Ciberseguridad en la industria nuclear

WINS Academy

CONTENIDO

A QUIÉN SE DIRIGE ESTE MÓDULO

El público objetivo de este módulo incluye a gerentes con responsabilidad en seguridad física, o personal del organismo regulador o de un departamento gubernamental, que deseen comprender los antecedentes y las implicaciones de la ciberseguridad en la industria nuclear. El contenido técnico es de iniciación y no requiere conocimientos previos sobre ciberseguridad.

TEMAS CLAVE

Las tecnologías digitales están integradas en prácticamente todos los aspectos de las operaciones de las instalaciones nucleares. Estas tecnologías forman parte de los sistemas de seguridad física nuclear, sistemas de seguridad, sistemas de contabilidad y control de materiales nucleares y los sistemas que respaldan a los servicios de respuesta a emergencias. En los últimos años, las personas y los grupos con intenciones maliciosas han reconocido que el cambio de sistemas analógicos a sistemas digitales en la industria nuclear ha aumentado las oportunidades de realizar ciberataques.

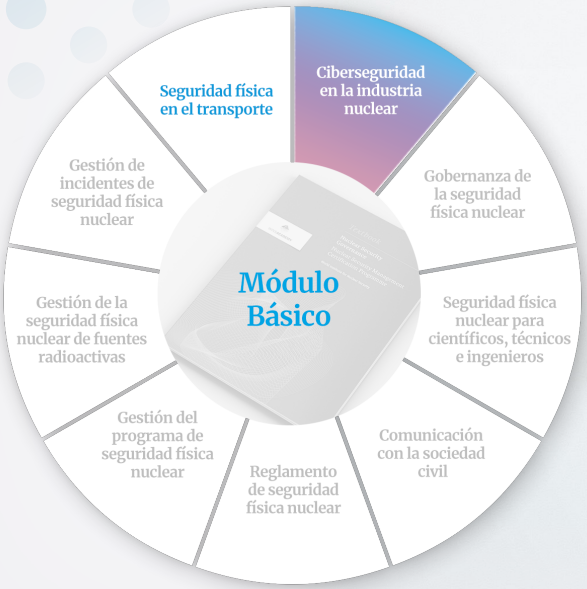
La base de la ciberseguridad es la protección de los sistemas de tecnología de la información y los sistemas de tecnología de la operación frente a ciberataques. Este módulo presenta la importancia de la ciberseguridad en la industria nuclear para ayudar a reflexionar acerca sobre cómo se podría mejorar la ciberseguridad en sus propias organizaciones. La ciberseguridad es un riesgo estratégico que debe gestionarse. Al realizar este módulo, usted puede ayudar a su organización a mejorar su resiliencia en materia de ciberseguridad.

OBJETIVOS DEL CURSO

El objetivo global de este módulo es proporcionar una descripción general de la ciberseguridad en la industria nuclear, incluidos los desafíos, terminología, mejores prácticas y normas relevantes. Completar con éxito este módulo lo ayudará a comunicarse de manera más efectiva con las y los profesionales especialistas en ciberseguridad y a tomar decisiones fundamentadas sobre ciberseguridad en su organización.

Al finalizar este módulo, Usted comprenderá:

- La ciberseguridad en el contexto de la industria nuclear
- Los actores de ciberamenaza (tanto actores internos como adversarios externos)
- Los sistemas de TI y TO dentro de las instalaciones nucleares que pueden ser objetivo de un ciberataque
- Las vulnerabilidades que podría aprovechar una ciberamenaza
- Los tipos de ciberataques que pueden llevar a cabo las ciberamenazas
- Vectores de ciberataque
- Las consecuencias potenciales de los ciberataques en una organización y en la sociedad en general
- La naturaleza de las distintas responsabilidades en materia de ciberseguridad en un Estado, incluidos los organismos reguladores, operadores y proveedores de la cadena de proveedores
- Los elementos clave y la importancia de desarrollar una estrategia de gestión de los riesgos de ciberseguridad eficaz como parte de una estrategia de gestión del riesgo organizativo o corporativo más amplia
- La necesidad de incorporar la ciberseguridad como un componente esencial de la cultura organizativa general y los métodos para establecer esta cultura en su organización
- Las capacidades de ciberseguridad necesarias en su organización
- Cuestiones relacionadas con la ciberseguridad en curso y emergentes en el entorno de trabajo
- Prácticas organizativas esenciales para la planificación, la preparación y la respuesta ante un incidente de ciberseguridad
- La importancia de la resiliencia en materia de ciberseguridad para la industria nuclear



ESQUEMA DEL MÓDULO

UNIDAD 1: CIBERSEGURIDAD EN LA INDUSTRIA NUCLEAR

1.1 Ciberseguridad
1.2 Actores de ciberamenaza
1.3 Objetivos de ciberataques: sistemas de las instalaciones nucleares
1.4 Ciberataques y sus consecuencias

UNIDAD 2: RESPONSABILIDADES NACIONALES EN MATERIA DE CIBERSEGURIDAD

2.1 Responsabilidades del Estado
2.2 Responsabilidades de los operadores
2.3 Gestión de la cadena de suministro

UNIDAD 3: GESTIÓN DE LOS RIESGOS DE CIBERSEGURIDAD

3.1 Riesgo
3.2 Estrategia de reducción de los riesgos de ciberseguridad
3.3 Evaluación de la gestión de los riesgos de ciberseguridad

UNIDAD 4: CULTURA DE CIBERSEGURIDAD

4.1 Cultura de ciberseguridad
4.2 Capacidad de ciberseguridad
4.3 Ciberseguridad y el entorno de trabajo

UNIDAD 5: PREPARACIÓN Y RESPUESTA A INCIDENTES DE CIBERSEGURIDAD

5.1 Planificación y preparación de la respuesta a incidentes de ciberseguridad
5.2 Respuesta a incidentes de ciberseguridad
5.3 Comunicación de incidentes de ciberseguridad

UNIDAD 6: ESCENARIOS DE CIBERSEGURIDAD

6.1 Escenario 1: Digitalización de sistemas y la cadena de suministro
6.2 Escenario 2: Regulación y evaluación de las amenazas
6.3 Escenario 3: Gestión de los riesgos de ciberseguridad
6.4 Escenario 4: Cultura de ciberseguridad
6.5 Escenario 5: Preparación y respuesta a incidentes de ciberseguridad