CVE-DOGC-B-24325035-2024

OTRAS DISPOSICIONES

DEPARTAMENTO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

RESOLUCIÓN EDF/4116/2024, de 19 de noviembre, por la que se establece el currículo del curso de especialización de Ciberseguridad en Entornos de las Tecnologías de Operación.

La ley orgánica 2/2006, de 3 de mayo, de educación, establece en el artículo 29.2, que los cursos de especialización forman parte de la formación profesional, en el artículo 42 que tienen carácter modular y cuya función es la de complementar o profundizar en las competencias de quienes ya dispongan de un título de formación profesional o cumplan las condiciones de acceso que para cada curso de especialización se determine.

El Real decreto 478/2020, de 7 de abril, ha establecido el Curso de especialización en Ciberseguridad en Entornos de las Tecnologías de Operación y ha fijado los aspectos básicos del currículum y mediante la Resolución EDU/1319/2022, de 29 de abril, se estableció el currículo del curso de especialización de Ciberseguridad en Entornos de las Tecnologías de Operación.

La Ley orgánica 3/2022, de 31 de marzo, de ordenación e integración de la formación profesional se ha desarrollado mediante el Real decreto 659/2023, de 18 de julio, por el que se desarrolla la ordenación del sistema de formación profesional, el cual establece en el Capítulo V del título II referido al grado E, la ordenación de los cursos de especialización.

El Real decreto 497/2024, de 21 de mayo, por el que se modifican determinados reales decretos por los que se establecen, en el ámbito de la Formación Profesional, cursos de especialización de grado medio y superior y se fijan las enseñanzas mínimas, para su adaptación al Real decreto 659/2023, de 18 de julio.

Por lo tanto, en concordancia con los cambios en la ordenación de los cursos de especialización y el nuevo régimen de aplicación, hay que establecer el currículo del curso de especialización de Ciberseguridad en Entornos de las Tecnologías de Operación.

Por todo ello,

Resuelvo:

-1 Establecer el currículo del curso de especialización de Ciberseguridad en Entornos de las Tecnologías de Operación, aplicable a partir del curso 2024-2025.

-2 Detallar, en el anexo 1, la identificación del curso de especialización.

-3 Detallar, en el anexo 2, el acceso al curso de especialización.

-4 Establecer, en el anexo 3, la relación de módulos profesionales que conforman el currículo del curso de especialización de Ciberseguridad en Entornos de las Tecnologías de Operación.

-5 El resto de elementos que definen este curso de especialización (perfil profesional, entorno profesional, prospectiva en el sector o sectores, objetivos generales, espacios y equipamientos y profesorado), son los establecidos en el Real decreto 478/2020, de 7 de abril y en el Real decreto 497/2024, de 21 de mayo.

CVE-DOGC-B-24325035-2024

-6 De acuerdo con lo previsto a la disposición adicional primera del Real decreto 478/2020, de 7 de abril, este curso de especialización no constituye una regulación del ejercicio de ninguna profesión regulada.

-7 A partir del 31 de agosto de 2024 se deja sin efecto la Resolución EDU/1319/2022, de 29 de abril.

Contra esta Resolución, que pone fin a la vía administrativa, las personas interesadas pueden interponer recurso contencioso administrativo ante la Sala contenciosa administrativa del Tribunal Superior de Justicia de Cataluña, en el plazo de dos meses a contar desde el día siguiente de su publicación en el Diari Oficial de la Generalitat de Catalunya, de conformidad con lo previsto en el artículo 46.1 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contenciosa administrativa. También puede interponer cualquier otro recurso que considere conveniente para la defensa de sus intereses.

Asimismo, previo al recurso contencioso administrativo, pueden interponer recurso de reposición ante la consejera de Educación y Formación Profesional, en el plazo de un mes a contar del día siguiente de su publicación en el DOGC, según lo dispuesto en el artículo 77 de la Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña y los artículos 123 y 124 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, o cualquier otro recurso que consideren conveniente para la defensa de sus intereses.

