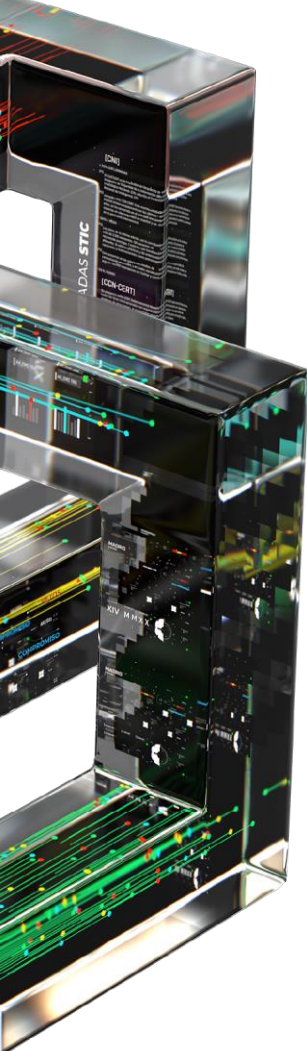
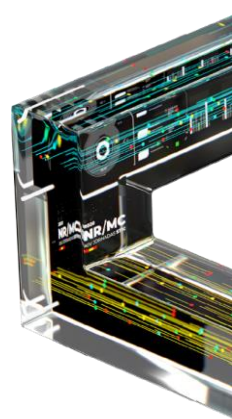




#XIVJORNADASCCNCERT

**ENAIRE, Operador de Servicios
Esenciales conforme al
Esquema Nacional de
Seguridad en Categoría ALTA**

Diciembre de 2020





Gerardo Sarmiento Fernández

ENAIRE

gsarmiento@enaire.es

Miguel A. Lubián

Grupo CÍES

miguel.lubian@grupocies.es

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

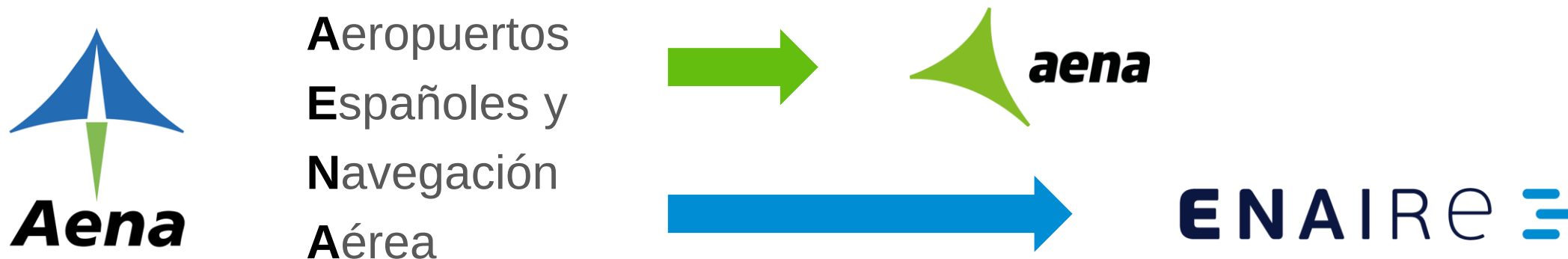


¿Qué es ENAIRE?

Certificación ENS en Categoría Alta

ENAIRe – Operador de Servicios Esenciales

Antes de comenzar, un poco de historia: ¿Qué es ENAIRe?



Entidad Pública Empresarial dependiente del Min. de Transportes, Movilidad y Agenda Urbana.
 Principal proveedor de servicios de navegación aérea y de información aeronáutica en España.
 Proveedor de servicios de comunicaciones, navegación y vigilancia (CNS).

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Breve descripción de la **experiencia** en primera persona, destacando:

- ✓ **Particularidades** como Operador de Servicios Esenciales.
- ✓ Dificultades y **retos** abordados durante el proceso.
- ✓ **Soluciones** aplicadas hasta lograr el objetivo.



Sistemas operacionales críticos involucrados en la
prestación de los servicios de **Navegación Aérea**

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Definición y
alcance

¿Qué queremos mejorar/certificar?



Dificultades y RETOS:

- **Complejidad** técnica de los sistemas.
- **Dispersión geográfica** de las instalaciones.
- **Estructura** funcional y organizativa.
- Desconocimiento del ENS por parte de los **usuarios**.



