

# El Esquema Nacional de Seguridad y la Formación

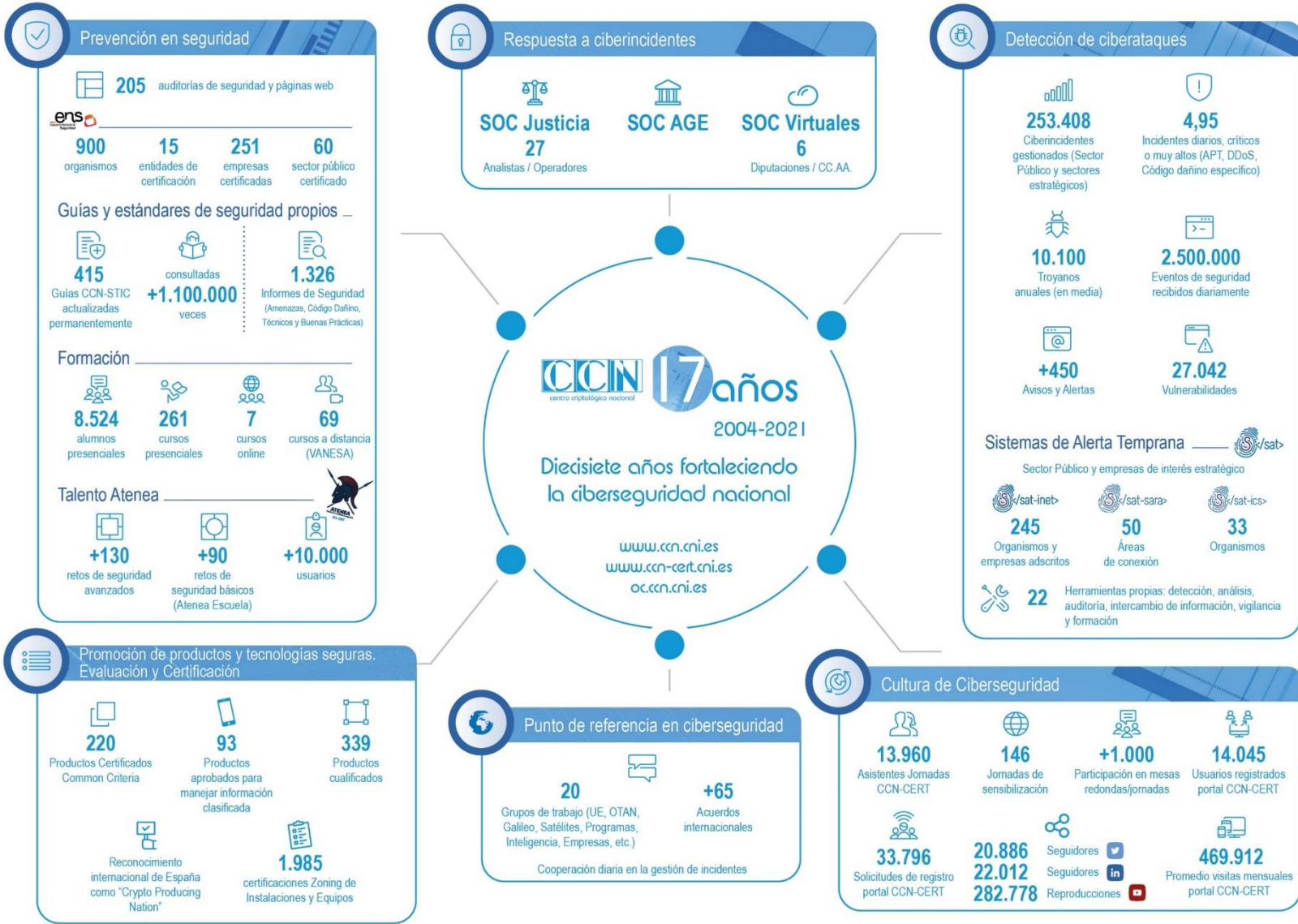
**Pablo López**

Jefe de Área de Normativa y Servicios de Ciberseguridad





# Centro Criptológico Nacional



# Transformación digital y ciberseguridad

Personas, procesos, tecnología, datos y ciberseguridad

## Datos

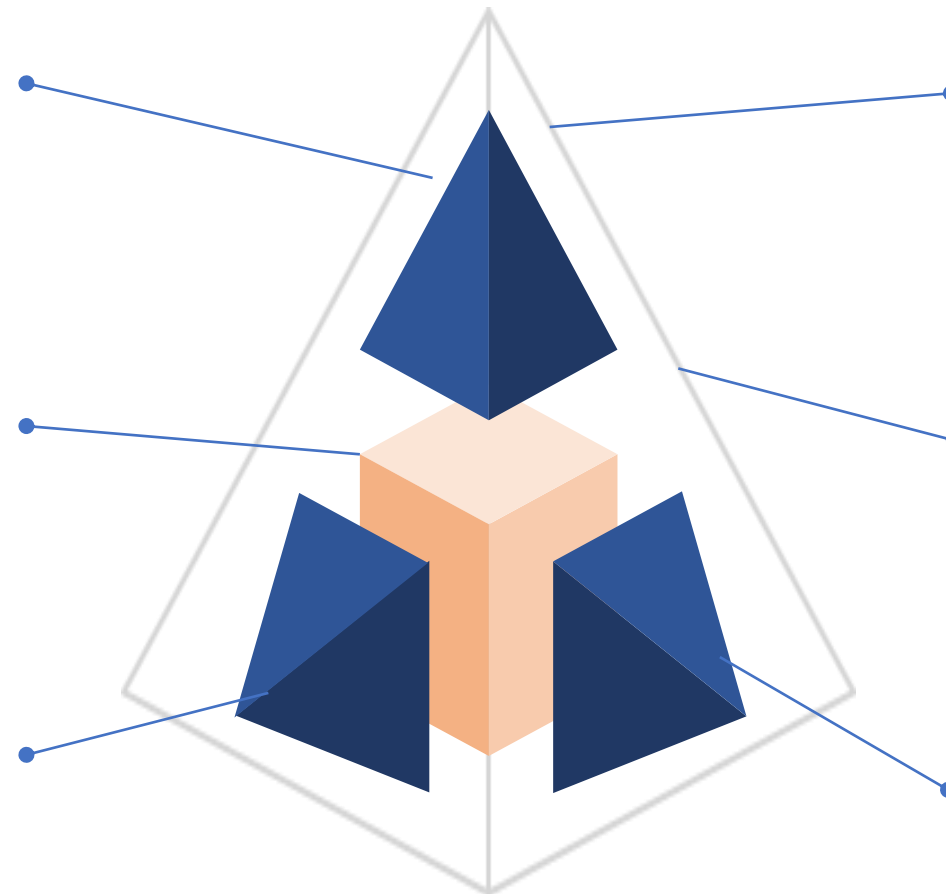
- Datos para nuevos y mejores servicios, decisiones, políticas públicas, transparencia y reutilización
- Estrategia de gestión del dato, CDO,...

