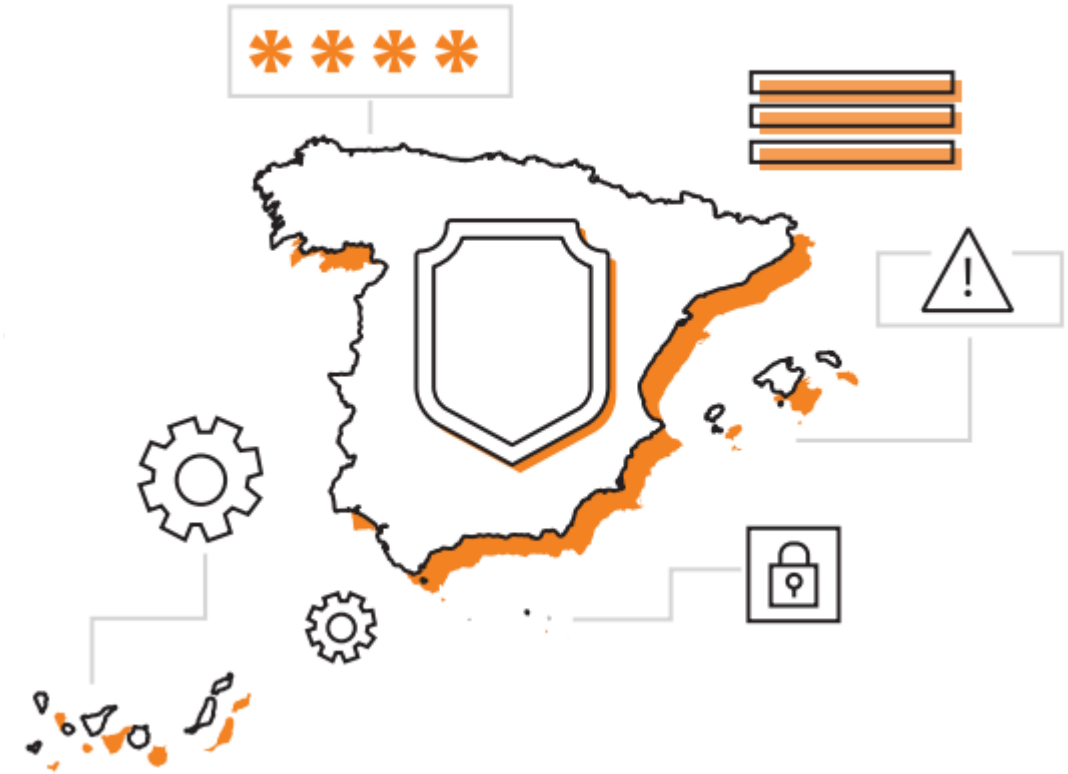
Postura de seguridad

Soy muy fan del ENS

Pablo López
Jefe Área Normativa y Servicios de Ciberseguridad
Centro Criptológico Nacional

Gobierno de la Seguridad y Cumplimiento

Esquema Nacional de Seguridad



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

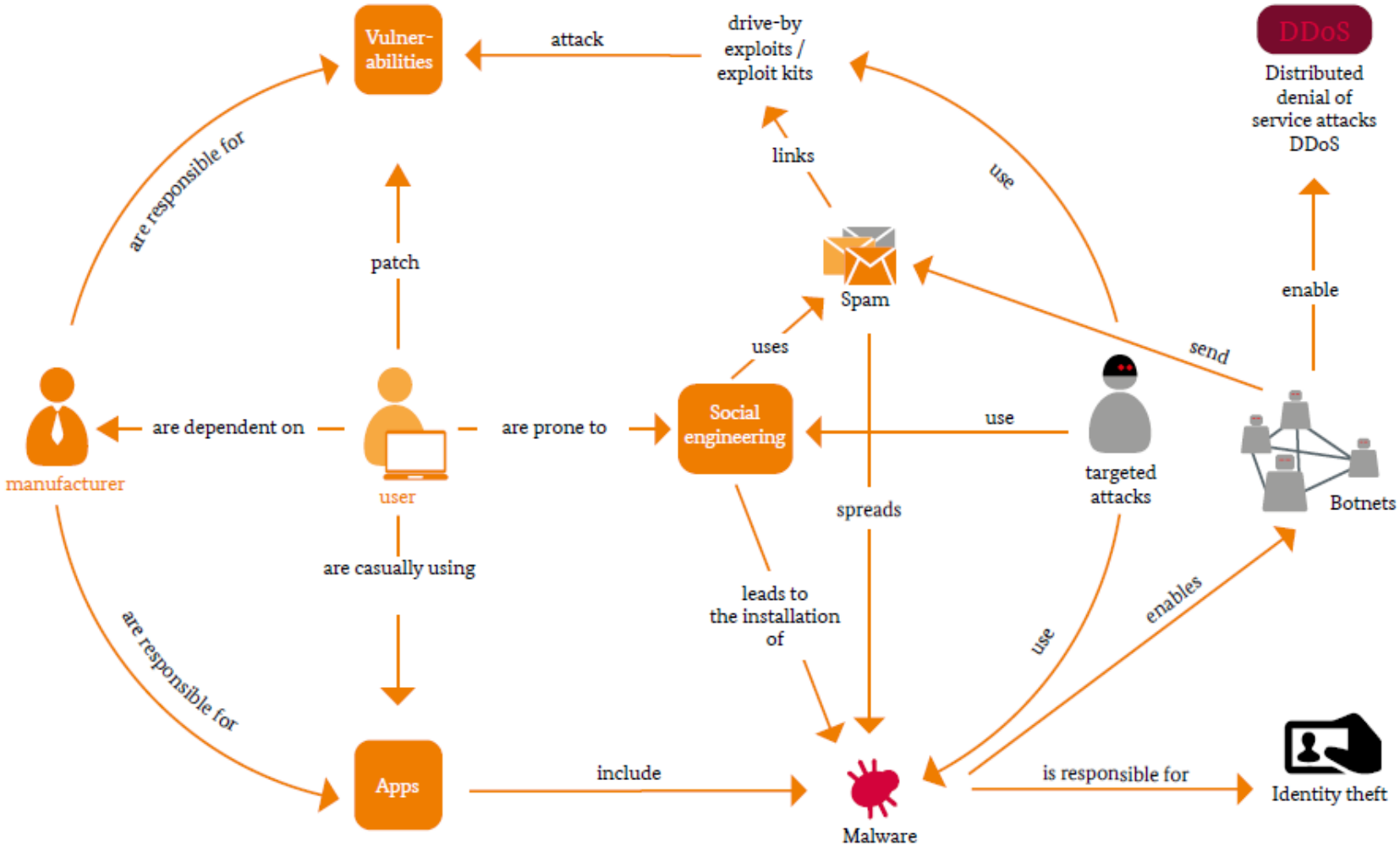
Interoperabilidad

- 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

Ecosistema al que enfrentarse - Realidad



Agentes de la amenaza

CAPACIDAD DE CIBERATAQUES

Ciberespionaje Robo Prop. Intelectual

- → Administración Pública / Empresas
- → Servicios de Inteligencia / Fuerzas Armadas/ Otras compañías

Cibercrimen

- → Robo de certificados y Tarjetas de Crédito / Fraude Electrónico
- → Lavado de dinero / Robo de Identidad
- → Crimen Organizado

Ciberguerra / Amenaza Híbrida

- → Cibersabotaje TIC / Redes OT
- → Infraestructuras Críticas / Servicios Esenciales

Hacktivismo

- → Ataques a servicios web / Compromiso de datos
- → Anonymous y otros grupos

Use de Internet por terroristas

- → Comunicaciones / Información de fuentes abiertas
- → Propaganda / Proselitismo

Ciberterrorismo

- → Cibersabotaje TIC / Redes OT
- → Infraestructuras Críticas / Servicios Esenciales

Contexto Dinámico / Cambiante

Tipología de ciberataque	Denominación	Actor	Tipología de ciberamenaza	TTP Mitre	Peligrosidad
Infostealer	Titan Stealer	KillNet KillMilk	Hacktivismo Hibrido	T1204 T1003 T1552 T1082 T1518 T1083 T1087 T1005	
Comprometimiento credenciales		KillNet KillMilk	Hacktivismo Hibrido	T1078?	
DDoS		NoName057	Hacktivismo Hibrido	T1498	
		KillNet	Hacktivismo Hibrido	T1498	
		Anonymous Sudan	Hacktivismo Hibrido	T1498	
Desfiguración		Moroccan Revolution	Hacktivismo Monetización	T1491.002	