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Definición y
alcance

¿Qué queremos mejorar/certificar?



SOLUCIONES aplicadas:

- Definición a alto nivel y **respaldo explícito de la alta dirección.**
 - Impulso necesario para la priorización, adaptación de procesos e inercias.
- Participación de personal técnico y creación de **grupos de trabajo.**
- **Valoración con los propietarios** de la Información y Servicios.
 - **Alta Disponibilidad, baja Confidencialidad.**
- Inventario de Activos, Análisis de Riesgo y su **preceptivo plan de tratamiento.**



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Documentación y
evidencias

¿Cómo satisfacemos los controles?



Dificultades y RETOS:

- **Complejidad** y extensión de los sistemas.
- Grado de **exigencia** de los controles.
- **Volumen documental** y procedimental existente.
- Satisfacción de requisitos y registro de **evidencias**.



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Documentación y
evidencias

¿Cómo satisfacemos los controles?



SOLUCIONES aplicadas:

- Participación de personal técnico y **respaldo de la dirección.**
- **Revisión técnica y documental** exhaustiva.
- Análisis detallado de **procedimientos y tecnología.**
- Registro y vinculación de controles con **evidencias** documentales.



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Auditoría y
cumplimiento

Normativa teórica vs Realidad práctica



Dificultades y RETOS:

- **Planificación** compleja a medio / largo plazo.
- Tecnología **específica**, escasos proveedores, desarrollos a medida.
- Despliegues y evolución constantes tras **validaciones** exhaustivas.
- Normativa y requisitos muy estrictos de **seguridad operacional**.



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Auditoría y
cumplimiento

Normativa teórica vs Realidad práctica



SOLUCIONES aplicadas:

- Sabemos que **somos seguros**: explicación de “qué” y “por qué”.
- Podemos **demostrarlo**: evidencias de “quién, cómo, dónde y cuándo”.
- Debemos **documentarlo**: elaboración de “medidas compensatorias y complementarias de vigilancia”.
- **Traducción** de “nuestra realidad” al “lenguaje ENS”.



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

1. Situación Inicial: El reto.
2. Definición de nuestra estrategia.
3. La Implementación.
4. Verificación: La Auditoría.
5. Lecciones aprendidas durante el proceso.

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Situación de partida: Año 2016

En ENAIRE, ¿**nos aplica el ENS**? ¿De forma supletoria a otras normativas que si tenemos claras? ¿Alguna predomina sobre otra? (Estado pre-Guía 830 CCN)

- Se cuestiona ámbito subjetivo y ámbito material.

En ENAIRE **no vemos forma sencilla de aplicar el ENS.**

- Singularidad de nuestro negocio (elemento nuclear no es el procedimiento administrativo/sede electrónica).
- Singularidad de nuestra tecnología (aquí todo es muy diferente, tanto en tecnología como sobre el “control efectivo” en la cadena de suministro).

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales



Sector Público Institucional

CGAE

Consejo General de
la Abogacía
Española

www.abogacia.es

Detalle ▼

27/12/2013

MEDIA

AÑO 2016

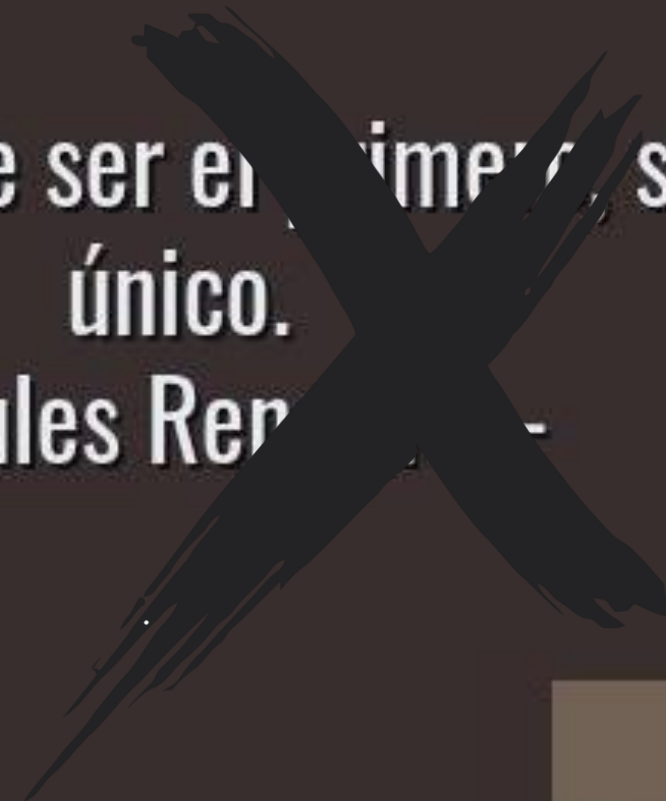
Certificación ENS en Categoría Alta



“

No se trata de ser el primero, sino el
único.

