ángeles
Formación y Talento en Ciberseguridad

e-vens
ENTORNO DE VALIDACIÓN ENS

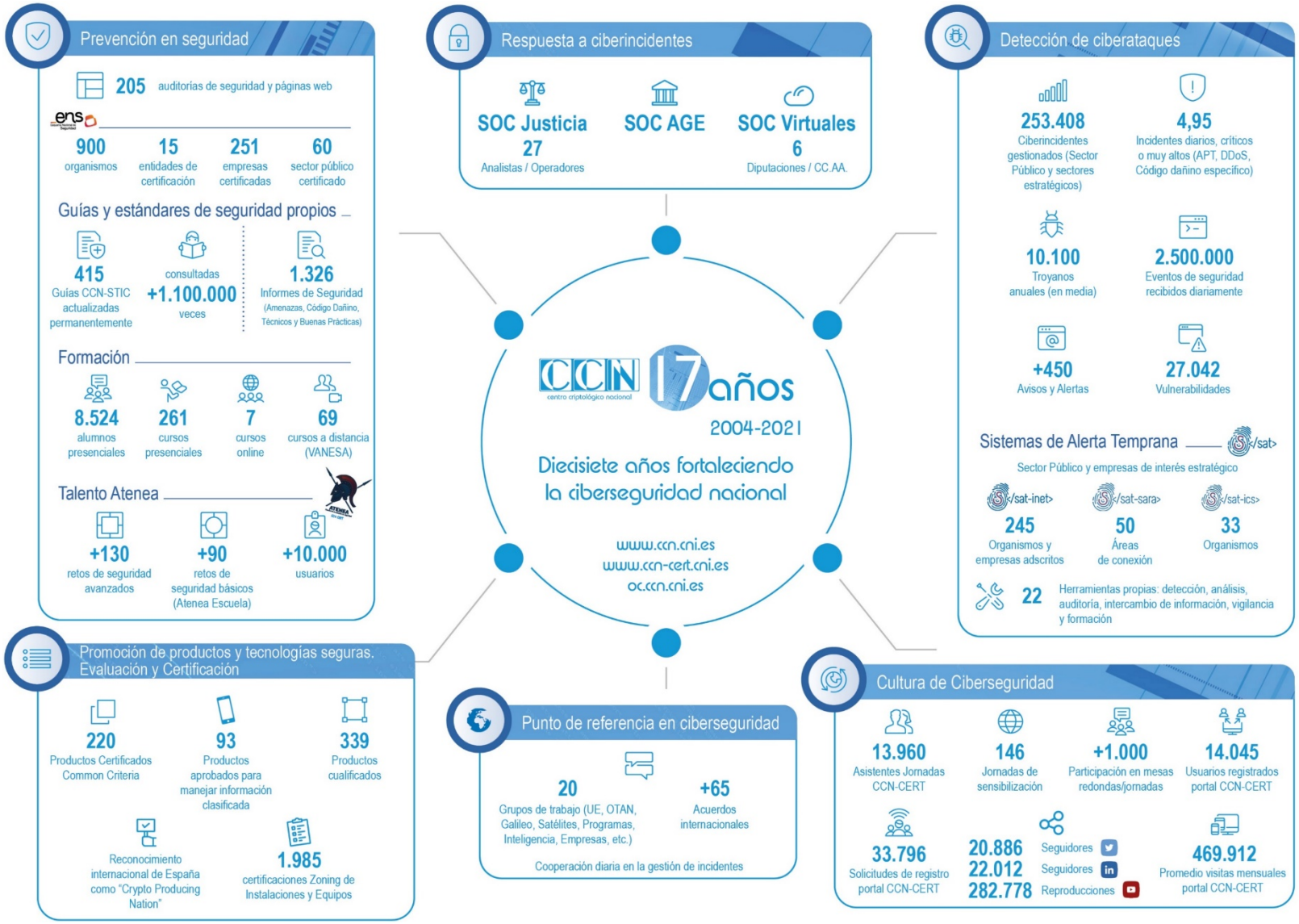
Prevención Proactiva

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

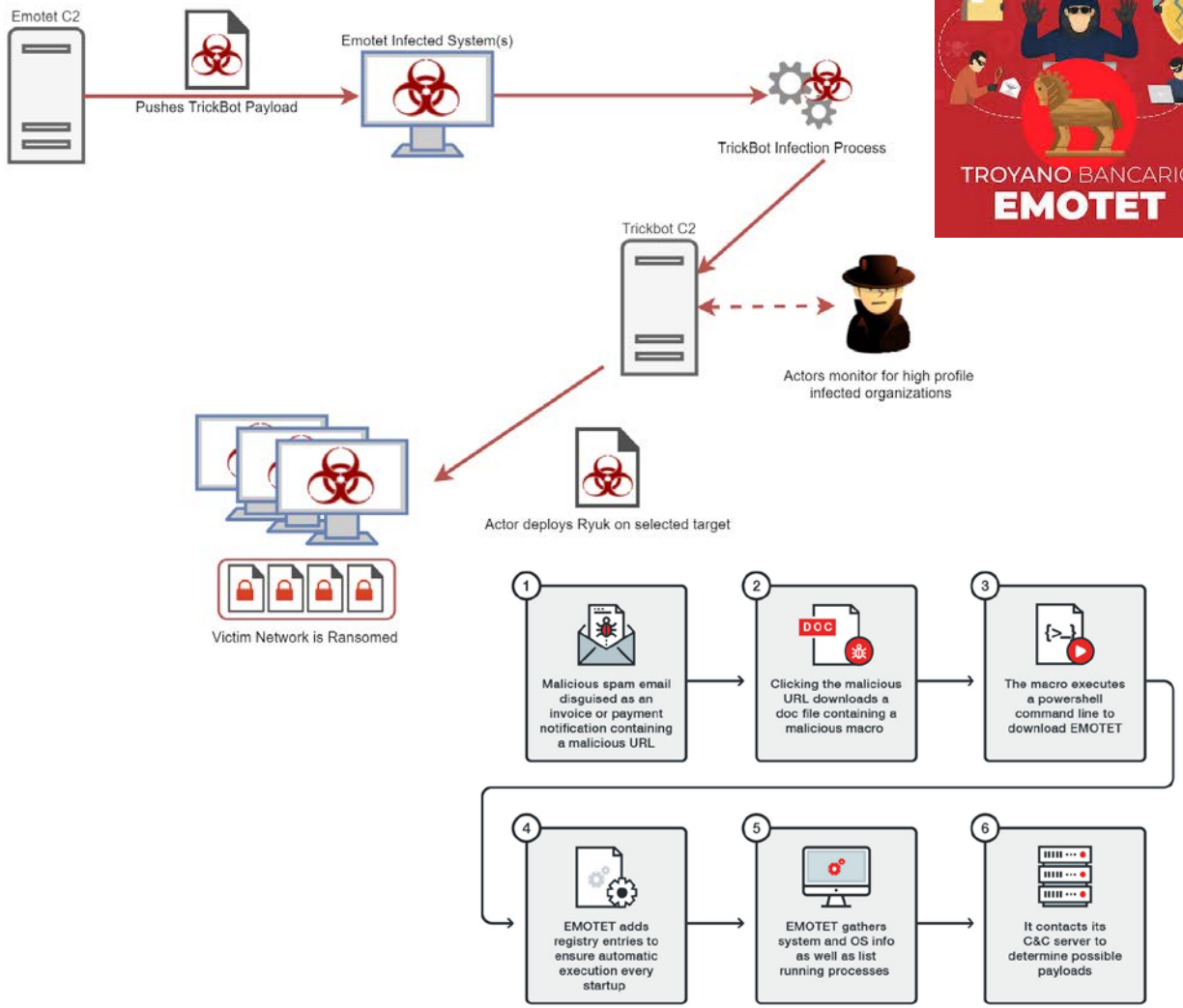
Interoperabilidad

- 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

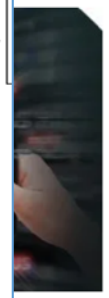
Situación de Seguridad – La realidad es muy tozuda…



El FBI investiga ataque al servicio de aguas y alcantarillado de North Carolina

16 octubre, 2018 Por **Hispasec** — **Deja un comentario**

Funcionarios federales están trabajando conjuntamente con una empresa local encargada del servicio de aguas de North Caroline, después de que se hayan detectado intrusiones en sus



expuso en un comunicado que habían

Home › Malware

"Emotet" Banking Malware Steals Data Via Network Sniffing

By Eduard Kovacs on June 30, 2014

Share Tweet Recomendar 19 RSS

A new banking malware spotted by Trend Micro intercepts and logs outgoing traffic in an effort to harvest sensitive information from victims.

