

RESPUESTA A LA RESOLUCIÓN TRIGÉSIMA SÉPTIMA APROBADA POR LA COMISIÓN DE TRANSICIÓN ECOLÓGICA Y EL RETO DEMOGRÁFICO, DEL CONGRESO DE LOS DIPUTADOS, EN LA SESIÓN CELEBRADA EL 20 DE MAYO DE 2025, A LOS INFORMES ANUALES DE 2021, 2022 y 2023 DEL CONSEJO DE SEGURIDAD NUCLEAR (CSN) SEGÚN LA CUAL “EL CONGRESO DE LOS DIPUTADOS INSTA AL CONSEJO DE SEGURIDAD NUCLEAR A QUE REMITA AL CONGRESO DE LOS DIPUTADOS, EN EL PLAZO DE UN MES, UN INFORME DETALLADO SOBRE EL ESTADO ACTUAL DE LA CERTIFICACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD Y LA GESTIÓN DEL CONOCIMIENTO DESARROLLADA EN LOS ÚLTIMOS AÑOS”

En lo concerniente al estado actual de la certificación del Esquema Nacional de Seguridad (ENS) hay que indicar lo siguiente:

Desde el año 2013 el CSN dispone de una Política de Seguridad de la Información (PSI) acorde al Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica.

Entre los años 2010 y 2022, el Esquema Nacional de Seguridad ha ampliado alcance y objetivos, ha perfeccionado y adaptado las exigencias a las estructuras reales de las organizaciones, y ha incorporado elementos normativos como los relativos a la protección de datos de carácter personal, referencias a las normativas de seguridad europeas en materia de ciberseguridad, y la propia normativa española en distinta materia específica. Igualmente, en el campo técnico como consecuencia de las lecciones aprendidas de los ciberataques, se ha incluido la obligatoriedad de incorporar medidas técnicas concretas y se ha recogido la casuística de los servicios en la nube.

El nuevo ENS (R.D. 311/2022, de 3 de mayo) obliga a adaptar y adoptar nuevas medidas en las tres dimensiones principales: Organizacional, Operacional y Técnica; algunas de estas medidas son sencillas de implementar requiriendo otras de un marco temporal y de inversiones más amplias.

La adaptación al nuevo ENS culmina con el proceso de certificación que implica que todas medidas deben estar completamente implementadas en la organización en el momento final de auditoría del ENS.

Por tanto, este proceso de certificación en el que el CSN está inmerso, es la finalización de un largo camino iniciado hace más de dos años con los primeros proyectos para incorporar las medidas más complejas al organismo.

Los principales cambios que se han adoptado son de dos tipos:

Por un lado, la adaptación de las infraestructuras y elementos técnicos a los nuevos requisitos de seguridad como, por ejemplo, la extensión del doble factor de seguridad en los accesos (2FA), la modernización de tecnologías de protección en cortafuegos, en núcleos de red o Wifi; o por ejemplo, adquirir capacidades adicionales de análisis e inteligencia locales y complementarias en coordinación de las generales como, por ejemplo, investigación de incidentes, *hacking* éticos, auditorías o análisis forense, entre otros, no solamente en plano digital sino también en el físico, como una mejor gestión de accesos y mayor “sensorización” frente a riesgos de agua o gases en los CPD o simplemente garantizar la continuidad

eléctrica para el equipamiento informático cuya eficacia se puso de manifiesto recientemente.

Por otro lado, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el nuevo Esquema Nacional de Seguridad, dispone como elemento fundamental de su aplicación la definición y aprobación de la Política de Seguridad de la Información (PSI) y su órgano de gobernanza, los responsables de la información y de servicio y principios inspiradores de la seguridad de la información, la gestión del riesgos y el propio sistema de gestión de la información entre otros, todo ello incluido en los 15 artículos de los que consta la nueva Política de Seguridad de la Información del CSN, que ha reemplazado la anterior y que está vigente en el momento de emisión de este informe. Dicha PSI se adoptó por Acuerdo del Pleno del Consejo de Seguridad Nuclear el pasado día 19 de febrero de 2025.

Volviendo al proceso de la certificación ENS, este requiere obligatoriamente pasar en primer lugar una preauditoría interna para comprobar que el estado de madurez y las medidas implantadas en el organismo son las necesarias de cara a afrontar posteriormente la auditoría final con suficientes garantías para conseguir dicha certificación.