1. Dos (2) vectores de ataque más utilizados para comprometer sistemas informáticos:
   - Combinaciones de ingeniería social dirigida a objetivos específicos
   - Explotación de vulnerabilidades de software no corregidas
2. Es previsible que actúen **actores oportunistas de ciberamenaza** explotando vectores surgidos del incremento de tensión geopolítica
3. Desde la perspectiva de ciberataques hacktivistas, los sistemas informáticos deben estar preparados **para prevenir, contener, rechazar o mitigar acciones DDoS,** y para disminuir al máximo la superficie de exposición **de dispositivos, sistemas y servicios digitales conectados a redes.**

Análisis de perspectiva para generar conciencia preventiva ante la actual situación de guerra

Varios escenarios

- Surgimiento de algún tipo de **conciencia patriótica** por parte de las APTs dedicadas al ransomware.
- Condicionamiento o direccionamiento estatal en operaciones de APTs.
- Oportunidad para las APTs de 'pescar en río revuelto' por la tensión entre bloques.
- Aparición de alguna APT de hacktivismo híbrido.
- Incremento de ciberataques sobre países OTAN o Estados Miembros de la Unión Europea.

Ciberamenazas oportunista y falsas banderas

Sobre el ciberespacio OTAN, Estados Miembros o, por extensión y solapamiento, sobre países de la Unión Europea.

Además

- **Invasión militar en Ucrania** ha generado un ecosistema de Hacktivismo propio inscrito en un ecosistema de ciberamenaza híbrida.
- Campañas de ciberataques mediante **cepas de ransomware** que tienen alcance global.

- **Filtración de información**
- Creación de **múltiples identidades digitales** para constituir una percepción colectiva

- **Combinación con ataques DDoS:** alquiler de una botnet para ataques dirigidos
- **Extorsión y filtraciones de información.**

Consideraciones sobre vulnerabilidades de software

Tipología de código dañino	Denominación	Actor	Tipología de ciberamenaza	TTP Mitre	Peligrosidad
Ransomware	Varias cepas	Varios	APT-F	T1486	
Ransomware sabotaje Tuneladores	DarkBit Mullvad VPN Ligolo	Muddy Water	APT-G	T1190 T1059.001 T1059.003 T1136 T1543 T1484 T1485	
Troyano Puerta Trasera	Jaguar Tooth	APT28	APT-G	T1190 T1078.001 T1590	
Consola web Gusano Troyanos puerta trasera	TONEINS TONESHELL PUBLOAD ABPASS, CCPASS HIUPAN ACNSHELL CLEXEC COOLCLIENT TROCLIENT NUPAKAGE	Mustang Panda	APT-G	T1583.004 T1587.001 T1585.002 T1588.002 T1608.001 T1566.002 T1204.001, 002 T1547.001 T1574.002 T1053.005 T1068 T1134 T1140 T1036 T1091 T1104 T1095 T1048	
Spyware, Infostealer	PseudoManuscrypt Crashtech Loader RacconStealer GCleaner Koi Fabookie	NullMixer	APT-F	T1588.001 T1566 T1204.001 T1204.002	
Exploit en Javascript		Winter Vivern	APT-G	T1566 T1189 T1190 T1114	

Leyenda:

APT-F. Ciberamenaza persistente avanzada motivada financieramente para la obtención de lucro criminal.

APT-G. Ciberamenaza persistente avanzada operando principalmente para servir a intereses geopolíticos de un Estado.

Medidas de reducción de superficie de exposición en la prevención de operaciones hostiles de ciberamenazas avanzadas

Actualizar parches de seguridad en sistemas informáticos propios y de sistemas de terceros autorizados a algún tipo de autenticación en el propio

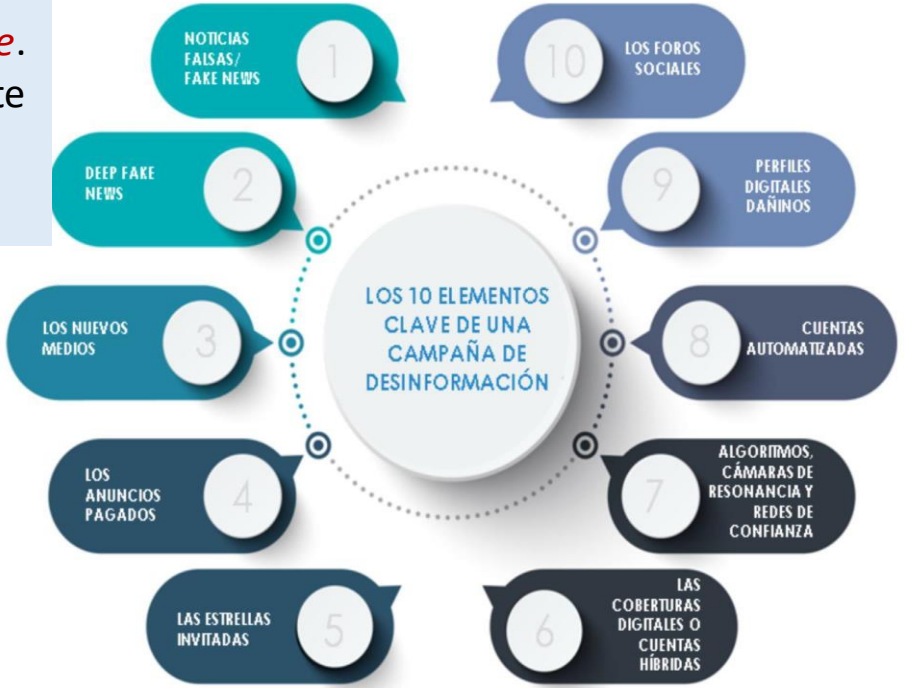
Establecer una sólida arquitectura de control de accesos:

- Mínimo privilegio
- Redes de confianza cero
- Esquemas reforzados (multifactor) de autenticación

Consolidar una práctica sistemática de revisión de configuraciones de software

Consideraciones sobre Información Maliciosa

Una campaña sistemática y maliciosa de distribución de *malinfo* entre la opinión pública pueden derivar en *indeseadas consecuencias e incremento de la incertidumbre*. La manera más efectiva de articular una prevención eficaz y una resiliencia efectiva ante acciones maliciosas de *malinfo* es PROTEGIENDO y ORIENTANDO al eslabón habitualmente más vulnerable de estos ataques: LAS PERSONAS.



Consecuencias de un ataque de *malinfo*

Necesidad de un **TOOLKIT**, cuyo objeto sea *establecer los marcadores preventivos, los indicadores de presencia y las características constituyentes* que permitan identificar una campaña generadora de *malinfo* **de una manera temprana, objetivada y basada en la evidencia**.

Escenario Habitual

Etapa 0: Inicio

Detección de una anomalía en los Sistemas

Materialización del ataque (Ejemplo: Ransomware)

- Cifrado del entorno Windows
- Backup
- Entorno de virtualización a nivel de host

Etapa 1.1: Análisis e investigación

Clasificación y notificación a entidades de control

- Clasificación del incidente (Guías CCN-STIC 817)
- Análisis del impacto en datos personales (notificación ante la AEPD).
- Denuncia FCSE.

Verificación de controles y medición del impacto

- Comprobación de medidas existentes:
  - Existencia de EDR
  - Existencia de microCLAUDIA
  - Existencia de 2FA en acceso remoto
  - Gestión de crisis / constitución de un Comité Crisis.

Etapa 1: Gestión del incidente

Actividades de contención

- Desconexión de equipos y apagado.
- Análisis de equipos para identificar el vector de entrada e intentar disponer del binario y posibles herramientas auxiliares de acceso remoto / cualquier indicador de compromiso.

Etapa 2: Recuperación

Identificación de directrices:

- Acceso a Internet cortado (se implementarán listas blancas)
- Generación y distribución de la vacuna
- Proceso de triaje para priorizar levantamiento de servicios (pasando por EDR + parches de seguridad) sobre una red limpia.