Barcelona, 19 de noviembre de 2024

Esther Niubó Cidoncha

Consejera de Educación y Formación Profesional

Anexo 1

Identificación

El curso de especialización en Ciberseguridad en Entornos de las Tecnologías de Operación queda identificado por los siguientes elementos:

Denominación: Ciberseguridad en Entornos de las Tecnologías de Operación.

Nivel: Formación Profesional de Grado Superior.

Duración: 720 horas.

Familia Profesional: Electricidad y electrónica (únicamente a efectos de clasificación de las enseñanzas de formación profesional).

Ramas de conocimiento: Ingeniería y Arquitectura

Créditos ECTS: 43.

Referente en la Clasificación Internacional Normalizada de la Educación: P-5.5.4.

El título de Máster se corresponde con un nivel 5C del Marc Espanyol de Calificaciones para el Aprendizaje Permanente.

Anexo 2

Acceso al curso de especialización

CVE-DOGC-B-24325035-2024

1. Los títulos que dan acceso a este curso de especialización son los siguientes:

Título de Técnico o Técnica Superior en Sistemas Electrotécnicos y Automatizados, establecido por el Real decreto 1127/2010, de 10 de septiembre.

Título de Técnico o Técnica Superior en Mecatrónica Industrial, establecido por Real decreto 1576/2011, de 4 de noviembre.

Título de Técnico o Técnica Superior en Automatización y Robótica Industrial, establecido por el Real decreto 1581/2011, de 4 de noviembre.

Título de Técnico o Técnica Superior en Sistemas de Telecomunicaciones e Informáticos, establecido por Real decreto 883/2011, de 24 de junio.

Título de Técnico o Técnica Superior en Mantenimiento Electrónico, establecido por Real decreto 1578/2011, de 4 de noviembre.

2. En caso de disponibilidad de plazas podrán acceder al curso de especialización las personas a que no tengan las titulaciones requeridas, siempre que cumplan los requisitos siguientes, que se enumeran por orden de preferencia:

a) Tener un título de técnico superior de formación profesional diferente de los que dan acceso y acreditar experiencia en el área profesional asociada al curso de especialización.

b) Tener un título de técnico superior de formación profesional diferente de los que dan acceso y acreditar tener conocimientos previos adecuados.

c) Acreditar tener conocimientos previos o experiencia laboral en el área profesional asociada al curso de especialización, a pesar de no tener un título de técnico superior de formación profesional.

Anexo 3

1. Relación de módulos profesionales.

5027. Ciberseguridad en Proyectos Industriales

Horas lectivas: 99 horas

Horas de estancia en la empresa: ninguna

Duración total: 99 horas

Equivalencia en créditos ECTS: 6

5028. Sistemas de Control Industrial Seguros

Horas lectivas: 99 horas

Horas de estancia en la empresa: ninguna

Duración total: 99 horas

Equivalencia en créditos ECTS: 7

5029. Redes de Comunicaciones Industriales Seguras

Horas lectivas: 132 horas

CVE-DOGC-B-24325035-2024

Horas de estancia en la empresa: ninguna

Duración total: 132 horas

Equivalencia en créditos ECTS: 9

5030. Análisis Forense en Ciberseguridad Industrial

Horas lectivas: 132 horas

Horas de estancia en la empresa: ninguna

Duración total: 132 horas

Equivalencia en créditos ECTS: 11

5031. Seguridad Integral

Horas lectivas: 132 horas

Horas de estancia en la empresa: ninguna

Duración total: 132 horas

Equivalencia en créditos ECTS: 10

C080. Proyecto de Ciberseguridad en Entornos de las Tecnologías de Operación

Horas lectivas: 126 horas

Horas de estancia en la empresa: ninguna

Duración total: 126 horas

2. Descripción de los módulos profesionales y de las unidades formativas

5027. Ciberseguridad en Proyectos Industriales

Horas lectivas: 99 horas

Horas de estancia en la empresa: ninguna

Duración total: 99 horas

Equivalencia en créditos ECTS: 6

Resultados de aprendizaje y criterios de evaluación

1. Determina los elementos de ciberseguridad a incluir en el diseño de un proyecto industrial analizando la seguridad ya implantada en la organización.

