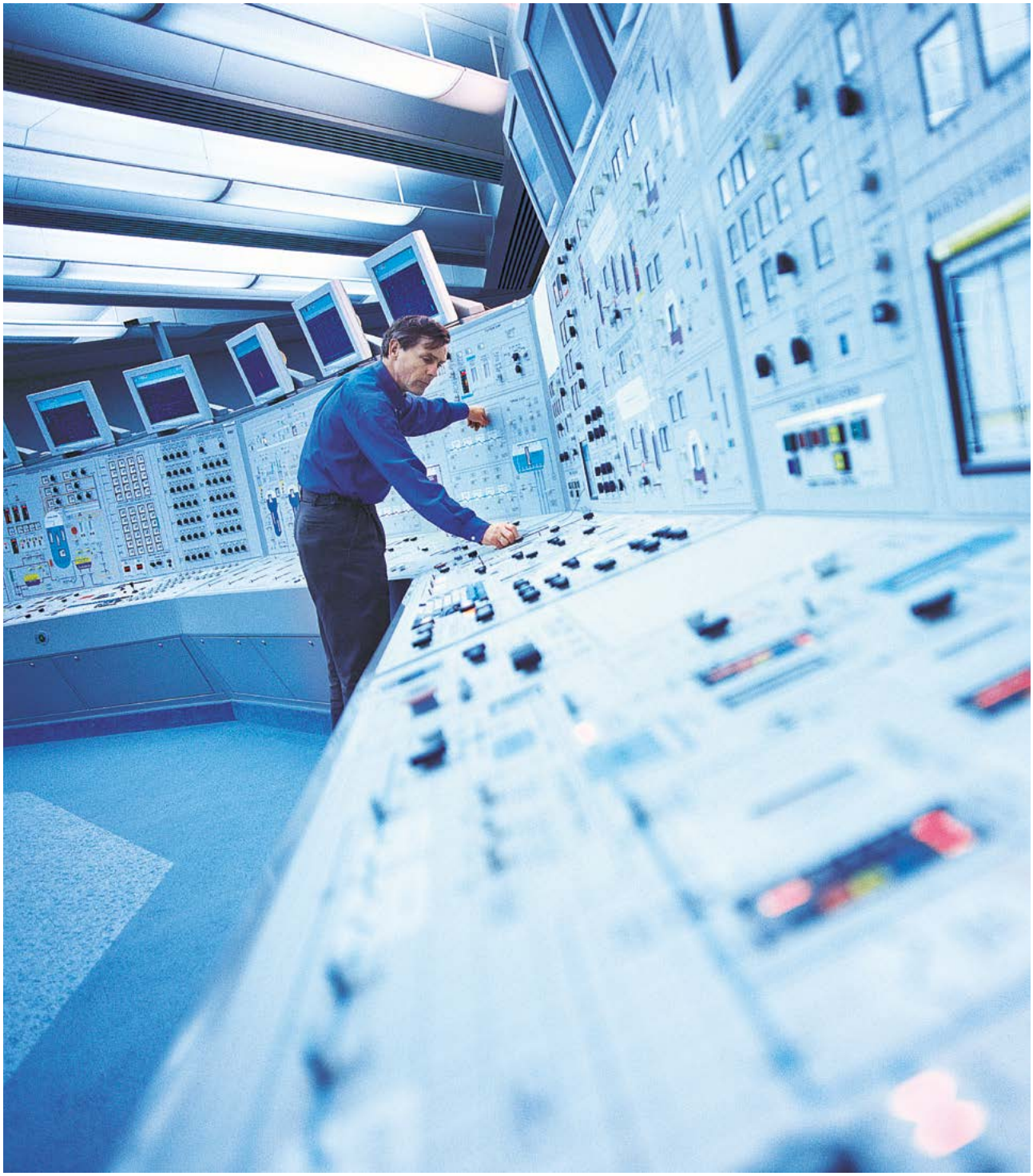
CENTRO DE CIBERSEGURIDAD INDUSTRIAL

EDICIÓN 2026

GUÍA DE INTERPRETACIÓN DEL ENS EN LA OPERACIÓN INDUSTRIAL

Ayuda a técnicos, auditores y decisores a interpretar ENS con visión OT

Cómo interpretar el ENS en entornos industriales sin introducir riesgo operacional



Edición: 2026

ISBN: 979-13-991104-3-2

Paseo de las Delicias, 30 - 2º
28045 Madrid
+34 910 910 751
info@cci-es.org
www.cci-es.org
blog.cci-es.org
@info_cci
www.linkedin.com/in/centrociberseguridadindustrial

El **Centro de Ciberseguridad Industrial (CCI)** es una organización independiente, sin ánimo de lucro, cuya misión es impulsar y contribuir a la mejora de la Ciberseguridad Industrial, en un contexto en el que las organizaciones de sectores como el de fabricación o el energético juegan un papel crítico en la construcción de la sociedad actual, como puntales del estado del bienestar.

El CCI afronta ese reto mediante el desarrollo de actividades de investigación y análisis, generación de opinión, elaboración y publicación de estudios y herramientas e intercambio de información y conocimiento sobre la influencia, tanto de las tecnologías, incluidos sus procesos y prácticas, como de los individuos, en lo relativo a los riesgos —y su gestión— derivados de la integración de los procesos e infraestructuras industriales en el Ciberespacio.

El CCI es, hoy, el ecosistema y el punto de encuentro de las entidades —privadas y públicas— y de los profesionales afectados, preocupados u ocupados de la Ciberseguridad Industrial; y es, asimismo, la referencia hispanohablante para el intercambio de experiencias y la dinamización de los sectores involucrados en este ámbito.

CONSEJOS

Alt+flecha izquierda para volver a la vista anterior después de ir a un hipervínculo

Haz **click** en **nuestro icono** y visita nuestra web

Haciendo **click** en la **banderas de la portada** podrás ver la actividad de CCI en cada uno de esos países

Haciendo **click** en el **número de página** volverás al índice

PATROCINADORES

PATROCINADORES **PLATINUM**

Telefónica Tech

PATROCINADORES **GOLD**

FORTINET
HackRTU INDUSTRIAL SECURITY
kaspersky
KPMG
IndraMind
PHOENIX CONTACT
Rockwell Automation
Schneider Electric
SECURE IT by LKS
SIEMENS
S2GRUPO
STORMSHIELD

PATROCINADORES **SILVER**

axians
CAPSA FOOD
Capgemini
CLAROTY
Deloitte.
FDB FOOD DELIVERY BRANDS
NTT DATA
nunsys GROUP
THALES
Ingecom IGNITION An Exclusive Networks Company
TECNICAS REUNIDAS
txOne networks

PATROCINADORES **BRONZE**

Atos
authUSB
BABEL
CIC Consulting Informático
Cyberium
getronics
gmv
InproOTech
NEOSECURE SABEMOS DE SEGURIDAD
tecnalia MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE
Teldat

ÍNDICE

AGRADECIMIENTOS

El Centro de Ciberseguridad Industrial (CCI) agradece a la Agencia Estatal de Administración Digital y al CCN-CERT por su colaboración en la revisión realizada sobre esta guía, así como las recomendaciones y comentarios técnicos aportados durante su desarrollo.

Las contribuciones recibidas han sido analizadas y consideradas por el equipo redactor. No obstante, la selección de contenidos, interpretaciones y conclusiones incluidas en la presente publicación responde exclusivamente al criterio del CCI, quienes asumen íntegramente la responsabilidad sobre el contenido final del documento.

INTRODUCCIÓN

La aplicación del Esquema Nacional de Seguridad (ENS) en entornos de tecnologías de operación (OT) plantea un reto recurrente, su marco es válido, pero su interpretación práctica se realiza, en muchos casos, desde un modelo mental eminentemente de sistemas de información, con visión "IT". Este enfoque conduce a la adopción de mecanismos o medidas que, aun siendo habituales en entornos de sistemas de información, no siempre son adecuados, viables o seguros en sistemas industriales.

Esta guía surge para abordar ese reto desde una premisa clara, el ENS no necesita ser modificado para aplicarse en OT, pero sí necesita ser correctamente interpretado en función del nivel operativo y físico de los sistemas industriales.

El propósito de esta guía es facilitar una interpretación del ENS adaptada a la tecnología de operación industrial, sin alterar en ningún momento su redacción, su estructura ni sus objetivos.

La guía no pretende crear un "ENS para OT" ni introducir requisitos adicionales, sino traducir los objetivos de seguridad definidos por el ENS a objetivos comprensibles y aplicables en entornos industriales, permitiendo que los mecanismos y/o medidas de cumplimiento se ajusten a la realidad operacional del proceso.

En este sentido, la guía parte de una distinción fundamental, el ENS define el "qué" debe fortalecerse; la operación industrial determina el "cómo" hacerlo sin introducir riesgo operacional.

En entornos OT, este "cómo" incluye no solo tecnología, sino también a las personas que operan el proceso. El operador industrial no es un usuario final, sino parte activa del sistema de seguridad física y funcional. Una interpretación correcta del ENS debe reconocer explícitamente el papel del factor humano como elemento de prevención, detección y respuesta ante situaciones anómalas.

La tabla incluida a continuación ilustra este principio, mostrando cómo un mismo objetivo ENS puede traducirse a un objetivo equivalente en OT y cumplirse mediante mecanismos o medidas distintas a las habituales en IT, pero plenamente alineados con el espíritu del ENS.