Por otro lado, y en un contexto general, el Centro de Operaciones de Ciberseguridad (COCS) de la Administración del Estado, dada la complejidad del proceso de certificación en el nuevo ENS de las entidades del sector público estatal, lanzó un programa de acompañamiento y ayuda para conseguir tal objetivo, que ha permitido al CSN realizar la preauditoría obligatoria de la certificación. Una vez que se han analizado las oportunidades de mejora a través del Plan de Acciones Correctivas (PAC), se han subsanado las cuestiones formales y administrativas, se han puesto en marcha o finalizado gran parte de las acciones a llevar a cabo lo cual permitirá concluir el proceso de certificación próximamente.

Como se ha señalado anteriormente, es importante contextualizar esta certificación en el marco general de sector público. Cabe reseñar la enorme dificultad para la adaptación al nuevo ENS por parte de un amplio número de entidades del sector público.

En concreto, hay que destacar que el CSN está entre el reducido grupo del 10 % de entidades del sector público con máximo nivel de certificación, lo que implica que se hayan reforzado los esfuerzos tanto humanos, como materiales y económicos que la organización está dedicando a su obtención.

Desde hace tiempo, el CSN dispone de un área específica en esta materia dentro de la Subdirección de Tecnologías de la Información (STI), y sus principales gestores disponen de habilitaciones máximas de gestión de seguridad, signo inequívoco de compromiso con la ciberseguridad. En diciembre de 2024, el CSN dotó de cinco nuevas plazas a la STI para afianzar la sistematización del desarrollo seguro y reforzar la gestión de las infraestructuras desde el punto de vista de la ciberseguridad.

En el año 2025, el presupuesto destinado a la ciberseguridad se ha reforzado destinándose, principalmente, en medidas de prevención y mejora de las infraestructuras y las comunicaciones (ej., actualización de cortafuegos, incremento de la fortificación de la red Wifi, mejora de control de acceso y, sobre todo, incorporación de servicios especializados para su gestión y análisis). Esta cantidad es casi el doble de lo presupuestado durante los años 2023 y 2024 juntos, debido a la necesidad de incorporación de medidas técnicas

requeridas por el Esquema Nacional de Seguridad como, por ejemplo, la extensión del segundo factor de autenticación en el acceso y en sistemas críticos, elemento de protección crucial en las organizaciones como lo ha puesto de manifiesto, en numerosas ocasiones, el Centro Criptológico Nacional (CCN-CERT).

La cantidad destinada al cumplimiento de las medidas del ENS (ciberseguridad) puede ser considerada de hecho dos o tres veces mayor si tenemos cuenta la contratación y uso de servicios indirectos de protección como, por ejemplo, el centro de respaldo y continuidad de Portal Web del CSN, que permitió operar con total normalidad durante el apagón eléctrico del lunes 28 de abril pasado, y que es una medida concreta que exige el ENS; como el “escudo anti-DDoS”, inteligencia de accesos y red, protección en movilidad, auditorías externas, elementos de limpieza y protección de navegación Web y correo electrónico, que se exigen en el ENS y de los que el CSN ya dispone igualmente.

Finalmente hay que indicar que, en el año 2025, el gasto en servicios de ciberseguridad (80 %) superó por primera vez a la inversión en elementos físicos y software (20 %), signo inequívoco de estado de madurez en ciberseguridad, siguiendo el principio de que lo primero es incorporar tecnología, posteriormente, avanzar en operación e inteligencia y finalmente, integrar y sistematizar toda la ciberseguridad en una visión 360 grados que abarque toda la protección de los sistemas de información del CSN.

En relación con la Gestión del conocimiento desarrollada en los últimos años:

Con motivo de la resolución decimoquinta del Congreso de los Diputados de junio de 2017 por la que se “insta al Consejo de Seguridad Nuclear a mantener, a través de una eficaz política de recursos humanos, la preservación de la gestión del conocimiento, como eje esencial de funcionamiento del órgano regulador basado en su capital humano”, el CSN inició un Plan de Gestión del Conocimiento focalizado principalmente en la transmisión del conocimiento del personal en edad de jubilación para evitar la pérdida del conocimiento tácito, en lo que se denominó Proceso RECOR, para garantizar un adecuado relevo generacional mediante la transmisión del conocimiento. En realidad, este proceso ya lo había iniciado el CSN con anterioridad, en el año 2015.