— Jules Renard —



”

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales



¿Vamos a hacer un
análisis general de
nuestra seguridad?

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Y aquí empezamos a ver que teníamos muchas iniciativas interesantes:

- Se **realizaban auditorías periódicas de seguridad técnica**, incluso por organismos reguladores externos (en nuestro caso AESA).
- Existe **muchísima documentación** sobre la operación.
- Los **conceptos básicos de seguridad** estaban muy superados (análisis de riesgos, BIA...).
- Cierta madurez en continuidad de negocio (**resiliencia**) por nuestra propia naturaleza.
- Existen grupos de coordinación con diversos **organismos en materia de ciberseguridad** (CCN-CERT, CNPIC, INCIBE, OCC, AESA, etc.) e incluso a nivel internacional (CANSO, SESAR, EASA, Eurocontrol, etc.).



En general, hay un **cierto orden en la materia**, sin perjuicio de riesgos intrínsecos, otros derivados de nuestros legacy o la propia evolución tecnológica que nos supone una mayor exposición.

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales



Luego, hicimos un
Assessment conforme
al ENS (GAP)

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Aunque en algunos controles puntuales salíamos muy bien parados...



- 5 Medidas de protección [mp]
 - 5.1 Protección de las instalaciones e infraestructuras [mp.if]
 - 5.1.1 Áreas separadas y con control de acceso [mp.if.1]
 - 5.1.2 Identificación de las personas [mp.if.2]
 - 5.1.3 Acondicionamiento de los locales [mp.if.3]
 - 5.1.4 Energía eléctrica [mp.if.4]
 - 5.1.5 Protección frente a incendios [mp.if.5]
 - 5.1.6 Protección frente a inundaciones [mp.if.6]
 - 5.1.7 Registro de entrada y salida de equipamiento [mp.i]
 - 5.1.8 Instalaciones alternativas [mp.if.9]

- 4.5 Continuidad del servicio [op.cont]
 - 4.5.1 Análisis de impacto [op.cont.1]
 - 4.5.2 Plan de continuidad [op.cont.2]
 - 4.5.3 Pruebas periódicas [op.cont.3]

<https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1001>

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

La realidad es que, en muchos de ellos, la situación era complicada:



- Bastantes medidas de seguridad nos parecían literalmente “**imposibles**” por nuestra singularidad.
- Con algunas medidas de seguridad **no nos sentíamos identificados.**
- Algunas medidas de seguridad, simplemente, **no las cumplíamos.**

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Muchas medidas de seguridad eran literalmente imposibles de cumplir:

- [op.ext.1] Existen servicios **externos** con **tecnología propietaria** y **sin** conformidad con ENS.
- [mp.eq.2] En una **posición de control** no te puedes plantear el **bloqueo del puesto de trabajo**.
- [op.acc.1] En una **posición de control** el concepto de **identificación / trazabilidad** no es como el concebido por el ENS.
- [op.mon] Imposibilidad de **monitorizar de forma tradicional** algunos sistemas críticos.
 - Los sistemas en tiempo real no son amigos de procesos que puedan generar “delays”.
- [op.exp.6] Sucede igual con la imposibilidad de incluir elementos de **protección de código dañino**.

El mundo **operacional** tiene una **inercia** compleja de alterar.

(Para introducir la seguridad desde el diseño.)

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Con otras medidas (menos) de seguridad no nos sentíamos identificados (en nuestra parte CORE):

- [mp.info.4] Política de [firma electrónica](#).
- [mp.info.5] [Sellos de tiempo](#).
- [mp.s.2] Algunos controles muy orientados a “sede electrónica.” La protección de servicios y aplicaciones web ([OWASP](#)) en servicios “core”.
- [mp.info.3] [Cifrado fuerte en algunas comunicaciones](#) no orientado a nuestro modelo operacional, pues aplicación implicaría una carga de CPU que no lo hace viable/factible en entornos en tiempo real (delays no asumibles).



