

PROGRAMA FORMATIVO:

Ciberseguridad

DATOS GENERALES DEL CURSO

1. **Familia Profesional:** Informática y Comunicaciones

Área Profesional: Sistemas y Telemática

2. **Denominación:** CIBERSEGURIDAD

3. **Código:** IFCT120EXP

4. **Nivel de cualificación:** 3

5. **Objetivo general:**

- Identificar y evaluar los riesgos en los sistemas de control industrial y los aspectos fundamentales de la ciberseguridad industrial y realizar un diagnóstico de la seguridad en los entornos industriales.
- Crear, aplicar e implementar un programa de ciberseguridad industrial en función de los riesgos identificados.

6. **Prescripción de los formadores:**

6.1. Titulación requerida:

Titulación universitaria u otros títulos equivalentes, o capacitación profesional equivalente acreditada

El formador deberá contar con formación previa y experiencia en el área de la ciberseguridad.

6.2. Experiencia profesional requerida:

Experiencia Profesional de al menos 12 meses en la ocupación relacionada con la especialidad a impartir, excluyendo la experiencia docente.

Experiencia demostrable como responsable de gestión de los riesgos de ciberseguridad en organizaciones industriales, y/o como consultor y auditor de sistemas de gestión de riesgos en entornos industriales

6.3. Competencia docente:

Será necesario tener experiencia metodológica o experiencia docente contrastada de al menos 500 horas de formación en especialidades relacionadas con la especialidad a impartir.

7. **Criterios de acceso del alumnado:**

7.1. Nivel académico o de conocimientos generales: Título de FP Grado superior, bachillerato, preferentemente en ramas técnicas, profesionales de automatización industrial y /o gestores de riesgos

Cuando el aspirante al curso no posea el nivel académico indicado, demostrará conocimientos suficientes a través de una prueba de acceso.

Se requiere inglés a nivel de lectura, conocimientos de sistemas operativos e informática.

8. Número de alumnos:

Máximo 25 participantes para cursos presenciales.

9. Relación secuencial de módulos:

- Módulo 1: Ciberseguridad Industrial e Infraestructuras Críticas Industriales
- Módulo 2: Diagnóstico de la Ciberseguridad Industrial
- Módulo 3: Diseño de un programa de gestión y estrategias de Ciberseguridad Industrial
- Módulo 4: Integración de la ciberseguridad industrial con el resto de tecnologías y disciplinas del ecosistema de la Industria 4.0.

10. Duración:

Horas totales: 100 horas

11. Requisitos mínimos de espacios, instalaciones y equipamiento.

11.1. Espacio formativo:

Aula de Informática: Superficie: 45 m² para grupos de 15 alumnos (3 m² por alumno).

Cada espacio estará equipado con mobiliario docente adecuado al número de alumnos, así mismo constará de las instalaciones y equipos de trabajo suficientes para el desarrollo del curso.

11.2. Equipamiento:

Los equipos tendrán unas características equivalentes a las enumeradas a continuación, consideradas siempre como mínimas:

Un ordenador por alumno y uno para el profesor con las siguientes características mínimas:

- CPU: procesador Intel Core i5 de 6 generación o similar.
- 16 GB de RAM
- Disco duro de 500 GB
- Lector-grabador DVD
- Tarjeta de red 10/100/1000 Mbps
- Teclado multimedia USB
- Ratón sensor óptico USB de 2 botones y rueda de desplazamiento.
- Monitor color de 17" TFT
- Licencia de sistema operativo WINDOWS 7 o similar.
- Licencia de software antivirus.
- Licencias del software del fabricante necesario para la impartición del curso.

Conectividad a Internet.

Impresora láser con conexión a red.

Pantalla y cañón de proyección.

A los alumnos se les proporcionará la documentación para la implantación de un sistema de gestión de la ciberseguridad industrial y buenas prácticas para el diagnóstico de ciberseguridad en entornos industriales.

Las instalaciones y equipamientos deberán cumplir con la normativa industrial e higiénico-sanitaria correspondiente y responderán a medidas de accesibilidad universal y seguridad de los participantes.

En el caso de que la formación se dirija a personas con discapacidad se realizarán las adaptaciones y los ajustes razonables para asegurar su participación en condiciones de igualdad.