El Proceso RECOR llevaba aparejado el desarrollo de una aplicación informática, denominada KITE, encargada de albergar todos los retornos (fichas de conocimiento, registros, videos, etc.) obtenidos del proceso practicado con las personas con conocimiento crítico y próximas a su jubilación, que está habilitada para consulta de todo el personal del CSN.

En respuesta a la resolución décima aprobada por la Comisión de Transición Ecológica y el Reto Demográfico, del Congreso de los Diputados, en la sesión celebrada el 27 de septiembre de 2022, el CSN ya informó de los avances de su programa de gestión del conocimiento a lo largo de los años 2020 y 2021.

El programa de gestión del conocimiento se ha ampliado con la creación de comunidades de conocimiento y está enfocado a identificar, manejar y compartir, de forma integrada y sistemática, el conocimiento y la información dentro del CSN, y permitir que sus

trabajadores, individual o colectivamente, creen, compartan y mantengan actualizados nuevos conocimientos, capacidades y aptitudes orientados al logro de los objetivos del CSN.

El modelo de gestión del conocimiento desarrollado hasta ahora puso en práctica un procedimiento de preservación del conocimiento, un procedimiento de transferencia del conocimiento y un procedimiento de comunidades del conocimiento, así como vídeos informativos y de sensibilización hacia el proceso RECOR. En ellos se explica en qué consiste el proceso, las responsabilidades del experto, y además se detalla gráficamente en qué consisten los productos (piezas de conocimiento) resultantes del proceso y el uso de la aplicación KITE y otros espacios asociados a este proceso.

En 2021, debido a las restricciones por la pandemia, las sesiones de preservación del conocimiento se realizaron también *on-line*, con personal funcionario que alcanzó su jubilación y con funcionarios con conocimientos clave que cambiaron de puesto de trabajo como consecuencia del concurso de méritos interno del CSN.

Se han desarrollado las plataformas y redes de conocimiento, siendo ya práctica habitual que los organismos internacionales como el OIEA, la NEA, etc. nos proporcionen la participación y los enlaces en sesiones webinars, con la posibilidad de que expertos internacionales impartan clases magistrales, en determinados temas de interés para el CSN en materias de seguridad nuclear y protección radiológica. Adicionalmente, hay redes de conocimiento de estos organismos internacionales con los que el CSN mantiene relaciones multilaterales, bien en el seno del Organismo Internacional de Energía Atómica (OIEA) a través de IAEA CONNECT, bien en el seno del Foro Iberoamericano de Organismos Reguladores, Radiológicos y Nucleares (FORO) a través de la Red LAPRAM (Red Latinoamericana de Protección Radiológica en Medicina).

Como estrategia para transferir el conocimiento en el CSN se realizaron las acciones que se enumeran a continuación: a) formato llamado “Aula RECOR” que contiene instrucciones para la preparación de sesiones de transferencia de conocimiento de expertos tanto internos como externos del CSN; b) sesiones de transferencia de conocimiento en las subdirecciones de Tecnología Nuclear, Instalaciones Nucleares e Ingeniería como consecuencia de cambios de puesto de trabajo; c) utilización del formato webinar que ha permitido que expertos internos y externos puedan socializar su conocimiento mediante una charla magistral.

A continuación, se enumeran las siguientes actividades concretas:

- El CSN participa en diferentes bases de datos de la NEA entre ellas: CODAP (*Component Operational Experience, Degradation & Ageing Project*), FIRE (*Fire Incident Record Exchange*), ICDE (*International Common-cause Failure Data Exchange*) e IRS (*International Reporting System for Operating Experience*). Se definió esta comunidad inicialmente para despertar el interés de este conocimiento en las nuevas promociones, 64 funcionarios del Cuerpo Técnico incorporados como inspectores del CSN, hasta el año 2022.
- El 21 de mayo de 2021 se celebró una sesión de socialización, derivada de esta comunidad de conocimiento denominada “Bases de Datos de la NEA”, presentado por los distintos coordinadores representantes del CSN en estos Grupos de CODAP, FIRE,

ICDE, IRS, donde se analizaron los objetivos, modos de trabajo, así como las enseñanzas aplicadas a la seguridad nuclear.