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Otras medidas de seguridad, simplemente, no las cumplíamos:

- No existía una [organización de la seguridad](#) conforme a los requisitos del ENS.
- Precisamos [adaptar los procesos](#) (no siempre nos tienen en cuenta todo lo necesario).
- Dificultad tradicional de aplicar [2FA](#).
- Desarrollo de [competencias digitales en seguridad](#).
- Falta de información por parte de los [prestadores](#) (las actuales guías on-premise).

Estas no suponían mayor problema, como en cualquier otro proyecto.

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales



Algo estaba fallando en la ecuación

Nuestra percepción de seguridad no era mala.

Pero no se correspondía con el grado de cumplimiento ENS.

Nuestros indicadores de seguridad son diferentes a los indicadores del ENS (IM/IC).

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales



IDEA

Vamos a buscar una
primera conformidad con
la parte tradicional
(BACK-END)

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales



Sabíamos que nos faltaba el CORE, que muchos **servicios eran instrumentales**, pero empezamos a introducir elementos clave en la organización.

(AÑO 2018)

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales



La certificación ENS ha contribuido a generar sinergias con los departamentos de sistemas.

$$1 + 1 = 3$$

¿Cómo lo aterrizamos?



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales



Y ahora, sabíamos que tocaba
empezar a trabajar de verdad:
“Buscar la conformidad con
ENS en nuestro CORE”.

(AÑO 2019)

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Se refuerza la [Oficina de Ciberseguridad](#), compuesta por los tradicionales:

- El [responsable de Seguridad](#) (CISO).
- Perfiles Red Team y Blue Team, pero, sobre todo, gran componente de [Gestión](#).
- Se incorpora un perfil nuevo: El [intérprete](#).

Traducir nuestra realidad al lenguaje del ENS, es decir, conectar la situación real con los requisitos del ENS.

Dilatada experiencia, domina el ENS, conoce del modelo de negocio, capacidad de interlocución.