- Priorización coordinada a través del Comité de Crisis.
- Cambio integral de todas contraseñas.
- Puesta en marcha de 2FA.
- Revisar segmentación de red.
- Gestión de cuentas locales (evaluando LAPS)

Necesidad de estar Preparado - Prevención Proactiva

Objetivos del framework

Escuchar, entender y apoyar

Facilitar la obtención de la Certificación de Conformidad conforme a un Perfil de Cumplimiento Específico (PCE)

Orientada a Entidades y Organismos con dificultades para abordar la Adecuación al framework de seguridad de referencia.

Apoyar con la implantación de medidas de seguridad:

35 medidas de RSE + identificación de un ciclo de mejora continua en base a la experiencia / realidad

Automatizar el proceso de Adecuación y Auditoria

Herramientas y Evidencias

Apoyar y complementar a través de Soluciones ABS / Guías CCN-STIC / Modelos proporcionados por el framework de seguridad

“El Framework funciona, se consigue llegar a todas las entidades

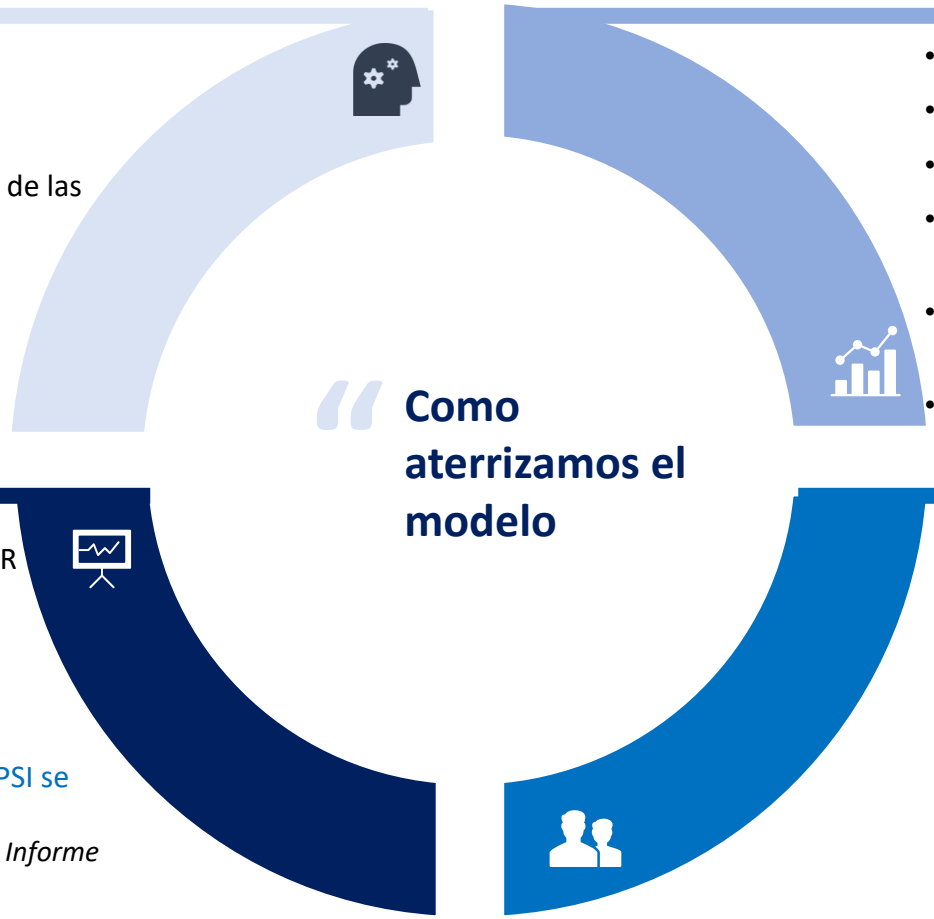
Como Aterrizamos el modelo

Implantación de Medidas de Seguridad

- Hoja de Ruta de implantación (priorización de medidas)
- Elaboración del Marco Normativo
- Implantación de medidas Técnicas de Seguridad a través de las herramientas ABS y Generación de Scripts
- Vigilancia continua y bastionado de la infraestructura

Reunión Kick Off

- Explicación del proyecto
- Identificación del alcance (servicio finalista)
- Explicación de la metodología que se va a seguir.
- Explicación de las herramientas que se van a utilizar en el proyecto
- Explicación de los servicios de postura de seguridad Ej. Threat Hunting y análisis de exposición
- Presentación del equipo de trabajo



Plan de Adecuación al Sistema

- Presentación de la ficha del servicio y Plan del informe AR
- Explicación de la valoración de los servicios del sistema
- Generar la Declaración de Aplicabilidad
- Propuesta de Plan de formación a través de Ángeles
- Una vez que se rellene la ficha del servicio y se valide la PSI se realizan las siguientes acciones:

1. *Determinación del nivel de riesgo asumible y obtención del Informe de riesgos (MVPCR)*
2. *Determinación inicial de la Declaración de aplicabilidad*
3. *Determinación de la categorización*
4. *Aprobación del plan de formación*

Diagnostico y análisis de procesos

- Familiarización y gestión del alta en las herramientas de gobernanza proporcionadas por el CCN.
- Elaboración de diagnóstico por parte de la organización
- Elaboración /Validación Política de Seguridad (Aproximación de roles)
- Explicación del bastionado

Objetivos del framework

HITO 01

Gobierno de la ciberseguridad: criterio y orden en la gestión a través de una estructura, definición de roles y asignación de responsabilidades.

HITO 02

Una *postura de seguridad* adaptada al medio, disuasoria de la amenaza y con riesgo residual asumible: **Perfil de Cumplimiento Específico (PCE).**

HITO 03

Un *modelo* que sirva para su adecuación e implantación.

HITO 04

Una herramienta que permita el *acompañamiento* junto a la obtención de evidencias: **Portal de Gobernanza de la Ciberseguridad** (INÉS-AMPARO)

HITO 05

Marco Normativo de referencia: política de seguridad y procedimientos asociados ya modelados y adaptados (medidas compensatorias y complementarias de vigilancia).

HITO 06

Soluciones de Seguridad adaptadas a la necesidad.

Que necesitamos para adecuarnos y conseguir una postura de seguridad adecuada

¿Cómo te ayuda el modelo facilitándote la vida?

De una forma factible y viable y gestionando con criterio

Prevención proactiva

- Postura de seguridad adaptada (Bastionado)
- Superficie de exposición para adaptar mi postura de seguridad (Ana)
- Generación de informes Automáticos para saber si el sistema es apto o no apto para poder conectarme y tomar decisiones (Clara)

Capacidad de seguridad

- Traslada a la realidad que tengo que hacer, desde el punto de vista de cumplimiento y desde el punto de vista de las evidencias técnicas ese es mi reto

Eficiencia

- Saca el máximo rendimiento a las posibilidades ya que es una tecnología que se adapta a diferentes ecosistemas

Acompaña

- No dejamos solos a nadie os acompañamos a hacerlo, porque entendemos vuestras necesidades
- Os ayudamos a interpretar datos y como solucionarlo
- ¿Qué tienes que hacer para mejorar?

Pautas para mejorar en función de tu nivel de madurez y estado actual de ciberseguridad

¿Cómo resolvemos el Top 5 de dificultades?

Suplantación de identidad

Cuentas Genéricas

Implantación de Doble Factor de Autenticación solución AuthPoint Agent for Windows

Ataques internos y externos

Aumento del Riesgo en la superficie de exposición

Elaboración de Scripts a medida sistemas Windows, Mac, Linux….

Gestión de dispositivos externos

Ciberamenazas a través de dispositivos de almacenamiento USB

Implantación de herramienta de auditoría, gestión y trazabilidad de todos los dispositivos conectados.

Acceso a información sin limites

Usuarios con acceso a información que no procede

Implantación de herramienta de protección centrada en proteger la información

Amenazas potenciales

Evadir las soluciones de seguridad existentes

Servicio de superficie de ataque y Threathunting

BUSQUEDA ACTIVA Y CONTINUA PARA HACER FRENTE A LAS DIFICULTADES

¿Cómo se lleva a la practica la solución?