Dubbed "Emotet" by the security company, the Trojan doesn't use phishing or form field insertion like other financial malware. Instead, it relies on network sniffing because this technique makes its malicious activities more difficult to detect.

The threat is distributed by cybercriminals with the aid of spam emails apparently related to money transfers or shipping invoices. The bogus notifications contain links that point to websites set up to serve the malware to victims.

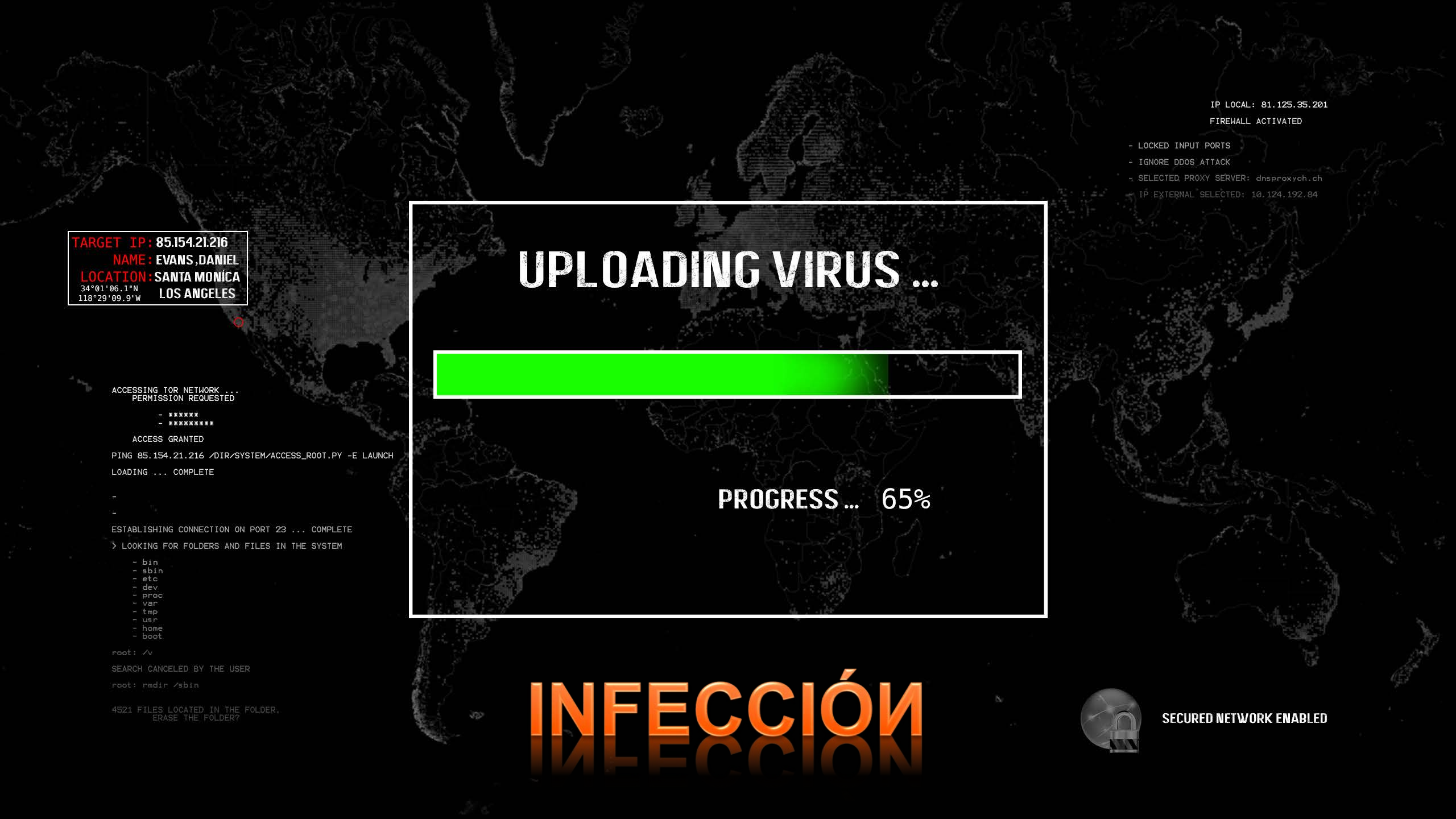
After infecting a computer, Emotet downloads a configuration file containing information on the targeted financial organizations. The files analyzed by Trend Micro contained a list of banks from Germany, this being the most affected country. Data from the company's Smart Protection Network indicates that while most infections are in the EMEA region, there are victims in the APAC region and North America as well.

Another component file downloaded by Emotet on infected systems is a DLL file that's responsible for intercepting and stealing outgoing network traffic. The component injects itself into all processes, including Web browsers in order to compare accessed websites against the list of organizations contained in the configuration file. When a match is found, the entire content of the website, including the data entered by the victim on it, is intercepted and saved.

Researchers have noted that the banking Trojan is also capable of intercepting data sent over secure connections by hooking APIs such as PR_OpenTcpSocket, PR_Write, PR_Close, PR_GetNameForIndentity, Closesocket, Connect, Send and WsaSend to monitor network traffic.

The stolen data is encrypted and placed in a registry entry, while component files are placed in separate registry entries, Trend Micro said.

CCN centro criptológico nacional


IP LOCAL: 81.125.35.201
FIREWALL ACTIVATED
- LOCKED INPUT PORTS
- IGNORE DDOS ATTACK
- SELECTED PROXY SERVER: dnsproxych.ch
- IP EXTERNAL SELECTED: 10.124.192.84
TARGET IP: 85.154.21.216
NAME: EVANS,DANIEL
LOCATION: SANTA MONICA
34°01'06.1"N
118°29'09.9"W
LOS ANGELES
UPLOADING VIRUS ...
PROGRESS ... 65%
ACCESSING IOR NETWORK ...
PERMISSION REQUESTED
- ******
- *********
ACCESS GRANTED
PING 85.154.21.216 /DIR/SYSTEM/ACCESS_ROOT.PY -E LAUNCH
LOADING ... COMPLETE
-
-
ESTABLISHING CONNECTION ON PORT 23 ... COMPLETE
> LOOKING FOR FOLDERS AND FILES IN THE SYSTEM
- bin
- sbin
- etc
- dev
- proc
- var
- tmp
- usr
- home
- boot
root: /v
SEARCH CANCELED BY THE USER
root: rmdir /sbin
4521 FILES LOCATED IN THE FOLDER,
ERASE THE FOLDER?
INFECCIÓN
SECURED NETWORK ENABLED

La Infección es también Low Cost

bitcoin

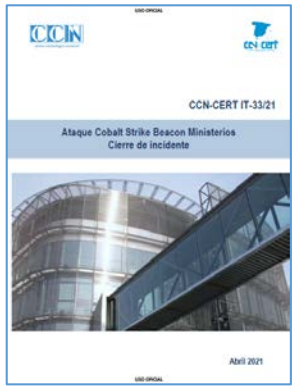
PWNED!