Objetivo ENS	Traducción a objetivo en OT	Mecanismo habitual en ENS	Mecanismo equivalente en OT
Fortalecer la integridad de los componentes críticos del sistema frente a modificaciones no autorizadas o accidentales	Fortalecer que la lógica de control, los parámetros y el comportamiento del proceso no cambian; si cambian, el sistema entra en un estado conocido y seguro, manteniendo coherencia física	Hashes de ficheros, control de integridad en disco, agentes EDR, verificación de binarios, control de cambios software	Control de modos RUN/ PROGRAM, bloqueo de escritura en PLC, alarmas por cambio de lógica, checksum o versión de programa validada tras FAT/SAT, estados seguros ante reinicio
Fortalecer la disponibilidad de los sistemas y servicios críticos	Fortalecer que el proceso industrial puede seguir operando de forma segura o degradada, o detenerse de manera controlada, sin pérdida de control ni riesgo para personas o instalaciones	Alta disponibilidad IT, clustering, balanceadores, reinicios automáticos, SLA de servicio	Diseño de estados degradados, redundancia funcional (no solo técnica), control de arranques/ paradas, lógica de fallback en PLC, procedimientos operativos seguros. Redundacia de redes industriales, con "failover automático". Asegurar suministro eléctrico.
Detección de incidentes de seguridad	Detectar desviaciones del comportamiento esperado del proceso, de la lógica o de los estados operativos antes de que escalen a un incidente físico u operativo	SIEM, correlación de logs, IDS/IPS IT, agentes de monitorización	Alarmas de plausibilidad física, detección de secuencias imposibles, monitorización pasiva de red industrial, eventos de cambio de estado operativo
Fortalecer el control de accesos a los sistemas	Fortalecer que solo personas y sistemas autorizados pueden modificar la lógica, los parámetros o los estados operativos del proceso	IAM, MFA, control de acceso lógico centralizado	Separación de roles ingeniería/operación, llaves físicas y lógicas, control de sesiones de ingeniería, gestión de usuarios locales en sistemas OT
Fortalecer la trazabilidad de acciones relevantes	Poder reconstruir qué cambios se hicieron en la lógica o configuración, cuándo y en qué condiciones operativas	Logs centralizados, auditoría de sistemas, registro de eventos IT	Registro de cambios de programas de control, versionado de lógica, bitácoras de operación, evidencias con FAT/SAT, registros de mantenimiento
Resiliencia frente a incidentes	Recuperar el control del proceso sin introducir nuevos riesgos, manteniendo la seguridad física y funcional	Backups, restauraciones rápidas, DRP IT	Restauración validada de lógica, pruebas de arranque seguro, procedimientos de recuperación industrial, pruebas periódicas en entorno controlado

A quién va dirigida esta guía

Está dirigida a todos los actores que intervienen en el diseño, operación, aseguramiento y evaluación de sistemas industriales sujetos al ENS, en particular:

- Operadores de infraestructuras y procesos industriales.
- Responsables de OT y automatización.
- Responsables de ciberseguridad industrial (ICSO).
- Auditores y evaluadores de conformidad con el ENS.
- Organismos y unidades del CCN implicadas en la interpretación y supervisión del ENS.
- Proveedores de tecnología, ingeniería, integración y mantenimiento industrial.

El objetivo es proporcionar un lenguaje común que permita a todos ellos interpretar y aplicar el ENS de forma coherente, técnica y operativamente segura.

Qué problema resuelve

En la práctica, muchas de las dificultades en la aplicación del ENS en entornos industriales no derivan del marco normativo en sí, sino de un sesgo IT en su interpretación.

Este sesgo se manifiesta, entre otros aspectos, en:

- La asimilación automática de objetivos de seguridad a tecnologías IT concretas.
- La priorización de mecanismos software frente a controles inherentes al propio proceso.
- La introducción de medidas que interfieren en la operación o comprometen la seguridad funcional.
- La dificultad para justificar controles industriales como cumplimiento válido ante auditorías.

La guía aborda este problema proporcionando criterios claros para separar objetivo y mecanismo o medida, permitiendo demostrar que un sistema industrial puede cumplir los objetivos del ENS sin replicar soluciones IT que no aportan valor o que introducen nuevos riesgos.

La guía se construye sobre los siguientes 5 principios:

1. **Compatibilidad total con el ENS.** Todas las interpretaciones propuestas se alinean con el texto y la finalidad del ENS, sin modificaciones normativas ni reinterpretaciones forzadas.
2. **Primacía del objetivo sobre el mecanismo.** El cumplimiento se evalúa en función de la consecución del objetivo de seguridad, no de la adopción de una tecnología o medida concreta.
3. **Respeto al marco de operación industrial.** Ninguna medida se considera válida si compromete la seguridad funcional, la disponibilidad del proceso o las certificaciones del sistema.
4. **Equivalencia funcional de controles.** Los controles técnicos propios de OT pueden considerarse equivalentes a los mecanismos ENS clásicos siempre que cumplan el mismo objetivo de seguridad.
5. **Demostrabilidad y trazabilidad.** Toda interpretación debe poder explicarse y justificarse de forma clara ante terceros, incluidos auditores y organismos supervisores.

EL ENS LEÍDO DESDE OT

Aplicar el ENS en entornos OT no consiste en “adaptar el ENS”, sino en leerlo correctamente desde un entorno distinto al que históricamente ha dominado su aplicación práctica. El ENS es un marco suficientemente amplio y robusto como para dar cabida a entornos industriales, siempre que se evite una interpretación automática basada en supuestos propios del mundo IT.

Qué exige realmente el ENS

El ENS exige, ante todo, lograr una serie de objetivos de seguridad asociados a la protección de los sistemas que soportan funciones y servicios críticos. Estos objetivos se articulan, entre otros, en torno a:

- La disponibilidad de los sistemas y servicios.
- La integridad de los componentes críticos.
- La trazabilidad y control de las acciones relevantes.
- La detección y gestión de incidentes.
- La resiliencia frente a fallos o ataques.

Es importante subrayar que el ENS define qué debe fortalecerse, pero no siempre prescribe de forma cerrada cómo debe hacerse. El propio diseño del ENS permite adaptar las medidas en función del tipo de activo, el impacto y el entorno de operación, además que permite establecer medidas compensatorias para cumplir con los objetivos del ENS en aquellos casos en los que no es posible las medidas especificadas en el Anexo II.

Para lograr adaptar las medidas es fundamental basarse en un análisis de riesgos que justifique las medidas, demostrando la relación directa entre el nivel de riesgo asumido por la organización, los objetivos de seguridad que deben protegerse y la proporcionalidad, adecuación y eficacia de los controles implantados.

Para que una organización pueda no aplicar determinadas medidas del ENS deben cumplirse tres condiciones. Primero, el riesgo residual resultante debe ser aceptado por el responsable de Negocio o la Alta Dirección; no puede comprometer la disponibilidad, integridad o seguridad de funciones críticas. Segundo, la medida no aplicada debe estar razonadamente sustituida o compensada por otras medidas equivalentes o por controles organizativos, procedimentales u operativos. Tercero, esa decisión debe estar documentada en el análisis de riesgos y aprobada por el nivel de responsabilidad adecuado, como una decisión de gobierno. Consultar Artículo 28 de ENS[1] y la guía CCN_STIC 819[2]

Aplicación práctica tradicional del ENS

Aunque el ENS es tecnológicamente neutro en su formulación, su aplicación práctica ha estado tradicionalmente influida por una serie de supuestos implícitos propios de entornos IT, entre ellos:

- Sistemas discretos, con software fácilmente parcheable.
- Posibilidad de reinicio sin impacto físico.
- Ciclos de vida cortos y alta rotación tecnológica.
- Capacidad de instalar agentes, sondas o software adicional.
- Separación clara entre seguridad lógica y seguridad física.

[1] *https://ens.ccn.cni.es/es/normativa* [2] *https://www.ccn-cert.cni.es/es/guias.html*

En entornos OT, muchos de estos supuestos no se cumplen:

- Los sistemas son deterministas y están acoplados a procesos físicos.
- Un reinicio puede generar riesgos operativos o de seguridad funcional.
- Los ciclos de vida se miden en décadas.
- La validación previa y las certificaciones limitan los cambios.
- La seguridad lógica y la seguridad física están profundamente entrelazadas.

Cuando estos supuestos no se hacen explícitos, se corre el riesgo de aplicar el ENS como si fuera un marco prescriptivo IT, generando fricciones innecesarias e incluso incrementando el riesgo global del sistema.

Separación clave: objetivo ENS vs mecanismo de cumplimiento

La clave para una correcta aplicación del ENS en OT está en separar claramente el objetivo de seguridad del mecanismo utilizado para alcanzarlo.

- El objetivo ENS expresa la garantía que debe ofrecer el sistema.
- El mecanismo de cumplimiento es la forma concreta de demostrar que esa garantía existe.

En IT, ciertos mecanismos se han convertido en soluciones de facto para cumplir determinados objetivos (por ejemplo, agentes de integridad, EDR o controles basados en ficheros). En OT, esos mismos objetivos pueden y deben cumplirse mediante mecanismos distintos, más alineados con el proceso industrial y con menor interferencia operacional.

Confundir objetivo con mecanismo conduce a errores frecuentes, como pensar que “si no hay el mecanismo IT habitual, no se cumple el ENS” o forzar la aplicación de controles que cumplen formalmente, pero degradan la seguridad real del sistema.

La guía parte de la premisa de que cumplir el ENS en OT es cumplir el objetivo, no replicar la solución IT. Para lo cual es necesario:

- Reconocer explícitamente la necesidad de adaptar las medidas a las condiciones de la operación industrial.
- Evaluar la seguridad en función del impacto, no de la tecnología empleada.
- No prohibir mecanismos alternativos siempre que se alcance el objetivo de seguridad.
- Prioriza la disponibilidad y la integridad en sistemas críticos, aspectos centrales en OT.

Lo que el ENS no hace es explicitar cómo debe interpretarse en sistemas industriales. Esa ausencia no es una limitación del marco, sino una oportunidad para desarrollar guías de interpretación sectorial que ayuden a aplicar el ENS con rigor y coherencia.

Esta guía se sitúa precisamente en ese espacio: no amplía ni restringe el ENS, sino que traduce sus objetivos al lenguaje y a la lógica de los sistemas OT, demostrando que el ENS puede cumplirse protegiendo el proceso, no solo el sistema.

CONDICIONES OT Y LAS VARIABLES QUE CAMBIAN LA INTERPRETACIÓN

Las tecnologías de operación industrial presentan un conjunto de características propias que condicionan de forma directa cómo deben interpretarse los objetivos de seguridad del ENS. Estas variables no invalidan el marco, pero sí alteran profundamente la forma en la que los objetivos se materializan y se demuestran.

Ignorar estas variables conduce a interpretaciones formales correctas, pero operativamente incorrectas. Tenerlas en cuenta permite aplicar el ENS con rigor y coherencia.

