



CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS

FORMACIÓN PERMANENTE EN CIBERSEGURIDAD: CIBERSEGURIDAD INDUSTRIAL

Bloque I. Peculiaridades de los sistemas de control industrial desde el punto de vista de la seguridad

- Introducción y revisión de conceptos.
- Arquitecturas y tecnologías.

Bloque II. Amenazas y vulnerabilidades en sistemas de control industrial e infraestructuras críticas

- Amenazas.
- Vulnerabilidades.
- Impacto. Riesgo.

Bloque III. Iniciativas y estándares

- Legislación europea y española. Entidades relevantes y fuentes de recomendaciones e información.
- Estándares. IEC-62443.

Bloque IV. Revisión crítica de incidentes relevantes

- Incidentes.

Bloque V. Introducción a los procedimientos y medidas de seguridad en el ámbito de los sistemas de control industrial

- Políticas y procedimientos. Privilegios y autenticación.
- Medidas de seguridad física. Medidas de seguridad de los equipos
- Seguridad de red.

Bloque VI. Arquitectura de seguridad en profundidad

- Seguridad perimetral y segmentación.
- Modelo de zonas y conductos.

Bloque VII. Medidas y tecnologías en el ámbito de la ciberseguridad industrial

- Tecnologías.
- Seguridad de los equipos.
- Filtrado de protocolos.

- Detección de intrusiones.

Bloque VIII. Detección y respuesta ante incidentes en entornos industriales

- Supervisión de eventos de seguridad.
- Procedimiento de respuesta ante incidentes.