Criterios de evaluación

1.1 Evalúa el diseño del proyecto industrial: alcance, estudios de viabilidad financiera y requisitos técnicos, organizativos y procedimentales.

1.2 Identifica los actores y responsables involucrados en el proyecto, así como sus funciones y competencias en materia de ciberseguridad.

CVE-DOGC-B-24325035-2024

1.3 Caracteriza las amenazas e identifica las vulnerabilidades de los componentes de las tecnologías de automatización del proyecto.

1.4 Desarrolla los estudios que contemplen la ciberseguridad desde los diferentes actores involucrados (cliente, ingeniería y fabricantes).

1.5 Define requisitos de ciberseguridad para los niveles de automatización del proyecto, así como sus flujos e interacciones.

2. Establece planes de gestión de compras determinando los requisitos de ciberseguridad a cumplir por los proveedores.

Criterios de evaluación

2.1 Establece el proceso de gestión de compras a los proveedores.

2.2 Implementa los documentos básicos del proceso de gestión de compras.

2.3 Realiza el análisis y gestión de los riesgos asociados a la cadena de suministro.

2.4 Establece los requisitos de ciberseguridad en el proceso de gestión de compras.

3. Establece las medidas de ciberseguridad en la ejecución y puesta en marcha de un proyecto industrial cumpliendo con los requisitos de calidad exigidos.

Criterios de evaluación

3.1 Realiza un análisis de funciones y responsabilidades de ciberseguridad en la ejecución y puesta en marcha del proyecto.

3.2 Realiza un análisis preliminar de impacto para identificar medidas de ciberseguridad.

3.3 Establece el plan detallado de medidas de ciberseguridad.

3.4 Tiene en cuenta los principios de economía circular.

3.5 Incorpora criterios de ciberseguridad en las pruebas de aceptación en fábrica (FAT).

3.6 Incorpora criterios de seguridad en las pruebas de aceptación.

3.7 Establece los planes de control de calidad y las auditorías.

3.8 Contempla la evaluación de ciberseguridad.

4. Implementa las actividades de ciberseguridad de la fase de operación y mantenimiento de un proyecto industrial documentando las actividades realizadas.

Criterios de evaluación

4.1 Identifica mejoras de ciberseguridad sobre la instalación.

4.2 Implementa mejoras de ciberseguridad sobre la instalación.

4.3 Implanta un proceso de gestión de cambio para introducir las mejoras operacionales que puedan afectar a la gestión de la ciberseguridad.

4.4 Implementa actividades de ciberseguridad correspondientes a la fase de operación.

4.5 Implementa actividades de ciberseguridad correspondientes a la fase de mantenimiento.

4.6 Documenta los procedimientos de ciberseguridad para la fase de operación y mantenimiento de un proyecto industrial.

4.7 Implementa planes de concienciación y formación de ciberseguridad.

CVE-DOGC-B-24325035-2024

5. Implementa las actividades de ciberseguridad en el desmantelamiento de las instalaciones cumpliendo con los requisitos establecidos en destrucción y/o conservación de los sistemas de una manera segura.

Criterios de evaluación

5.1 Define las actividades de ciberseguridad en el desmontaje, descontaminación, desclasificación, demolición y reposición de las instalaciones del proyecto.

5.2 Implementa las medidas de destrucción de los sistemas.

5.3 Verifica las medidas de destrucción de los sistemas.

5.4 Implementa las medidas de conservación de los sistemas.

5.5 Verifica las medidas de conservación de los sistemas.

5.6 Documenta las incidencias detectadas en el proceso de verificación.

Contenidos (orientativos)

1. Actividades de ciberseguridad en el diseño de un proyecto industrial:

1.1 Diseño conceptual del proyecto.

1.2 Diseño preliminar del proyecto-estudio de viabilidad.

1.3 Ingeniería básica o plan detallado del proyecto.

1.4 Ingeniería de detalle o definición de las tecnologías a utilizar por cada nivel de automatización y su interacción entre ellas.