Determinismo, latencias y dependencia física

En OT, los sistemas no solo procesan información: controlan procesos físicos en tiempo real. Esto introduce tres elementos clave:

- **Determinismo:** el sistema debe responder de forma predecible ante estímulos conocidos. Variaciones no controladas en tiempos de respuesta pueden traducirse en comportamientos físicos no deseados.
- **Latencias:** retrasos introducidos por mecanismos de seguridad pueden romper la lógica del control, aunque el sistema "siga funcionando".
- **Dependencia física:** el estado del software está directamente acoplado al estado del proceso físico, y viceversa.

Desde esta perspectiva, una medida de seguridad que en IT es neutra (por ejemplo, inspección profunda, agentes residentes o análisis en línea) puede alterar el comportamiento del proceso en OT, incumpliendo el objetivo último del ENS: proteger el servicio.

Por ello, en OT la seguridad se evalúa también en términos de coherencia temporal y física, no solo lógica.

Seguridad funcional y seguridad de personas

En sistemas industriales, la ciberseguridad no puede analizarse de forma aislada de la seguridad funcional ni de la protección de las personas.

- Existen funciones cuya finalidad principal es llevar el sistema a un estado seguro ante fallos.
- Hay mecanismos diseñados específicamente para prevenir daños físicos, no accesos no autorizados.
- La pérdida de control o un comportamiento errático puede tener consecuencias directas sobre personas, instalaciones o el entorno.

Esto implica que una medida de ciberseguridad nunca es válida si degrada la seguridad funcional, aunque formalmente mejore un control lógico. En OT, proteger la integridad del sistema significa, ante todo, garantizar que el proceso se comporta de forma segura incluso cuando algo falla.

En este marco de condiciones, el operador y el personal de operación forman parte de la propia línea de defensa de seguridad. Muchas decisiones críticas, como detener un proceso, ignorar una alarma falsa o ejecutar un procedimiento de emergencia, se toman antes de que cualquier control técnico actúe. Una medida de ciberseguridad que dificulte, confunda o retrase estas decisiones degrada la seguridad real del sistema, aunque formalmente refuerce un control lógico.

El ENS, cuando prioriza la disponibilidad y la integridad en sistemas críticos, es plenamente coherente con esta visión, siempre que se interprete desde el proceso y no solo desde el sistema.

Ciclos de vida largos y obsolescencia gestionada

A diferencia de los entornos IT, donde los ciclos de vida son cortos y la sustitución es frecuente, en OT los sistemas:

- Permanecen en operación durante décadas.
- Conviven con tecnologías obsoletas pero funcionales.
- No pueden ser actualizados sin planificación, validación y, en ocasiones, paradas prolongadas.

La obsolescencia en OT no es un fallo de gestión, sino una condición estructural del sistema. Por tanto, la aplicación del ENS no puede basarse en supuestos de actualización continua o sustitución rápida de componentes.

Esto obliga a interpretar objetivos como la integridad, la detección o la resiliencia desde una lógica de control del cambio y estabilidad, más que desde una lógica de actualización permanente.

Validación previa, certificaciones y no interferencia operacional

Muchos sistemas OT están sujetos a procesos formales de validación (FAT, SAT), certificaciones regulatorias o requisitos contractuales que limitan qué puede cambiarse y cuándo.

Introducir nuevos mecanismos de seguridad puede:

- Invalidar certificaciones.
- Obligar a repetir procesos de validación costosos.
- Introducir riesgos no contemplados en el diseño original.

Por este motivo, en OT es esencial el principio de no interferencia operacional: una medida de seguridad solo es aceptable si no altera el comportamiento validado del sistema ni compromete su operación segura.

Este principio no contradice el ENS; al contrario, lo refuerza, ya que evita introducir controles que, bajo la apariencia de cumplimiento, aumentan el riesgo real.

Riesgo tecnológico vs riesgo operacional

En IT, el análisis de riesgos suele centrarse en el riesgo tecnológico: pérdida de confidencialidad, integridad o disponibilidad del sistema de información.

En OT, a este riesgo se suma, incluso en muchos casos predomina, el riesgo operacional, que incluye:

- Pérdida de control del proceso.
- Daños físicos o ambientales.
- Impacto en la seguridad de las personas.
- Paradas no controladas o degradaciones inseguras.

Una interpretación correcta del ENS en OT exige equilibrar ambos riesgos. Una medida que reduce el riesgo tecnológico, pero incrementa el riesgo operacional no mejora la seguridad del sistema, aunque formalmente "endurezca" la infraestructura. Implementar el ENS debe mitigar el riesgo global del sistema y protegerlo tanto en IT como en OT.

Cuadro resumen de consideración de las variables OT al interpretar el ENS

Variable OT clave	Qué cambia respecto a IT	Impacto en la interpretación del ENS	Riesgo de una mala interpretación
Determinismo del sistema	El sistema debe comportarse de forma predecible en tiempo real	Las medidas no pueden introducir variabilidad temporal ni comportamientos no deterministas	Cumplir formalmente el ENS degradando el control del proceso
Latencias	Retrasos mínimos pueden generar fallos físicos	La eficacia de una medida no se evalúa solo por su función, sino por su impacto en el proceso	Introducir controles que rompen la lógica de control
Dependencia física	Software y proceso físico están acoplados	La integridad se interpreta como coherencia física, no solo lógica	Proteger el sistema pero desproteger el proceso
Seguridad funcional	El sistema debe fallar de forma segura	Las medidas ENS no pueden interferir con funciones de seguridad	Aumentar el riesgo para personas e instalaciones
Seguridad de personas	Consecuencias directas sobre la integridad física	La disponibilidad e integridad tienen prioridad estructural	Enfocar el ENS como protección de datos en lugar de protección del servicio
Ciclos de vida largos	Sistemas operan durante décadas	El cumplimiento no puede basarse en actualización continua	Penalizar sistemas estables por no seguir dinámicas IT
Obsolescencia gestionada	Tecnología antigua pero validada	La gestión del riesgo prima sobre la sustitución tecnológica	Forzar cambios que aumentan el riesgo global
Validación previa (FAT/SAT)	Cambios requieren revalidación	El control del cambio es más relevante que la frecuencia del cambio	Introducir medidas que invalidan el diseño aprobado
Certificaciones y requisitos regulatorios	Limitan modificaciones técnicas	La seguridad debe respetar el sistema certificado	Incumplir

TIPOLOGÍA DE ACTIVOS OT Y SU ENCAJE EN EL ENS

Uno de los factores que más distorsiona la aplicación del ENS en entornos industriales es la homogeneización indebida de los activos OT. Bajo una lectura IT, se tiende a considerar que todos los activos son esencialmente sistemas de información con distintas criticidades. En OT, esa simplificación impide la interpretación adecuada del ENS en este marco de condiciones.

Este capítulo establece una tipología clara de activos OT y explica cómo deben interpretarse los objetivos del ENS en cada caso, sin forzar analogías tecnológicas.

En OT, los activos:

- Cumplen funciones radicalmente distintas dentro del proceso.
- Tienen niveles de acoplamiento físico diferentes.
- Admiten grados muy distintos de intervención técnica.
- Soportan impactos distintos ante fallos o incidentes.

El ENS permite modular las medidas en función del tipo de activo, el impacto y el entorno. Aplicar el mismo patrón de cumplimiento a todos los activos OT no es rigor, es pérdida de condiciones adecuadas en la operación industrial. Por ello, la interpretación correcta del ENS exige partir de una clasificación funcional de activos OT, no de una equivalencia directa con activos IT.

Categorías principales de activos OT

A efectos de interpretación del ENS, los activos OT pueden agruparse en varias categorías, entendiendo que cada una condiciona de forma distinta el “cómo” del cumplimiento. En OT, clasificar activos no sirve solo para agrupar tecnologías, sino para delimitar hasta dónde puede llegar una medida de seguridad sin romper el sistema. Cada tipo de activo impone límites distintos a la forma de cumplir los objetivos del ENS, pero no a los objetivos en sí.

1. Sistemas de control

Incluyen PLC, RTU y controladores embebidos. Son activos altamente deterministas, directamente acoplados al proceso físico y, en muchos casos, con funciones de seguridad integradas. En estos activos:

- La integridad se interpreta como integridad de la lógica y del comportamiento
- La disponibilidad se vincula a estados seguros, no solo a continuidad de servicio.
- La instalación de agentes o software adicional suele ser inviable y siempre deberá ser compatible con las aplicaciones de control y supervisión.

Límites para este tipo de activo:

- Cualquier mecanismo que introduzca latencia, carga no determinista o software adicional no validado rompe el objetivo ENS en lugar de cumplirlo.
- La integridad solo es válida si preserva el determinismo y la seguridad funcional.

Correspondencia en PILAR (62443): ** [plc] PLC – Programmable Logic Controller * [rtu] RTU – Remote Terminal Unit * [pac] PAC – Programmable Automation Controller * [ied] IED – Intelligent Electronic Device * [sis] Safety Instrumented System*

2. Sistemas de control distribuido (DCS)

Sistemas integrados, con fuerte dependencia del proveedor y arquitecturas cerradas o semi-cerradas. En estos activos:

- El control del cambio es más relevante que la inspección continua.
- La trazabilidad se apoya en procedimientos y evidencias de ingeniería.
- La resiliencia se diseña desde la arquitectura, no desde parches rápidos.
- La integridad en DCS es equivalente en objetivo a la del PLC, pero se demuestra a otro nivel (sistema distribuido vs controlador individual).
- La integridad del DCS implica que la configuración y la lógica de control del sistema distribuido no cambian fuera de los procedimientos autorizados, que las modificaciones son trazables, validadas y coherentes a nivel de sistema completo y el comportamiento global del proceso permanece dentro de los parámetros de diseño.

Límites para este tipo de activo:

- La integridad se gobierna a nivel de arquitectura y procedimientos, no mediante inspección continua intrusiva.
- Introducir mecanismos que no estén soportados por el fabricante puede invalidar el diseño y romper la garantía de integridad.