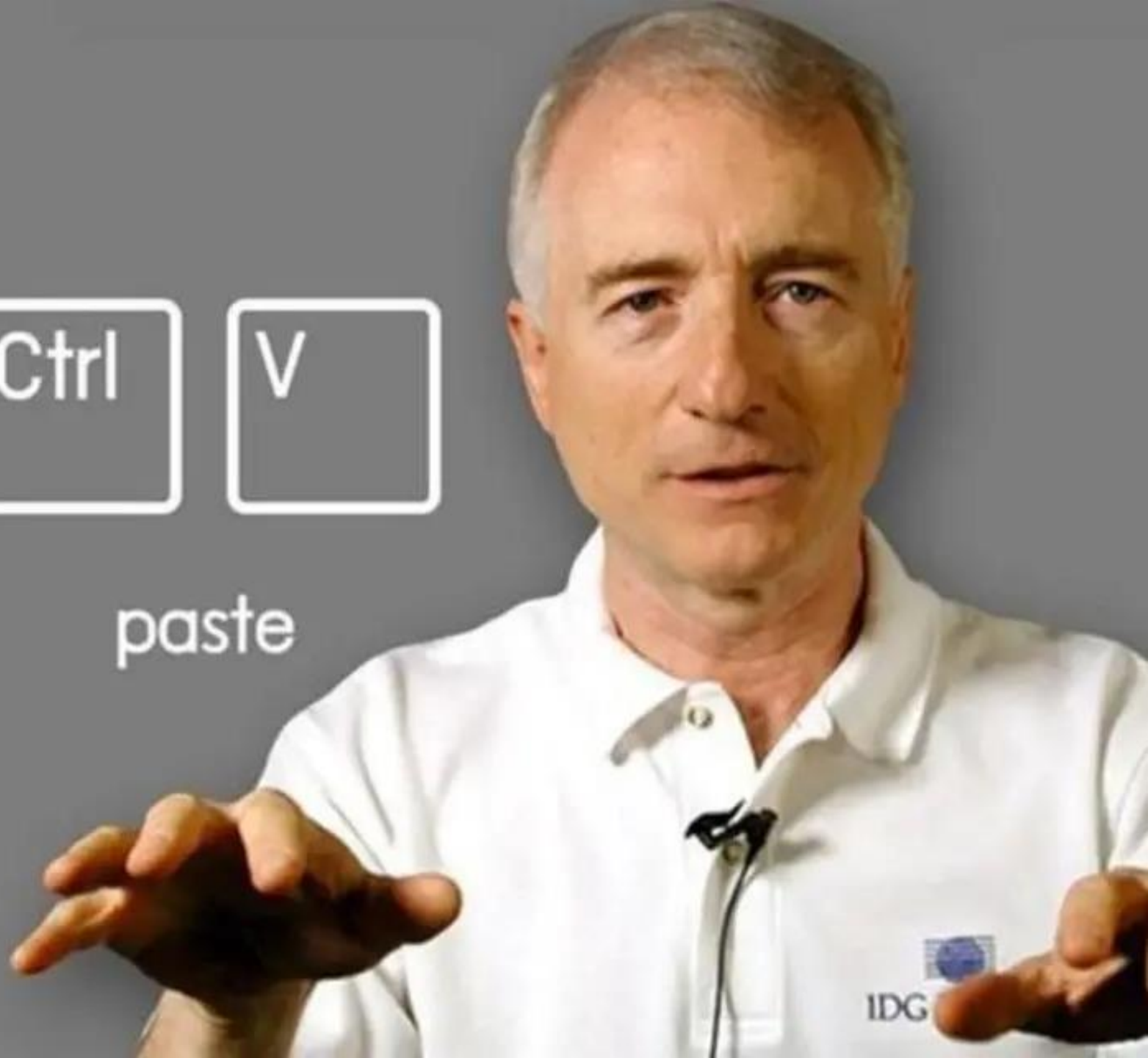
Larry Tesler





copy

paste



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

1

Analizando la **exposición de motivos** de cada control (Anexo II).

Artículo 3 del Código Civil

- 1. *Las normas se interpretarán según el sentido propio de sus palabras, en relación con el contexto, los antecedentes históricos y legislativos, y la realidad social del tiempo en que han de ser aplicadas, atendiendo fundamentalmente al espíritu y finalidad de aquella.*

No habíamos realizado un adecuado ejercicio de interpretación de la norma.



ABSTRACT PUBLICADO CCN (05/05/2020)

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Ahora vemos el ENS como un traje a medida, que responde a nuestras necesidades.

Perfil de cumplimiento específico.