Trazando una metodología que a partir de una situación inicial, vamos buscando hitos que nos permita mejorar la postura de seguridad que es nuestra amenaza

Alfabetización a los usuarios desde su punto de vista para que entiendan que es el ENS

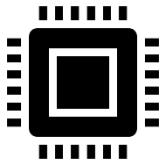
Aportamos el acompañamiento necesario para ir de la mano

Diagnóstico de Seguridad. Conocer el sistema para saber hasta que punto es resiliente

Trato diferenciador. Disponemos de un portal que te ayuda

Análisis de contexto. Visión Global de la Amenaza y Análisis de la superficie de exposición de la propia entidad

Definimos roles y estructuras que a la hora de priorizar nos den un criterio

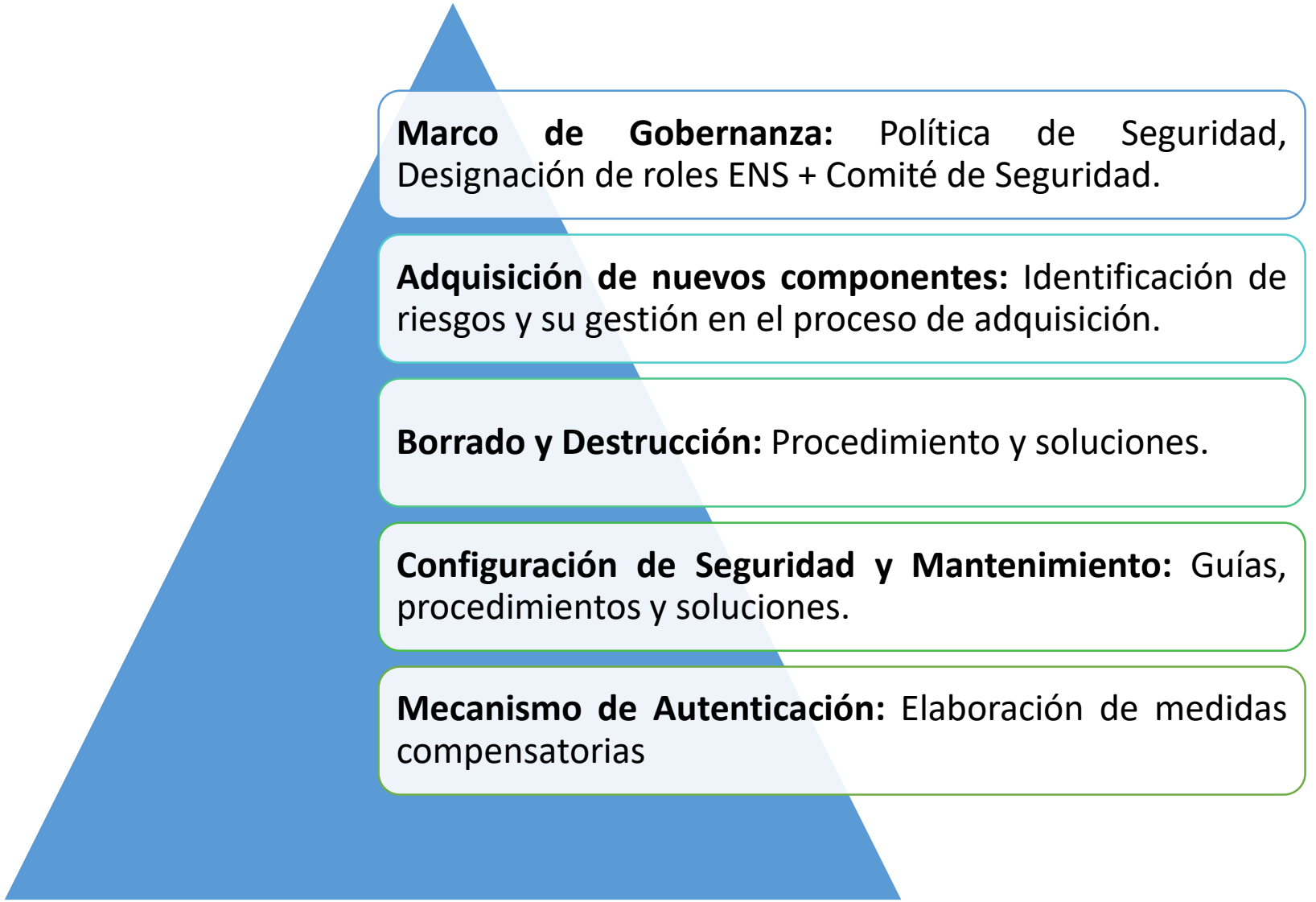


Desarrollamos tecnologías y las evolucionamos

Análisis de Riesgos dinámico que te permite en cada momento adaptarte

Cumplimiento. Protocolizar todo para disminuir la probabilidad de error y reducirla al mínimo

Top 5 Medidas que requieren mayor esfuerzo en la Adecuación



Marco de Gobernanza: Política de Seguridad, Designación de roles ENS + Comité de Seguridad.

Adquisición de nuevos componentes: Identificación de riesgos y su gestión en el proceso de adquisición.

Borrado y Destrucción: Procedimiento y soluciones.

Configuración de Seguridad y Mantenimiento: Guías, procedimientos y soluciones.

Mecanismo de Autenticación: Elaboración de medidas compensatorias

+ 10

Modelos de documentos de marco normativo y desarrollo procedimental para la adecuación al framework de seguridad de referencia

Lecciones Aprendidas Medidas compensatorias en organismos similares

Análisis del Contexto de la Seguridad del servicio finalista.

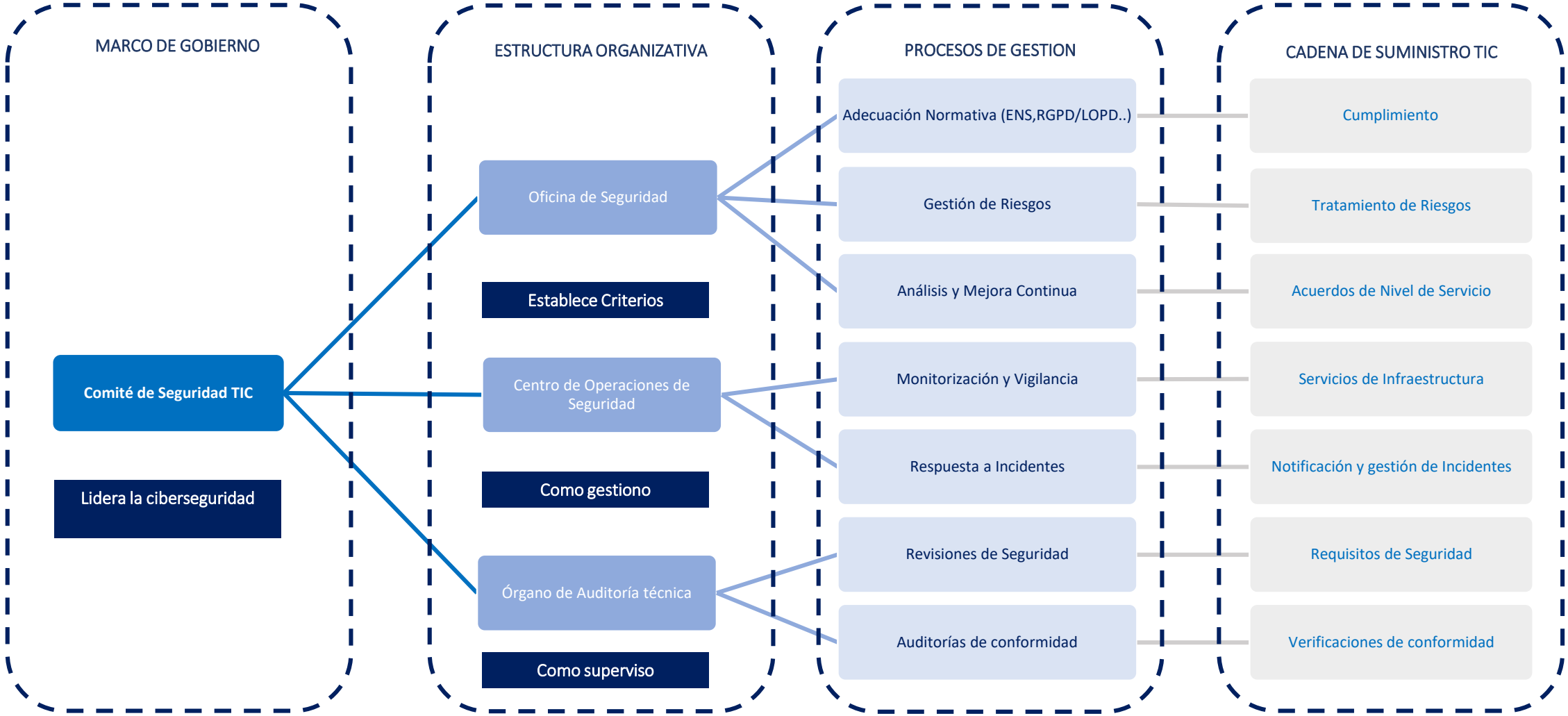
Caducidad de contraseñas
El Organismo no cuenta actualmente con una infraestructura de Active Directory, de modo que todos los equipos Windows tienen cuentas exclusivamente locales.