1.5 Actividades de ciberseguridad en la fase de diseño.

2. Requisitos de ciberseguridad en el proceso de gestión de compras:

2.1 Establecimiento del proceso de gestión de compras y elaboración de los documentos básicos del mismo.

2.2 Análisis y gestión de riesgos en la cadena de suministro.

2.3 Implementación de las medidas de ciberseguridad "extremo a extremo".

3. Medidas de ciberseguridad en la ejecución y puesta en marcha del proyecto industrial:

3.1 Construcción del proyecto.

3.2 Principios de la economía circular en la industria 4.0.

3.3 Incorporación de las actividades de soporte a la construcción.

3.4 Ejecución del plan detallado de seguridad física y lógica.

3.5 Actualización de la documentación de ingeniería.

3.6 Mediciones en las instalaciones.

3.7 Compleción de la construcción de los sistemas.

3.8 Ejecutar los planes de control de calidad y las auditorías.

4. Actividades de ciberseguridad en la fase de operación y mantenimiento de un proyecto industrial:

4.1 Periodo de optimización y seguimiento inicial de la operación.

4.2 Proceso de gestión de cambio.

CVE-DOGC-B-24325035-2024

4.3 Actividades de seguridad correspondientes a la fase de operación y mantenimiento.

5. Actividades de ciberseguridad en el desmantelamiento de las instalaciones:

5.1 Actividades de desmontaje, descontaminación, desclasificación, demolición y reposición.

5.2 Gestión de la destrucción de los sistemas desde el punto de vista de la ciberseguridad.

5.3 Gestión de la conservación desde el punto de vista de la ciberseguridad.

5028. Sistemas de Control Industrial Seguros

Horas lectivas: 99 horas

Horas de estancia en la empresa: ninguna

Duración total: 99 horas

Equivalencia en créditos ECTS: 7

Resultados de aprendizaje y criterios de evaluación

1. Determina los cambios para la convergencia de las tecnologías IT (Tecnologías de la información) y OT (Tecnologías de la operación) analizando la situación de dichos entornos en organizaciones.

Criterios de evaluación

1.1 Caracteriza los procesos de transformación digital en la industria.

1.2 Analiza y diferencia los conceptos de tecnologías de la información (IT), y las tecnologías de la operación (OT).

1.3 Detecta las necesidades tecnológicas en los entornos IT y OT.

1.4 Identifica tecnologías avanzadas de aplicación.

1.5 Identifica los retos que comporta para los departamentos de IT y OT en lo relativo al trabajo con las tecnologías avanzadas.

1.6 Realiza un análisis de convergencia a nivel de prácticas de trabajo, organización y compartición de datos con IT.

1.7 Determina los cambios relevantes que exigirán una alta profesionalización, visión de futuro, liderazgo y eficiencia.

2. Evalúa escenarios de riesgo tecnológico en sistemas de control de instalaciones industriales aplicando metodologías reconocidas.

Criterios de evaluación

2.1 Identifica los diferentes tipos de activos que componen una instalación industrial.

2.2 Caracteriza diferentes tipos de amenazas para los diferentes activos.

2.3 Localiza datos de interés sobre vulnerabilidades conocidas en sistemas de control industrial.

2.4 Compara diferentes herramientas de diagnóstico.

2.5 Identifica y evalúa la seguridad de credenciales y los medios de control de acceso.

2.6 Evalúa el *firmware* y/o configuración de un dispositivo mediante procedimientos de ingeniería inversa.

CVE-DOGC-B-24325035-2024

2.7 Automatiza acciones de verificación de la configuración de dispositivos y sistemas.

2.8 Crea un *testbed* gemelo de un sistema de control industrial significativo imitando su configuración.

2.9 Elabora y ordena una lista de riesgos asociados a los sistemas de control de una instalación industrial.

3. Documenta los procesos de diagnósticos, análisis y otros relativos a sistemas de una instalación industrial en relación con la ciberseguridad, generando informes de distintos niveles de complejidad.