Certificación ENS en Categoría Alta

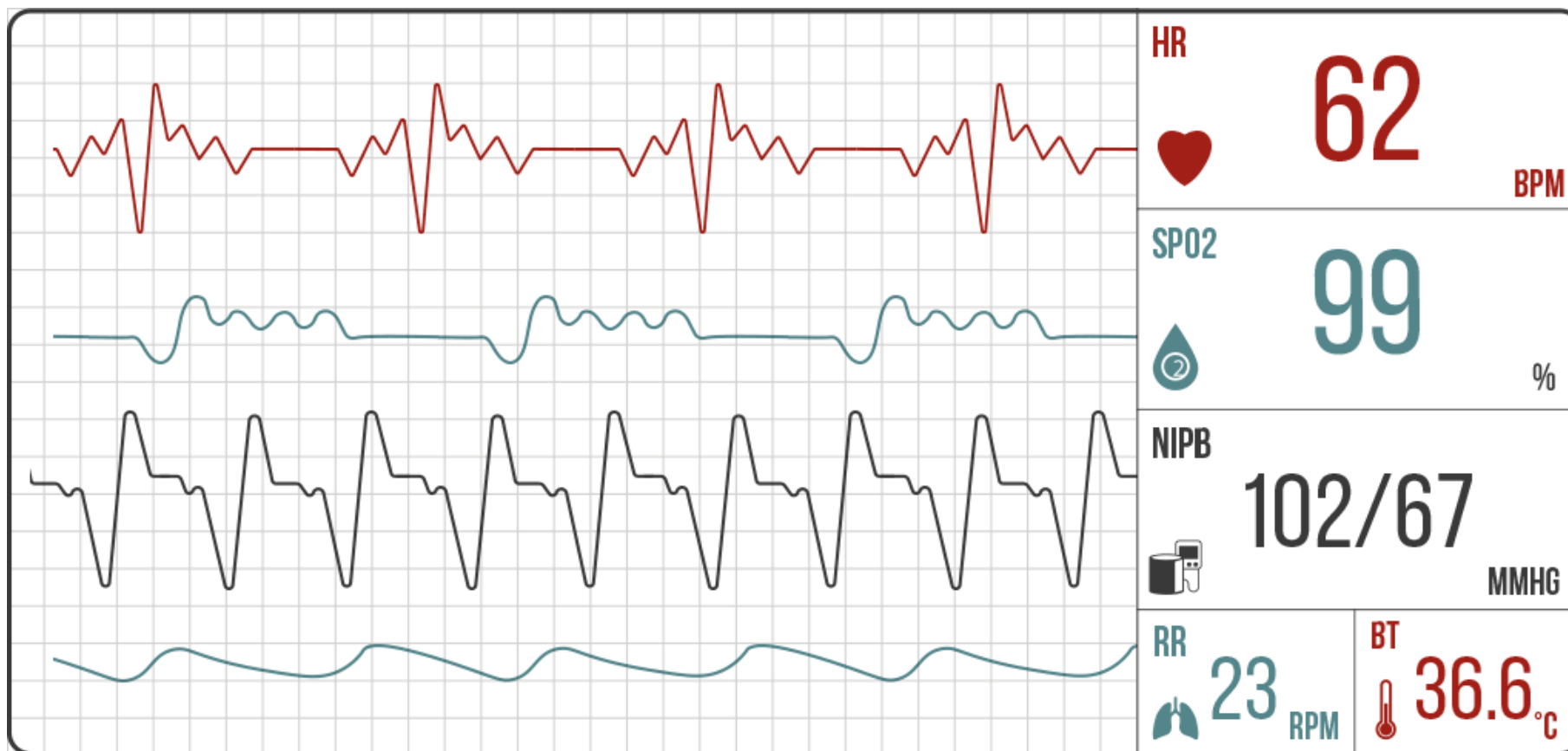
ENAIRE – Operador de Servicios Esenciales



“Que las posiciones de control **no tengan doble factor de autenticación, incluso ni un factor (contraseña), ni bloqueo del puesto de trabajo, no implica ningún tipo de problema en el ENS**, habilitando las adecuadas medidas compensatorias así como los preceptivos complementos de vigilancia.”

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales



Fuente: Imagen Grupo CIES y Ozona Consulting (Herramienta Obsidian)

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

2



Conecta a la organización,
hablando en su idioma.

ENS-glish.
PIC-glish.
GDPR-glish.

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

3

Rastrea iniciativas interesantes, impulsadas por otras áreas, y que contribuyen notablemente al ENS.

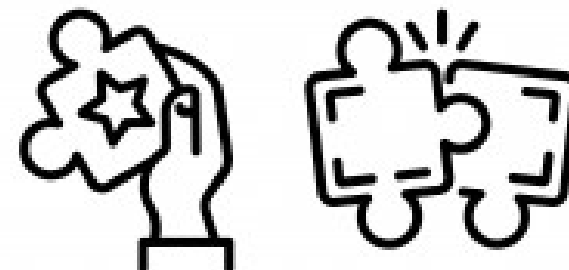


Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales



Algunas iniciativas precisan incorporar medidas de seguridad, utilizando las guías de bastionado del CCN.



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Los compañeros de viaje son esenciales:

- **CCN:** Máxima colaboración (Incluso, un ENS dual).
- **Certificadora:** Adecuada flexibilidad para interpretar.
- **Oficina de Ciberseguridad:**
 - CISO.
 - Hilo conductor.
 - “Expertise” de las consultoras.

BORRADOR DE TRABAJO

Proyecto de Real Decreto .../..., de ..., por el que se regula el Esquema Nacional de Seguridad.