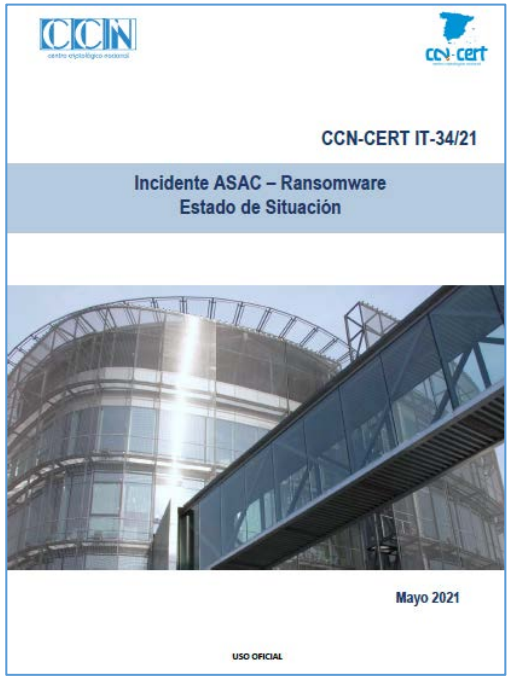
evilginx.

Dominio
+
VPS
+
Correo
+
1 hora trabajo

30 $

CCN
centro criptológico nacional

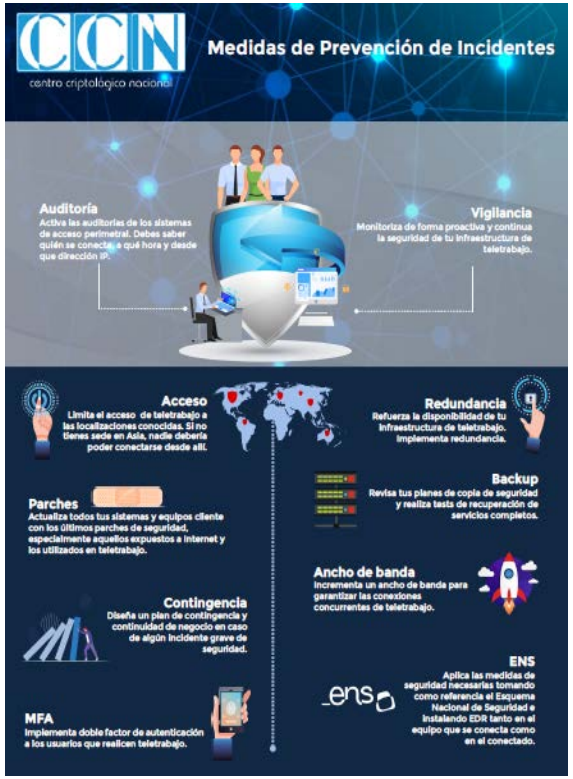




Ataques Cobalt Strike + Ransomware
¿Qué esta pasando?

1. **Compra de credenciales** de acceso remoto a la organización en el mercado negro.
2. Entrada en la red por un acceso remoto a la misma y **elevación de privilegios** a administrador en un servidor.
3. Instalación de **herramientas de control remoto** (ej. COBALT STRIKE) y movimiento lateral para controlar toda la red.
4. **Robo de información de la organización** (datos personales o propiedad industrial) que le permita la extorsión y fuerce el pago del rescate
5. **Cifrado de datos de la organización y solicitud de rescate**.

Lecciones aprendidas - Humildad para aprender



1. **Auditoría.** Activa las auditorías de los sistemas de acceso perimetral.
2. **Vigilancia.** Monitoriza de forma proactiva y continua la seguridad de la infraestructura de teletrabajo.
3. **Acceso. Limita el acceso de teletrabajo a las localizaciones conocidas**.
4. **Redundancia.** Refuerza la disponibilidad de tu infraestructura de teletrabajo.
5. **Parches.** Actualiza todos tus sistemas y equipos cliente con los últimos parches de seguridad, especialmente aquellos expuestos a Internet y los utilizados en teletrabajo.
6. **Respaldo/Backup.** Revisa tus planes de copia de seguridad y realiza test de recuperación.
7. **Ancho de banda.** Incrementa un ancho de banda para garantizar las conexiones concurrentes de teletrabajo.
8. **Contingencia.** Diseña un plan de contingencia y continuidad de negocio.
9. **MFA.** Implementa **doble factor de autenticación** a los usuarios que realicen teletrabajo.
10. **ENS.** Aplica las medidas de seguridad necesarias tomando como referencia el Esquema Nacional de Seguridad.

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.

Prevención Proactiva: Cumplimiento y Vigilancia

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

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…

Prevención Proactiva: Cumplimiento y Vigilancia

Marco Operacional

Medidas de Operación

Medidas de Protección

Infraestructura de Seguridad

Marco Organizativo

Medidas de Gestión

PROYECTOS

Adecuación _ENS

El Centro Criptológico Nacional ha desarrollado el Asistente del Plan de Adecuación de INES y el Asistente de Implantación y Gestión de la Conformidad - AMPARO, como herramientas de Apoyo para la Obtención y Gestión de la Declaración/Certificación de Conformidad en el ENS, que junto con EMMA y ANA permiten, además, realizar la Gestión Continua de la Seguridad.

[01] Plan de Adecuación del Sistema

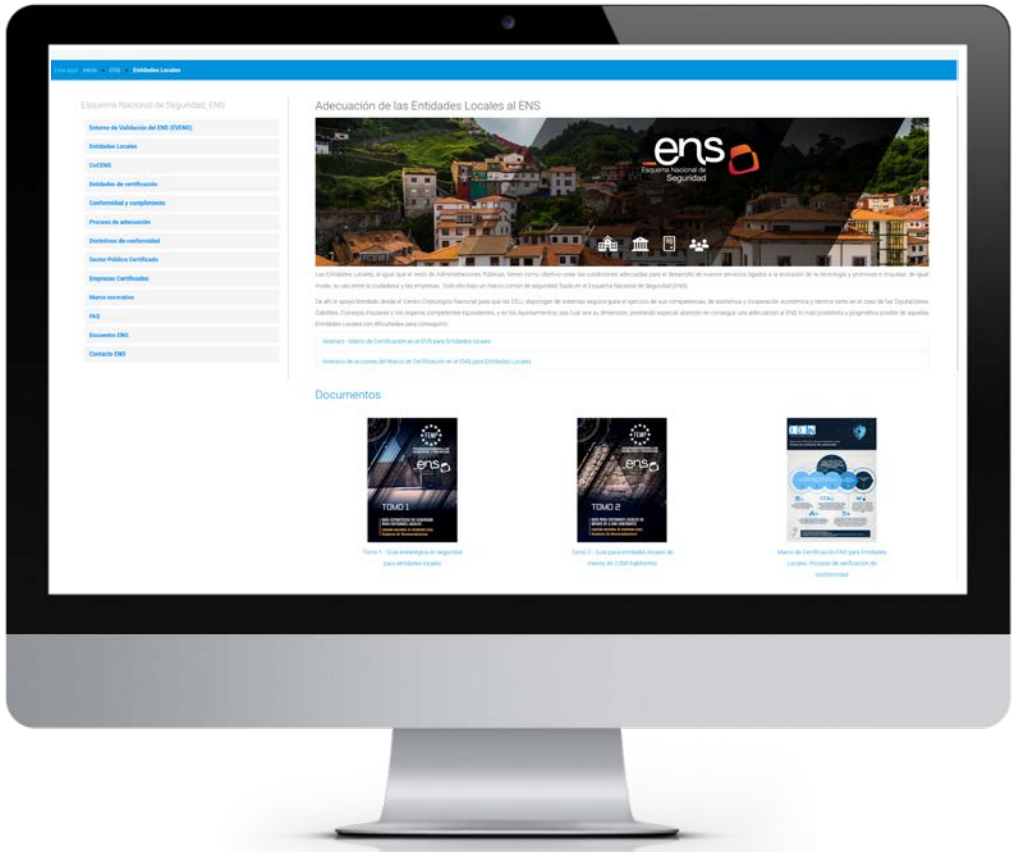
- **Identificar el Alcance del Sistema**
- **Categorizar el sistema**
- **Declaración de aplicabilidad**
- **Análisis de riesgos**
- **Perfiles de cumplimiento | Validación**
- **Política de Seguridad**