- Por otra parte, en 2021 se participó en las dos reuniones anuales *on-line* en el grupo de trabajo del OIEA denominado *Steering Committee on Regulatory Capacity Building and Knowledge Management*, que aborda las materias relacionadas con la estrategia de formación y educación en materia de seguridad nuclear y protección radiológica 2021-2030.

Webinars desarrolladas en el año 2021 en el CSN

Fecha	Título
09/04/2021	“El valor del conocimiento tácito”
21/05/2021	“Sesión de Socialización y Transmisión del Conocimiento: Bases de Datos de la NEA”
22/10/2021	“Lecciones aprendidas y buenas prácticas del Proyecto Gestión del Conocimiento en Red Eléctrica de España – REE”
29/10/2021	“Presentación de la Comunidad: Análisis de Incertidumbre y Sensibilidad”
12/11/2021	“Liderazgo y Relevo Generacional”
26/11/2021	“La utilidad de la aplicación corporativa KITE Catálogo para la gestión del conocimiento en el CSN”

Durante 2022 se han desarrollado dos procesos de preservación del conocimiento de forma telemática y presencial, con funcionarios mayores de 64 años de las siguientes áreas: a) Instalaciones del Ciclo y Desmantelamiento (AICD) y b) Experiencia Operativa y Normativa (AEON) y cuatro procesos con funcionarios con conocimientos clave que cambiaron de puesto de trabajo de las siguientes áreas: a) Protección Radiológica de los Trabajadores (APRT), b) Servicios de Protección Radiológica (STPR), c) Gestión de Vida y Mantenimiento (GEMA) y d) Análisis Probabilista de Seguridad (AAPS).

Como estrategia para transferir el conocimiento en el CSN se ha utilizado el formato webinar en estas condiciones de situación de teletrabajo del personal, y que ha permitido que expertos internos puedan socializar su conocimiento mediante una charla magistral, en un total de siete sesiones.

Webinars desarrolladas en el año 2022 en el CSN

Fecha	Título
21/01/2022	“Cómo se hacen las inspecciones en instalaciones radiactivas”
18/02/2022	“Vigilancia de la contaminación interna en trabajadores de medicina nuclear”
07/04/2022	“El transporte de material radiactivo en España. Actualidad y futuro. Retos reguladores”
22/04/2022	“Colaboración con el proyecto HALDEN (OCDE) – Adaptación del sistema Copma II para simulación”
27/05/2022	“Análisis del transporte de material radiactivo en España entre 2000 y 2020”
24/06/2022	“Operación a largo plazo de las centrales nucleares”
28/10/2022	“Estado de desmantelamiento de la central nuclear José Cabrera”

En lo relativo a las comunidades del conocimiento, cabe señalar que la comunidad de conocimiento de análisis de incertidumbre y sensibilidad (AI&S) en el CSN se presentó oficialmente el 29 de octubre de 2021. A finales de ese año se configuró el núcleo básico de la comunidad el líder y el equipo motor. Durante el año 2022, la comunidad inició sus actividades, que han consistido en una serie de entrevistas a personas del Cuerpo Técnico del CSN y, además, una entrevista a un investigador externo al CSN.

En el año 2023 se ha dado un nuevo enfoque a la gestión del conocimiento, incluyendo esta metodología en uno de los procesos de apoyo, en el denominado proceso de “*Creación y desarrollo de competencias*” que tiene por objetivo que el personal adscrito al Consejo de Seguridad Nuclear disponga de todos los atributos necesarios (competencias) para llevar a cabo sus funciones. Este proceso responde al concepto básico de *Capacity Building* del OIEA. Este proceso de apoyo incluye la formación, la gestión del conocimiento, becas y cátedras. Dentro de la formación cabe destacar que se ha finalizado en el año 2023 el desarrollo de la metodología SAT (*Systematic Approach to Training*) para la elaboración de los Planes Anuales de Formación. Esta metodología, elaborada por el OIEA, clasifica al personal en puestos tipo, para cada puesto tipo identifica las tareas que tiene que llevar a cabo y para cada tarea las competencias necesarias, de tal manera que a cada funcionario se le da la formación que realmente necesita para llevar a cabo sus tareas, cubriendo todo el arco de competencias dentro de cada unidad organizativa.

Estas competencias se consiguen también a través de programas de actividades complementarias, todas ellas necesarias, que en este proceso se identifican en dos bloques principales, lo relativo a la formación SAT y lo relativo a la gestión del conocimiento.

