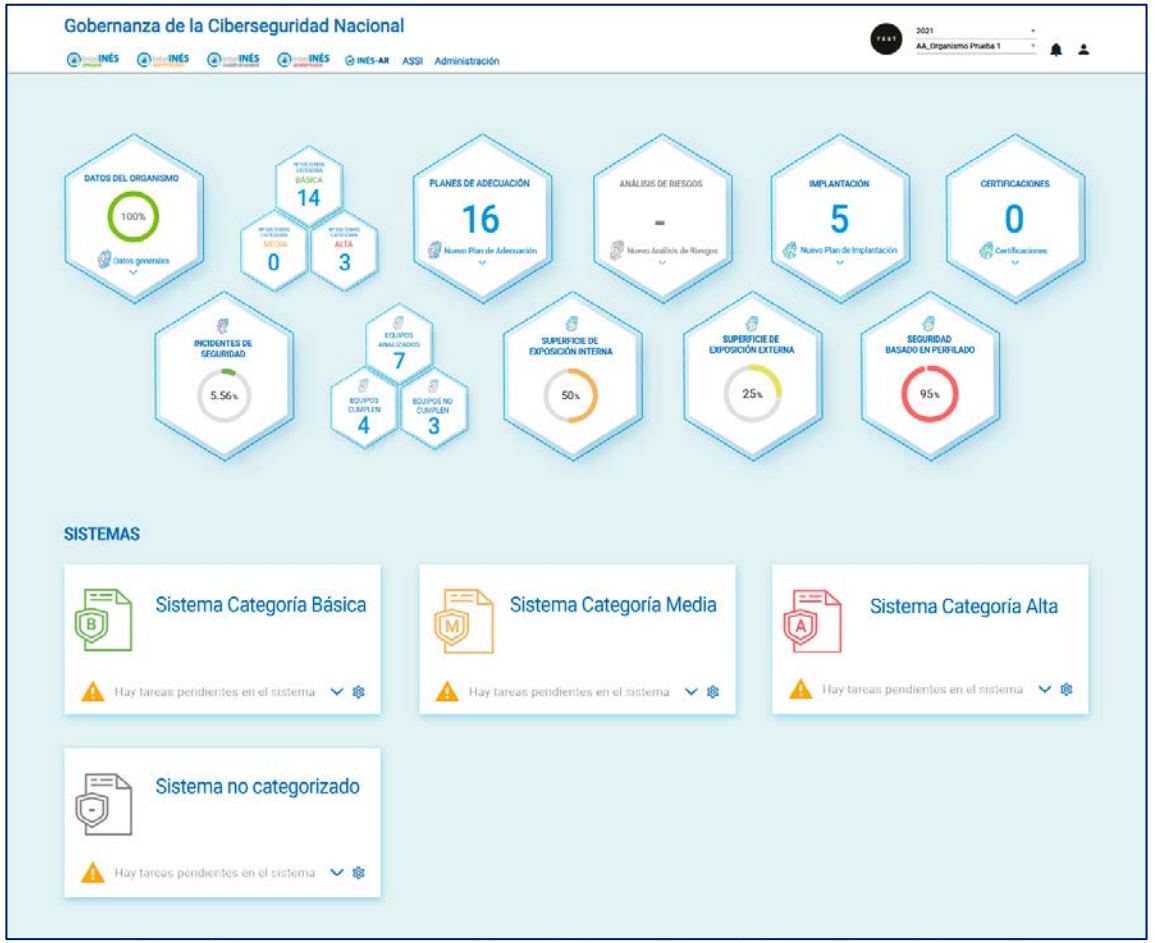
Riesgo: + a -



Prevención Proactiva
Cumplimiento y Vigilancia

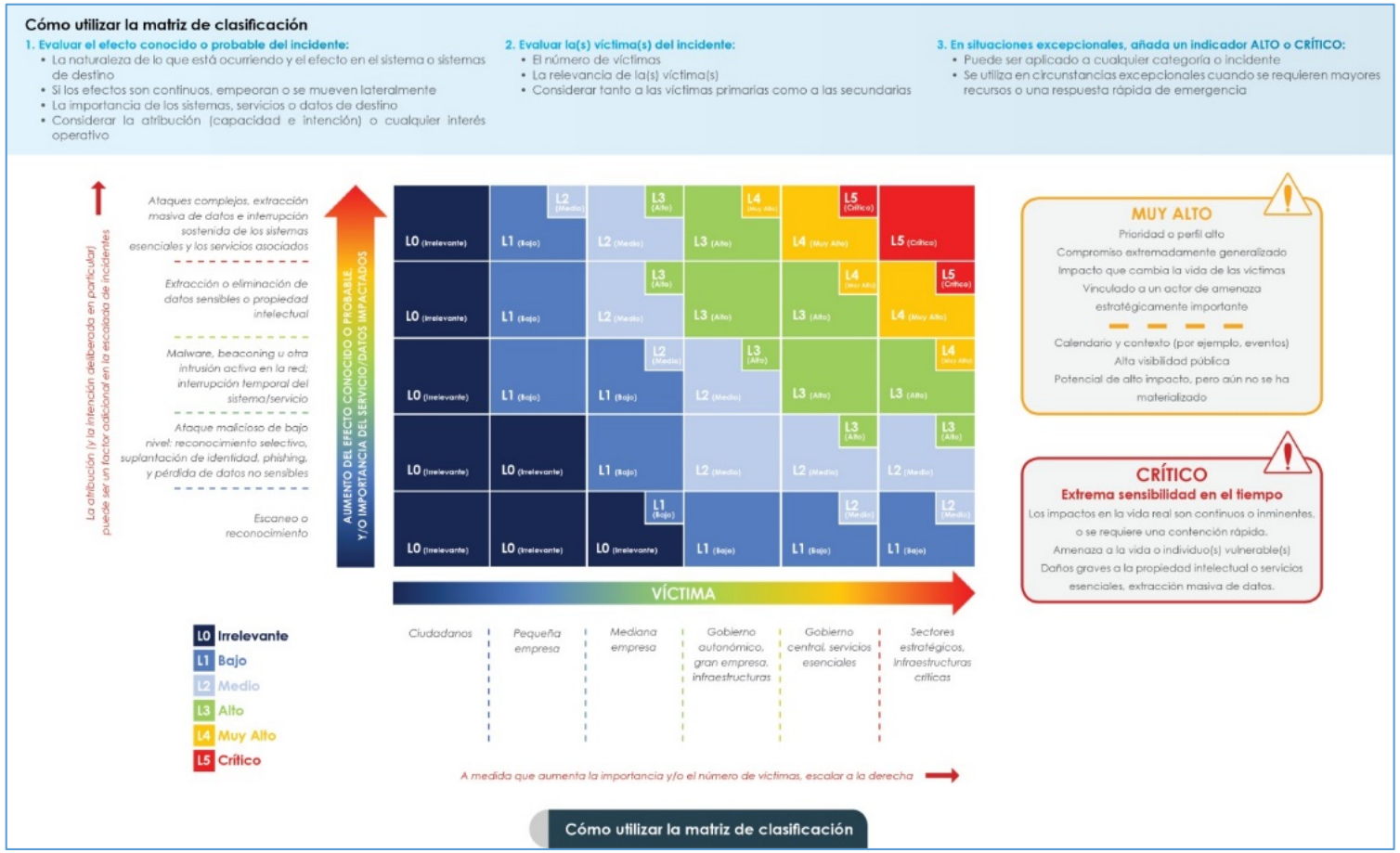
Gobernanza y Toma de Decisiones

- Parametrización de activos
- Relación entre activos y amenazas
- Extracción de valores clave
- Inteligencia de gestión de riesgos
- Adaptación a la amenaza