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



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

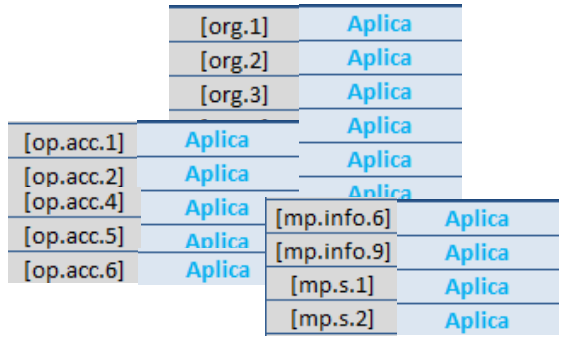
reco...	control	ENS
	[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)	L2-L3
5	[org] Marco organizativo	L2-L3
5	[org.1] Política de Seguridad	L2-L3
5	[org.2] Normativa de seguridad	L2-L3 (L2)
5	[org.3] Procedimientos de seguridad	L2-L3 (L2)
5	[org.4] Proceso de autorización	L2-L3
8	[op] Marco operacional	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



[org.1]	Aplica
[org.2]	Aplica
[org.3]	Aplica
[op.acc.1]	Aplica
[op.acc.2]	Aplica
[op.acc.4]	Aplica
[op.acc.5]	Aplica
[op.acc.6]	Aplica
[mp.info.6]	Aplica
[mp.info.9]	Aplica
[mp.s.1]	Aplica
[mp.s.2]	Aplica

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

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** 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

Gestiona y coordina los servicios de ciberseguridad

Instalación y operación de herramientas

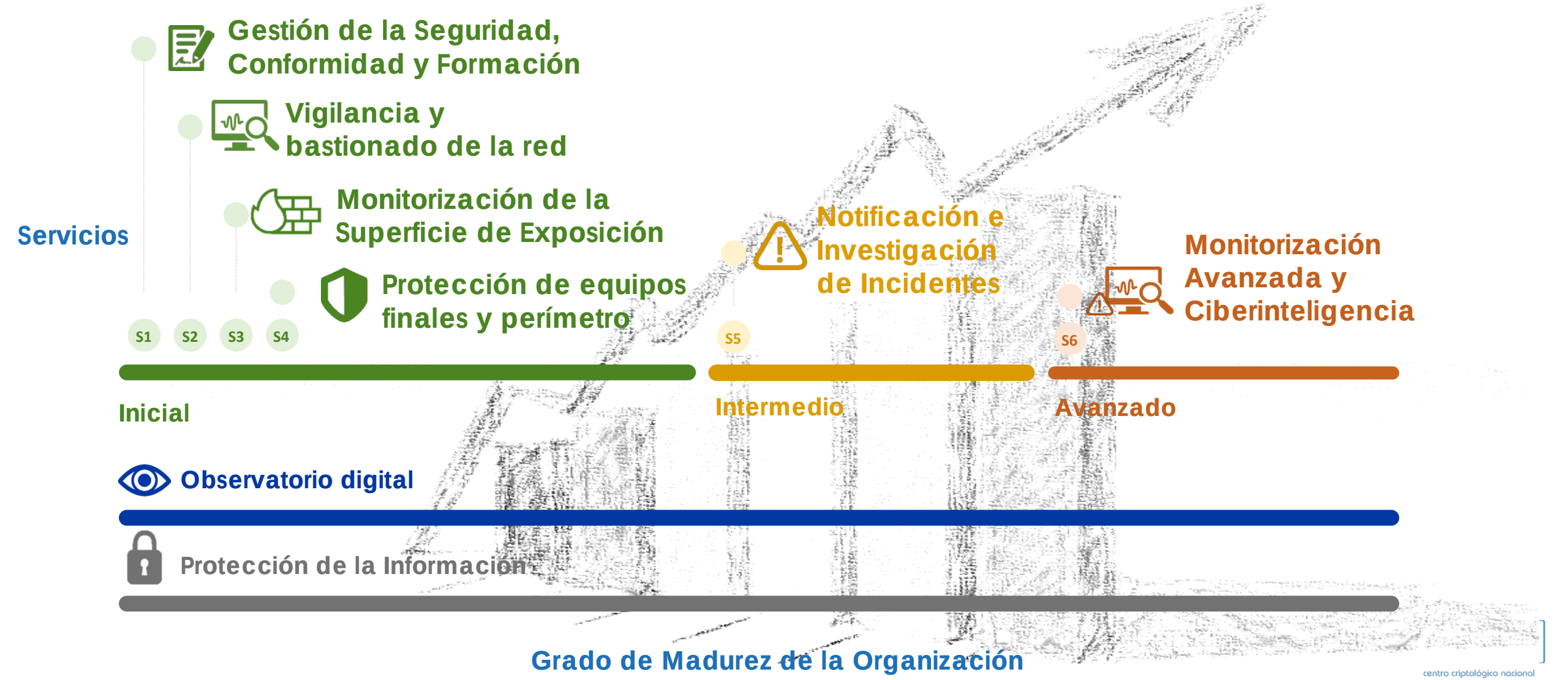
Se responsabilizará de la instalación y operación de Herramientas Centralizadas de Ciberseguridad

Instalación, configuración, parametrización y personalización de una serie de soluciones, en principio proporcionadas por el Centro Criptológico Nacional (CCN), que den apoyo y soporte al cumplimiento normativo y adecuación al ENS:

/inés> /amparo> /pilar>	Cumplimiento de Esquema Nacional de Seguridad
/emma>	Control de acceso a las infraestructuras de red
/ana> /clara>	Monitorización de la superficie de exposición
/lucía>	Registro, seguimiento e Intercambio de incidentes de seguridad
/carmen>	Identificación de Amenazas Persistentes Avanzadas(APT)
/gloria>	Correlación compleja de eventos (SIEM) u otra alternativa
/sat-inet>	Sonda de control de tráfico de red