Criterios de evaluación

3.1 Identifica los elementos de los informes dirigidos a personal técnico y directivo, estableciendo las diferencias.

3.2 Elabora un informe técnico de diagnóstico de ciberseguridad destinado a personal directivo.

3.3 Elabora un informe técnico de diagnóstico de ciberseguridad destinado a personal técnico de operación.

3.4 Identifica los instrumentos, herramientas y técnicas de comunicación del informe técnico de acuerdo con el destinatario.

3.5 Desarrolla las formas de gestionar conflictos y reticencias a la hora de presentar informes de resultados.

3.6 Analiza los informes técnicos de diagnóstico para obtener propuestas de mejora.

4. Diseña políticas de seguridad para sistemas de control industrial teniendo en cuenta los análisis realizados, estándares del sector y la normativa de aplicación.

Criterios de evaluación

4.1 Identifica diferentes mecanismos de autenticación de personas, dispositivos y sistemas.

4.2 Identifica los procedimientos necesarios en cuanto al alta, mantenimiento y baja de credenciales de acceso.

4.3 Realiza procesos de gestión de usuarios de una instalación industrial siguiendo las políticas de una organización.

4.4 Elabora y justifica políticas de seguridad física y control de acceso a las diferentes zonas de una instalación industrial.

5. Configura sistemas de control industrial minimizando los posibles escenarios de riesgo.

Criterios de evaluación

5.1 Identifica los requisitos de seguridad para la actualización y el parcheado de los sistemas de control industrial.

5.2 Identifica los requisitos de seguridad para la gestión de antivirus de los sistemas de control industrial basados en PC's.

5.3 Identifica los requisitos de seguridad para las copias de seguridad de las configuraciones e información de los sistemas de control industrial.

5.4 Configura y parametriza los sistemas de control industrial de acuerdo con los requisitos de protección establecidos.

5.5 Configura y parametriza los sistemas de control industrial de acuerdo con los controles de auditoría establecidos.

6. Detecta anomalías en sistemas de control industrial utilizando herramientas de monitorización y procedimientos de análisis.

Criterios de evaluación

CVE-DOGC-B-24325035-2024

6.1 Identifica y caracteriza herramientas de monitorización de eventos de seguridad.

6.2 Configura las herramientas de monitorización para el descubrimiento automático de sistemas de control industrial conectados.

6.3 Define las reglas de actuación sobre las herramientas de monitorización para establecer los eventos a monitorizar.

6.4 Identifica los principios fundamentales de comportamiento de un gestor de eventos de seguridad (SIEM, *Security Information* and *Event Management*).

6.5 Detecta comportamientos sospechosos.

6.7 Documenta las anomalías opuestas.

Contenidos (orientativos)

1. Cambios para la convergencia de las tecnologías IT y OT:

1.1 Tecnologías de la operación (OT), detectar y/o cambiar los procesos físicos a través de la monitorización y el control de dispositivos.

