

CLP4NET Course Description Form

Descripción detallada	
Nombre completo del curso	Seguridad informática y seguridad de la información
Propósito del curso	Este curso está basado en documentos orientativos del OIEA y proporciona una introducción a los principios básicos de seguridad informática y seguridad de la información para profesionales de la seguridad física nuclear. En este módulo se analiza cómo aplicar técnicas de seguridad de la información y de seguridad informática en el proceso de protección de materiales nucleares y de otros materiales radiactivos. También explica cómo los Estados miembros deben proteger sistemas como estos contra posibles ataques.
Audiencia objetivo	Este curso está diseñado para participantes de formación presencial y para otras actividades de formación de recursos humanos implementados por el OIEA y por sus Estados miembros, así como para el personal de instalaciones nucleares interesado y para el público en general.
Programa	<ol style="list-style-type: none"> 1. ¿Qué es la seguridad informática? 2. Blancos potenciales 3. Amenazas y sus orígenes
Expectativas de aprendizaje	<p>Después de completar este curso, el alumno debería ser capaz de:</p> <ol style="list-style-type: none"> 1.1 Definir el concepto de seguridad informática 1.2 Identificar los principios de seguridad de la información 1.3 Describir los diferentes dominios de seguridad física 1.4 Describir la puesta en marcha de una defensa en profundidad 1.5 Describir la gestión de la seguridad informática 1.6 Definir medidas de seguridad informática 1.7 Describir la política 1.8 Describir la respuesta a incidentes 2.1 Identificar el papel que desempeñan los sistemas informáticos y las computadoras en diferentes aspectos relacionados con materiales nucleares y otros materiales radiactivos 2.2 Enumerar los puntos de enfoque clave 2.3 Aportar un ejemplo de integración de computadoras en una central nuclear 2.3 Enumerar las principales diferencias entre tecnología de la información (TI) y tecnología operacional (OT) 3.1 Identificar las características de una amenaza 3.2 Describir las ciberamenazas de agentes internos 3.3 Describir estudios de casos reales y posibles escenarios 3.4 Definir la ingeniería social en el contexto de la seguridad informática 3.5 Enumerar ejemplos de ataques a redes 3.6 Describir los ataques que pueden producirse en sistemas de control industrial (SCI) 3.7 Identificar riesgos emergentes 3.8 Identificar nuevos blancos 3.9 Identificar comportamientos humanos que aumentan el riesgo para los sistemas informáticos
Área de conocimientos	
Palabras clave	Seguridad informática y seguridad de la información
Cursos previos obligatorios	Ninguno
Idioma	Inglés, árabe, chino, español, francés, ruso
Interactividad	Autoestudio
Formato	Aprendizaje electrónico online
Duración	1 h
Evaluación	Sin evaluar
Certificación	Certificado de participación

CLP4NET Course Description Form

Número de versión	v2.01
Fecha de la versión	
Requisitos técnicos extraordinarios	N/A
Autores y propietarios	
Titular de la propiedad intelectual	OIEA
Derechos de autor y otras restricciones	Copyright del OIEA
Contacto	nsnselearning@iaea.org
Identificadores de etiquetas de taxonomía web del OIEA	3077; 3105; 3232; 3303; 3740; 3744; 3764
Nombres de etiquetas de taxonomía web del OIEA	Seguridad informática y seguridad de la información; Departamento de Seguridad Nuclear Tecnológica y Física; Seguridad nuclear tecnológica y física; Aprendizaje online; Seguridad física; Aspectos de seguridad física de las instalaciones nucleares; Seguridad física de materiales nucleares y de otros materiales radiactivos