Referencia: TR-109-2023	**Carácter nacional o internacional del proyecto: Proyecto nacional**

Línea estratégica de I+D+i principal: Transversales. Otras a determinar.

Título del proyecto subvencionado	**Entidad/es Investigadora/s Colaboradora/s**	**Año inicio-finalización previsto**
Análisis cuantitativo y fenomenológico de las amenazas cibernéticas a infraestructuras críticas nucleares y su impacto en la protección radiológica (CIBER-CLEAR).	Universidad de Granada	2023-2026

DESCRIPCIÓN Y OBJETIVOS DEL PROYECTO

Este proyecto de investigación tiene como objetivo explorar la importancia de la ciberseguridad en las infraestructuras nucleares, identificar las amenazas a las que se ven expuestas y, sobre todo, proponer recomendaciones a nivel regulatorio para mejorar esta situación y minimizar los riesgos.

La ciberseguridad de las infraestructuras nucleares se ha convertido en un tema de gran importancia. A medida que la tecnología digital se integra cada vez más en los sistemas de control y operación de estas instalaciones, se incrementa el riesgo de ataques cibernéticos que podrían comprometer la seguridad y el funcionamiento seguro de las centrales nucleares.

La importancia del tema radica en que las centrales nucleares representan infraestructuras críticas que tienen el potencial de causar un impacto significativo en la seguridad nacional, el medio ambiente y la vida de las personas en caso de un incidente grave. Los ataques cibernéticos pueden ser utilizados para acceder a sistemas de control, manipular datos o incluso interrumpir el suministro de energía nuclear. Por lo tanto, es esencial contar con medidas de ciberseguridad efectivas para proteger estas infraestructuras vitales, ya que un ataque exitoso podría tener consecuencias desastrosas. Además, el aumento en la digitalización de las centrales nucleares y la interconexión con otras redes aumenta la superficie de ataque y la complejidad de proteger estos sistemas.

Las necesidades actuales en materia de ciberseguridad de las infraestructuras nucleares requieren una mayor inversión en investigación y desarrollo de tecnologías de seguridad avanzadas, como sistemas de detección de intrusiones, análisis de vulnerabilidades y técnicas de protección de datos. Asimismo, se necesita fortalecer la colaboración entre los organismos reguladores, las instituciones gubernamentales y las industrias nucleares para establecer estándares y mejores prácticas de ciberseguridad. Partiendo de un análisis etiológico de este fenómeno, este proyecto pretende atender estas cuestiones desde un equipo multidisciplinar. Propone el diseño de instrumentos que propicien una constante actualización de conocimiento en lo que respecta a la ciberseguridad de infraestructuras nucleares:

1. Estudio de las políticas y medidas de seguridad promovidas para la protección de las infraestructuras críticas nucleares frente a ciberataques.
2. Examen de la etiología de los ciberataques a infraestructuras críticas y operadores de servicios esenciales en general, como punto de partida.
3. Examen de la etiología de los ciberataques a centrales nucleares.
4. Consideración de los tipos penales aplicables a crímenes radiológicos. Desarrollo de técnicas y análisis forenses nucleares.
5. Identificación de los principales desafíos cibernéticos para las instalaciones nucleares civiles.
6. Estudio de prospectiva observacional sobre las actuaciones llevadas y/o promovidas por otros organismos reguladores homólogos al CSN, así como en el seno de organizaciones internacionales (IAEA, NEA, entre otras) en relación con la normativa en materia de ciberseguridad.
7. Evaluación de las vulnerabilidades cibernéticas de las instalaciones nucleares y de las instalaciones radiactivas de 1ª y 2ª categoría.
8. Análisis de los mecanismos y criterios necesarios para la implementación de la ciberseguridad en un apropiado esquema de seguridad nuclear.
9. Estudio de la pertinencia de promover un Plan Coordinado de Ciberseguridad para las centrales nucleares españolas.
10. Consideración de los estándares actuales en materia de ciberseguridad nuclear y establecimiento de paralelismos regulatorios.
11. Formulación de eventuales propuestas de mejora.

12. Propuesta regulatoria de la responsabilidad de los titulares de las centrales nucleares que previenen, detectan y responden frente a ciberataques.
13. Colaboración técnica y jurídica para el cumplimiento de los objetivos del Plan Nacional de Ciberseguridad en lo que respecta a las instalaciones nucleares y radiactivas.
14. Diseño de charlas y formaciones en materia de ciberseguridad a los trabajadores y titulares de las plantas, en colaboración con el CSN.
15. Realización de pruebas de *hacking* ético que, en Ingeniería Telemática, pretende identificar amenazas de ciberseguridad en redes concretas para fortalecer el sistema de seguridad y mitigar los riesgos cibernéticos.
16. Acercamiento de la investigación propuesta a la sociedad.
17. Publicación de herramientas e instrumentos diseñados para paliar las lagunas: El modelo-guía de *Compliance,* la Guía de Seguridad Cibernética, el catálogo de riesgos y el Código de Buenas Prácticas; y puesta en marcha de una Red de expertos en el área para el espacio europeo e hispanoamericano que permitirá asegurar una constante y permanente actualización de los contenidos normativos y técnicos, en función de las necesidades, realidades y exigencias de la sociedad -a nivel nacional e internacional-. Además, tendrá a su disposición un Código de Buenas Prácticas en materia de ciberseguridad, un modelo de Guías con recomendaciones sobre la misma área y otros instrumentos.

Con este proyecto, se pretende paliar una falta de regulación actual en España en lo que respecta a la ciberseguridad de infraestructuras críticas nucleares, así como colaborar en la aportación de criterios y aspectos teórico-prácticos en este campo y ser un serio aporte para que el Estado español siga siendo referente en materia de ciberseguridad. Permitirá al CSN el desarrollo de criterios de producción normativa y propuestas de futuro desarrollo legislativo.

Se prevé además, fomentar la cultura de defensa de los trabajadores de infraestructuras nucleares para proteger activos críticos, prevenir interrupciones operativas, proteger información confidencial y promover el cumplimiento de la normativa y regulación en ciberseguridad con el fomento de una colaboración y respuesta efectiva que harán constar en el Código de Buenas Prácticas.