Equipos Legacy
Existen algunos equipos de laboratorio que cuentan con sistemas operativos sin soporte.

Concienciación
El Plan de Concienciación y Formación asociado al modelo µCeENS en base al Perfil de plantea dificultades para llevarse a cabo, ya que existe una gran rotación de personal adscrito a proyectos de investigación.

Declaración de aplicabilidad firmada por el responsable de la Seguridad

Aproximación al Marco de Gobernanza



Identificación del ciclo de mejora continua

¿Después de obtener la certificación que hacemos?

01/ Selección de medidas de seguridad a incorporar **definición de un plan progresivo de mejora de la seguridad.**

02/ Definición de **hoja de ruta** para cumplir con ese plan.

03/ **Apoyo en la identificación de otras medidas de seguridad** que pueden cumplir.

04/ **Redefinir, completar y mejorar** las normas y procedimientos. Evolucionar el Esquema.

> **Seguimos evolucionando con el modelo**

1 **Avanzando en la adopción de medidas:** mejorando la postura de seguridad de los organismos certificados.

2 **Consolidando la metodología** de acompañamiento, automatización e integración en el Portal de Gobernanza.

Eje del nuevo modelo y ciclo de mejora continua

Simplificación y evolución

Formación y diagnóstico

- Diagnóstico de adecuación por Modelo 73 medidas
- Documento de Seguridad

Consolidación del acompañamiento

- Mayor autonomía
- Disminución de los tiempos
- Propuesta de medidas de acuerdo al contexto del organismo

Implantación

- Soluciones técnicas
- Plan de formación

Mejora continua permanente

- Mejorar la postura de seguridad de los organismos con independencia de la categorización

Proceso mejora continua

Actuaciones de mantenimiento

29 mejoras que son el resultado progresivo de aplicar, con la recurrencia que requieren, las herramientas que nos ofrece µCeENS

org, op.pl, op.acc, op.exp, op.mon, mp.per mp.eq, mp.com, mp.si, mp.info, y mp.s

Medidas a corto plazo

14 mejoras necesarias para mejorar la postura de seguridad de la organización y mantener los niveles de seguridad requeridos

op.pl, op.exp, op.nub, op.mon, mp.if, mp.com, mp,sw y mp.si.

Medidas a medio plazo

9 mejoras necesarias para mejorar la postura de seguridad de la organización y mantener los niveles de seguridad requeridos

op.pl, op.acc, op.exp, mp.if, y mp.si.

Medidas a largo plazo

7 mejoras Necesarias para la organización: requieren mayor esfuerzo e inversión

op.pl, op.exp, op.mon y mp.if.

Nivel de esfuerzo incremental teniendo en cuenta la capacidad de la organización y los recursos disponibles

Hoja de ruta a seguir en el Portal de Gobernanza: contenido y autoayuda

Ventajas en la aplicación del framework de seguridad

Adecuación, implantación y Ciclo de mejora continua

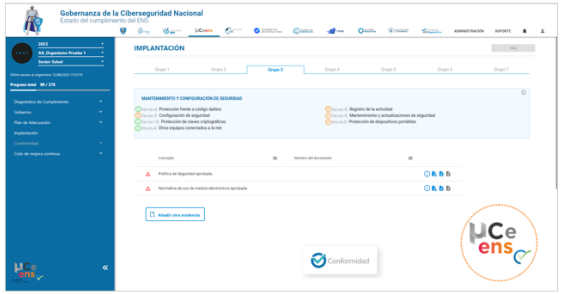
1. **Adopción de una Postura de seguridad adaptada al medio**, disuasoria de la amenaza y con riesgo residual asumible: Perfil de Cumplimiento Específico (PCE)
2. **Selección del plan de adecuación en base al diagnóstico:** Modelo µCeENS o estándar.
3. **Acompañamiento asistido** / automatizado en el Portal
4. **Guía de modelos y procedimientos requeridos** (automatizados)
5. **Simplificación / unificación del proceso de Certificación**: Evidencias de herramientas propias o de la solución ABS (cuando aplique).
6. **Identificación de medidas** (una o más) para mejorar la postura de seguridad (por ej.: en base al riesgo del Sector).
7. **Plan de formación continuo:** trazabilidad y adaptado según necesidades

Adoptar una postura de seguridad realista

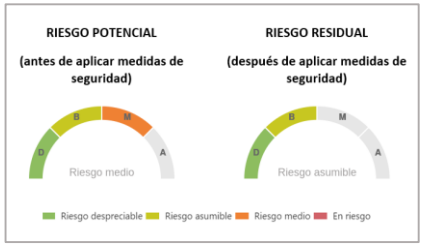
La aproximación del Modelo pivota alrededor de la postura de seguridad en tres (3) pilares como punto de partida y evolución del mismo

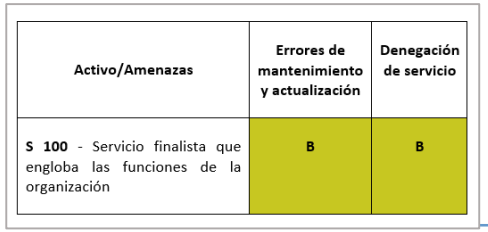
1. **Postura de seguridad** de la organización en base al **contexto cambiante de la amenaza**

2. **Postura de seguridad** determinada en función del **nivel de Madurez de la organización**



3. **Postura de seguridad** validada por el **cumplimiento normativo** mediante un **Perfil de Cumplimiento Específico (PCE)**





Activo/Amenazas	Errores de mantenimiento y actualización	Denegación de servicio
S 100 - Servicio finalista que engloba las funciones de la organización	**B**	**B**

Caso de Uso. PCE en base a CCN-STIC 890C

Definición del alcance: Servicio Finalista, prestado a terceros y descritos en las funciones del organismo

- **Recopilación de evidencias propias o Automatizadas con las Soluciones ABS mediante carga automática (Plataforma de Gobernanza).**
- **Modelos de Plantillas de documentos y procedimientos predefinidos adaptables a todo tipo de organizaciones.**
- **Plan de formación integrado en ÁNGELES.**
- **Tips de ayuda en la plataforma que te ayudan a cumplir con las medidas de seguridad**

Definición de Proceso de Mejora Continua adaptado a las organizaciones con actuaciones de mantenimiento, actuaciones a corto, medio y largo plazo

- **Obtención de la certificación entre 3-4 meses**
- **No es requisito para la certificación que el sistema lleve implantado al menos 3 meses.**
- **El proceso de Auditoría está totalmente Automatizado**
- **Tasa de certificación del 100%**

Comunidad ENS es una realidad

Somos lo que defendemos

La aportación real de nuevo ENS es un cambio cultural, una actitud y una manera de entender la ciberseguridad.

Innovación

Buscar **soluciones prácticas** a problemas del día a día con **estrategias simples y creativas** dando soluciones que sean **escalables**.

Eficiencia

Producto básico, mínimo viable, sin extras, pero de la misma calidad **sin sacrificar la funcionalidad** en el proceso (profesionalización y automatización de procesos).

Fidelizar

Atender a las necesidades dando un **apoyo y soporte dimensionado** a los recursos y nivel de madurez identificados.

Reconocer

Acción de distinguir como consecuencia de **alcanzar los objetivos marcados**.