Dentro del proceso de Creación y Desarrollo de Competencias, y como actividades que ayudan en el objetivo de conseguir personal con las competencias requeridas para el desempeño de las funciones del CSN, están las relativas a las convocatorias de becas para la formación especializada en materia de seguridad nuclear y protección radiológica en el propio CSN, lo que facilita que los becarios seleccionados por un proceso competitivo ya sean los que tienen más méritos acordes a las funciones del CSN pero que además les permite adquirir una formación que les habilitará para el proceso de reclutamiento posterior.

Además, dentro también del proceso de Creación y Desarrollo de Competencias, se consideran también las convocatorias de Cátedras, en las que el CSN financia programas de estudios en los que los aspectos de seguridad nuclear y protección radiológica tienen un papel destacado y cuyo objetivo es:

- a) Incentivar la formación de personal técnico altamente cualificado en seguridad nuclear y protección radiológica y conseguir atraer talento.
- b) Ampliar conocimientos y especialización del alumnado, personal investigador y profesorado de la universidad, a través de sus propios planes de estudios, cursos de especialización y participación activa en proyectos de investigación afines.
- c) Promover actividades de investigación en el ámbito de la seguridad nuclear y la protección radiológica, que contribuyan a ampliar el conocimiento, producir desarrollos innovadores y difundir sus resultados.

Por otra parte, como estrategia para transferir el conocimiento en el CSN se ha utilizado el formato webinar que ha permitido que expertos internos del CSN puedan socializar su conocimiento, en un total de seis sesiones en 2023:

Webinars desarrolladas en el año 2023 en el CSN

Fecha	Título
20/01/2023	“Proyecto europeo de investigación DISCO. (Modern Spent Fuel Disolution and Chemistry in Failed Container Conditions)”
17/02/2023	“Nueva Red de estaciones automáticas (REA) de Vigilancia Radiológica ambiental “
22/06/2023	“Almacenamiento Geológico Profundo (AGP) y la situación en España”
14/07/2023	“Guía de calibración y verificación”
27/10/2023	“Documento del foro sanitario de tratamiento de fallecidos con material radiactivo “
17/11/2023	“Desmantelamiento de la central nuclear Santa María de Garoña”

Además de estas actuaciones, el Plan de Recursos Humanos 2024-2030, aprobado en diciembre de 2024, incorpora un enfoque estratégico integral desde la gestión de los recursos humanos, en el que la gestión del conocimiento es una herramienta esencial que debe acompañar los procesos de provisión de puestos de trabajo, de manera que el reemplazo generacional se nutra de herramientas que permitan mecanismos formales e informales de formación entre el personal que entra y sale del organismo.

La gestión del conocimiento se enmarca dentro de la línea 2 del Plan de RR. HH. “Gestión del talento” y es uno de los 11 programas del mencionado Plan de RR. HH., el programa 5, en concreto. Este programa contribuye al objetivo general del Plan de RR. HH., asegurar los recursos humanos necesarios, en términos cuantitativos y cualitativos, que permitan dar cumplimiento a los retos del CSN en el corto y medio plazo y, por lo tanto, que garanticen el cumplimiento de la misión del organismo, y los siguientes objetivos específicos:

- OE4. Adecuar las competencias profesionales del personal a las necesidades de la organización.
- OE5. Aprovechar el talento de los recursos humanos del CSN con el objeto de crear y compartir conocimiento corporativo.
- OE6. Mejorar el desempeño y la motivación del personal al servicio del CSN.

CUADRO 24. LÍNEAS DE ACTUACIÓN DEL PLAN DE RECURSOS HUMANOS DEL CSN.



En este contexto, la gestión del conocimiento se define como el enfoque integrado y sistemático encaminado a identificar, gestionar y compartir los conocimientos de una organización, así como a posibilitar que grupos de personas creen colectivamente nuevos conocimientos para facilitar la consecución de los objetivos de la organización.

El Programa prevé 3 acciones:

- La elaboración de mapas de conocimiento y mapas de conocimiento crítico.
- El diseño y puesta en marcha de actividades colaborativas que permitan el desarrollo de instrumentos de gestión del conocimiento.
- Desarrollo de mecanismos que permitan la transferencia del conocimiento por parte de las personas que dejan la organización (jubilaciones, traslados, etc.) con carácter sistemático.