## 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

# Por qué es necesaria la seguridad de información y servicios

- Los ciudadanos esperan que los servicios se presten en condiciones de confianza y seguridad equivalentes a las que encuentran cuando se acercan personalmente a las oficinas de la Administración.
- Buena parte de la información y los servicios manejados por las AA.PP. **constituyen activos nacionales estratégicos.**
- Los servicios se prestan en un escenario complejo que requiere cooperación.
- La información y los servicios están sometidos a riesgos provenientes de acciones malintencionadas o ilícitas, errores o fallos y accidentes o desastres.
- Es necesaria una **gestión continuada de la seguridad.**



# 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**

# 10 años del

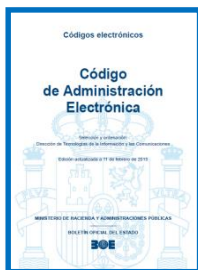


## Actualizado en 2015

- ✓ 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

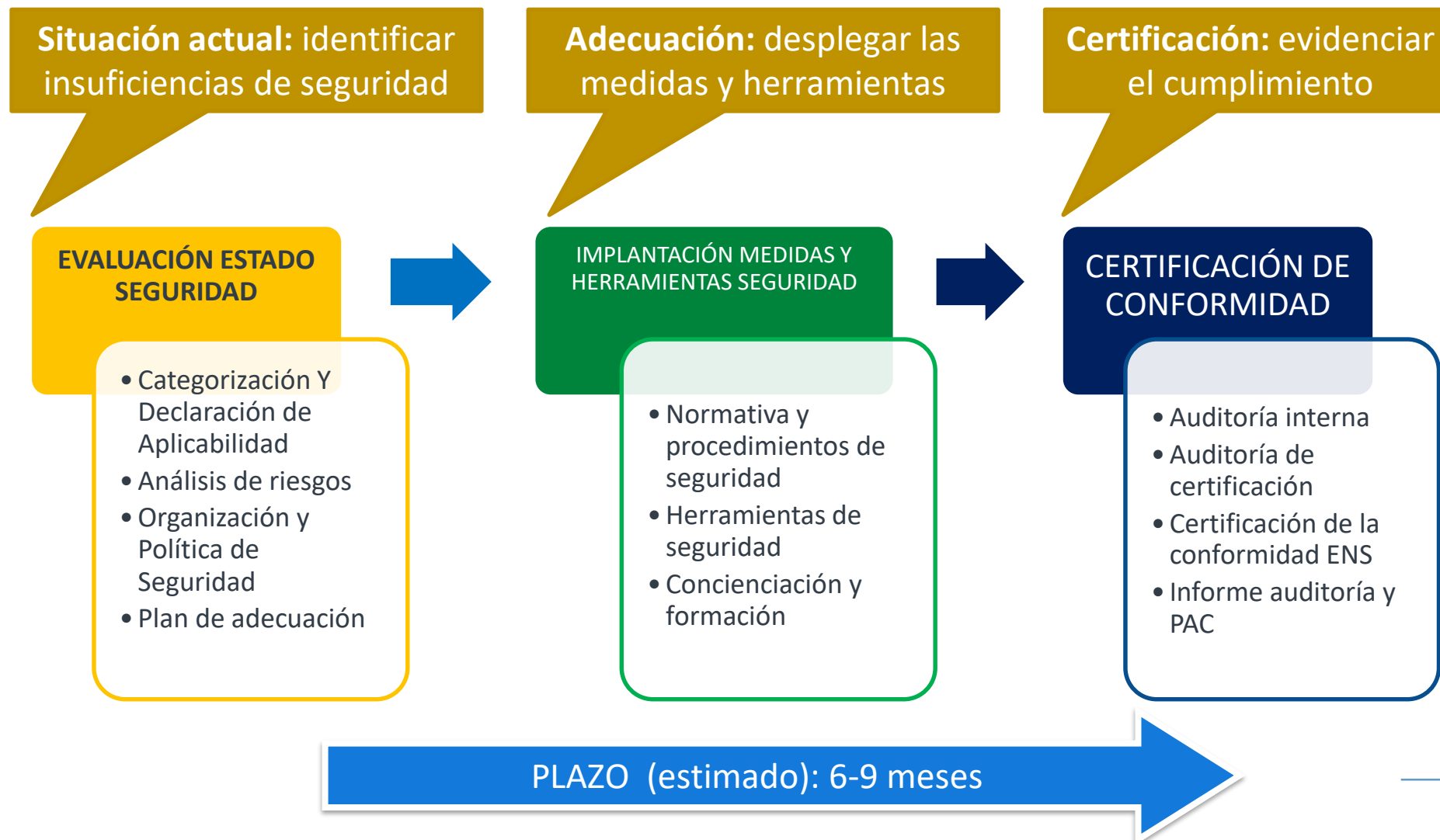
- ✓ 6 ediciones del informe INES
- ✓ 768 entidades en 2018, 30% más que en 2017
- ✓ 1080 en 2019, 22 % más que en 2018
- ✓ La campaña permanece abierta todo el año

## Soporte

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



# Hoja de Ruta de la Adecuación



## Clave: Declaración de Aplicabilidad



Documento que formaliza la **relación de medidas de seguridad que resultan de aplicación** al sistema de información, conforme a su categoría, y que se encuentran recogidas en el Anexo II del Real Decreto 3/2010, de 8 de enero, que lo regula.

Se deberá revisar tras la realización del Análisis de Riesgos, modulando el riesgo que se quiere asumir, dando lugar a la **Declaración de Aplicabilidad Final**:

- Criterios de aplicabilidad
- Medidas que no aplican
- Medidas añadidas
- Medidas adaptadas
- Medidas compensatorias
- Medidas complementarias de vigilancia

CCN-CERT BP/14 Declaración de Aplicabilidad en el ENS (Perfil de Cumplimiento)

Así mismo el CCN deja a disposición, como Anexos al documento, una Plantilla y un Simulador para realizar la Declaración de Aplicabilidad.