Cada equipo tiene sus objetivos específicos
Todos tienen una misión común

El ENS nos ayuda a implantar las medidas de seguridad, ya que nos indica como debemos realizarlo de una forma práctica

Servicios en la nube [op.nub]

1

Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC .

Unifica las medidas de seguridad entre organizaciones.
El ENS nos ayuda a cumplir una 27001 de manera premium.

Seguridad de la información para el uso de servicios en la nube

2

Los procesos de adquisición, uso, gestión y finalización de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.

ISO nos dice que tenemos que hacer y cómo se debería implantar**,** pero deja el control tan abierto con sus “deberías” (tener en cuenta que en el 5.23 aparece 9 veces la palabra debería) **que dos (2) organizaciones en las que aplique esta medida de seguridad no se pueden equiparar a nivel de seguridad global ya que van a ir a mínimos aplicando la teoría del debería que no es obligatorio (concepto de cumplimiento).**

El ENS nos ayuda a obtener una visión global de las medidas de seguridad que se aplican en las organizaciones

1

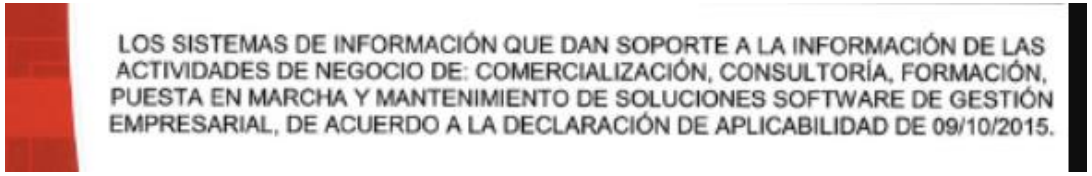
En ENS podemos ver las medidas de seguridad aplicables por cada nivel de seguridad (certificado) y tener una visión más amplia del nivel de seguridad que se está aplicando en la organización.

CATEGORÍA MEDIA	C	I	T	A	D	Total de medidas
	MEDIO	*MEDIO*	*MEDIO*	*MEDIO*	*MEDIO*	*68*

Podemos comparar entre 2 proveedores que prestan el mismo servicio quien tiene mayores medidas de seguridad.

2

En los certificados de ISO 27001 se hace referencia a la versión vigente de la declaración de aplicabilidad de acuerdo a los criterios establecidos en la 27006. Sin embargo, no se puede saber el número de controles reales implantados en una organización.



Falta de transparencia.

El Dinamismo del ENS

1

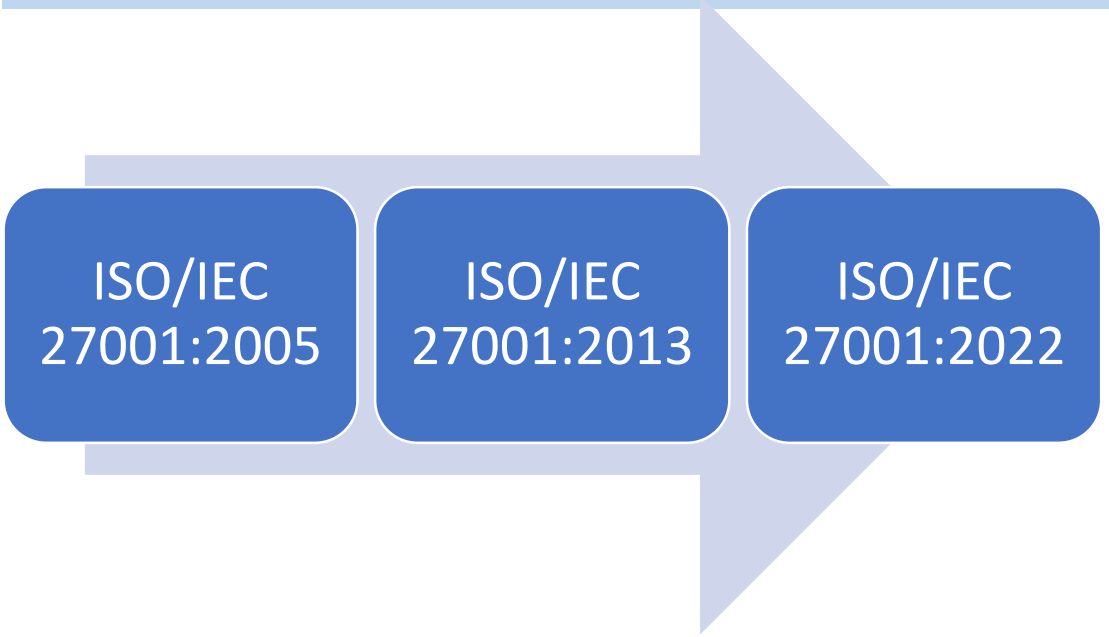
El ENS con las guías y los abstract se están actualizando continuamente al nivel de seguridad actual.

Desde Enero de 2023 hasta Julio se han publicado y actualizado + de 40 guías de seguridad

CCN-STIC-1451 Procedimiento de empleo seguro Extreme Networks Virtual Services Platform (VSP) Series Switches	Jul 2023	Jul 2023	Descargar
CCN-STIC-1453 Procedimiento de empleo seguro Cortafuegos OPNsense	Jul 2023	Jul 2023	Descargar
CCN-STIC-1444 Procedimiento de Empleo Seguro FortiAnalyser	Jul 2023	Jul 2023	Descargar
CCN-STIC-1443 Procedimiento de Empleo Seguro FortiManager	Jul 2023	Jul 2023	Descargar
CCN-STIC-1225 Procedimiento de Empleo Seguro SPLUNK	Jul 2023	Jul 2023	Descargar
CCN-STIC-1222 Procedimiento de Empleo Seguro Agente Cortex XDR	Jul 2023	Jul 2023	Descargar
CCN-STIC-825 Esquema Nacional de Seguridad. Certificaciones 27001	Nov 2013	Jul 2023	Descargar
CCN-STIC-889I Guía de Configuración segura para Oracle SaaS Fusion Applications	Jul 2023	Jul 2023	Descargar
CCN-STIC-889H Guía de Configuración segura para Oracle SaaS Enterprise Performance Management EPM	Jul 2023	Jul 2023	Descargar
CCN-STIC-889G Perfil de Cumplimiento Específico Oracle Cloud SaaS Servicio de Cloud Corporativo	Jul 2023	Jul 2023	Descargar

2

El proceso de revisión de las ISO se estima que se debe realizar cada cinco (5) años, aunque en la mayoría de las ocasiones estos plazos se incrementan hasta los ocho (8) y nueve (9) años.



Adaptación del ENS a las necesidades del sector

1

Se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad.

El ENS permite crear perfiles de cumplimiento dentro del esquema adaptándose a las necesidades de diferentes sectores para fomentar la seguridad Ej SOCS, OT, Organismos Pagadores, Universidades….

Estos perfiles se desarrollan en colaboración con expertos de cada sector.

2

Iso 27001 nunca es suficiente para adaptarse a las necesidades de cada sector por lo que en la mayoría de las ocasiones se deben implementar normas adicionales y continuamente se están desarrollando nuevos marcos normativos al lado de la ISO 27001.

TISAX ENX ASSOCIATION

PINAKES

HIPAA

ISO 27017	ISO 27701	ISO 27018	ISO 9001	ISO 22301
Controles específicos de la nube	Administración de la información sobre la privacidad	Protección de datos personales	Estándar de calidad internacional	Seguridad y resistencia

Unificación de criterio técnico de las certificadoras

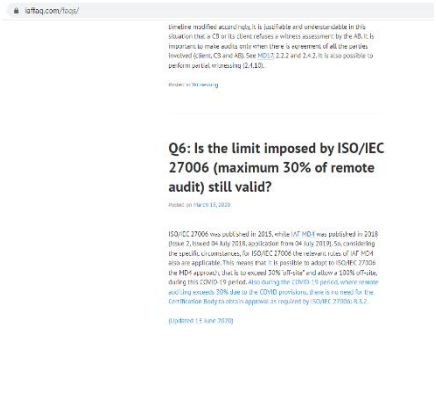
1

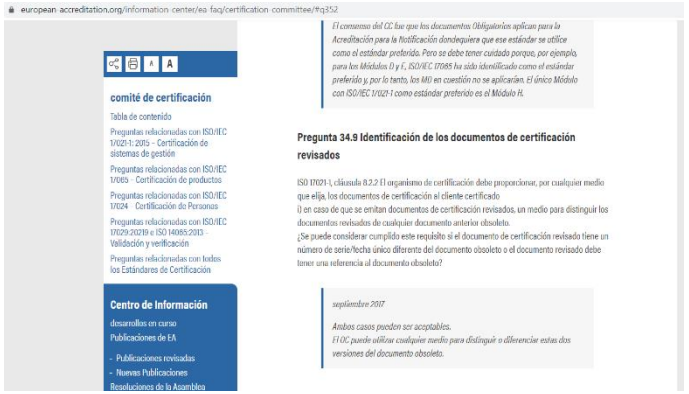
El CoCENS fue creado como órgano colegiado que incorporara a todas las partes, ayudar a la adecuada implantación del ENS y, en consecuencia, a una mejor prestación de los servicios públicos, que es uno de los objetivos más importantes del ENS.