CCN centro criptológico nacional

Hoja de Ruta – Operación de la Ciberseguridad



Hoja de Ruta – Prevención Proactiva

Plan de Adecuación al Sistema

Implantación de Seguridad

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

Inicial - Gestión de la Seguridad, Normativa y Formación

Marco Organizativo

- Política de Seguridad
- Normativa de Seguridad
- Procedimientos De Seguridad

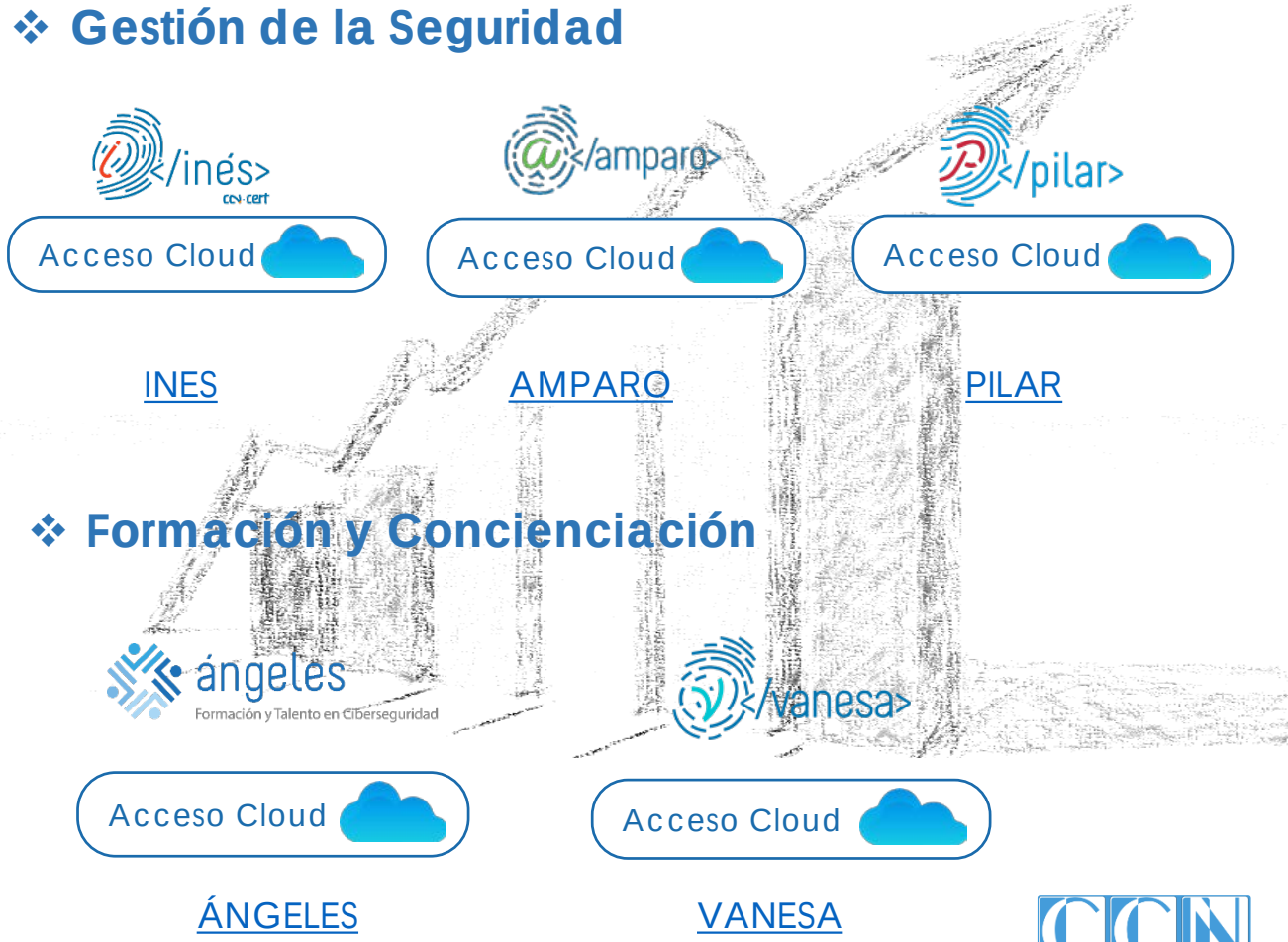
Marco Operacional

- Análisis de Riesgos
- Métricas e Indicadores

Medidas de Protección

- Formación
- Concienciación

❖ Gestión de la Seguridad



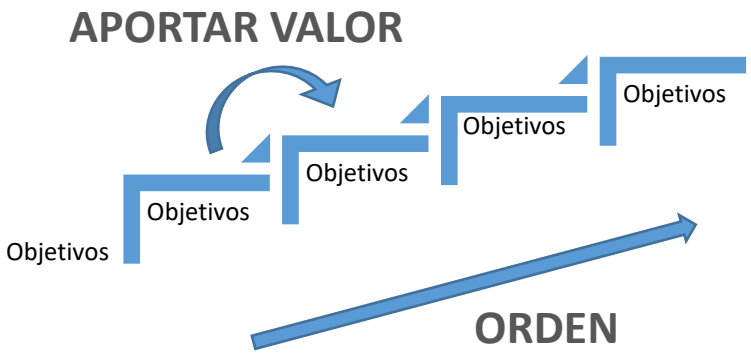
❖ Formación y Concienciación

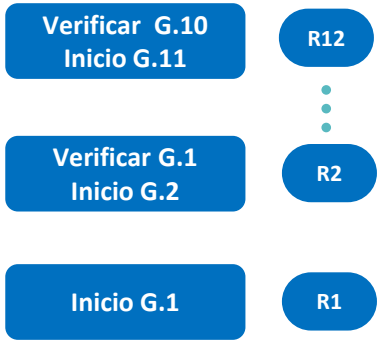
e-vens
ENTORNO DE VALIDACIÓN ENS

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**

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

Inicial - Perfiles de personal

Perfil	Funciones
Dirección / Coordinación	• Dirección y Seguimiento • Revisión de la Planificación y Ejecución • Gestión del Equipo de Trabajo • Interlocución con Responsables
Oficina Seguridad TIC	• Análisis previo de situación en materia de ENS • Diseño y elaboración del Plan de Adecuación al ENS • Asesoramiento en materia de adecuación y cumplimiento normativo: elaboración de procedimientos específicos de adecuación (marco normativo) • Formación, capacitación y talento • Cultura ciberseguridad. Concienciación y sensibilización • Seguimiento del plan de adecuación ENS. • Elaboración de acciones correctivas (PAC)
Operación Ciberseguridad	• Ejecución de los Procesos de adecuación de las entidades al ENS • Despliegue de herramientas de Ciberseguridad centralizadas • Monitorización y administración de las herramientas de Ciberseguridad • Análisis y detección de amenazas de seguridad y desarrollo de técnicas de prevención • Mantenimiento y Soporte • Reuniones de seguimiento

Inicial - Gestión de la Seguridad, Normativa y Formación

Mínima

- Comité de Seguridad y DPO
- Plan de Adecuación (Plan Director de Seguridad)

Media

- SGSI (cumplimiento del ENS)
- Participación en órganos directivos
- Asesoramiento externo
- Campañas constantes de concienciación

Avanzada

- Oficina cumplimiento (ENS)
- Gobierno de Seguridad de la Información

Madurez: Gestión/Inteligencia	Coste Medio Año (dedicaciones año)
Mínima	1 hora/usuario
Media	2 horas/usuario
Avanzada	4-12 horas/usuario

Inicial - Protección de equipos finales y perímetro

Marco Organizativo

Marco Operacional

- Protección código dañino
- Detección de intrusión
- Registro actividad de usuarios

Medidas de Protección

- Protección de Equipos portátiles
- Perímetro seguro

❖ Protección de Equipos Finales

EDR y Endpoints

CYTOMIC

Instalación On-Premise y Licenciamiento

Productos certificados

CLAUDIA

❖ Protección Perimetral

Firewall

FORTINET SOPHOS Check Point SOFTWARE TECHNOLOGIES LTD paloalto networks

Instalación On-Premise y Licenciamiento

Productos certificados

CCN centro criptológico nacional

Inicial - Determinación de la Superficie de Exposición

Marco Organizativo

Marco Operacional

- Requisitos de acceso
- Configuración de seguridad
- Inventario de activos
- Gestión de la configuración
- Mecanismos de autenticación

Medidas de Protección

- Protección de Equipos portátiles
- Protección de servicios web

❖ Monitorización de la Superficie de Exposición

Instalación On-Premise

CLARA

Instalación On-Premise

ANA

❖ Configuración y bastionado de equipos

Equipos y Servidores

Bastionado

Auditoría de Servicios Web

Ejecución en Remoto

Guías STIC

¿Qué es CLARA?

- Evaluación del cumplimiento de medidas:
  - Identificación de configuración de Endpoint, Sistemas específicos o seguridad personalizada.
  - Personalización de agrupación de activos basado en servicios.
  - Análisis continuo del sistema.
  - Evaluación de actividad del sistema.
- Cualificación completa de los activos: S.O. y Software
- Análisis de actividad de usuarios y del sistema
- Capacidad de análisis retrospectivo en respuesta frente a incidentes, a través de la identificación de cambios en los sistemas