# Servicios en Cloud – Escenario de Nube

1

## Escenario de Cloud Sensible

Recoge los servicios que componen el escenario, requisitos de seguridad generales, operativa y aprovisionamiento del tenant y explicaciones sobre el uso del bastionado y aprovisionamiento automático.



2

## Requisitos de Seguridad

Recoge la especificación completa de las configuraciones de seguridad de cada uno de los servicios del tenant y la explicación de sus valores.



3

## Plantillas de configuración

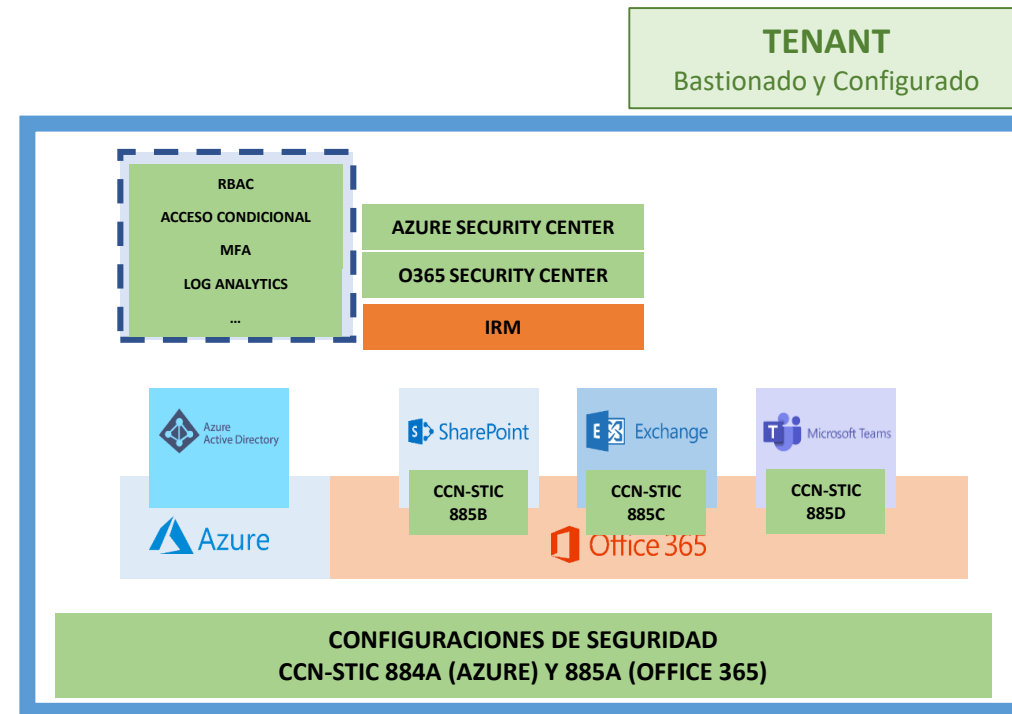
Plantillas para la configuración y bastionado automático del tenant en base a las necesidades específicas de cada organismo.



4

## Scripts de Bastionado Automático

Conjunto de Scripts para ejecutar el bastionado y el aprovisionamiento automático del tenant y en base a la información incluida en las plantillas de configuración.





## 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**



### Determinación de la superficie de exposición

Identificando **VULNERABILIDADES**, **DEFICIENCIAS DE CONFIGURACIÓN** y **BRECHAS DE SEGURIDAD** de los Sistemas TIC. Análisis de tráfico de red **EN BUSCA DE ANOMALÍAS**.



### Cibervigilancia

Prospección del ciberespacio (redes sociales) haciendo **PROSPECTIVA DE TENDENCIAS** de la ciberamenaza. Identificación información maliciosas (**MALINFO**) dirigida a **SOCAVAR LA SEGURIDAD** y **ESTABILIDAD** del ecosistema.



### Ciberinteligencia

Revisión completa de cuál es la **SUPERFICIE DE ATAQUE** de una entidad. Identificar las debilidades y carencias que puede conocer un atacante a priori (**FASE DE RECONOCIMIENTO**).

# Prevencción Proactiva: Cumplimiento y Vigilancia



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



## Gestión Continua de la Seguridad



*Extender una cultura de protección dentro de la organización.*



/inés>  
 /pilar>  
 /amparo>  
 /clara>  
 /rocío>  
 /emma>  
**EMMA-VAR**  
 /ana>  
 /carla>

/sat-inet>  
 /sat-sara>  
 /sat-ics>

**Sonda distribuida**

/gloria>  
 /mónica>  
 /ada>  
 /maria> /marta>

**2020**

/carmen>  
 /claudia>

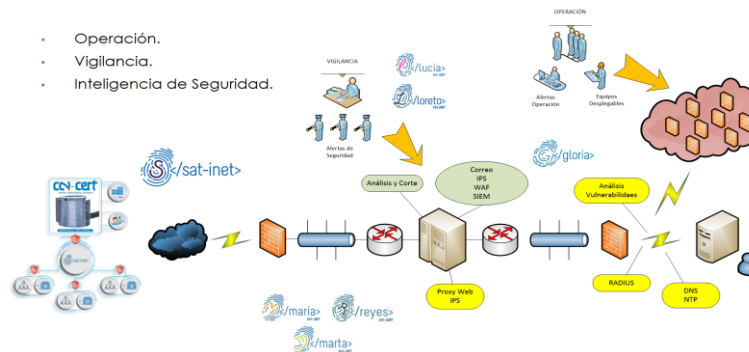
/paula>  
**Alicia**

**Soluciones basadas en IA**

**2021**

/lucía>  
 /loreto>  
 /reyes>

- Operación.
- Vigilancia.
- Inteligencia de Seguridad.



/vanesa>  
 ATENEA  
 Formación y Talento en Ciberseguridad

/ángeles>  
 Formación y Talento en Ciberseguridad

/elena>  
 Formación y Talento en Ciberseguridad

## Las "chicas" del CCN que nos ayudan a estar protegidos

por Comunicación doingIT en ciberseguridad, Ciberseguridad para todos, RGPD, tecnología en 23/10/2019



Estos días leía un artículo en el que ponía que menos del 25% de las mujeres se dedican a la ciberseguridad. Quizás tenga mucho que ver también ese número con el hecho de que el número de mujeres en carreras tecnológicas (las llamadas STEM) es muy pequeño. Pero este artículo no va de eso, en doingIT tenemos a una de las que suma a ese 25%, por lo que no nos podemos quejar ... este artículo va de Pilar, Carmen, Lucía, Loreto .... ¿Quiénes son?