Correspondencia en PILAR (62443): *PILAR no contiene una etiqueta única para "DCS" porque lo evalúa como un conjunto interoperable. Para reflejar un DCS en PILAR, se debe modelar mediante la combinación de:* * [server] Control server *(para los servidores de control del DCS)* * [hmi] HMI – Human Machine Interface *(para las consolas de operación del DCS)* * [plc] / [pac] *(para los controladores distribuidos específicos)*

3. Sistemas de supervisión y operación

Incluyen SCADA, HMI y estaciones de operación. En estos activos:

- Existe mayor proximidad a entornos IT.
- Es posible aplicar ciertos mecanismos ENS clásicos, con cautela.
- La prioridad sigue siendo no interferir con la operación.

Son activos “frontera”, donde la traducción ENS–OT suele ser híbrida. Límites para este tipo de activo:

- Los mecanismos ENS clásicos son más aplicables, pero no a costa de la usabilidad operativa.
- La seguridad no puede introducir errores de interpretación al operador.

Correspondencia en PILAR (62443): * [hmi] HMI – Human Machine Interface * [server] Control server * [telemetry] Telemetry

4. Redes industriales y comunicaciones

Incluyen buses de campo, Ethernet industrial y redes de control. En estos activos:

- La disponibilidad y el determinismo son críticos.
- La monitorización pasiva suele ser preferible a la inspección activa.
- La segmentación tiene una lectura funcional, no solo lógica.
- La integridad aquí significa que los datos de control llegan completos, en orden y a tiempo sin que se introduzcan tramas, comandos o retrasos no autorizados y se preserve la sincronización del sistema.

El ENS se cumple aquí protegiendo flujos de proceso, no solo paquetes. Los limites en este tipo de activos:

- La monitorización de seguridad debe ser preferentemente pasiva.
- La seguridad no puede alterar tiempos de ciclo ni prioridades de comunicación.

Correspondencia en PILAR (62443): * [bridge] Bridge *(aplicable a switches, routers y pasarelas de red)* * Nota adicional de la rama *[network]* de PILAR: *[network equipment]*

5. Sistemas de gestión industrial

Historiadores, MES, servidores de ingeniería, gateways, sistemas de mantenimiento. En estos activos:

- Hay mayor margen para mecanismos ENS tradicionales.
- Debe evaluarse cuidadosamente su impacto directo e indirecto sobre el proceso.
- Su criticidad no siempre es evidente, pero puede ser estructural.
- La integridad significa que los datos históricos y de configuración son fiables, que las herramientas de ingeniería no introducen cambios no autorizados y se preserva la coherencia entre diseño, operación y mantenimiento.

Límites para este tipo de activos:

- Siempre evaluar el impacto indirecto sobre el proceso.

Correspondencia en PILAR (62443): * [historian] Historian * [ems] EMS – Energy Management System * [dms] DMS – Distribution Management System * [meter] Meter

6. Instalaciones e Infraestructura Técnica de Soporte

Sistemas automatizados auxiliares que, si bien no operan el proceso productivo principal de forma directa, son críticos para mantener las condiciones operativas ambientales, eléctricas o de seguridad física de los activos OT. Interpretación ENS: Al estar a menudo basados en IoT o redes automatizadas comerciales, combinan vulnerabilidades de entornos corporativos con impactos en el mundo físico.

Límites para este tipo de activos:

- Su interconexión con las redes de control principales debe estar fuertemente aislada para evitar vectores de ataque de salto de zona.

Correspondencia en PILAR (62443): * [hvac] HVAC – Heating, ventilation and air conditioning * [home] Home control network

Valoración de activos OT dentro del ENS

La valoración de activos OT conforme al ENS debe realizarse considerando simultáneamente:

- Su función dentro del proceso industrial.
- El impacto de su fallo sobre personas, proceso y entorno.
- Su capacidad real de admitir medidas de seguridad.
- Su papel en la cadena de control y decisión.

Esto implica que dos activos tecnológicamente similares pueden requerir interpretaciones ENS distintas si su rol operativo es diferente. Esta guía propone que la valoración de activos OT en ENS no se base únicamente en el activo en sí, sino en:

activo + función + condiciones operativas.

Una vez reconocida esta tipología:

- Los objetivos del ENS se mantienen constantes.
- Los mecanismos de cumplimiento se ajustan por categoría de activo.
- Se evita aplicar controles contraproducentes o peligrosos.
- Se mejora la coherencia entre seguridad formal y seguridad real.

Este enfoque permite aplicar el ENS de forma selectiva, razonada y defendible, alineada tanto con el marco normativo como con la realidad industrial.

IMPACTOS OT REALES Y SU REFLEJO EN EL ENS

En entornos OT, los impactos derivados de un incidente de seguridad no se limitan al ámbito tecnológico. Afectan de forma directa al proceso físico, a las personas y, en muchos casos, al entorno y a la continuidad del servicio esencial que se presta.

Una correcta interpretación del ENS en OT exige partir de estos impactos reales y traducirlos adecuadamente a los conceptos de disponibilidad e integridad definidos por el marco, evitando reducciones simplistas propias del entorno IT.

Impacto sobre personas

En sistemas industriales, determinados fallos de control, pérdida de visibilidad o comportamientos no esperados del proceso pueden derivar en riesgos directos para la seguridad de las personas.

Desde la perspectiva del ENS:

- La integridad implica que el sistema no adopta comportamientos peligrosos por modificaciones no autorizadas, errores lógicos o estados incoherentes.
- La disponibilidad implica que las funciones necesarias para operar o detener el proceso de forma segura están accesibles cuando se necesitan.

En OT, un sistema “disponible” que no puede tener un comportamiento seguro no cumple el objetivo del ENS, aunque esté técnicamente operativo.

Impacto sobre el proceso industrial

El proceso industrial es el núcleo del sistema OT. Cualquier alteración no controlada puede generar:

- Productos fuera de especificación.
- Daños a equipos o infraestructuras.
- Pérdida de control del proceso.
- Paradas no planificadas o arranques inseguros.

En este marco de condiciones de operación industrial:

- La integridad se interpreta como la preservación del comportamiento esperado del proceso.
- La disponibilidad se vincula a la capacidad de operar, degradar o detener el proceso de manera controlada.

Una parada controlada puede ser una medida de preservación de la disponibilidad en OT, aunque desde una lectura IT se interprete como indisponibilidad.

Impacto sobre el entorno físico y ambiental

En determinados sectores, una pérdida de control puede tener consecuencias ambientales relevantes, regulatorias o sociales.

Desde la óptica del ENS:

- La integridad del sistema incluye la coherencia entre las órdenes de control y sus efectos físicos.
- La disponibilidad incluye la capacidad de actuar a tiempo para evitar o mitigar impactos ambientales.

Este tipo de impacto refuerza la necesidad de interpretar el ENS desde el servicio que se presta y no solo desde la infraestructura tecnológica.

Impacto regulatorio y reputacional

Los incidentes OT pueden implicar:

- Incumplimientos normativos sectoriales.
- Activación de planes de emergencia.
- Pérdida de confianza de clientes, reguladores o ciudadanía.

En estos casos, una lectura excesivamente técnica del ENS puede llevar a sobreproteger sistemas secundarios mientras se infra protegen elementos críticos del proceso.

Ejemplos de interpretación OT del ENS

La interpretación OT del ENS obliga a identificar los activos cuyo fallo tiene consecuencias sistémicas, aunque no sean los más visibles desde el punto de vista IT.

Para estos ejemplos no se está teniendo en cuenta el análisis de riesgos, el cual será fundamental para determinar la criticidad de los activos a proteger, solo muestra algunos casos que permiten entender mejor los escenarios posibles.

Servidor SCADA

Desde una lectura IT, el servidor SCADA suele aparecer como activo crítico, es un sistema centralizado, tiene un sistema operativo estándar con usuarios, red, acceso remoto. Sin embargo, en muchos procesos industriales, el SCADA puede reiniciarse sin pérdida de control y el proceso sigue funcionando de forma autónoma.

Por el contrario, una modificación no detectada en la lógica de un PLC, podría alterar secuencias físicas provocando estados peligrosos que podrían generar daños antes de ser visible en el SCADA.

En este caso la interpretación OT del ENS sería: el PLC es prioritario desde el punto de vista sistémico, aunque desde IT sea “menos visible” y más difícil de instrumentar con controles clásicos.

Servidor de backups vs estación de ingeniería

En entornos OT, el valor de las copias de seguridad no reside principalmente en la conservación de información documental o administrativa, sino en la capacidad de recuperar configuraciones, lógicas de control, parametrizaciones, recetas, versiones validadas de sistemas y estados operacionales necesarios para devolver el proceso a una condición segura y funcional.

Por ello, la criticidad real de un backup en este contexto depende de qué elementos operacionales contiene, de su validez técnica, de su trazabilidad y de su capacidad real de ser restaurados en condiciones operativas.

En muchas auditorías ENS se aplican controles exhaustivos sobre plataformas de backup desde una perspectiva tradicional orientada a protección de información. Sin embargo, en OT resulta más relevante asegurar la integridad y disponibilidad de copias válidas de configuraciones de PLC, SCADA, HMI, estaciones de ingenie-

ría, sistemas instrumentados, historiadores o activos críticos de automatización, ya que son estos elementos los que permiten recuperar la operación real del proceso industrial.

En consecuencia, la prioridad en OT no debería centrarse únicamente en la robustez del servidor de backup, sino en garantizar que existen versiones operacionales confiables, coherentes y verificadas de los sistemas que gobiernan el proceso físico."

En cambio, una estación de ingeniería tiene capacidad directa de modificar lógica y parámetros pudiendo alterar el proceso sin dejar evidencias inmediatas, al estar conectada de forma intermitente, escapa a controles continuos.

En este caso la interpretación OT del ENS sería: la estación de ingeniería es un activo con impacto sistémico mucho mayor, aunque desde IT no se perciba como "infraestructura crítica".

Firewall perimetral vs red de control interna

Desde IT, el firewall perimetral es un activo clave, es punto de entrada, control de tráfico y proporciona métricas de seguridad. En OT un fallo del firewall puede afectar a la conectividad, pero en escasas ocasiones afecta al control interno del proceso.

Por el contrario, una red de control mal segmentada internamente puede propagar errores o comandos no autorizados, incluso puede romper el determinismo o amplificar fallos locales a nivel de planta.

En este caso la interpretación OT del ENS sería: la red interna de control puede ser más crítica que el perímetro IT, aunque sea menos visible en diagramas corporativos.