METODOLOGÍA

</ana>

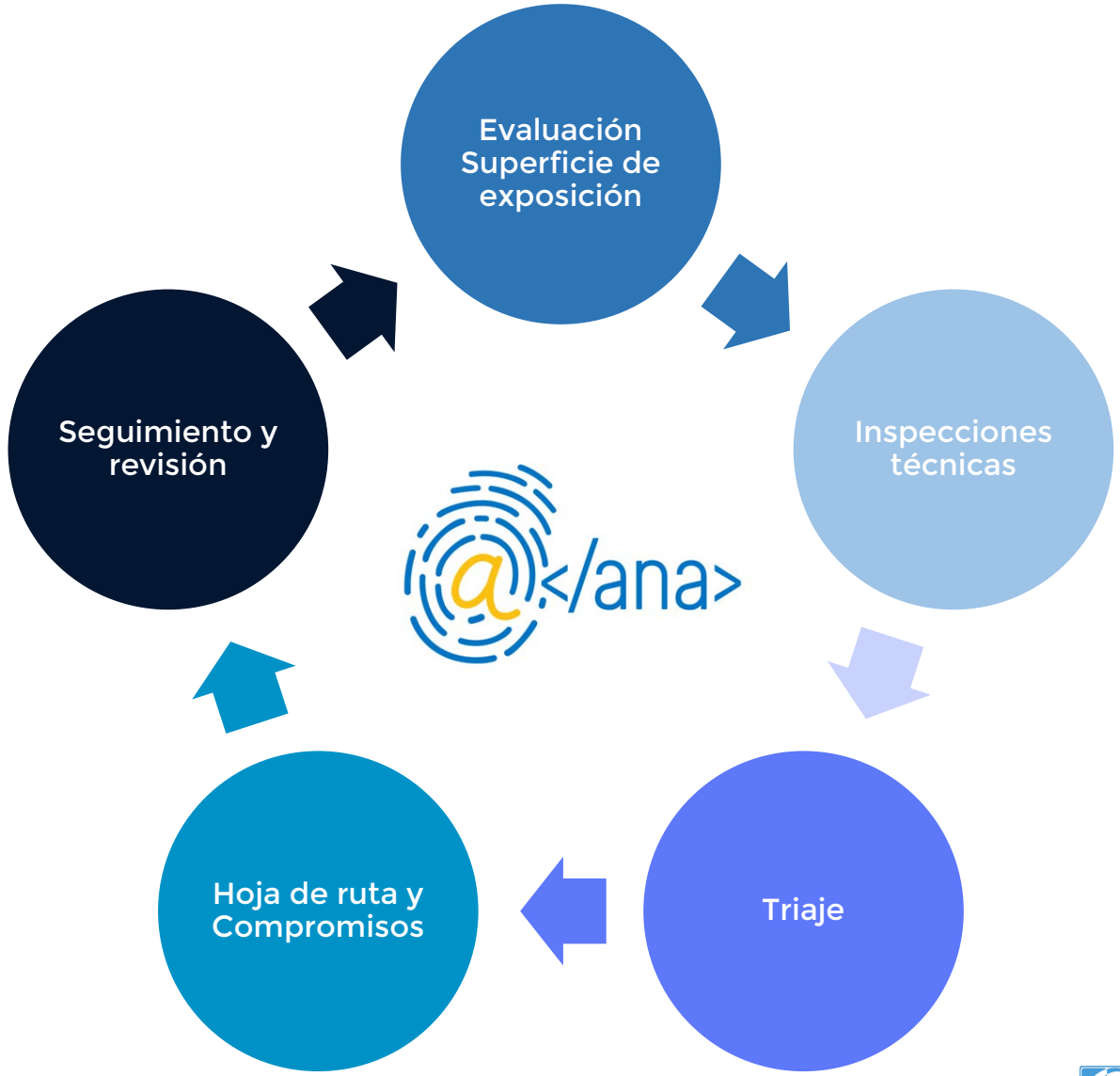
Metodología de trabajo:

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



Inicial - Vigilancia y bastionado de red

Marco Organizativo

Marco Operacional

Requisitos de acceso	Acceso Remoto	Inventario de activos
Configuración de seguridad	Gestión de la configuración	Detección de intrusión

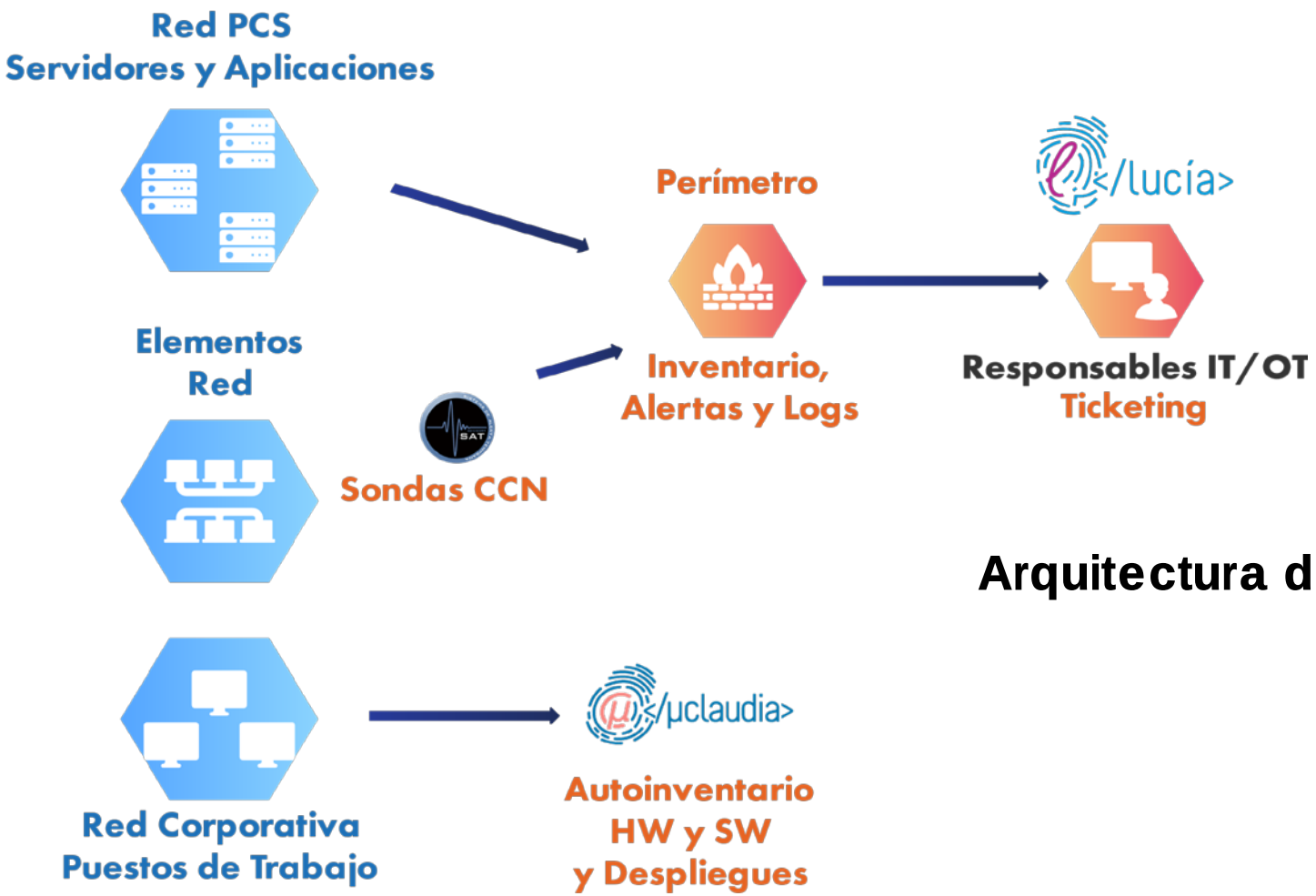
Medidas de Protección

- **Vigilancia de red y protección de comunicaciones**

- **Bastionado en Equipos de Comunicaciones**

Guías STIC

Inicial - Protección de equipos finales y perímetro



Arquitectura de Seguridad Inicial

Protección de la Información

Marco Organizativo

Marco Operacional

- Requisitos de acceso

Medidas de Protección

- Autenticidad e Integridad
- Protección de Confidencialidad
- Etiquetado
- Calificación de la información