1.2 Tecnologías de la información (IT, equipos informáticos para tratar datos).

1.3 Cambios relevantes en entornos IT y OT para favorecer la convergencia.

2. Evaluación de escenarios de riesgo tecnológico:

2.1 Tipos de sistemas de control industrial.

2.2 Amenaza y tipos de amenaza.

2.3 Evaluación del riesgo.

2.4 Riesgos externos.

2.5 Tipos de credenciales y sistemas de control de acceso.

2.6 Búsqueda de información sobre vulnerabilidades conocidas en sistemas de control industrial.

2.7 Herramientas de diagnóstico.

2.8 Creación de *testbeds* gemelos.

3. Documentación de los procesos en ciberseguridad:

3.1 Elaboración de informes técnicos.

3.2 Adaptación del lenguaje al receptor del informe.

3.3. Presentación de resultados.

4. Diseño de políticas de seguridad:

4.1 Identificación de personas, dispositivos y sistemas.

4.2 Gestión de roles, usuarios y permisos.

4.3 Políticas de seguridad física y de control de acceso.

5. Configuración de sistemas de control industrial:

CVE-DOGC-B-24325035-2024

5.1 Configuración de usuarios y/o direcciones IP habilitadas a controlar los sistemas.

5.2 Envío de registros (*Logs*), a sistemas externos.

5.3 Gestión de actualizaciones de los sistemas.

5.4 Copias de seguridad de una configuración deseada y su custodia.

6. Detección de anomalías en sistemas de control industrial:

6.1 Monitorización de sistemas de control industrial.

6.2 Herramientas de monitorización de eventos de seguridad.

6.3 Herramientas de descubrimiento automático de activos.

6.4 Reglas de actuación e inspección basadas en firmas.

5029. Redes de Comunicaciones Industriales Seguras

Horas lectivas: 132 horas

Horas de estancia en la empresa: ninguna

Duración total: 132 horas

Equivalencia en créditos ECTS: 9

Resultados de aprendizaje y criterios de evaluación

1. Determina los niveles de seguridad en un entorno industrial automatizado analizando las características de los protocolos y comunicaciones utilizados y proponiendo soluciones a nuevos requerimientos de seguridad.

Criterios de evaluación

1.1 Caracteriza dispositivos de control en un entorno de automatización industrial.

1.2 Describe los diferentes elementos de supervisión y sistemas SCADA.

1.3 Identifica los diferentes sistemas de optimización y gestión.

1.4 Especifica los niveles de seguridad en los diferentes campos de automatización industrial (campo, control, supervisión, optimización y gestión).