Sistema corporativo de identidad vs gestión local de accesos OT

Desde IT el sistema corporativo de identidad (IAM) es central permitiendo priorizar MFA, políticas y centralización. En OT la pérdida temporal del IAM no siempre impide operar y existen mecanismos locales de operación segura.

Pero una gestión deficiente de accesos locales en PLC, DCS o estaciones de operación, permitiría cambios no trazables, dificultaría la atribución e introduciría riesgo estructural.

Interpretación OT del ENS: el control local de accesos a activos OT críticos puede ser más relevante que la integración con sistemas corporativos avanzados.

Cómo se reflejan estos impactos en disponibilidad e integridad ENS

Principios para reflejar correctamente la disponibilidad e integridad en entornos OT:

- **Disponibilidad en OT**
  No significa "el sistema está encendido", sino el sistema permite mantener o llevar el proceso a un estado seguro y controlado cuando es necesario.
- **Integridad en OT**
  No significa solo "el software no ha sido modificado", sino el sistema se comporta de acuerdo con el diseño validado y de forma físicamente coherente.

Cualquier mecanismo que cumpla formalmente el ENS, pero degrade estas capacidades no mejora la seguridad real del sistema, aunque mejore métricas parciales.

Dimensiones ENS:

- Disponibilidad: las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren
- Confidencialidad: La información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados
- Autenticidad: una entidad (persona o proceso) es quien dice ser o bien que garantiza la fuente de la que proceden los datos
- Integridad: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada
- Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad

Consecuencia práctica para la aplicación del ENS

Una interpretación correcta del ENS en OT implica que:

- Los impactos físicos y operativos se consideran parte del impacto de seguridad.
- La disponibilidad y la integridad se evalúan a nivel de proceso, no solo de sistema.
- Se aceptan mecanismos distintos siempre que reduzcan el riesgo global.
- Se evitan controles que optimizan la seguridad lógica a costa de la seguridad operacional.

Este enfoque no amplía el ENS ni lo restringe, permite su aplicación exactamente a aquello que pretende proteger en entornos industriales.

PRINCIPIO DE NO INTERFERENCIA OPERACIONAL

El principio de no interferencia operacional parte de una idea sencilla pero imprescindible en entornos industriales: una medida de ciberseguridad no es aceptable si degrada, altera o pone en riesgo la función para la que el sistema existe. En OT, "proteger" nunca puede estar por encima de "hacer funcionar con seguridad operacional o funcional". A diferencia de IT, donde parar un servicio suele ser un problema de negocio, en OT interferir puede convertirse en un problema físico, ambiental o de seguridad de las personas.

Cuando se hace referencia a "no interferir" en OT, no significa no tocar nada o congelar los sistemas. Interferir significa introducir cambios que rompen supuestos operacionales básicos: determinismo, tiempos de respuesta, estabilidad del sistema, validaciones previas o condiciones certificadas de funcionamiento. Una medida interfiere cuando modifica el comportamiento temporal del sistema, introduce latencias no previstas, altera flujos de comunicación críticos, cambia versiones o configuraciones que estaban validadas, o añade dependencias externas que no existían. También se interfiere cuando se obliga a operar fuera de procedimientos conocidos o se introduce complejidad que la organización no puede gestionar en situación de estrés.

Esto incluye interferir en la capacidad del operador para interpretar correctamente el estado del proceso y actuar con rapidez y seguridad. En OT, confundir al operador es una forma directa de interferencia operacional.

Desde esta óptica, una medida del ENS debería interpretarse como válida en OT solo si reduce riesgo neto, no riesgo "en el papel". Es válida cuando mejora la capacidad de detectar, resistir o recuperarse de un incidente sin degradar la operación ni introducir nuevos modos de fallo. Por ejemplo, una segmentación bien diseñada que limite la propagación de un incidente sin afectar a los tiempos de proceso es coherente con OT. En cambio, esa misma segmentación, aplicada de forma rígida, que rompa flujos necesarios para la operación o el mantenimiento, introduce más riesgo del que elimina. El problema no es la medida en sí, sino su aplicación sin considerar las condiciones de operación industrial.

Aquí aparece una tensión clave entre ciberseguridad y seguridad funcional, que no son lo mismo ni pueden tratarse como capas independientes. La seguridad funcional se centra en evitar daños físicos mediante sistemas certificados, comportamientos deterministas y estados seguros conocidos. La ciberseguridad, en OT, debe actuar como una capa que protege esas funciones, no como una fuerza que las reconfigura sin entenderlas. Cualquier medida que obligue a modificar lógica, tiempos, secuencias o estados de seguridad funcional debe considerarse de alto riesgo y requerir un análisis específico. En muchos casos, la prioridad no es "cerrar" el sistema, sino lograr que, ante un incidente, el sistema falle de forma segura y predecible.

Por eso, aceptar o rechazar una medida no puede basarse únicamente en "cumple ENS", sino en criterios prácticos de interferencia. Una medida debería aceptarse en las siguientes situaciones:

- Ha sido validada en condiciones equivalentes a las de producción.
- No altera el comportamiento temporal del proceso.
- No introduce dependencias externas críticas.
- Puede mantenerse durante todo el ciclo de vida del sistema.
- Si la organización sabe operarla en condiciones normales y de crisis.

Debería rechazarse, o al menos replantearse en estos 4 casos:

- Requiere cambios frecuentes en sistemas certificados.

- Añade complejidad operativa no asumible.
- Desplaza riesgos hacia la seguridad funcional.
- Su fallo genera un impacto mayor que el riesgo que pretende mitigar.

En el fondo, este principio introduce una idea incómoda pero esencial en OT, no siempre lo "más seguro técnicamente" es más resiliente. El ENS permite esta lectura, aunque no la explicite, porque su objetivo es proteger servicios esenciales, no imponer mecanismos ciegos. Interpretarlo desde la visión OT no es debilitarlo, es alinearlo con la realidad física e industrial que pretende proteger. Aquí es donde la guía aporta valor sin cuestionar el ENS, pero sí cuestiona la forma automática sin considerar el marco de condiciones de operación industrial al aplicarlo.

Ejemplos de controles ENS bien y mal aplicados en condiciones de OT

Control ENS (familia)	Bien aplicado en OT	Mal aplicado en OT	Riesgo que introduce la mala aplicación	Quién debe decidir en OT
Segmentación de red	Zonas y conductos alineados con el proceso, flujos mínimos necesarios	Microsegmentación rígida heredada de IT	Paradas, pérdida de control del proceso	Ingeniería + Operación
Gestión de parches	Parches evaluados, probados y aplicados en ventanas operativas	Parcheo automático o periódico	Inestabilidad, pérdida de certificaciones	Ingeniería + Fabricante
Control de accesos	Roles operativos claros, accesos compatibles con OT	MFA intrusivo en HMI o ingeniería	Bloqueos en emergencia, errores humanos	Operación
Registro y monitorización	Monitorización pasiva y contextualizada	Inspección activa del tráfico industrial	Pérdida de determinismo	ICSO + Ingeniería + Operación
Gestión de cambios	Cambios excepcionales ligados a riesgo real	CAB IT para cualquier ajuste mínimo	Bypass y descontrol real	ICSO + Operación
Copias de seguridad	Backups industriales probados en restauración	Copias IT no verificadas	Falsa capacidad de recuperación	Ingeniería
Protección antimalware	Listas blancas adaptadas al sistema	Antivirus tradicional con escaneos	Consumo de recursos, bloqueos	Ingeniería
Gestión de vulnerabilidades	Priorización por impacto operativo	Escaneos activos indiscriminados	Caídas de equipos	ICSO
Autenticación centralizada	Uso selectivo sin dependencia crítica	Dependencia total de servicios IT	Pérdida de acceso en caída IT	ICSO
Cifrado de comunicaciones	Cifrado en enlaces no deterministas	Cifrado en control en tiempo real	Latencias y desincronización	Ingeniería
Gestión de proveedores	Requisitos realistas y asumibles	Exigencias IT copiadas del ENS	Proveedores críticos invisibles	Dirección + ICSO
Respuesta a incidentes	Prioriza personas y estado seguro	Playbooks IT de aislamiento	Riesgo físico y operacional	Dirección + Operación+ICSO

CONTROLES COMPENSATORIOS OT COMO CUMPLIMIENTO ENS

El concepto de control compensatorio en OT parte de una realidad incuestionable: no siempre es posible implantar el mecanismo técnico que el ENS presupone, pero sí es posible alcanzar el mismo objetivo de protección por otros medios. Un control compensatorio no es un arreglo ni una excepción; es una medida deliberada que reduce el riesgo de forma equivalente cuando el control "estándar" no es viable sin interferir en la operación. En OT, los controles compensatorios son frecuentes porque los sistemas no se diseñaron para ser modificados continuamente, sino para ser estables, predecibles y seguros en el plano físico.

Aquí es fundamental distinguir entre equivalencia funcional y equivalencia tecnológica. El ENS, como esquema de seguridad, define objetivos: controlar accesos, limitar propagación, detectar incidentes, preservar integridad o disponibilidad. Lo que no define, aunque a veces se interprete así, es que esos objetivos deban alcanzarse con una tecnología concreta. En IT, equivalencia funcional y tecnológica suelen coincidir; en OT, casi nunca. Pretender equivalencia tecnológica en OT suele implicar introducir agentes, software, cifrado o dependencias que alteran el sistema.

La equivalencia funcional, en cambio, permite usar controles de proceso, arquitectura, procedimientos operativos o incluso diseño físico para alcanzar el mismo nivel de protección.

En este marco, los procedimientos operativos, la formación específica del personal y la experiencia acumulada del operador constituyen controles compensatorios legítimos desde la perspectiva del ENS, siempre que estén documentados, entrenados y alineados con la protección del proceso.

Desde esta lógica, la aceptación razonada de controles OT es no solo válida, sino necesaria. Por ejemplo, la imposibilidad de aplicar MFA en un HMI crítico puede compensarse con control físico estricto del puesto, segregación de funciones, procedimientos de operación supervisados y registro manual de accesos. La ausencia de cifrado en una red de control en tiempo real puede compensarse con aislamiento fuerte, ausencia de conectividad externa directa y monitorización pasiva continua. La imposibilidad de aplicar parches frecuentes puede compensarse con control de cambios extremadamente restrictivo, listas blancas de software y pruebas exhaustivas antes de cualquier modificación. En todos estos casos, el riesgo residual se gestiona, no se ignora, y el objetivo del ENS se cumple sin forzar el sistema.