❖ Protección y monitorización de ficheros

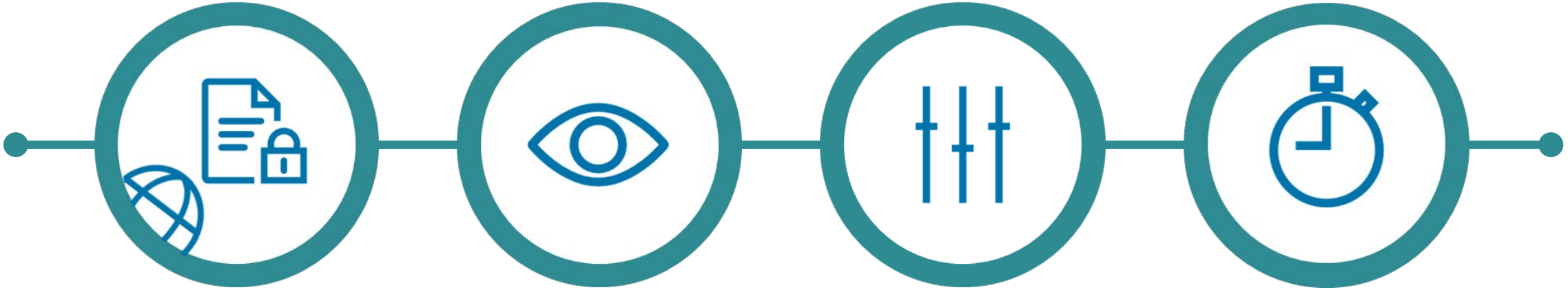
Instalación On-Premise

CARLA

Catálogo de Productos:
Listado de Productos Cualificados

Prevención Proactiva: cumplimiento y vigilancia

PROTECCIÓN EN CUALQUIER LUGAR



Dentro de la red, en la nube, en el equipo de un tercero

VISIBILIDAD Y TRAZABILIDAD

Monitorizar accesos, intento de acceso bloqueados

CONTROL SOBRE EL DATO

Restringir permisos dependiendo de dato y usuario

RESPUESTA RÁPIDA FRENTE A ALERTAS

Revocación de accesos al dato en tiempo real

Inicial - Protección de equipos finales y perímetro

Medidas de protección

Inicial

- Seguridad Perimetral (UTM, NGFW)
- Seguridad en el puesto de trabajo (endpoint)

Intermedio

- Capas extra en el perímetro (IPS, WAF,...)
- Capas extra (Cifrado, Navegación, DLP, MDM,...)

Avanzado

- Detección de intrusos (IDS, IPS)
- Gestores de eventos (SIEM, "Machine Learning", BI,...)
- Protección especializada (corporativa, industrial, nube)

Madurez: (Armas/Medios)	Coste Medio Año
Inicial	20-25 €/usuario
Intermedio	50-60 €/usuario
Avanzada	100-200 €/usuario

Servicios a prestar

Monitorización

Monitorización y operación de las herramientas instaladas.

Coordinación

Coordinación de los servicios de ciberseguridad.

- Servicio Mitigación ataques de Denegación de Servicio.
- Servicios de gestión de Incidentes de Seguridad.
- Servicio de cibervigilancia.
- Servicio de ciberresiliencia.
- Ejercicios de ciberseguridad.
- etc.

Gestión

Gestión de incidencias de Seguridad de forma centralizada.

Soporte

Soporte en el día a día en materia de ciberseguridad.

- Apoyo en el soporte al uso de las herramientas.
- Resolución incidencias en operación o uso de herramientas.
- Apoyo en la gestión de incidentes de seguridad.
- Monitorización de los sistemas para detectar actividades inusuales o accesos a información no autorizados.
- Analizar las medidas de seguridad implementada.
- Protección de la información.
- Adopción de medidas de control y supervisión.
- Ejecución de diagnósticos ante cambios en las infraestructuras.

Prevención Proactiva: cumplimiento y vigilancia

Plan de Adecuación del Sistema

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

Implantación de Seguridad

6. Mapa Normativo
7. Implantación de Medidas Técnicas de Seguridad
8. Aprobación del SGSI por el COMSEG
- Normativas y Procedimientos de Seguridad

Conformidad

9. Auditoría Interna de Verificación
10. Auditoría de Certificación
11. Certificación de Conformidad

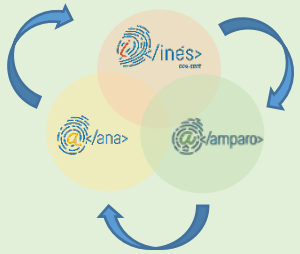
CERTIFICACIÓN DE CONFORMIDAD CON EL

ens Esquema Nacional de Seguridad

Categoría ALTA

RD 3/2010

Gestión Continua de la Seguridad



1. Prevención
2. Operación
3. Respuesta
4. Formación
5. Mejora continua

CCN centro criptológico nacional

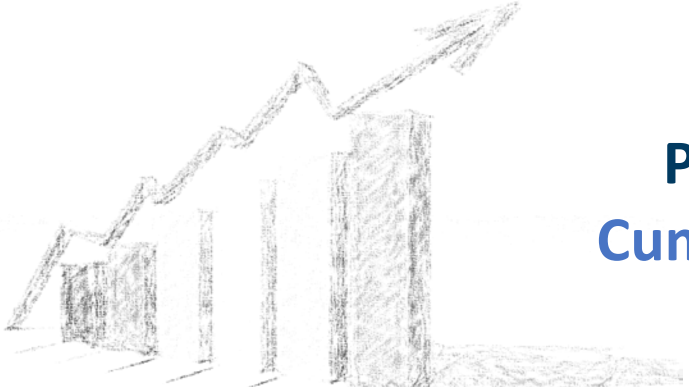
Mejora Continua

(Hoja de Ruta)

- Madurez +

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

+ Riesgo -



ángeles
Formación y Talento en Ciberseguridad

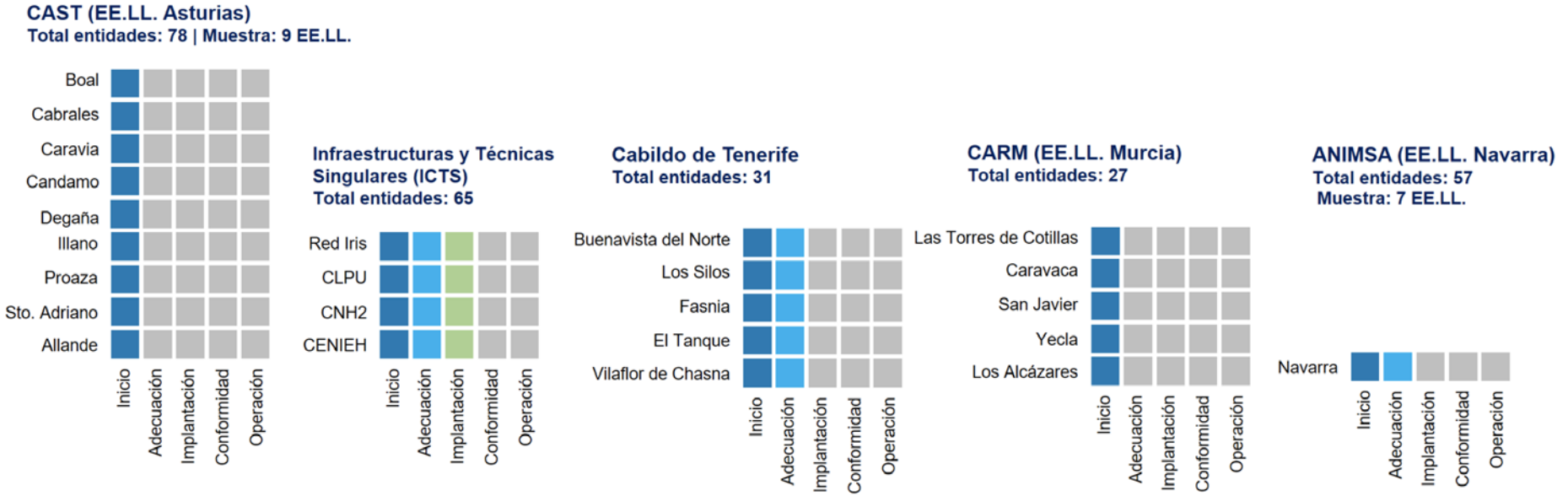
evens
ENTORNO DE VALIDACIÓN ENS

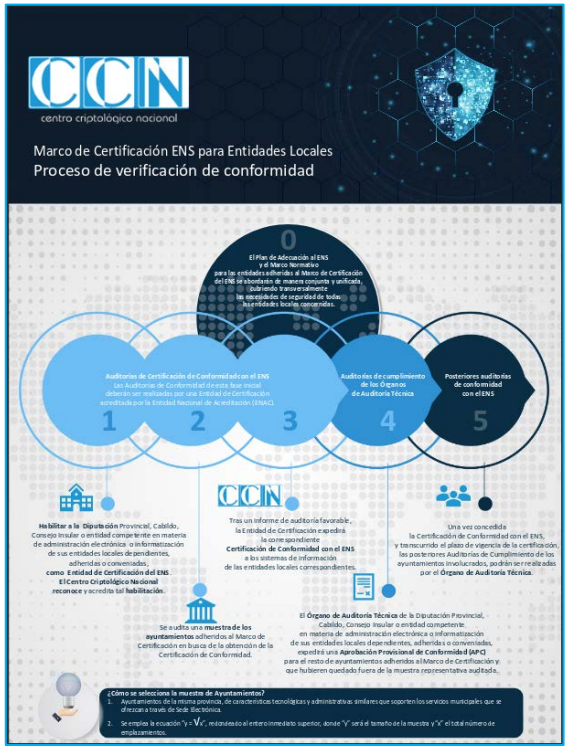
Prevención Proactiva
Cumplimiento y Vigilancia