ÍNDICE

CAPÍTULO I. Disposiciones generales

Artículo 1. Objeto

Artículo 2. Definiciones y estándares

Artículo 3. Ámbito de aplicación

CAPÍTULO II. Principios básicos

Artículo 4. Principios básicos del Esquema Nacional de Seguridad

Artículo 5. La seguridad como un proceso integral

Artículo 6. Gestión de la seguridad basada en los riesgos

Artículo 7. Prevención, detección y respuesta

Artículo 8. Líneas de defensa

Artículo 9. Vigilancia continua y reevaluación periódica

Artículo 10. Responsabilidades diferenciadas

CAPÍTULO III. Requisitos mínimos

Artículo 11. Requisitos mínimos de seguridad

Artículo 12. Organización e implantación del proceso de seguridad

Artículo 13. Análisis y gestión de riesgos

Artículo 14. Gestión de personal

Artículo 15. Profesionalidad

LA AUDITORÍA



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Durante el proceso de auditoría contamos con un **problema añadido: la pandemia.**

- Se hizo una parte importante de la auditoría **en remoto**.
- Se precisó un revisión **in situ** para la verificación de una serie de controles.
- La certificadora **supo adaptarse** a la doble situación (pandemia + singularidad de un operador esencial).
- Es tu **mejor aliado** para potenciar cambios.



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

Lecciones aprendidas



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

ASPECTOS CLAVE

1. La operadores esenciales **partimos con mucha base** para afrontar un proceso de certificación.
2. **Formación**: Los responsables hacen ejercicios de: “Qué pasaría si...”.
3. En nuestro caso, hemos identificados nuestros controles críticos, muy cercanos en la dimensión de **disponibilidad**.
4. El **CCN** nos da instrumentos de **adaptación sin perder rigor**.
5. La figura del **intérprete, apoyada por el CISO, fue nuestra clave del éxito**.
6. La papel de la **certificadora** aportó valor, adoptando una postura muy **constructiva**.
7. Ahora vemos el **ENS como un traje a medida**, que responde a nuestras necesidades.



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

BENEFICIOS DE LA CONFORMIDAD

1. El proceso **ha generado una implicación y conexión con ciertas áreas** que ha contribuido de forma muy positiva, ayudando a **cambiar procesos y romper inercias**.
2. Un buen ENS debe articular una visión holística, lo que contribuye, de forma notable, en la mejora de otras **áreas** (juntos, pero no revueltos).
3. Nos ha **simplificado superar las exigencias de nuestros organismos de control** (AESA).
4. Nuestro gigante (sistemas y mundo operacional) tiene un hermanito que se hace mayor y con quien podrá compartir inquietudes (**sinergias**).



Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales

El **Director General** destaca la necesidad de integrar la ciberseguridad en su hoja de ruta.



Noticia

Esquema Nacional de Seguridad para ENAIRE

17/11/2020



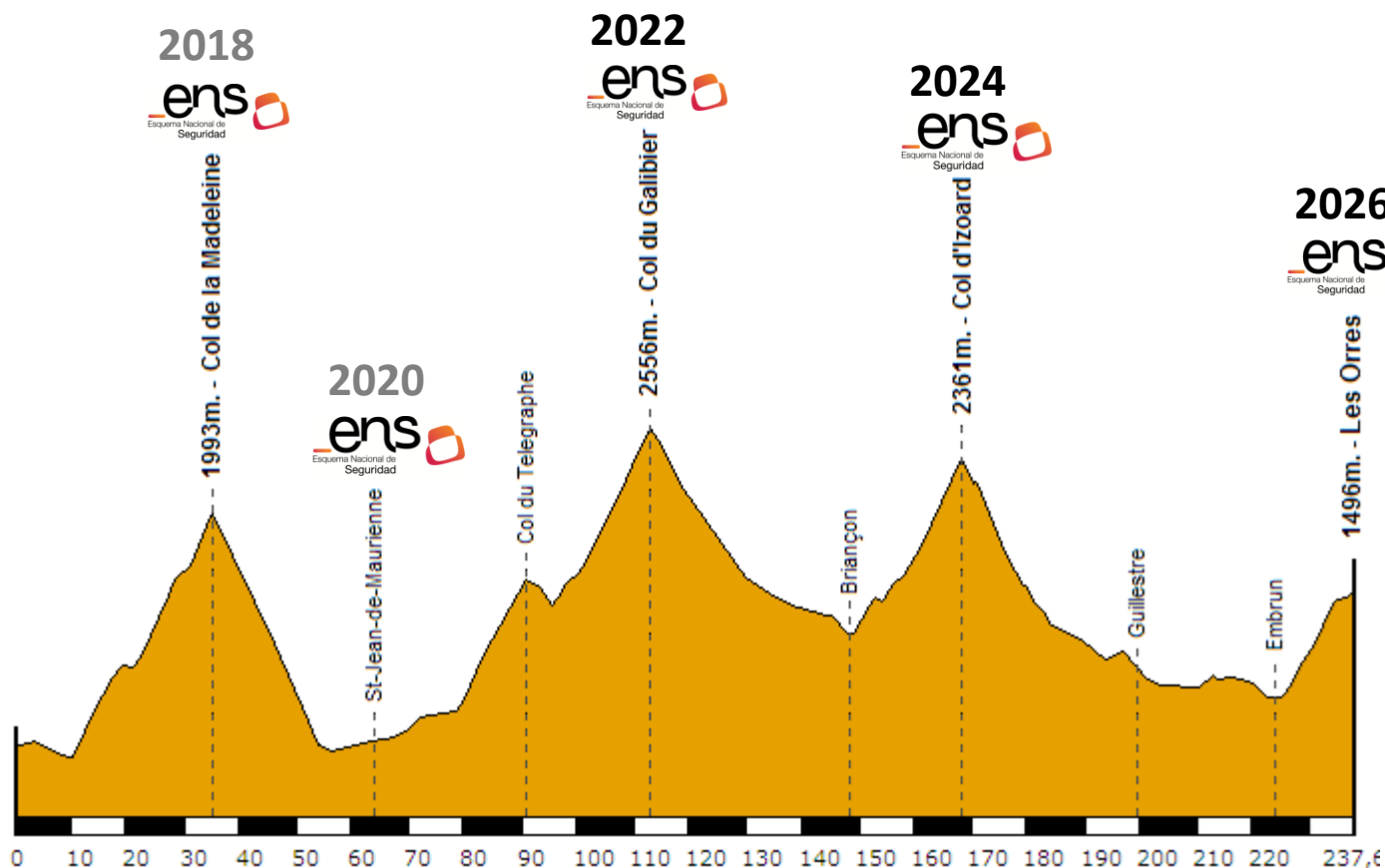
En la imagen, de izquierda a derecha, Javier Candau, Jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional, Ángel Luis Arias, Director General de ENAIRE, y Rafael García Meiro, CEO de AENOR.