## Gestión Continua de la Seguridad



**Determinación  
Activos  
Esenciales**



**Salvaguardas  
(AR Residual)**



**Superficie de  
Exposición**



**Adaptación al  
Puesto de  
Trabajo**



**Contexto de la  
Amenaza  
(Incidentes)**



**Protección y  
Trazabilidad del  
Dato**

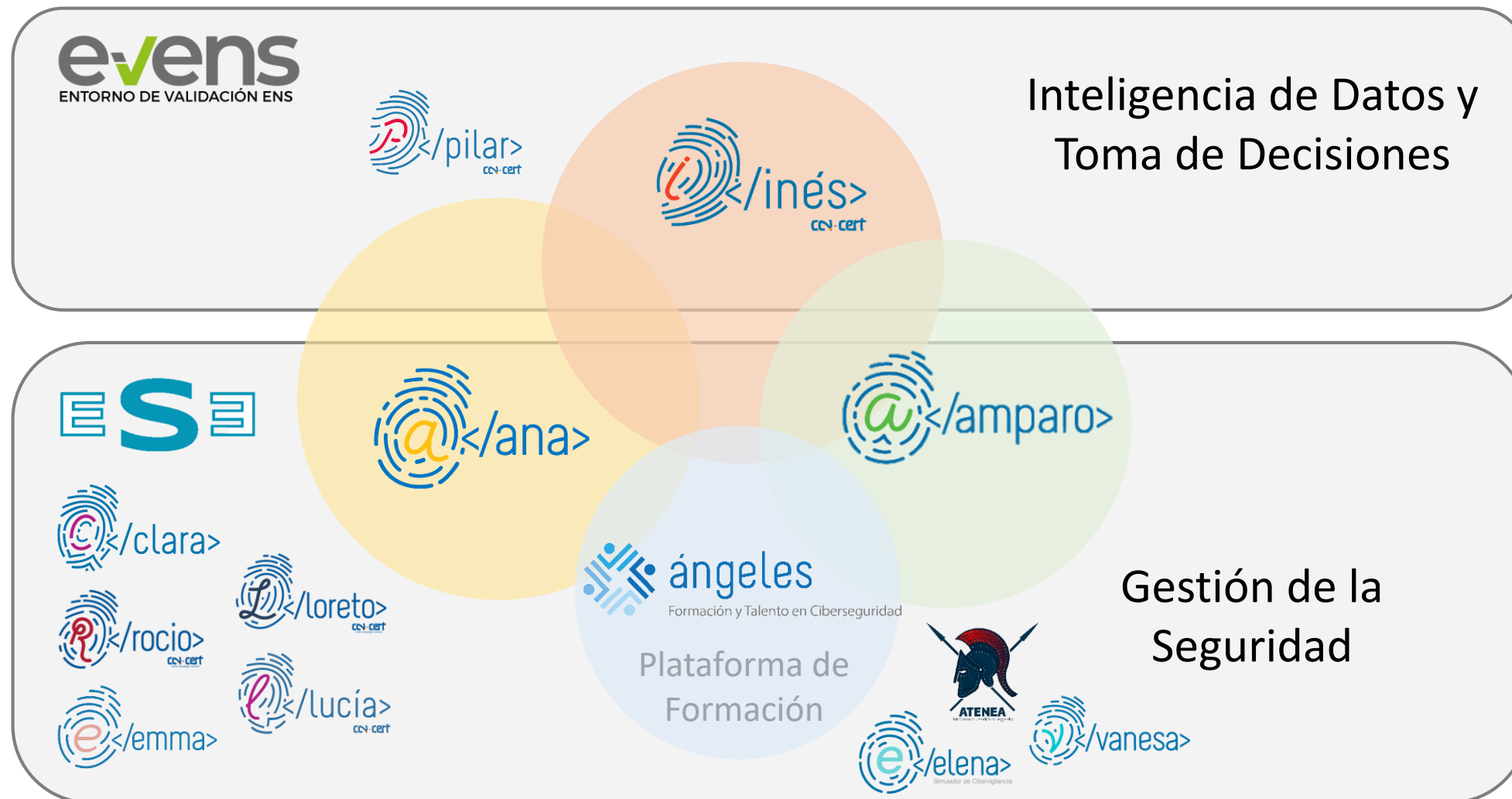


**Evolución  
Dinámica  
(Mejora Continua)**





# Gestión Continua de la Seguridad



# Necesidad de Evaluación Continua

ANA - Superficie de Exposición

### Gestión de Conformidades

Sistemas certificados	Sistemas en APS	Sistemas en proceso	No acreditados
<b>4</b>	<b>4</b>	<b>5</b>	<b>5</b>

Próximos a caducar: 1  
Próxima inspección en: 48 Días

### Mejora Continua

### Estado de cumplimiento

Cumplimiento	Correcto	Incorrecto
<b>73%</b>	<b>14</b>	<b>3</b>

Número de dispositivos: 17

### Entidades dependientes

Entidades	Equipos	Cumplimiento
<b>6</b>	<b>54</b>	<b>72%</b>

Accesos bloqueados: 47

### Soporte de vulnerabilidades

- CVE-2019-14586 - EDK II 23/11/2020
- CVE-2019-3689 - SUSE Linux 18/11/2020
- CVE-2020-26072 - Cisco 18/11/2020
- CVE-2020-26075 - Cisco 18/11/2020

### Gestión de vulnerabilidades

Críticas	Altas	Medias
<b>1</b>	<b>9</b>	<b>15</b>

Bajas: 112  
Sin relevancia: 0

### Evolución de vulnerabilidades

## METODOLOGÍA

# </ana>

Metodología de trabajo:

### CONOCER

antes de empezar

### INSPECCIONAR

de forma estandarizada y metodológica

### HOJA DE RUTA

Con la entidad, el objetivo último es minimizar el riesgo

### ACOMPañAMIENTO

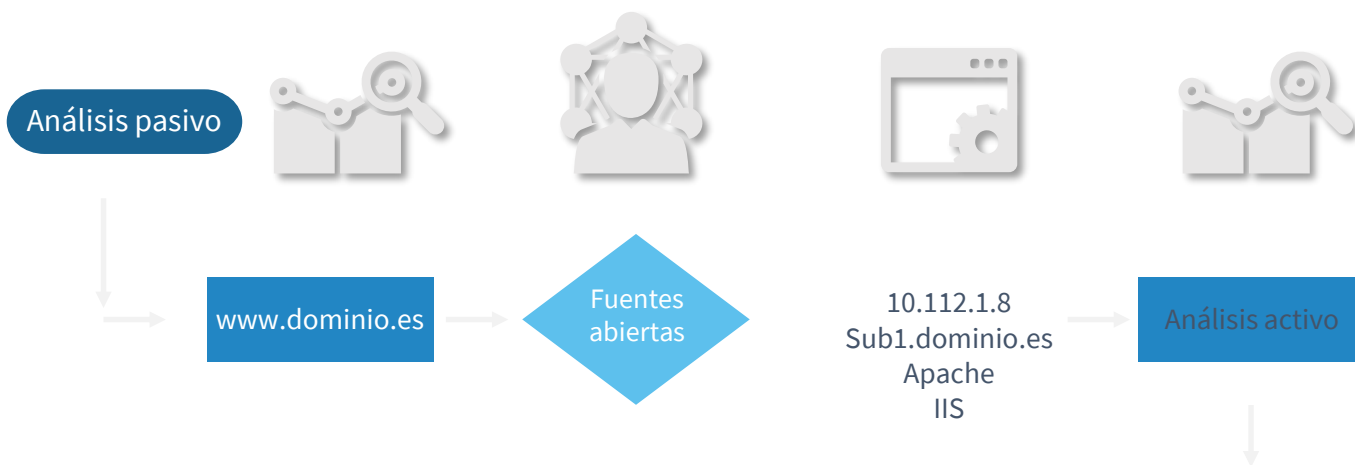
Durante la ejecución del plan establecido







# Descubrimiento automático De la superficie de exposición



Como funciona el descubrimiento de la superficie de exposición externa

## CONFIGURACIÓN



### Definición

De una manera sencilla, se introducen los parámetros de configuración de los dominios a inspeccionar. Esta configuración se realiza desde ANA determinando los tipos de análisis a realizar (pasivos y activos)

## Lanzamiento

ANA se comunica con el módulo de ejecución y le transmite los parámetros de configuración previamente definidos



## DESCUBRIMIENTO

## IMPORTACIÓN



### Incorporación de datos


Se incorporan los datos a ANA de una manera automática incorporándose activos, servicios y vulnerabilidades

## Panel de control

ANA visualizará los resultados en el panel de control, desde donde se podrá visualizar y descargar los informes de resultados del descubrimiento



## VISUALIZACIÓN



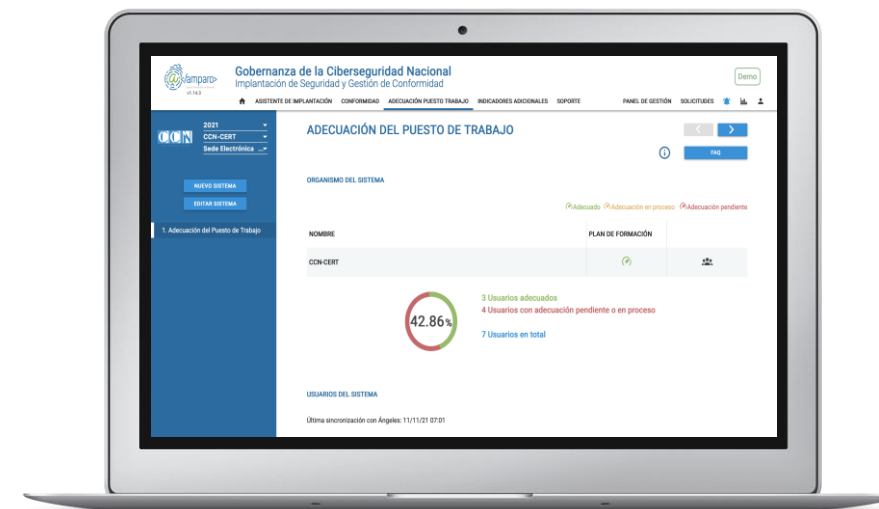
Medir, Mejora  
Continua y Vigilar...  
**claves para superar la  
incertidumbre**

---

# *La importancia de Medir la Seguridad*







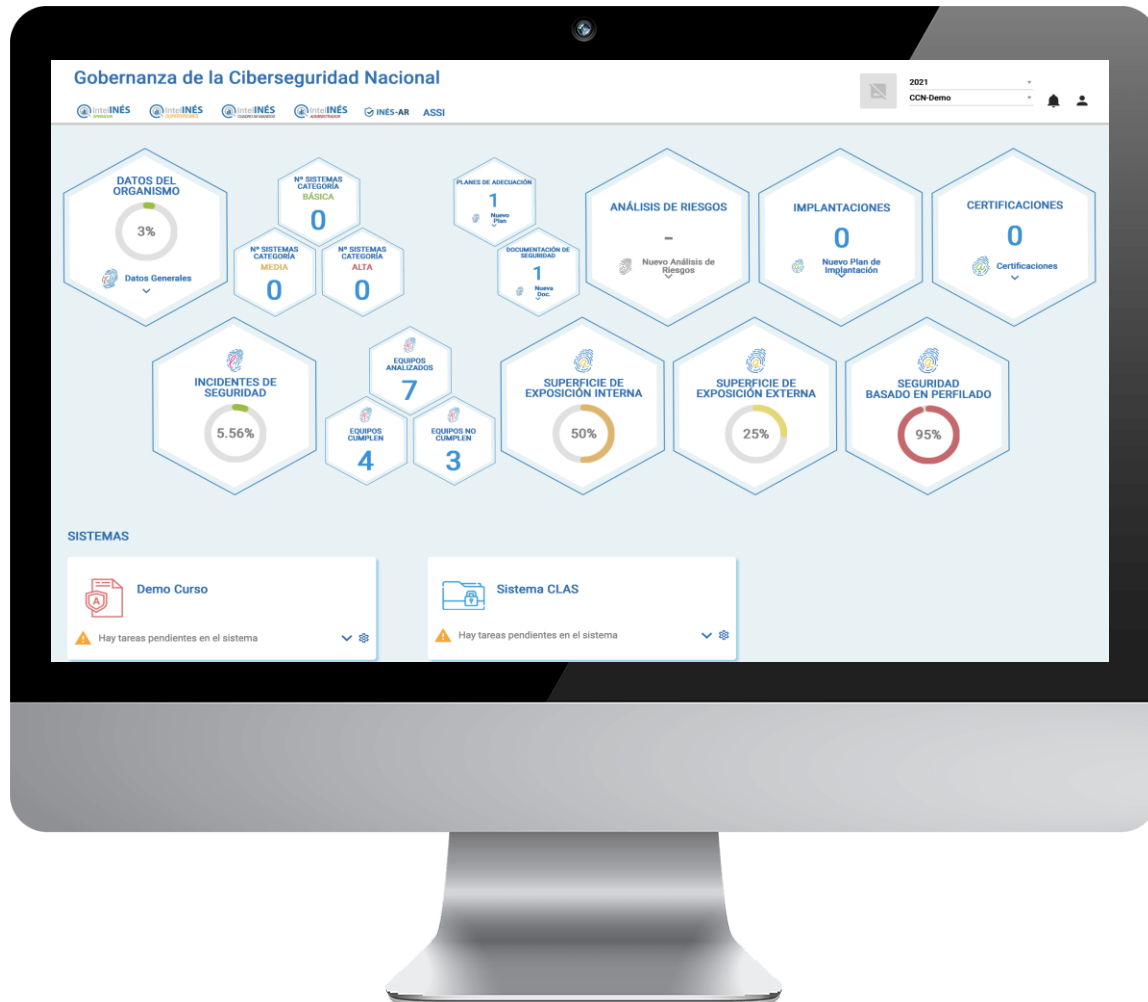
- El CCN-CERT cada vez ofrece más servicios que buscan facilitar la implementación de seguridad para, en última instancia, conseguir el cumplimiento con ENS.
- Entorno que **engloba todo lo referente al ENS** para facilitar el acceso a la información y la correcta implantación y validación de normativa.
- **Características principales:**
  - Simplicidad y potencia.
  - Facilidad de navegación y búsqueda.
  - Colaboración.
  - Reutilización de recursos.
  - Indicadores de situación.
  - Estrategia y ayuda en la toma de decisiones.