1. **Realización de reuniones cuatrimestrales para unificación de criterios de todas las certificadoras. Cuenta de correo electrónico a disposición de todas las partes interesadas para informar de problemáticas, resolución de dudas.**
2. **Publicación de todos los criterios y directrices de forma gratuita en la página del CCN**
   https://ens.ccn.cni.es/es/certificacion/cocens
4. **Cuando te viene de origen otro certificado de otra entidad ya sabes que cumple unos mínimos.**

2

Iso 27001 diferencia de criterios entre certificadoras “me certifico con XXXX porque me pide menos”, procesos de transferencia dolorosos por la correcta interpretación de la norma… Demasiadas fuentes de información de “interpretaciones”, las certificadoras no tienen voz ni voto. Diferencia entre entidades de acreditación Ej. ANAB no tiene Áreas Técnicas en 27001 y las acreditadoras Europeas sí.

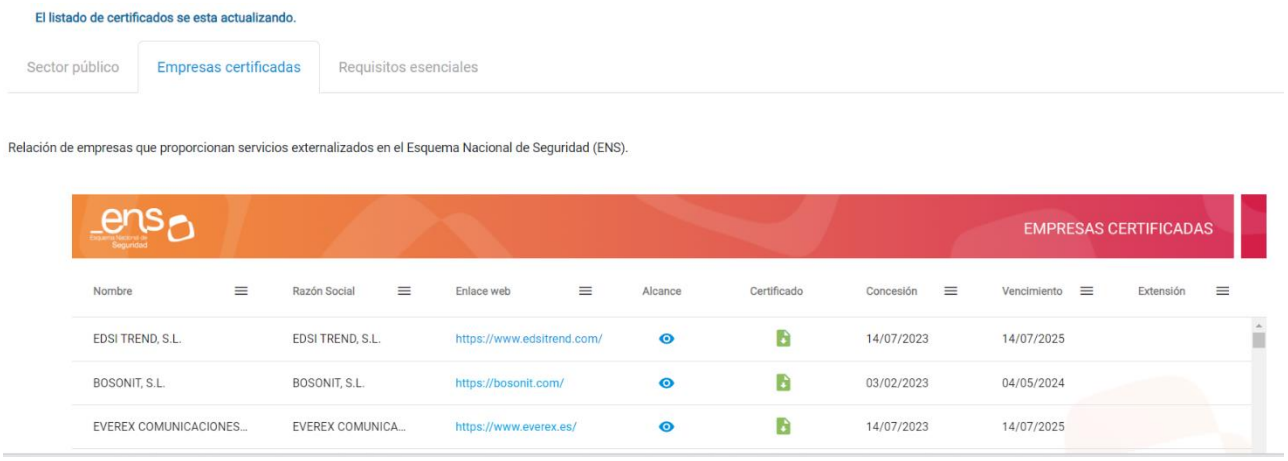




Just in time del estado de los certificados

1

En cualquier momento se puede consultar el estado de un certificado de ENS.



2

Iso 27001 a menudo se reproducen problemáticas para saber si un cliente esta certificado o no, ya que es imposible consultar la validez de un certificado en estado real de todas las certificadoras.

Robustez del ENS y Vigilancia continuada del esquema

1

Los informes de ENS quedan a disposición del CCN CERT. Notificación de Resumen de Hallazgos de las certificadoras.

Notificación de Resumen de Hallazgos

En caso de realizar el proceso de auditoría por medios ajenos a AMPARO, se podrá incluir únicamente el Resumen de Hallazgos de Auditoría:

- **(Organismo) –** Adecúa el sistema y solicita la auditoría por medios ajenos a AMPARO.
- **(Entidad Auditora)** – Ejecuta la Auditoría de Conformidad por medios ajenos a AMPARO.
- **(Entidad Auditora) –** Da de alta el sistema auditado en AMPARO como un sistema nuevo.
- **(Entidad Auditora) -** Ahora tiene **acceso a las medidas del ENS** (sin documentación) y los paneles de No Conformidades.
- **(Entidad Auditora) – Completa las No Conformidades y Observaciones** de acuerdo a lo observado en la auditoría.
- **(Entidad Auditora)** – Completadas las No Conformidades, modifica el estado del sistema a **Conforme**.

1. **Permite conocer en qué medidas de seguridad están más inmaduras las organizaciones “Top ten de no conformidades” para dotarles de herramientas e instrumentos de mejora de la seguridad.**
2. **Permite que una entidad de certificación sea auditada por el CCN para saber su estado de seguridad.**

2

Iso 27001 no dispone de una base de datos de conocimiento que nos alerte de la problemática que tienen las organizaciones a la hora de implantar los controles.

1. **No hay una vigilancia continuada**

Flexibilidad Auditorías en remoto y extensión validez de certificados

1

Será posible realizar inspecciones en modo remoto durante las Auditorías de Certificación del ENS (iniciales o de renovación, sobre clientes conocidos o desconocidos), usando medios telemáticos (como, por ejemplo, videoconferencia y compartición de escritorio remoto), siempre que se considere dicha actividad como viable por parte de la Entidad de Certificación y acorde con los procedimientos de auditoria establecidos, habiendo previamente analizado el riesgo derivado de evaluar telemáticamente a su cliente, y poder justificarlo adecuadamente ante ENAC y el Centro Criptológico Nacional.

1. **Permite solicitar una extensión del certificado de 3 o 6 meses.**

2

Iso 27001 **no permite realizar más de un 30%** de la Auditoría en remoto salvo autorización expresa de la entidad de Acreditación, aspecto que viene recogido en la ISO 27006.

