PROGRAMA OFICIAL ISA / CIBERSEGURIDAD INDUSTRIAL

# IC34

2134 / IMPLEMENTACIÓN

## Diseño e implementación de ciberseguridad de los IACS

| CURSO | DURACIÓN | CEU | VERSIÓN |
|---|---|---|---|
| IC34 | 3 días | 2.1 | 3.02 |

La segunda fase del ciclo de vida de la ciberseguridad de los sistemas industriales (IACS), definido en ISA/IEC-62443-1-1, se centra en las actividades asociadas con el diseño y la implementación de contramedidas de ciberseguridad.

Diseño e implementación de ciberseguridad de sistemas de automatización y control industrial (IC34V) se enfoca en estas actividades para un IACS nuevo o existente, a fin de alcanzar el nivel de seguridad objetivo asignado a cada zona o conducto del IACS.

Esto incluye seleccionar las contramedidas adecuadas en función de su capacidad de nivel de seguridad y de la naturaleza de las amenazas y vulnerabilidades identificadas en la fase de evaluación. La fase también incluye pruebas de aceptación de ciberseguridad de la solución integrada para validar que las contramedidas estén correctamente implementadas, que el IACS haya alcanzado el nivel de seguridad objetivo y que se hayan satisfecho los objetivos de la especificación de requisitos de ciberseguridad.

## Programa de certificación

IC34 es el tercer curso del Programa de Certificación de Ciberseguridad ISA/IEC-62443. Al aprobar el examen se obtiene el certificado de Especialista en Diseño de Ciberseguridad ISA/IEC-62443. La inscripción al curso incluye la tarifa de un examen.

Al completar el curso con éxito, se proporcionará un certificado de finalización que indica el número total de CEU obtenidas.

## Requisitos previos obligatorios

Completar con éxito cualquier versión del curso Uso de las normas ISA/IEC-62443 para proteger sus sistemas de control (IC32) y aprobar el examen del certificado de Especialista en Fundamentos de Ciberseguridad ISA/IEC-62443 son requisitos previos obligatorios para este curso.

## Prerrequisito recomendado

Curso ISA Evaluación de la ciberseguridad de sistemas IACS nuevos o existentes (IC33), o conocimientos y experiencia equivalentes.

# Audiencia y objetivos

## ¿Quiénes deben tomar IC34?

- Ingenieros y gerentes de sistemas de control
- Integradores de sistemas
- Ingenieros y gerentes de TI en instalaciones industriales
- Gerentes de planta
- Personal de seguridad y gestión de riesgos de la planta

## Objetivos de aprendizaje

- Interpretar los resultados de una evaluación de riesgos de ciberseguridad de un sistema de control industrial (ICS).
- Desarrollar una especificación de requisitos de ciberseguridad (CRS).
- Desarrollar un diseño conceptual basado en la información de una CRS bien elaborada.
- Explicar el proceso y los entregables del ciclo de vida de desarrollo de seguridad (SLD).
- Realizar la configuración y puesta en marcha básicas de un firewall.
- Diseñar una solución de acceso remoto seguro.
- Desarrollar una especificación de endurecimiento del sistema.
- Implementar un sistema básico de detección de intrusiones en la red (IDS).
- Desarrollar un plan de pruebas de aceptación de ciberseguridad.
- Prueba de aceptación de ciberseguridad en fábrica (CFAT).
- Prueba de aceptación de ciberseguridad en sitio (CSAT).
- Realizar una CFAT o CSAT básica.

## Ejercicios de laboratorio

- Construcción del tablero
- Firewalls
- Definición de una política y un procedimiento para USB
- Endurecimiento de dispositivos de red
- Acceso remoto
- Uso de ISA/IEC-62443-3-3 para validar el nivel de seguridad alcanzado (SL-A)

# Temario completo

## 01 Introducción al ciclo de vida de la ciberseguridad de los ICS

- Fase de evaluación
- Fase de implementación
- Fase de mantenimiento
- Proceso de diseño conceptual

## 02 Interpretación de los resultados de la evaluación de riesgos

- Especificaciones de requisitos de ciberseguridad
- Desarrollo de un diseño conceptual
- Especificación del diseño conceptual
- Proceso de diseño detallado

## 03 Ciclo de vida de desarrollo de seguridad (SDL)

- Tipos de tecnología
- Selección de la tecnología adecuada
- Desarrollo de un diseño detallado
- Documentación del diseño y de la especificación
- Ejemplos de diseño e implementación

## 04 Ejemplo de diseño de firewall

- Ejemplo de diseño de acceso remoto
- Ejemplo de diseño de endurecimiento del sistema
- Ejemplo de diseño de detección de intrusiones
- Pruebas

## 05 Desarrollo de planes de pruebas

- Prueba de evaluación de ciberseguridad en fábrica (CFAT)
- Herramienta de evaluación de ciberseguridad (CSAT)

Nota terminológica: la página emplea denominaciones distintas para SLD/SDL y CFAT/CSAT en los objetivos y en el temario. Se conservan aquí las siglas y las denominaciones de cada apartado.

# Recursos y condiciones del curso

## Normas recomendadas

**ISA-62443-1-1-2007** - Seguridad para sistemas de automatización y control industrial - Parte 1-1: Terminología, conceptos y modelos.

**ISA-62443-2-1 (99.02.01)-2009** - Seguridad para sistemas de automatización y control industrial - Parte 2-1: Establecimiento de un programa de seguridad de sistemas de automatización y control industrial.

**ISA-62443-3-2-2020** - Seguridad para sistemas de automatización y control industrial - Parte 3-2: Evaluación de riesgos de seguridad para el diseño de sistemas.

**ISA-62443-3-3 (99.03.03)-2013** - Seguridad para sistemas de automatización y control industrial - Parte 3-3: Requisitos y niveles de seguridad del sistema.

## Lecturas recomendadas

- Biblioteca de ciberseguridad.
- Principios de seguridad de sistemas de control y automatización industrial, segunda edición, por Ronald L. Krutz, PhD, PE.

## Idioma de los materiales y de la evaluación

Para la audiencia de habla hispana (y portuguesa) el material de estudio se dispone en idioma inglés. La evaluación de certificación profesional se encuentra disponible únicamente en idioma inglés, al igual que la serie de normas ISA/IEC-62443. La traducción independiente de las normas no está aprobada ni autorizada por el Comité ISA99.

## Alcance de la formación ISA

Los principales objetivos de la formación ISA son asegurar que los participantes comprendan e interpreten correctamente los requisitos de la serie de normas ISA/IEC-62443 y lo que debe hacerse. Si bien los ejercicios y los productos utilizados en el laboratorio ayudan a comprender los conceptos, no está entre los objetivos de ISA recomendar una solución específica ni mostrar cómo cumplir los múltiples requisitos.

## Instructor

**Maximillian G. Kon**. Fundador, CEO y director general de WisePlant Group LLC. Ingeniero electrónico especializado en sistemas de control y telecomunicaciones. Consultor especializado en ciberseguridad y seguridad industrial. Instructor oficial de ISA, con más de 20 años de experiencia en sistemas industriales y sistemas críticos en todo tipo de industrias.

**Consulta los detalles del curso IC34**

WiseCourses.com/courses/2134ven302/