Necesidad de Métricas



- La solución INES facilita la **recogida y consolidación de información** para el Informe del Estado de la Seguridad.
- A partir de 2020, **campaña abierta todo el año para cargar/actualizar datos** por parte de las entidades, solo se cierra para consolidar la base de datos en febrero de cada año.
- Las **EE.LL. y las universidades** son las entidades que necesitan realizar un mayor esfuerzo para conseguir la adecuación con el ENS.
- Las **auditorías de adecuación** empiezan a formar parte del calendario de ciberseguridad de las entidades.





- Se dotará a la administración pública de una potente solución que **ayude a simplificar** todos los aspectos referentes al ENS, incluida la toma de decisiones.
- Los organismos sabrán su **estado de cumplimiento y madurez** en cada momento.
- El objetivo principal es **facilitar la integración** de todo lo relativo y relacionado con el ENS.

## Explotación de la Información – Inteligencia de los datos

- ✓ Informes del estado de seguridad
- ✓ Explotación y análisis de los datos
- ✓ Extracción de conclusiones
- ✓ Toma de decisiones en base al análisis





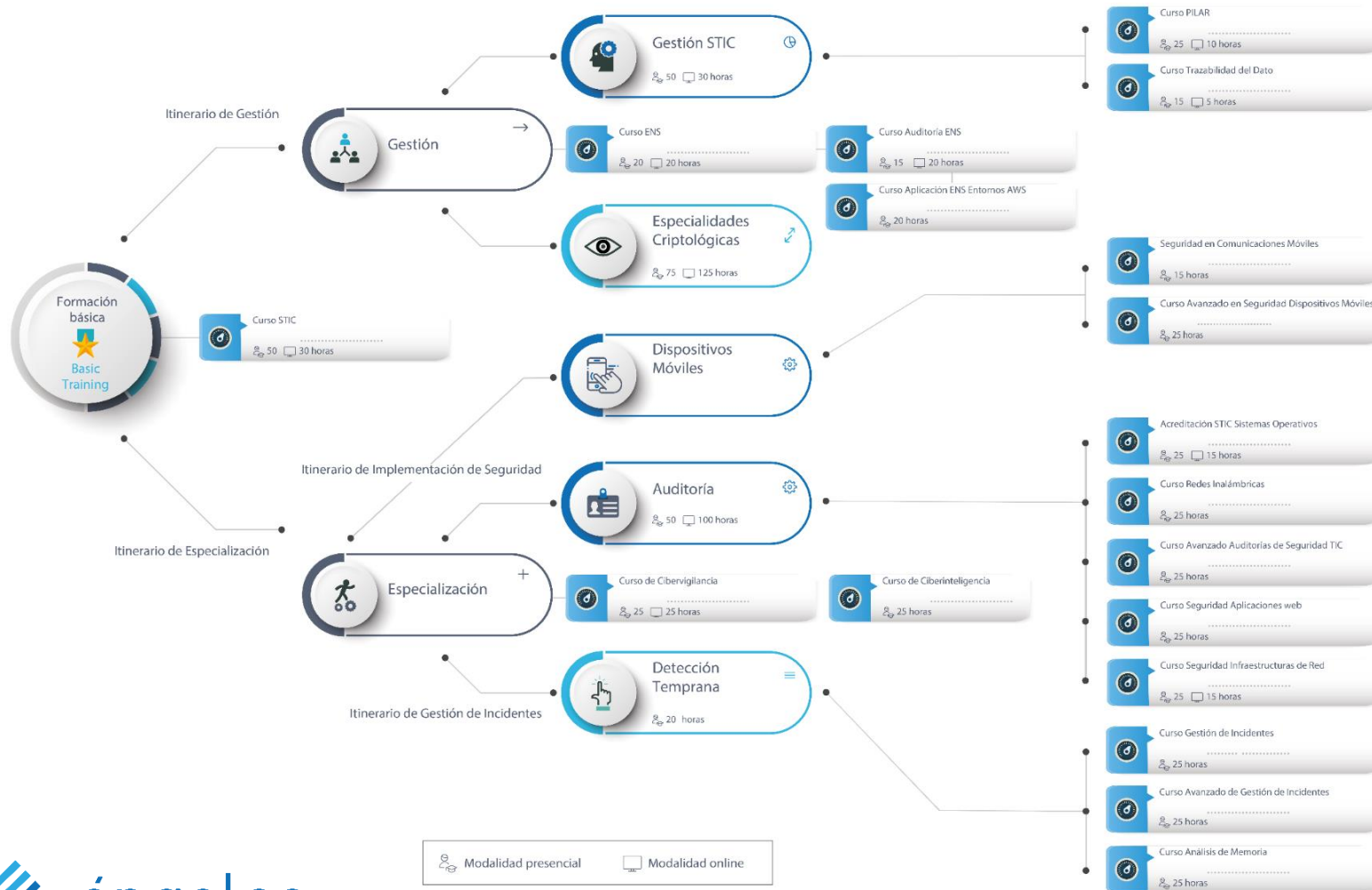
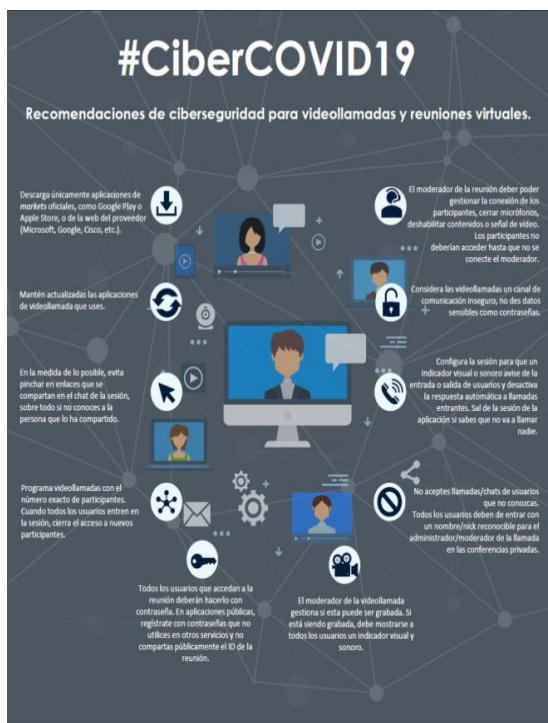
ángeles