1.5 Establece las diferencias entre el sistema analizado y el sistema futuro en términos de seguridad.

1.6 Documenta las propuestas de adaptación en términos de seguridad de acuerdo con los nuevos requerimientos.

2. Evalúa escenarios de riesgo tecnológico en redes industriales aplicando metodologías reconocidas.

Criterios de evaluación

2.1 Identifica los diferentes tipos de dispositivos que componen la red de una instalación industrial.

2.2 Caracteriza la arquitectura de red física y lógica de una instalación industrial.

2.3 Identifica las diferentes zonas de seguridad que deberían existir en la red de una instalación industrial.

2.4 Clasifica los riesgos asociados a la red de una instalación industrial.

2.5 Evalúa el nivel de riesgo asociado a la red de una instalación industrial.

CVE-DOGC-B-24325035-2024

3. Implementa redes industriales aplicando técnicas de *switching* y de enrutamiento.

Criterios de evaluación

3.1 Caracteriza el *switching* en redes industriales.

3.2 Implementa topologías en *Ethernet* industrial.

3.3 Implementa topologías en anillo.

3.4 Implementa acoplamientos de segmentos entre anillos de forma redundante.

3.5 Interconecta redes OT a redes IT.

3.6 Examina el tráfico de red con los analizadores de red.

3.7 Caracteriza el enrutamiento en las redes industriales.

3.8 Implementa conexiones simples con redes ofimáticas.

3.9 Implementa conexiones redundantes con redes ofimáticas

3.10 Implementa conexiones a redes *legacy*.

3.11 Implementa conexiones a redes con detección automática de camino.

3.12 Implementa restricciones de enrutado por medio de *ACL's*.

4. Implementa redes industriales inalámbricas aplicando los estándares del sector.

Criterios de evaluación

4.1 Caracteriza las tecnologías inalámbricas.

4.2 Implementa métodos de acceso y organización de las células.

4.3 Implementa *roaming*.

4.4 Identifica la localización de los puntos de acceso.

4.5 Selecciona las antenas.

4.6 Diseña redes *wifi* para instalaciones industriales.

4.7 Implementa redes *wifi* para instalaciones industriales.

5. Implementa accesos remotos en entornos industriales garantizando la seguridad de las comunicaciones.

Criterios de evaluación

5.1 Caracteriza las comunicaciones remotas más utilizadas.

5.2 Implementa comunicaciones seguras a través de comunicaciones no seguras.

5.3 Conecta redes privadas industriales a redes públicas aplicando diferentes tecnologías.

5.4 Implementa accesos remotos en base al principio de mínima superficie.

6. Diseña la red de automatización aplicando la segmentación necesaria en las redes de la organización.

Criterios de evaluación

6.1 Implementa la segmentación en redes de automatización.

6.2 Implementa *VLAN's* (red de área local virtual) para la estructuración de las redes.

CVE-DOGC-B-24325035-2024

6.3 Asigna equipos en *VLAN's* estáticas y dinámicas

6.4 Prioriza *VLAN's*.

6.5 Realiza segmentaciones de células de automatización mediante cortafuegos industriales.

6.6 Realiza segmentaciones entre IT y OT mediante *NGF* (*Next Generation Firewall*).

7. Identifica vulnerabilidades en dispositivos de redes industriales proponiendo contramedidas.

Criterios de evaluación

7.1 Identifica vulnerabilidades conocidas en dispositivos y redes industriales.

7.2 Valora el alcance de las vulnerabilidades.

7.3 Caracteriza diferentes herramientas de diagnóstico.

7.4 Relaciona las herramientas de diagnóstico con su aplicación a las diversas situaciones.

7.5 Automatiza acciones de verificación de la configuración de dispositivos y redes.

7.6 Crea un *testbed* gemelo de un segmento significativo de una red industrial imitando la configuración tanto de los dispositivos como de la red.

7.7 Realiza tests de penetración exhaustivos en un *testbed* gemelo de una instalación industrial.

8. Detecta incidentes en tiempo real en redes industriales aplicando procedimientos de análisis y utilizando las herramientas adecuadas.

Criterios de evaluación

8.1 Caracteriza diferentes herramientas de análisis de tráfico en entornos industriales.

8.2 Selecciona las herramientas en función de sus prestaciones.

8.3 Diseña y configura un sistema de detección de intrusiones (*IDS*, *Intrusion Detection System*) para sistemas de control industrial.

8.4 Detecta e investiga comportamientos sospechosos en una infraestructura mediante el análisis del tráfico de red.

8.5 Documenta los comportamientos anómalos observados.

9. Define procedimientos de verificación y supervisión obteniendo métricas de cumplimiento de las políticas de seguridad.

Criterios de evaluación

9.1 Identifica métricas de cumplimiento de políticas de seguridad.

9.2 Analiza diferentes registros de sistemas de control industrial para detectar cambios no autorizados en las políticas de seguridad.

9.3 Caracteriza diferentes herramientas de monitorización de redes de automatización industrial.

9.4 Instala herramientas de monitorización de red.

10. Configura dispositivos de redes industriales minimizando los posibles escenarios de riesgo.

Criterios de evaluación

10.1 Define los parámetros de protección de los dispositivos.

10.2 Configura dispositivos de red para poder ser auditados a posteriori.

CVE-DOGC-B-24325035-2024

10.3 Identifica los requisitos de seguridad para las actualizaciones del firmware de los dispositivos de red.

10.4 Identifica los requisitos de seguridad para las copias de seguridad de las configuraciones de los dispositivos de red.

10.5 Configura los dispositivos de red acorde a los parámetros de protección definidos.

Contenidos (orientativos)

1. Niveles de seguridad en un entorno industrial automatizado:

1.1 Niveles de automatización industrial.

1.2 Dispositivos de control y supervisión disponibles en el mercado.

1.3 Opciones de comunicaciones y protocolos industriales avanzados existentes en el mercado.

1.4 Comunicación *OPC UA* que permite la comunicación de equipos y sistemas industriales para la recolección y control de datos.