El punto crítico no es tanto qué control se aplica, sino cómo se justifica. Por eso, **documentar la equivalencia en "lenguaje ENS" es esencial para que auditores, responsables de seguridad y organismos de control entiendan la decisión**. Esto implica describir claramente qué objetivo del ENS se pretende cubrir, por qué el control estándar no es viable en las condiciones de operación industrial, qué medida compensatoria se aplica, qué riesgo reduce y qué riesgo residual permanece.

Es importante dejar constancia de que la decisión no es técnica exclusivamente, sino consciente, contextualizada y alineada con la protección del servicio esencial. Cuando se documenta así, el control compensatorio deja de ser una excepción y pasa a ser una forma legítima de cumplimiento.

INTERPRETACIÓN OT DE LAS PRINCIPALES FAMILIAS DE MEDIDAS ENS

Cuando el ENS habla de integridad, el marco mental habitual es el de ficheros, binarios y configuraciones almacenadas. En OT, la integridad es algo más amplio y, a la vez, más concreto: es la integridad de la lógica de control, de la secuencia de ejecución y de la coherencia entre lo que el sistema calcula y lo que el proceso físico hace. Un sistema industrial puede tener todos sus ficheros intactos y, sin embargo, estar comprometido si la lógica ha sido alterada, si se ejecuta fuera de secuencia o si las señales ya no representan fielmente el estado físico. Por eso, en OT proteger la integridad implica controlar quién puede modificar lógica, cuándo se puede descargar, cómo se valida, y cómo se detectan desviaciones entre comportamiento esperado y real. La integridad no se demuestra solo con hashes; se demuestra con estabilidad del proceso y consistencia física.

En disponibilidad, la diferencia es aún más evidente. En IT, disponibilidad suele equivaler a “servicio arriba”. En OT, disponibilidad significa capacidad de mantener el proceso en condiciones seguras, incluso cuando algo falla. Un sistema puede estar “disponible” desde el punto de vista técnico y ser inaceptable desde el punto de vista operativo si no permite operar con seguridad y/o calidad. Aquí entran conceptos como estados seguros conocidos, modos degradados controlados y procedimientos de recuperación progresiva. La disponibilidad en OT no se mide solo en tiempo de caída, sino en la capacidad del sistema para absorber fallos sin provocar daños, y para volver a operar sin introducir nuevos riesgos. Esto conecta directamente con la seguridad funcional y con la preparación de la organización, no solo con la tecnología.

El control de cambios y configuración en sistemas es otra familia del ENS que requiere una lectura específica. En OT, cambiar no es un acto administrativo, es un acto técnico con consecuencias físicas. Los sistemas suelen estar certificados, validados o ajustados durante años para un comportamiento concreto. Por eso, el control de cambios no puede basarse únicamente en flujos formales, sino en la excepcionalidad del cambio, su validación previa y su trazabilidad a lo largo del ciclo de vida. Mantener una configuración estable, conocida y reproducible es, en muchos casos, más importante que estar “actualizado”. Desde esta perspectiva, no cambiar sin análisis es una medida de seguridad, no una debilidad.

Por último, la monitorización y detección en OT debe asumir una restricción fundamental: observar sin perturbar. La instalación de agentes invasivos, escaneos activos o mecanismos que inspeccionan tráfico sin conocer los protocolos industriales puede introducir fallos difíciles de diagnosticar. En OT, la monitorización eficaz suele ser pasiva, basada en la observación del tráfico, del comportamiento del proceso y de desviaciones respecto a patrones conocidos. Detectar no es solo identificar malware, sino reconocer comportamientos anómalos del sistema industrial, incluso cuando no hay indicadores clásicos de compromiso IT.

La detección temprana en OT es más una cuestión de comprensión del proceso que de despliegue masivo de sondas o herramientas.

las familias de medidas del ENS siguen siendo válidas en OT, pero su significado cambia cuando el sistema deja de ser lógico y pasa a ser físico. Interpretarlas correctamente no rebaja el nivel de exigencia; lo eleva, porque obliga a entender cómo funciona realmente el proceso industrial que se quiere proteger.

Interpretación de las principales familias ENS con enfoque IT vs OT

Familia ENS	Interpretación típica en IT	Interpretación necesaria en OT	Qué cambia realmente
Integridad	Protección de ficheros, binarios, bases de datos y configuraciones	Protección de la lógica de control, secuencia de ejecución y coherencia física del proceso	De “no se modifica el archivo” a “no se altera el comportamiento del proceso”
Disponibilidad	Servicio accesible, sistemas operativos funcionando	Proceso en estado seguro, operación degradada controlada, recuperación progresiva	De uptime técnico a continuidad operativa segura
Control de cambios	Cambios frecuentes, gestionados por flujo y aprobación	Cambios excepcionales, validados previamente antes de su implementación y ligados al ciclo de vida industrial	Cambiar es un riesgo en sí mismo
Configuración	Configuración estándar, alineada con hardening	Configuración estable, conocida y reproducible	Estabilidad > actualización
Control de accesos	Identidades centralizadas, MFA, políticas dinámicas	Accesos ligados a roles operativos y situaciones reales	Acceder rápido y seguro puede ser crítico
Autenticación	Dependencia de servicios centrales (AD, IAM)	Autonomía local y tolerancia a fallos IT.	El control no puede caer
Monitorización	Agentes, EDR, escaneos activos	Monitorización pasiva y análisis de comportamiento	Observar sin interferir
Detección	IOC, firmas, malware conocido	Desviaciones de proceso y comportamiento anómalo	Detectar lo “imposible” físicamente
Gestión de vulnerabilidades	Escaneos periódicos y remediación rápida	Priorización por impacto operacional y exposición real	No todo se puede ni se debe “arreglar”
Copias de seguridad	Backups frecuentes, restauración lógica	Restauración funcional del proceso y estados seguros	Restaurar no es solo cargar datos
Registro de eventos	Logs técnicos centralizados	Evidencias operativas y trazabilidad del comportamiento	La evidencia también es física
Respuesta a incidentes	Aislar, apagar, contener	Mantener seguridad de personas y proceso	Contener no puede agravar el daño

GESTIÓN DEL CICLO DE VIDA INDUSTRIAL

La gestión del ciclo de vida industrial parte de una diferencia estructural con IT: los sistemas OT no se despliegan, se construyen, validan, operan y envejecen. El cumplimiento del ENS, por tanto, no puede concentrarse en el momento de la certificación, sino que debe acompañar al sistema durante toda su vida útil, adaptándose a cada fase sin romper la coherencia del conjunto.

En la puesta en marcha y validación inicial, especialmente en las fases de FAT (Factory Acceptance Test) y SAT (Site Acceptance Test), el foco no está solo en que el sistema funcione, sino en que lo haga de forma segura y reproducible. Es el momento donde se fijan muchos de los supuestos que condicionarán el cumplimiento ENS durante años: arquitectura de red, roles de acceso, mecanismos de respaldo, procedimientos de operación y criterios de cambio. Integrar requisitos ENS en FAT/SAT no significa añadir controles al final, sino verificar que las decisiones de diseño no introducen dependencias innecesarias, que los mecanismos de protección no interfieren con el proceso y que la operación puede mantenerse incluso ante fallos razonables. Lo que no se valida aquí será muy difícil de corregir después.

Durante la operación normal y supervisión, el cumplimiento ENS se manifiesta más en la estabilidad que en la actividad. En OT, cumplir no es cambiar, es saber exactamente cómo está el sistema y detectar cuándo deja de estarlo. La supervisión debe centrarse en mantener la configuración conocida, vigilar desviaciones del comportamiento esperado y asegurar que los accesos, procedimientos y dependencias siguen siendo los previstos.

Muchas no conformidades ENS en OT no aparecen por ataques sofisticados, sino por deriva operativa, cambios informales o pérdida de conocimiento acumulado con el paso del tiempo.

En sistemas de larga vida, la pérdida de conocimiento humano puede convertirse en el principal factor de riesgo ENS. Mantener el cumplimiento implica no solo conservar configuraciones técnicas, sino también asegurar la transferencia de conocimiento operativo y la capacitación continua de quienes interactúan con el sistema.

La fase de cambios, mantenimiento y paradas programadas es probablemente la más crítica desde el punto de vista del riesgo. Aquí el ENS se pone a prueba de verdad. Cada intervención rompe, aunque sea temporalmente, el estado validado del sistema. Por eso, el cumplimiento no puede basarse solo en autorizaciones formales, sino en análisis de impacto operativo, pruebas previas, reversibilidad y capacidad de volver a un estado seguro conocido. En OT, una parada programada mal gestionada puede introducir más riesgo que años de operación estable. El ENS, bien interpretado, exige precisamente lo contrario: rigor extremo cuando se toca el sistema.

El fin de vida, la sustitución y la gestión del legado industrial son aspectos tradicionalmente poco tratados en esquemas de seguridad, pero en OT son inevitables. Sistemas que siguen siendo críticos, pero que ya no pueden actualizarse, certificarse o integrarse con tecnologías modernas, deben seguir cumpliendo ENS desde una lógica de contención y compensación. Aquí entran en juego el aislamiento progresivo, la reducción de exposición, los controles organizativos y la planificación de la sustitución como medida de seguridad en sí misma. El mayor riesgo no es tener sistemas legacy, sino no reconocerlo ni gobernarlo.

Todo esto converge en una pregunta clave: **¿cómo mantener el cumplimiento ENS a lo largo de décadas?** La respuesta no está en multiplicar controles, sino en mantener coherencia. Esto implica documentar decisiones estructurales, preservar el conocimiento del sistema, revisar periódicamente la adecuación de los controles a las condiciones de operación industrial real y aceptar que el cumplimiento es dinámico. Un sistema industrial puede seguir cumpliendo ENS sin cambiar durante años, siempre que el entorno, los riesgos y las dependencias sigan siendo los mismos. Cuando eso cambia, el cumplimiento debe revisarse, no asumirse.