No permite solicitar extensión de los certificados

En las Auditorias de Ciclo Inicial

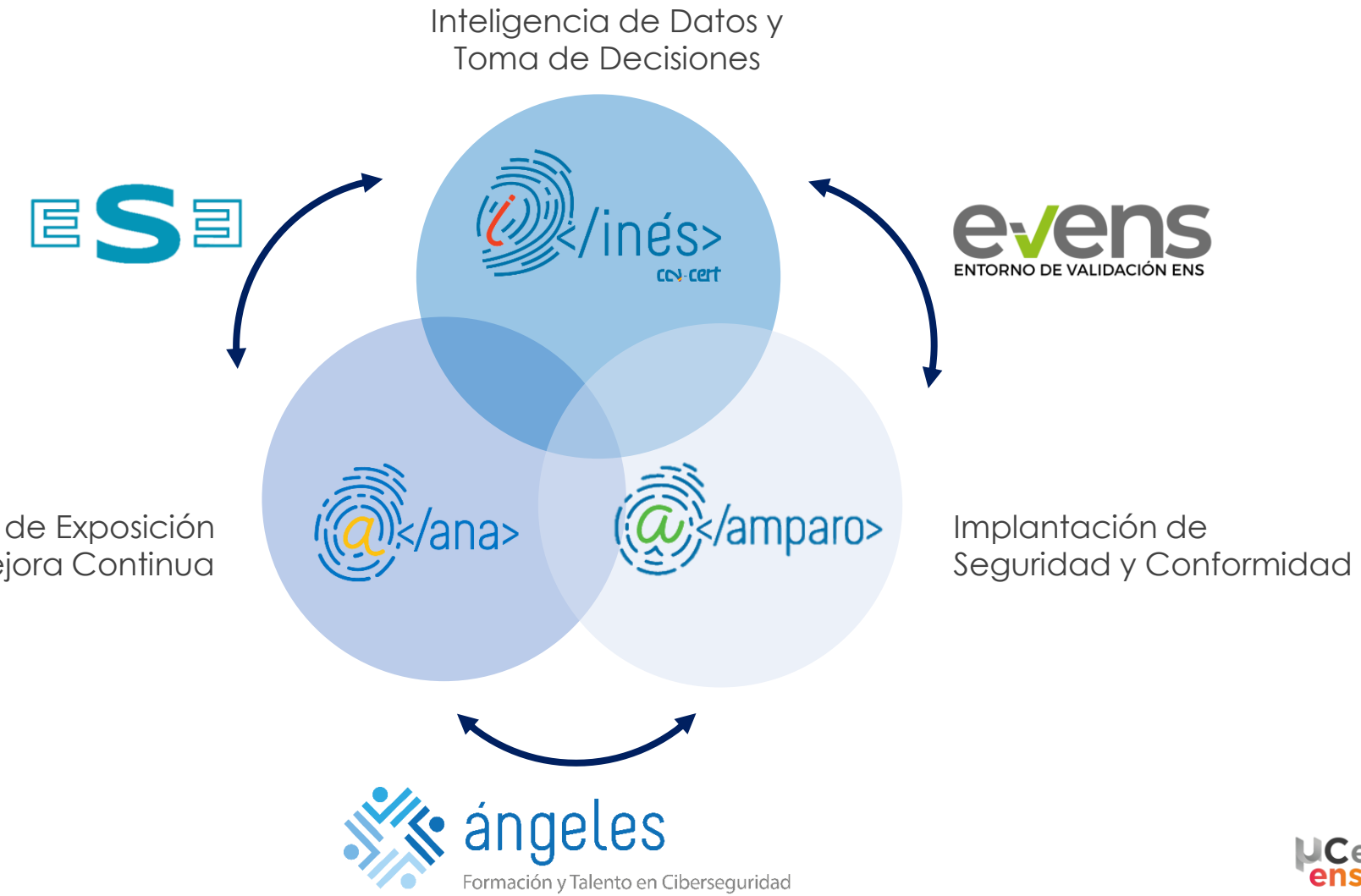
- Las As1 se deben realizar antes de los 12 meses desde la fecha de concesión
- Las As2 se deben realizar a los 24 meses desde la fecha de concesión con un intervalo de +- 3 meses

En el caso de que las Auditorías no se realicen dentro del ciclo de la certificación se suspende el certificado .

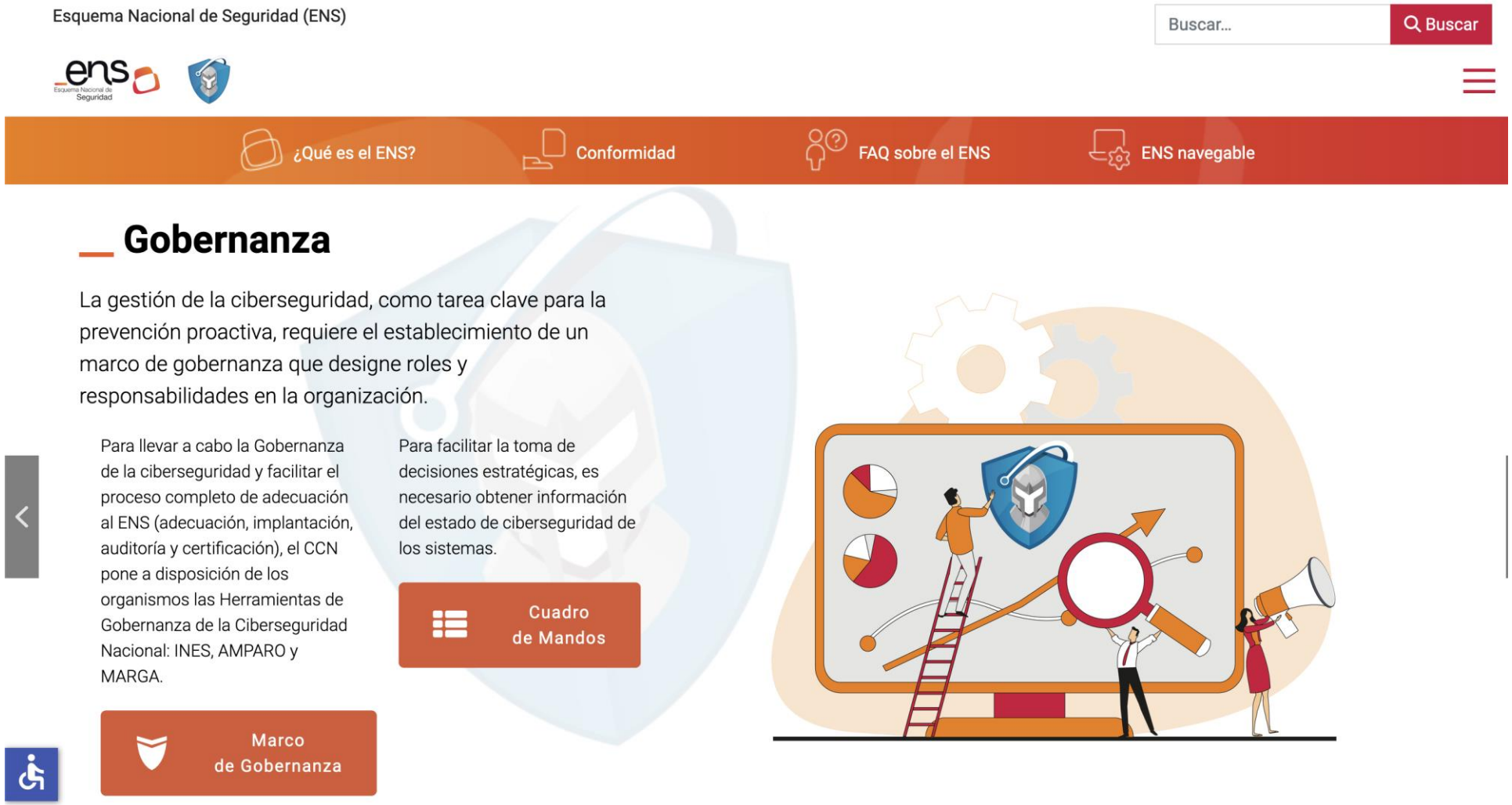
Las defensas deben adaptar su aproximación a la prevención, detección y respuesta

- **Implantar y conseguir la adecuación al ENS:** Estándar de referencia para conseguir una postura de seguridad adaptada a la potencial amenaza.
- **Despliegue de tecnologías certificadas / cualificadas** impulsando el empleo de catálogos, sellos de certificación y otros esquemas para IoT o control industrial.
- **Aplicar la mejora continua como estrategia:** Dinámica e inercia para implementar ciberseguridad basada en contrastar la superficie de ataque priorizando la postura de seguridad.
- **Formación y educación continua:** Sensibilizar a usuarios, responsables Tic y dirección.
- **Metodología del desarrollo seguro** para analizar y evaluar las amenazas, identificar los puntos débiles, implementar soluciones seguras, acelerar el desarrollo, y, en definitiva, mejorar la postura de seguridad de la organización.
- **Vigilancia Continua** en todas las redes, sistemas y en sus interconexiones (ZERO TRUST).
- **Automatizar la respuesta** para concentrar los recursos en los ataques complejos.
- **Intercambio automatizado y continuo** como prioridad.

Gestión Continua de la Seguridad



Nuevo Portal ENS



Aproximación posibilista…

Camino a seguir…

1. Estrategia de ciberseguridad.
2. Gobernanza de la ciberseguridad.
3. **Desarrollo reglamentario posibilista.**
4. CSIRT de referencia, sectoriales y SOCs.
5. **Capacidad de detección y alerta temprana.**
6. **Incremento de vigilancia (SOC).**
7. Capacitación y búsqueda de talento.
8. **Cooperación pública-privada. (comunidad**)
9. Intercambio de información. (confianza)
10. Comunicación y promoción. (ser referencia)

¡Muchas gracias!

CONTACTO

normativa@ccn.cni.es

ccn@ccn.cni.es

PÁGINAS WEB

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es

CCN
centro criptológico nacional