CCN
centro criptológico nacional

Iniciativas

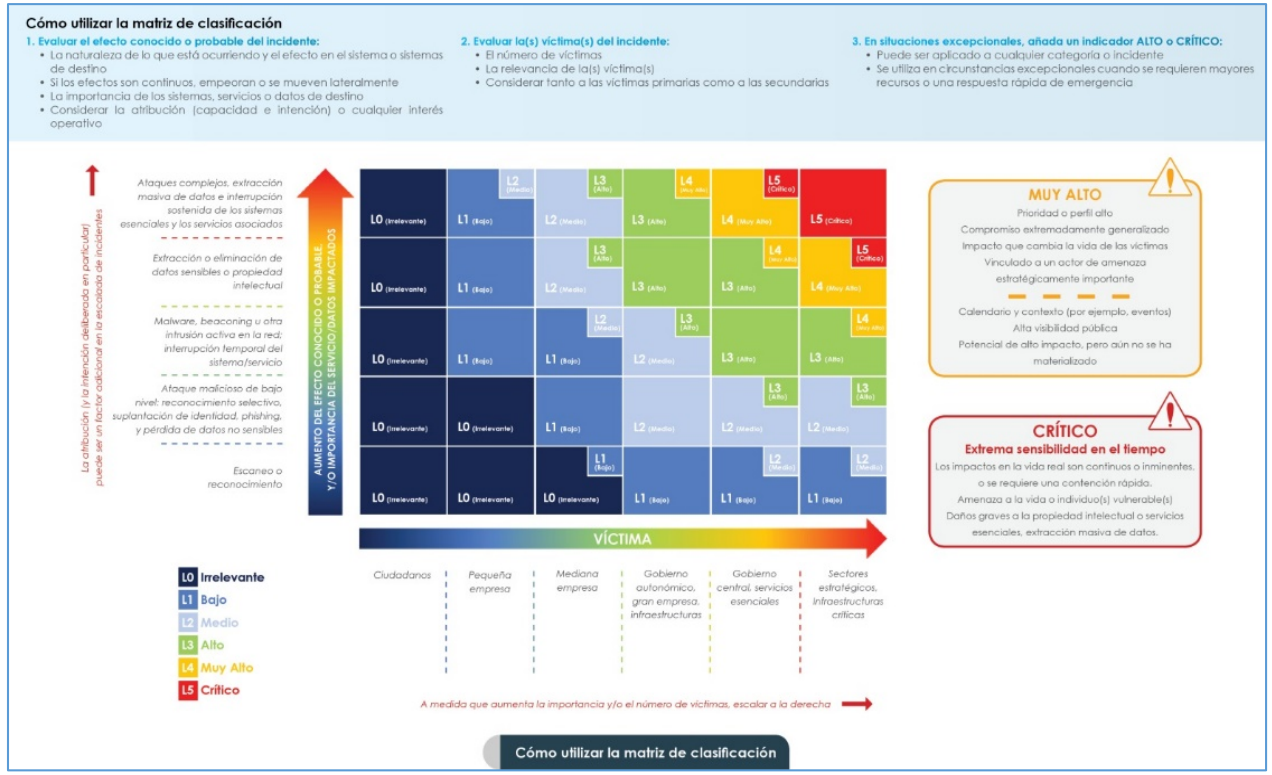
Tras el diseño e implantación del ENS para EELL, han surgido iniciativas para su aplicación directa en diferentes proyectos pilotos, como organismos superiores de los que dependen los diferentes órganos.





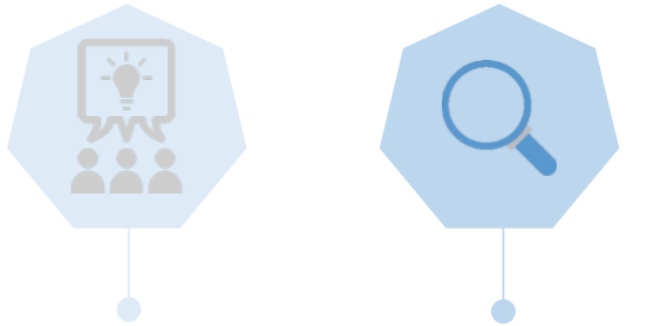
Prevención Proactiva

El reto está en 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
- Mejora en la notificación de incidentes
- Eficiencia de los recursos disponibles

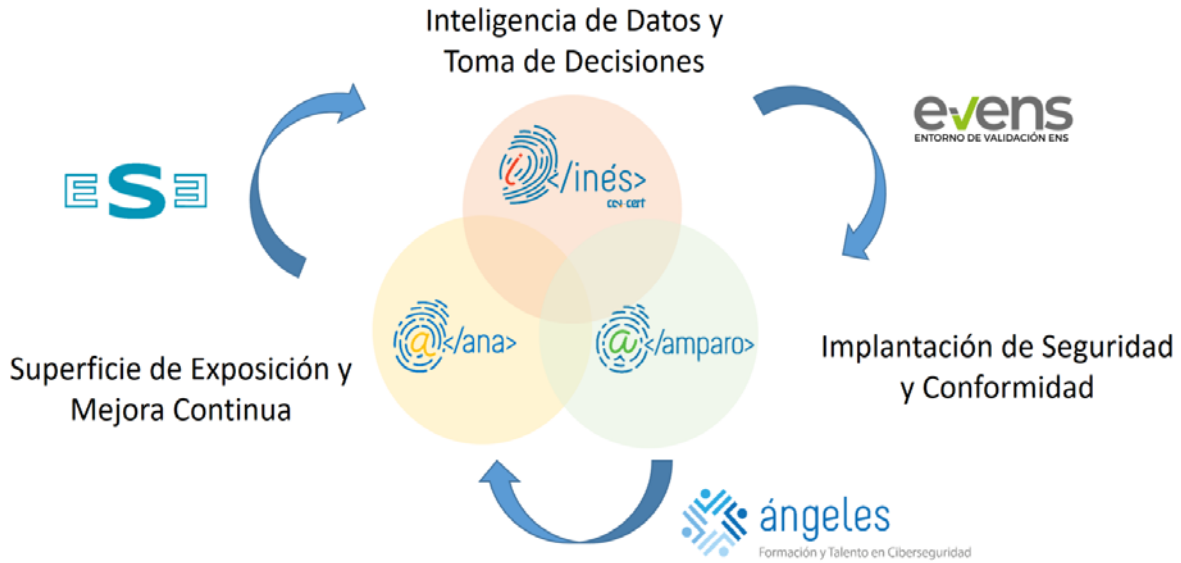


Más información de ataques

Mayor visibilidad sobre incidentes

Conclusiones

- Ecosistema de la Ciberseguridad
- Implementar Seguridad
- Mejora Continua
- Sensibilización y capacitacıon
- Toma de decisiones



La importancia de Construir Comunidad

CN-CERT
centro criptológico nacional

CCN
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