Interpretación del ciclo de vida industrial desde el ENS (enfoque OT)

Fase del ciclo de vida industrial	Qué significa "cumplir ENS" en esta fase	Riesgos típicos si se aplica con sesgo IT	Enfoque correcto desde OT
Diseño y puesta en marcha (FAT/SAT)	Verificar que las decisiones de diseño no introducen riesgos estructurales y que los controles no interfieren en la operación	Añadir controles al final, sin validar impacto operacional	Diseñar y validar con ENS desde el inicio, priorizando estabilidad y coherencia
Validación inicial	Asegurar que el sistema arranca en un estado seguro, conocido y reproducible	Dar por válido un sistema que "funciona" pero no es gobernable	Validar comportamiento, no solo funcionalidad
Operación normal	Mantener el sistema dentro de los supuestos validados	Confundir cumplimiento con cambios continuos	Estabilidad, trazabilidad y detección de desviaciones
Supervisión	Detectar anomalías sin interferir en el proceso	Monitorización invasiva o genérica	Monitorización pasiva y contextualizada
Mantenimiento rutinario	Intervenir sin romper el estado validado del sistema	Cambios informales o sin análisis de impacto	Cambios excepcionales, documentados y reversibles
Paradas programadas	Momento crítico para revisar y reforzar seguridad	Aprovechar la parada para "modernizar" sin control	Planificación, pruebas y retorno a estado seguro
Cambios evolutivos	Adaptar el sistema sin perder coherencia	Introducir dependencias IT no evaluadas	Análisis de impacto operativo y de ciclo de vida
Incidentes	Mantener seguridad de personas y proceso	Aislar o apagar sistemas sin criterio OT	Contención compatible con operación segura
Fin de vida	Reducir exposición y dependencia	Mantener sistemas obsoletos sin control	Aislamiento progresivo y planificación de sustitución
Sustitución	Transferir funciones críticas sin pérdida de control	Migraciones aceleradas por cumplimiento	Transición gradual y validada
Legado industrial	Aceptar limitaciones técnicas con controles compensatorios	Exigir controles imposibles	Gobernar el riesgo residual
Revisión periódica	Confirmar que las condiciones de operación industrial no han cambiado	Dar por válido el cumplimiento histórico	Revisión basada en cambios reales del entorno

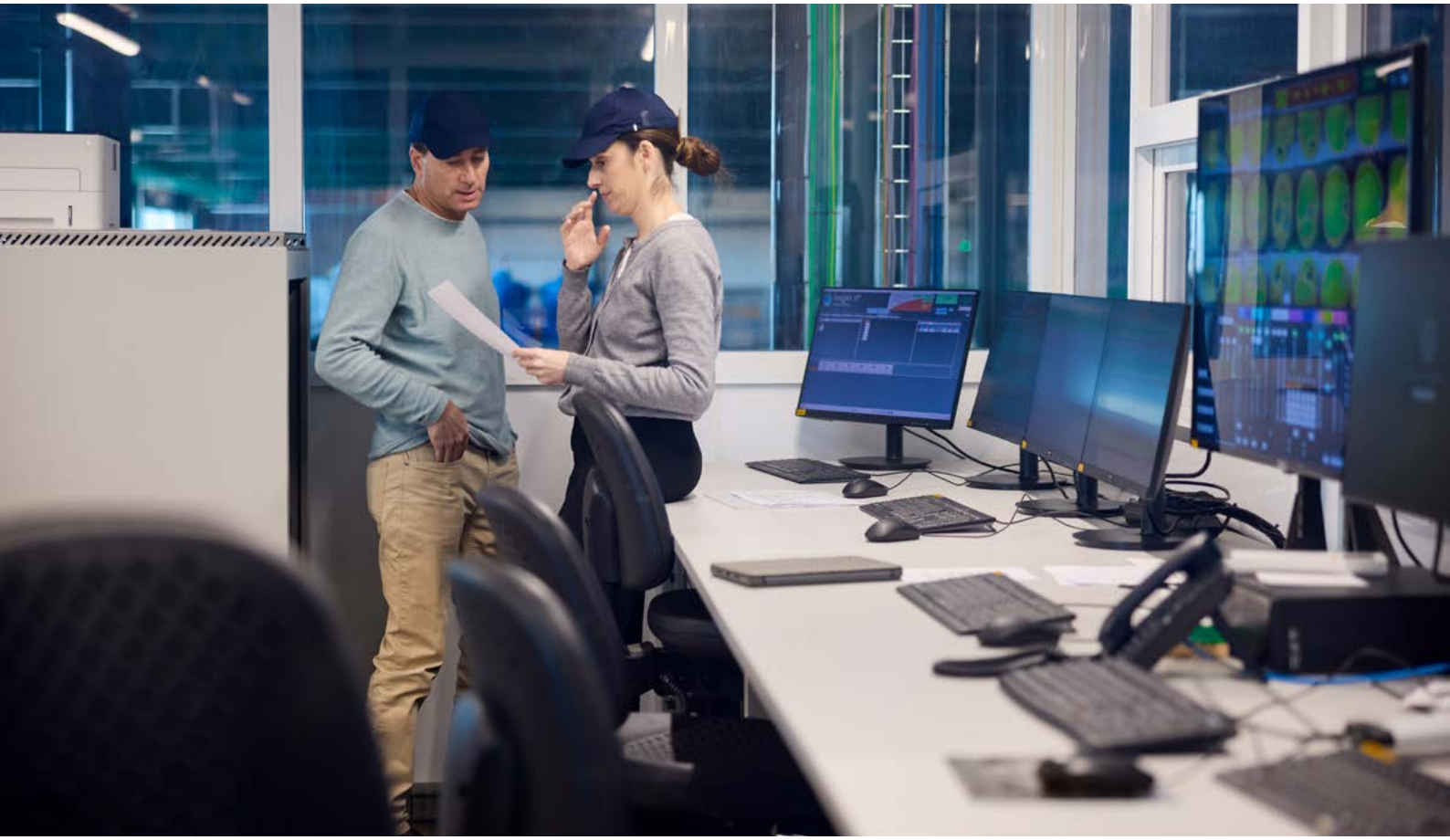
FACTOR HUMANO EN OT

En entornos OT, el factor humano no puede abordarse como un elemento accesorio o exclusivamente formativo. El operador industrial no es un "usuario" en el sentido IT del término, sino una parte activa del sistema de control y de la línea de defensa física y funcional del proceso. Muchas decisiones críticas que afectan a la seguridad del sistema se toman en el plano humano, antes de que cualquier mecanismo técnico pueda actuar.

Desde una interpretación ENS en un marco de operación industrial, implica reconocer que una parte del cumplimiento efectivo del esquema reside en la capacidad de las personas para operar, interpretar y reaccionar de forma segura ante situaciones normales, anómalas o de emergencia. Ignorar este hecho conduce a modelos de cumplimiento formalmente correctos, pero operativamente frágiles.

En sistemas industriales, el operador actúa simultáneamente como sensor, decisor y actuador. Es quien detecta comportamientos anómalos del proceso que no siempre generan alarmas técnicas, quien decide cuándo una desviación es aceptable o peligrosa, y quien ejecuta acciones que pueden llevar al sistema a estados seguros o inseguros. Desde esta perspectiva, confundir, sobrecargar o limitar indebidamente al operador es introducir riesgo, no mitigarlo.

El ENS, aunque no lo explicite de forma detallada, reconoce este principio cuando exige fortalecer la disponibilidad e integridad de los sistemas que soportan servicios esenciales. En OT, estas garantías no pueden cumplirse únicamente mediante controles tecnológicos, sino que requieren que las personas que interactúan con el sistema comprendan su funcionamiento, sus límites y los riesgos asociados a determinadas decisiones bajo presión.



La formación complementaria en OT, por tanto, no equivale a concienciación genérica en ciberseguridad. No se trata de sensibilizar sobre amenazas abstractas, sino de formar en:

- Reconocimiento de desviaciones del comportamiento normal del proceso.
- Comprensión de las consecuencias físicas de determinadas acciones técnicas.
- Actuación segura ante fallos técnicos, errores humanos o incidentes de seguridad.
- Conocimiento claro de qué no debe hacerse en situaciones de estrés operativo.

Desde el punto de vista del ENS, los procedimientos operativos, la capacitación específica del personal y la experiencia acumulada constituyen controles organizativos y operativos plenamente válidos, siempre que estén formalizados, entrenados y alineados con la protección del proceso. En muchos casos, estos elementos actúan como controles compensatorios frente a la imposibilidad de implantar mecanismos IT clásicos sin interferir en la operación.

Además, en sistemas de ciclo de vida largo, la pérdida de conocimiento humano se convierte en un riesgo estructural. Cambios de personal, jubilaciones o externalizaciones pueden degradar la capacidad de control del sistema incluso cuando la tecnología permanece estable. Mantener el cumplimiento ENS en estos entornos exige asegurar la transferencia de conocimiento, la actualización de procedimientos y la continuidad de la formación a lo largo del tiempo.

Una interpretación correcta del ENS en OT debe, por tanto, asumir que:

- El operador es parte del sistema de seguridad.
- Las personas pueden ser una barrera de protección o un amplificador de riesgo.
- La seguridad real depende tanto de la coherencia técnica como de la coherencia humana.

En consecuencia, cumplir ENS en OT no es solo proteger sistemas, sino capacitar a quienes los gobiernan en tiempo real. Reconocer explícitamente este hecho no debilita el marco, sino que lo alinea con la realidad física y operativa de los procesos industriales que pretende proteger.

ALGUNOS CASOS PRÁCTICOS DE INTERPRETACIÓN ENS EN OT

Estos casos son únicamente ilustrativos y no deberían tomarse como válidos en todas las situaciones.

PLC: integridad de lógica y comportamiento

En un PLC, la integridad no se juega en ficheros ni en sistemas operativos, sino en la lógica de control y en su ejecución determinista. Desde una lectura ENS con un marco de operación industrial, cumplir integridad significa que solo personas y procesos autorizados pueden modificar la lógica, que cualquier cambio está validado previamente y que el comportamiento del proceso físico sigue siendo coherente con lo esperado.