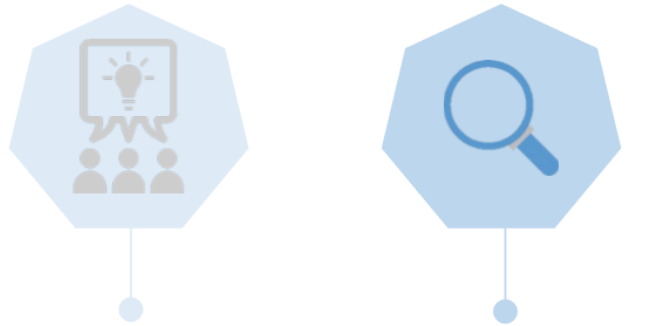
Prevención **Proactiva**

El reto: conseguir que el cumplimiento y la vigilancia vayan de la mano adaptadas al nivel de madurez y recursos disponibles de las entidades



Ventajas

- Gestionar servicios de ciberseguridad
- Medición superficie de exposición
- Adaptación a la amenaza
- Contextualización de los incidentes
- Eficiencia de los recursos disponibles

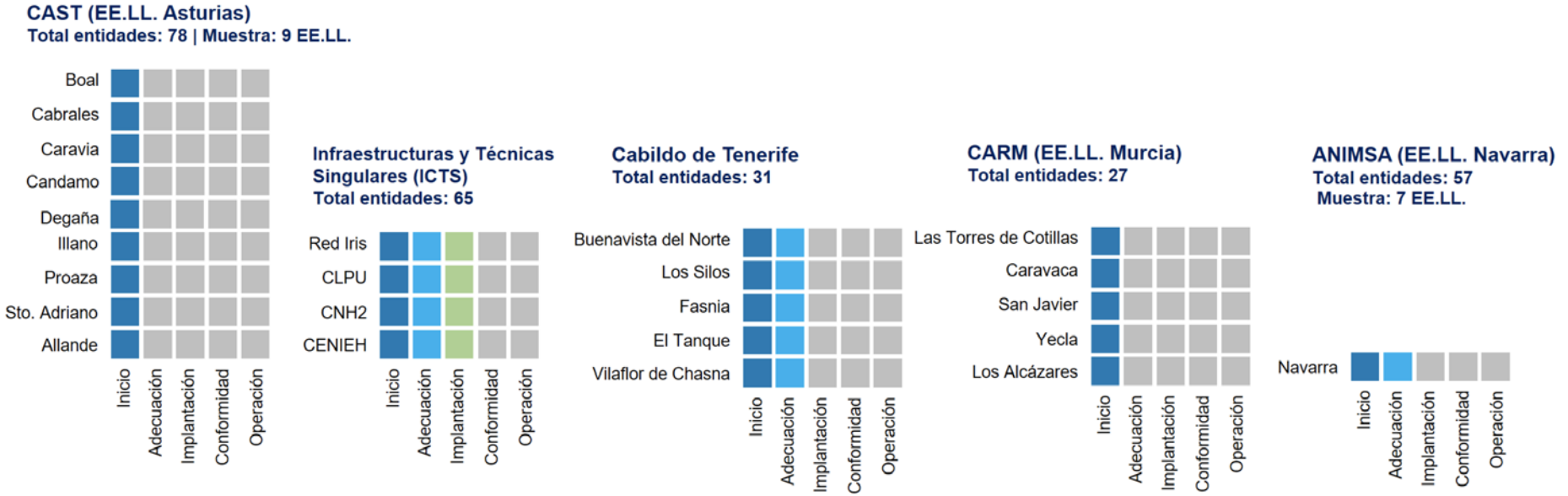


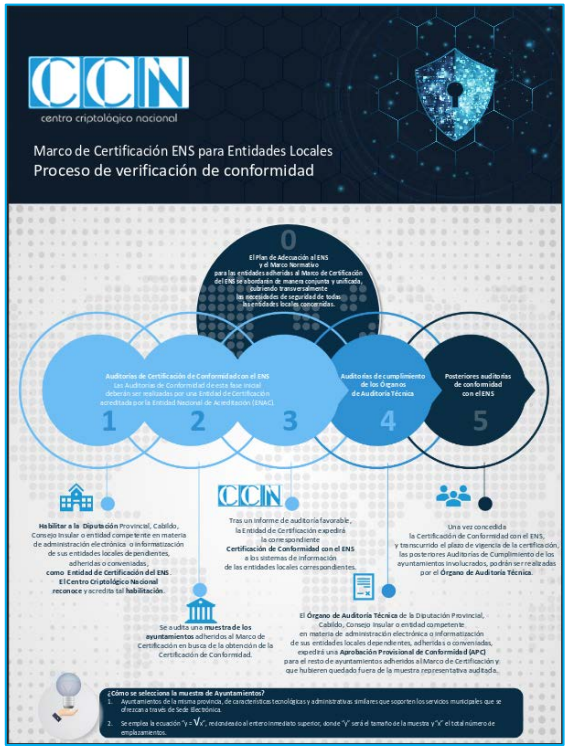
Más información de ataques

Mayor visibilidad sobre incidentes

Iniciativas

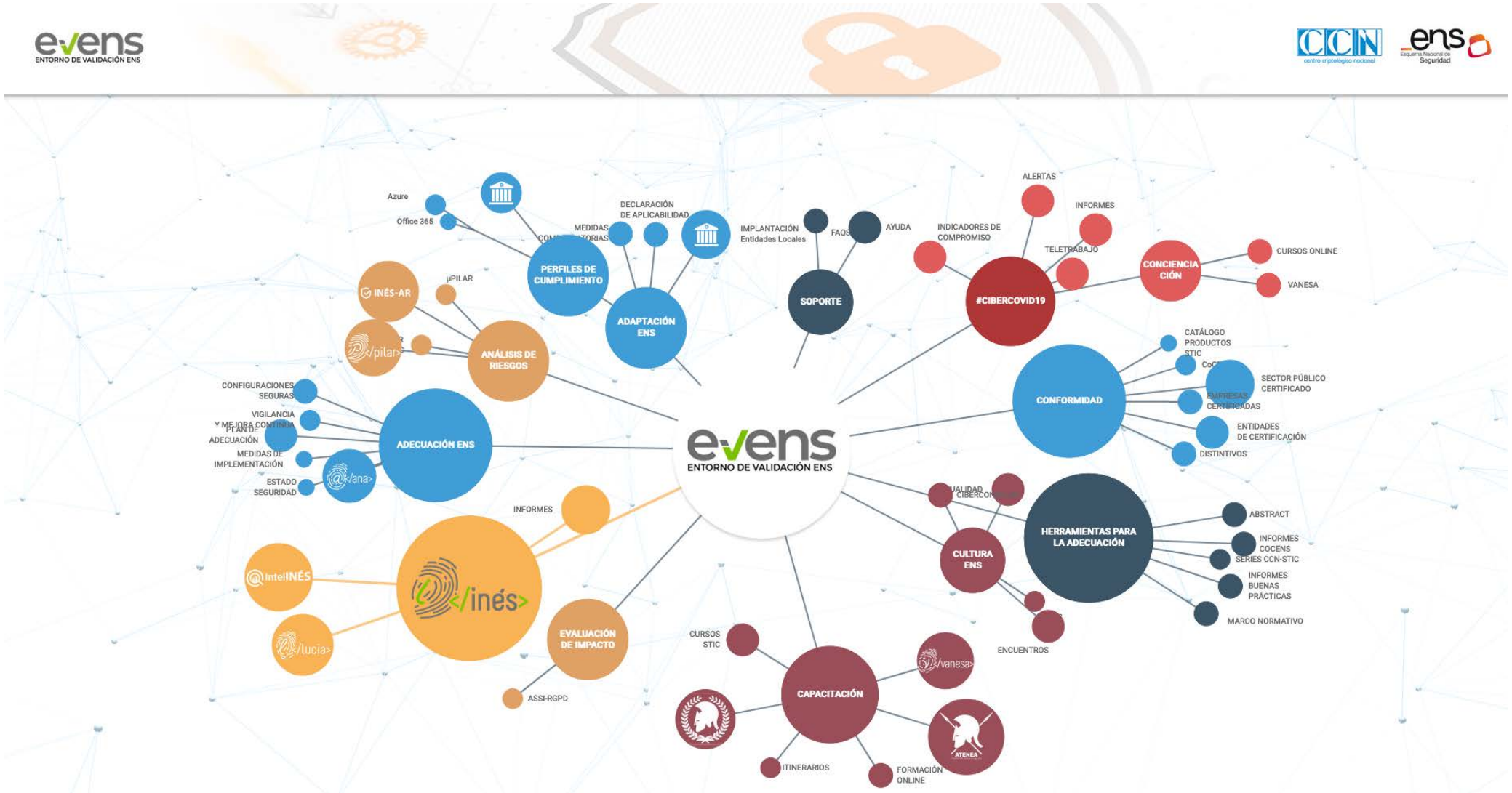
Tras el diseño e implantación del ENS para EELL, han surgido iniciativas para su aplicación directa en diferentes proyectos pilotos, como organismos superiores de los que dependen los diferentes órganos.