12. Requisitos oficiales de los centros

Para la impartición de esta especialidad formativa el Centro ha de estar homologado como:

Centro de formación

13. Evaluación del aprendizaje

Se llevará a cabo una evaluación continua y sistemática durante el proceso de aprendizaje y al final del mismo para comprobar si los alumnos han alcanzado los objetivos establecidos en cada módulo y, por consiguiente, han realizado el curso con el aprovechamiento requerido.

14. Certificación oficial no

MÓDULOS FORMATIVOS

Módulo 1

Denominación: Ciberseguridad Industrial e Infraestructuras Críticas Industriales

Objetivo: Comprender las amenazas y retos de los sistemas de automatización y control industrial, así como las buenas prácticas aplicables a las infraestructuras críticas.

Duración: 20 horas

Contenidos teórico prácticos:

- 1.1 Conceptos de automatización y ciberseguridad industrial. Situación actual
 - 1.1.1 Marco legal y normativo, estándares
 - 1.1.2 CCI (Centro de Ciberseguridad Industrial), CCN, INCIBE, NIST y otros
 - 1.1.3 Buenas prácticas aplicables a las infraestructuras críticas y ciberseguridad industrial
- 1.2 Retos y amenazas actuales en Ciberseguridad
 - 1.2.1 Aproximación a los Sistemas de Control Industrial y Automatización industrial
 - 1.2.2 Tecnologías de automatización industrial y escenarios de riesgo
 - 1.2.3 Malware en entornos industriales 4.0

Módulo 2

Denominación: Diagnóstico de la Ciberseguridad Industrial

Objetivo:

Adquirir el conocimiento del estado de la ciberseguridad en una instalación industrial mediante el diagnóstico e identificación de puntos débiles y los ciberriesgos que la instalación posee.

Duración: 30 horas

Contenidos teórico prácticos:

- 2.1 Diagnóstico técnico y organizativo de la ciberseguridad industrial.
 - 2.1.1 Amenazas y vulnerabilidades de los sistemas de control industrial.
 - Riesgos tecnológicos de las infraestructuras críticas industriales
 - Buenas prácticas para el diagnóstico
 - Consecuencias de los riesgos tecnológicos en IACS.
- 2.2.1 Evaluando el riesgo
 - Medidas de protección
 - Medidas de Seguridad:
 - Encriptación de datos
 - Copias de seguridad
 - Gestor de contenidos

Contenidos prácticos:

- Identificación Sistemas de Control Industrial: Vulnerabilidades y Amenazas
 - Análisis de un Caso Práctico: identificación vulnerabilidades, contramedidas...
- Aspectos Organizacionales y de Gestión del Diagnóstico de la Ciberseguridad

Módulo 3

Denominación: Programa y Diseño de estrategias de Ciberseguridad Industrial

Objetivo: Conocer, diseñar e implementar un sistema de gestión de ciberseguridad industrial

Duración: 40 horas

Contenidos teórico prácticos:

- 3.1 Ámbitos de aplicación de un sistema de gestión de ciberseguridad Industrial
 - Estrategia de ciberseguridad nacional
 - Mapa de ruta de la ciberseguridad industrial en España
 - Esquema Nacional de Seguridad
- 3.2 Diseño y preparación de programas de ciberseguridad en sistemas de control industrial basado en análisis de riesgos y estándares
 - 3.2.1 Implementación de un sistema de gestión de ciberseguridad industrial
 - 3.2.2 Seleccionando y aplicando medidas de protección
 - 3.2.3- Aplicación de estrategias y técnicas de defensa para la protección de los sistemas de automatización industrial.
- 3.3 Hacking y estrategia de Defensa
 - 3.2.1 Técnicas y herramientas de hacking

Contenidos prácticos:

- Diagnóstico Estándares Aplicables: Recomendaciones
- Paso a paso del estableciendo un Programa de Ciberseguridad
- Construcción de un Sistema de Gestión de ciberseguridad industrial

Módulo 4

Denominación: Integración de la ciberseguridad industrial con el resto de tecnologías y disciplinas del ecosistema de la Industria 4.0.

Objetivo: Saber integrar el sistema de ciberseguridad industrial en el entorno de la Industria 4.0

Duración: 10 horas

Contenidos teórico prácticos:

- 4.1 Ecosistema Industria 4.0
 - 4.1.1 Riesgos de las tecnologías
- 4.2 Integración del Sistema de Ciberseguridad en el entorno Industria 4.0