No siempre es necesario, ni deseable, instalar agentes de integridad o mecanismos de protección propios de IT si estos interfieren con el ciclo de ejecución del PLC. En su lugar, el cumplimiento se apoya en el control de accesos a la ingeniería, la protección de las descargas de lógica, la existencia de una versión de referencia validada y la capacidad de detectar desviaciones de comportamiento del proceso, incluso aunque la lógica "aparente" no haya cambiado.

SCADA: operación, usuarios y trazabilidad

En sistemas SCADA, la interpretación ENS gira alrededor de la operación continua y la trazabilidad de acciones relevantes. Cumplir no implica forzar esquemas complejos de identidad heredados de IT, sino asegurar que los usuarios operan con roles claros, que las acciones críticas quedan registradas y que existe una separación real entre operación, mantenimiento y administración. En OT, la trazabilidad no se limita a logs técnicos, sino que incluye saber quién actuó, sobre qué parte del proceso y en qué marco operativo. Un SCADA puede cumplir ENS sin integrarse plenamente en un IAM corporativo si existen mecanismos locales robustos, procedimientos operativos claros y capacidad de reconstruir lo ocurrido ante un incidente.

DCS: cambios controlados y dependencia del proveedor

En un DCS, el foco ENS se desplaza hacia el control de cambios y la gestión de dependencias críticas. Estos sistemas suelen estar estrechamente ligados al proveedor, con herramientas propietarias y ciclos de actualización muy controlados. Cumplir ENS no significa romper esa relación, sino gobernarla.

La interpretación correcta en la mayoría de las situaciones requiere asegurar que los cambios son excepcionales, documentados y validados, que el acceso del proveedor está controlado y supervisado, y que la organización entiende qué partes del sistema están bajo su control directo y cuáles no. La dependencia del proveedor no es, por sí misma, un incumplimiento ENS; lo es no reconocerla ni gestionarla como un riesgo estructural.

Redes industriales: segmentación y monitorización pasiva

En redes industriales, el ENS suele leerse como una exigencia de segmentación, control y monitorización. En OT, esta exigencia se cumple cuando la red refleja la lógica del proceso industrial, no cuando replica arquitecturas IT. La segmentación debe proteger flujos críticos sin romperlos, y la monitorización debe observar

sin interferir. El uso de técnicas pasivas, conocimiento de protocolos industriales y detección de desviaciones de comportamiento es coherente con el ENS, incluso aunque no existan agentes ni inspección activa profunda. El cumplimiento aquí se demuestra con estabilidad, visibilidad y capacidad de reacción, no con volumen de herramientas desplegadas.

La aplicación del ENS en entornos industriales requiere en la mayoría de situaciones que la arquitectura de red se diseñe explícitamente bajo el principio de **zonas y conductos**, alineando la segmentación lógica y física con el proceso industrial, sus dependencias operativas y sus niveles reales de criticidad. No se trata únicamente de separar redes, sino de definir dominios de confianza claros, flujos permitidos y puntos de control donde la supervisión y la protección tengan sentido operativo.

Esta aproximación permite limitar la propagación de incidentes, preservar la disponibilidad del proceso y facilitar una monitorización pasiva eficaz, proporcionando al operador capacidad de interpretar señales con una visión comprensible y accionable del estado real del proceso y actuar conforme a procedimientos entrenados, lo cual es un factor determinante para que los controles ENS sean efectivos en la práctica.

RELACIÓN DE ESTA GUÍA CON OTROS MARCOS

Esta guía no pretende sustituir ni reinterpretar otros marcos técnicos, normativos o de buenas prácticas existentes. Su objetivo es actuar como capa de interpretación, ayudando a aplicar el ENS en entornos OT de forma coherente con la realidad industrial, apoyándose precisamente en esos otros marcos cuando aportan rigor técnico, experiencia acumulada o criterios contrastados.

La guía se sitúa, por tanto, en un plano distinto, no prescribe controles, sino que explica cómo leer y justificar el cumplimiento del ENS cuando el sistema a proteger es físico, determinista y de larga vida.

Relación con IEC 62443

La serie IEC 62443 constituye el marco de referencia internacional más sólido para la seguridad de sistemas de automatización y control industrial. Su foco está en definir requisitos técnicos, organizativos y de ciclo de vida específicos para entornos OT, incluyendo arquitectura en zonas y conductos, niveles de seguridad, gestión del cambio y desarrollo seguro.

Esta guía no replica ni sustituye IEC 62443. Al contrario, la utiliza como apoyo natural para demostrar cumplimiento ENS en tecnologías de operación industrial. En muchos casos, las medidas definidas en IEC 62443 permiten materializar los objetivos del ENS de forma más adecuada que los mecanismos IT clásicos, especialmente en lo relativo a integridad de lógica, disponibilidad segura y control de cambios. Desde esta perspectiva, IEC 62443 aporta el cómo técnico en OT donde el ENS define el qué debe fortalecerse.

Relación con guías técnicas del CCN

Las guías técnicas del CCN constituyen una referencia esencial para la correcta aplicación del ENS en entornos de tecnologías de la información y seguridad en el control de proceso y SCADA, que proporcionan criterios homogéneos para auditoría, certificación y supervisión.

Esta guía no contradice ni modifica dichas guías. Lo que hace es complementarlas cuando se aplican a entornos OT, explicando cómo interpretar sus objetivos y recomendaciones cuando los supuestos implícitos IT no se cumplen plenamente.

En este sentido, la guía mantiene intactos los objetivos de seguridad definidos por el ENS, pero aportando un marco de condiciones adecuadas para la operación industrial para justificar mecanismos alternativos o compensatorios que facilitan el diálogo técnico entre responsables OT, auditores y organismos supervisores. El resultado no es una excepción al ENS, sino una aplicación más fiel a su finalidad última que consiste en proteger servicios esenciales sin introducir nuevos riesgos.

Relación con buenas prácticas de codificación segura de PLC

Las buenas prácticas de codificación segura de PLC publicadas por el CCI y desarrolladas por PLC Security, se centran en un nivel muy específico: la lógica de control y su comportamiento seguro. Estas prácticas aportan criterios concretos para evitar errores, comportamientos inseguros o modificaciones no deseadas en sistemas de control.

Esta guía no entra en ese nivel de detalle técnico. Sin embargo, reconoce explícitamente que la integridad en OT se juega en la lógica y el comportamiento, no solo en ficheros o sistemas operativos. En este sentido, las buenas prácticas de codificación segura de PLC son un ejemplo claro de cómo un control técnico OT puede cumplir objetivos ENS de integridad, disponibilidad y resiliencia.

CONCLUSIONES

A lo largo de esta guía se ha puesto de manifiesto la idea central de que el ENS es un marco sólido, coherente y suficientemente flexible. Las dificultades reales en entornos OT no provienen de sus objetivos, sino de una interpretación sesgada basada en supuestos IT que no siempre se cumplen cuando los sistemas controlan procesos físicos, operan en tiempo real y tienen ciclos de vida de décadas.

Aplicar el ENS sin tener en cuenta el marco de condiciones de operación industrial conduce, en demasiadas ocasiones, a cumplir formalmente mientras se degrada la seguridad real del sistema. Esta guía demuestra que no es necesario modificar el ENS para evitarlo; basta con leerlo correctamente, separando objetivos de mecanismos y entendiendo qué significa proteger un servicio esencial cuando ese servicio es industrial, físico y operativo.

Cumplir ENS en OT no consiste en instalar más tecnología, ni en replicar controles IT allí donde no encajan. Consiste en gobernar el proceso industrial, tomar decisiones conscientes sobre riesgo, cambio, dependencia y operación, y ser capaz de explicarlas y defenderlas ante terceros. En este marco de operación industrial, la estabilidad, la trazabilidad, la validación previa y el control del ciclo de vida son tan relevantes como cualquier mecanismo técnico avanzado.

La seguridad en OT debe entenderse como coherencia del sistema físico-digital. Coherencia entre la lógica y el comportamiento del proceso. Coherencia entre las medidas de seguridad y la seguridad funcional. Coherencia entre lo que el sistema puede hacer y lo que las personas que lo operan entienden y son capaces de gestionar. Cualquier control que rompa esa coherencia, aunque mejore métricas parciales, no incrementa la seguridad global del sistema.

Esta guía también deja claro que el cumplimiento debe acompañar al sistema a lo largo de su vida útil y revisarse cuando cambian las condiciones de operación industrial y se demuestra mediante gobierno, no mediante actividad artificial. En este sentido, el operador, el ingeniero y el responsable de ciberseguridad industrial forman parte inseparable del modelo de seguridad, junto con la tecnología.

Como evolución natural de este enfoque, se abre el camino hacia la definición de un perfil ENS-OT, no como un nuevo esquema ni como una excepción, sino como una especialización legítima que reconozca explícitamente las particularidades de los sistemas industriales. Un perfil que facilite auditorías más coherentes, decisiones mejor informadas y una aplicación del ENS alineada con la realidad de los procesos que sostienen servicios esenciales.

En definitiva, cumplir el ENS en entornos OT no es un ejercicio de adaptación normativa, sino un ejercicio de madurez técnica y organizativa. Cuando se gobierna el proceso, se protege el servicio. Y cuando se protege el servicio, el ENS cumple exactamente la función para la que fue diseñado.

REFERENCIAS

Esquema Nacional de Seguridad (ENS)
https://ens.ccn.cni.es/es/que-es-el-ens

Centro de Ciberseguridad Industrial. (2024).
Auditoría de Ciberseguridad en instalaciones industriales
https://www.cci-es.org/activities/auditoria-de-ciberseguridad-ot/

Centro de Ciberseguridad Industrial. (2021).
Modelo de Control Interno en la Digitalización Industrial
https://www.cci-es.org/activities/modelo-de-control-interno-en-la-digitalizacion-industrial/

Centro de Ciberseguridad Industrial. (2022).
Prácticas seguras de codificación de PLC: lista de las 20 principales
https://www.cci-es.org/activities/top20plc/

Curso de responsable de auditoría de ciberseguridad en entornos industriales
https://www.cci-es.org/c06-curso-de-responsable-de-auditoria-de-ciberseguridad-en-entornos-ot/

Paseo de las Delicias, 30 - 2º
28045 Madrid

+34 910 910 751

info@cci-es.org
www.cci-es.org
blog.cci-es.org
@info_cci