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

Prevención Proactiva: cumplimiento y vigilancia

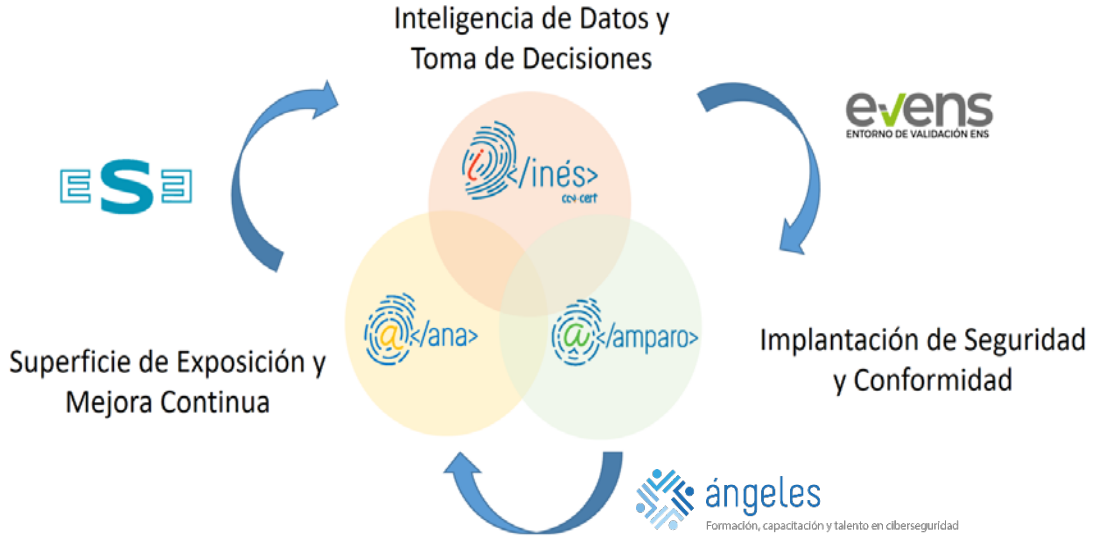


Conclusiones

- Implementar seguridad
- Medir superficie de exposición
- Sensibilización y capacitación
- Mejora Continua
- Toma de decisiones

Prevención Proactiva
Cumplimiento y Vigilancia

Gestión Continua



centro criptológico nacional

La importancia de Construir Comunidad

CN-CERT centro criptológico nacional

1. Aumentar la capacidad de Vigilancia.
2. Herramientas de Gestión Centralizada.
3. Política de seguridad.
4. Aplicar configuraciones de seguridad.
5. Empleo de productos confiables y certificados.
6. Concienciación de usuarios.
7. Compromiso de dirección (Dueños del Riesgo)
8. Legislación y Buenas Prácticas.
9. Intercambio de Información.
10. Trabajar como si se estuviera comprometido.

Muchas

Gracias

E-mails

servicios ciber@ccn.cni.es

ccn@ccn.cni.es

Web sites:

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es