Formación, capacitación y talento en ciberseguridad

# Plataforma de formación



# La concienciación es necesaria, pero la **EDUCACIÓN** ya no es una opción... es una **OBLIGACIÓN**.



# </ÁNGELES> Plataforma de formación

Formación

Talento

Simulación

Ciberconsejos

Buenas prácticas

Usuarios Registrados



En ÁNGELES se encuentran disponibles diferentes cursos online para que los usuarios puedan mejorar su nivel de conocimiento en diferentes ámbitos de la ciberseguridad.



Al mismo tiempo, a través de ÁNGELES los usuarios pueden visualizar webinars online sobre diferentes temáticas en torno a la ciberseguridad.



# </ÁNGELES> Plataforma de formación

Formación

Talento

Simulación

Ciberconsejos

Buenas prácticas

Usuarios Registrados

ATENEA, es la plataforma del CCN-CERT en la que podrás demostrar tu conocimiento y destreza ante diferentes desafíos de seguridad. Aquí encontrarás retos de distinta dificultad y de muy diversas temáticas: Criptografía y Esteganografía; Exploiting, Forense, Análisis de tráfico, Reversing, etc.

ATENEA ha sido desarrollada por el CCN-CERT con el fin de que cualquier persona que tenga inquietudes en el campo de la ciberseguridad pueda poner a prueba su conocimiento. Entre sus principales objetivos se encuentran:

- Concienciar al personal TIC sobre los riesgos existentes en este campo.
- Involucrar a los profesionales con experiencia en ciberseguridad con el fin de que puedan demostrar su ingenio y capacidad.
- Mostrar a las personas con menos experiencia en la seguridad TIC que los retos son divertidos y que la seguridad no es una ciencia secreta que nunca entenderían.



# </ÁNGELES> Plataforma de formación

Formación

Talento

Simulación

Ciberconsejos

Buenas prácticas

Usuarios Registrados

Es la plataforma del CCN-CERT para practicar técnicas, tácticas y procedimientos en labores de ciberinvestigación. Permite a los usuarios tomar el rol del analista en un entorno simulado de investigación basado en situaciones reales, que posibilita desarrollar y poner en práctica las técnicas, tácticas y procedimientos necesarios para realizar labores de ciberinvestigación.

## Sistema



Situaciones reales simuladas



Con variados escenarios



Intuitivo y robusto



Testado por expertos



## Incluye



Todos los recursos necesarios desde el comienzo



Estadísticas detalladas



Ranking de mejores participantes

ELENA es un entorno de simulación de técnicas de investigación y análisis en cibervigilancia dirigido específicamente a la formación de analistas.

Recrea itinerarios que emulan tareas que un analista o investigador de cibervigilancia se encontrará en su trabajo, con el propósito de entrenar habilidades en los siguientes aspectos:

- 1) Investigar la identidad real tras un alias, o el origen y alcance de un contenido amenazante que se está divulgando en redes sociales.
- 2) Técnicas de investigación para desanonimizar perfiles, como la interrogación a bases de datos sobre datos de registro y/o de configuración de un sitio web, o los límites de obtención de datos en redes sociales.
- 3) Técnicas de análisis para optar por itinerarios eficientes de investigación y extraer conclusiones relevantes a partir del cruce eficaz de información procedente de distintas fuentes digitales.

# </ÁNGELES> Plataforma de formación

Formación

Talento

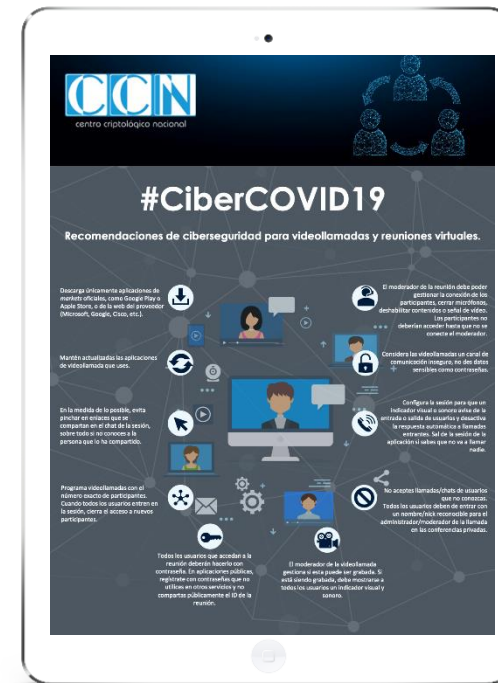
Simulación

Ciberconsejos

Buenas prácticas

Usuarios Registrados

El CCN también ofrece a través de ÁNGELES diferentes recomendaciones para prevenir y detectar vulnerabilidades y riesgos asociados al uso diario de las nuevas tecnologías.