AENOR ha otorgado a ENAIRE, gestor nacional de navegación aérea, el certificado del **Esquema Nacional de Seguridad** tras superar con éxito la correspondiente auditoría de conformidad.

De este modo, certifica con la Categoría Alta sus sistemas operacionales críticos, directamente involucrados en la provisión de servicios de navegación aérea.

Certificación ENS en Categoría Alta

ENAIRE – Operador de Servicios Esenciales



Seguimos

Certificación ENS en Categoría Alta

ENAIRe – Operador de Servicios Esenciales

ENAIRe 



25%



50%



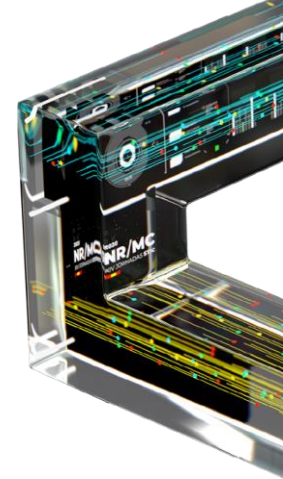
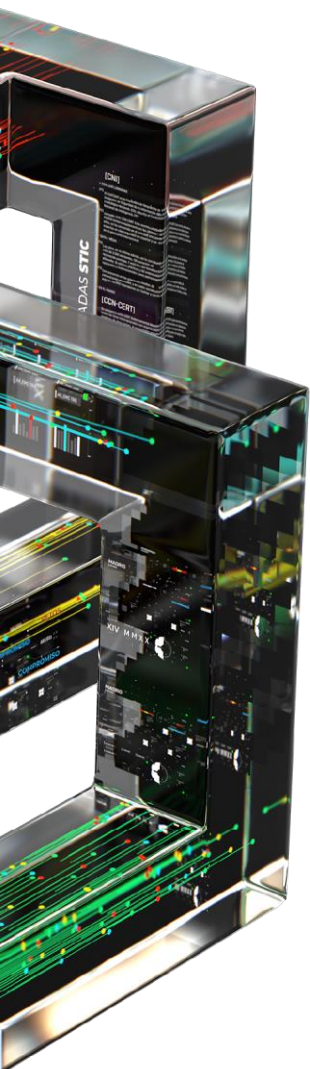
75%



90%



95%



MUCHAS GRACIAS

#XIVJORNADASCCNCERT