# </ÁNGELES> Plataforma de formación

Formación

Talento

Simulación

Ciberconsejos

Buenas prácticas

Usuarios Registrados



CCN-CERT BP/01 Principios y recomendaciones básicas en Ciberseguridad

Informe  
Otros recursos



CCN-CERT BP/02 Correo electrónico

Informe  
Otros recursos



CCN-CERT BP/03 Dispositivos móviles

Informe  
Otros recursos



CCN-CERT BP/04 Ransomware

Informe



CCN-CERT BP/05 Internet de las Cosas

Informe



CCN-CERT BP/06 Seguridad y riesgos de los navegadores web

Informe



CCN-CERT BP/07 Recomendaciones implementación HTTPS

Informe



CCN-CERT BP/08 Redes Sociales

Informe  
Otros recursos



CCN-CERT BP/09 Recomendaciones de protección DoS en cortafuegos

Informe



CCN-CERT BP/10 Recomendaciones de seguridad para CDN

Informe



CCN-CERT BP/11 Recomendaciones redes WIFI corporativas

Informe



CCN-CERT BP/12 Cryptojacking

Informe  
Otros recursos

Asimismo, desde esta plataforma, los usuarios podrán descargarse guías de Buenas Prácticas, elaboradas por el CCN, cuyo objetivo es ayudar a hacer un uso más seguro de la tecnología. En estas guías, se profundiza en las recomendaciones ofrecidas en los ciberconsejos.

# </ÁNGELES> Plataforma de formación

Formación

Talento

Simulación

Ciberconsejos

Buenas prácticas

Usuarios registrados

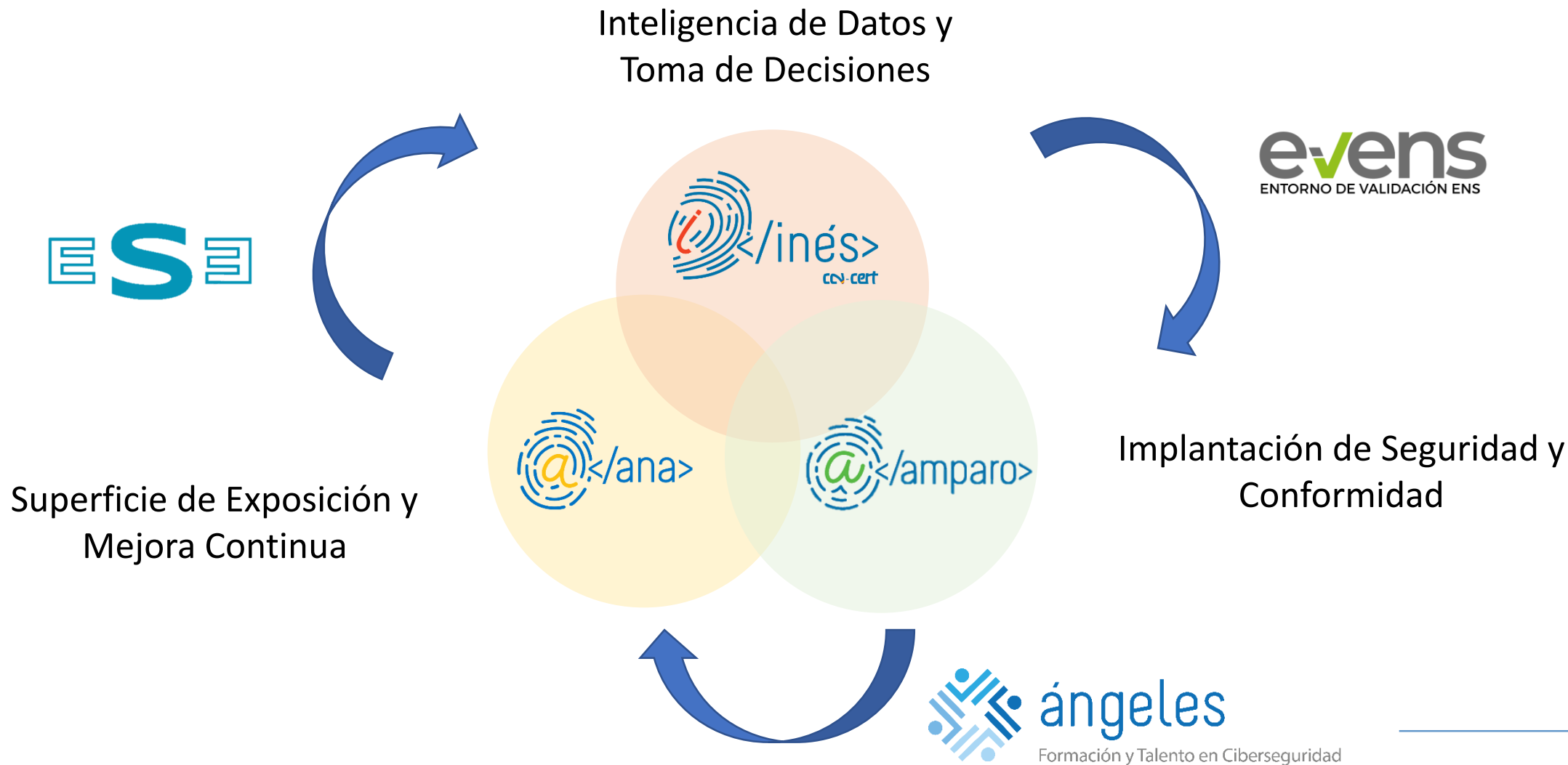


Los usuarios registrados en ÁNGELES también podrán descargar desde ÁNGELES los certificados de finalización de las actividades formativas. Al mismo tiempo, desde esta área personal, los usuarios podrán acceder a su expediente académico, en el que especifican las horas de formación recibidas a través de ÁNGELES y el estado de los cursos realizados.

Asimismo, desde ÁNGELES los usuarios podrán descargar su expediente académico en formato PDF, que se actualiza automáticamente con la información y los detalles de los nuevos cursos que los usuarios realizan en la plataforma.



# Gestión Continua de la Seguridad





## Contacto

---

**Pablo López**

Jefe Área Normativa y Servicios de Ciberseguridad

[jnormativa@ccn.cni.es](mailto:jnormativa@ccn.cni.es)