2. Evaluación de escenarios de riesgo tecnológico en redes industriales:

2.1 Tipo de dispositivos de una red industrial.

2.2 Arquitectura de red física y lógica.

2.3 Zonificación (red de control, de supervisión, corporativa, etc.).

2.4 Evaluación del riesgo.

2.5 Riesgos externos.

3. Implementación de redes industriales aplicando técnicas de *switching* y de enrutamiento:

3.1 Analizar la técnica de *switching* en redes industriales.

3.2 *LAN, MAN, WAN, GAN*.

3.3 Topologías típicas en *Ethernet* Industrial.

3.4 Topologías en anillo con *HRP Hihg-Speep Redundancy Protocol*.

3.5 Acoplamiento de segmentos entre anillos de forma redundante.

3.6 *RSTP* (*Rapid Spanning Tree Protocol*).

3.7 Conexiones redundantes entre *RSTP* y anillos.

3.7.1 Acoplamiento entre segmentos de automatización y redes IT.

3.8 Topologías con *PRP* (*Parallel Redundancy Protocol*) y *HSR* (*High-Availability Seamless Redundancy Protocol*).

3.9 Enrutamiento en redes industriales.

3.10 Conexiones simples con redes ofimáticas.

3.11 Las tablas de enrutamiento.

3.12 Conexiones redundantes con redes ofimáticas mediante *VRRP* (*Virtual Router Redundancy Protocol*).

3.13 Conexiones a redes *legacy* mediante *RIP* (*Routing Information Protocol*).

4. Implementación de redes industriales inalámbricas:

CVE-DOGC-B-24325035-2024

4.1 Tecnologías de *Wireless* (*WIMAX, IWLAN, Bluetooth, WirelessHart*).

4.2 Estándar *WLAN*.

4.3 Métodos de acceso y organización de las células.

4.4 *Roaming*.

4.5 Seguridad (*TKIP y WPA2*) y tasas de transmisión.

4.6 Encriptación.

4.7 *WDS* (*Wireless Distribution System*).

4.8 Diferencia entre *PCF* (*Point Coordinated Function*) frente a *DCF* (*Distributed Coordination Function*).

4.9 Comunicaciones *Wifi* en tiempo real – determinismo en *Wifi* (*iPCF*).

5. Implementación de accesos remotos seguros en entornos industriales:

5.1 Comunicaciones remotas (*LAN, WAN, MAN y GAN*).

5.2 Comunicaciones seguras vía redes no seguras (*VPN*).

5.3 *IPsec VPN* y *OpenVPN*.

5.4 Interconexión de redes privadas industriales a redes públicas: *NAT* (*Network Address Translation*).

5.5 Principio de mínima superficie de ataque a la hora de implementar accesos remotos.

6. Diseño de la red de automatización mediante segmentación:

6.1 Segmentación en las redes de automatización.

6.2 Estructuración de redes con *VLAN's*: estáticas y dinámicas.

6.3 Segmentación de célula con cortafuegos industriales.

6.4 Segmentación entre entornos IT y OT con *NGF* (*Next Generation Firewall*).

7. Identificación de vulnerabilidades en dispositivos de redes industriales:

7.1 Búsqueda de información sobre vulnerabilidades conocidas en dispositivos de redes industriales.

7.2 Herramientas de diagnóstico.

7.3 Creación de *testbeds* gemelos.

7.4 Test de penetración no intrusivos que garantizan la continuidad del proceso productivo.

8. Detección de incidentes en tiempo real en redes industriales:

8.1 Análisis de tráfico.

8.2 Sistemas de detección de intrusiones (*IDS, IPS*).

9. Definición de procedimientos de verificación y supervisión:

9.1 Métricas de cumplimiento de políticas.

9.2 Gestión de registros (*Logs*).

9.3 Monitorización de redes.

CVE-DOGC-B-24325035-2024

10. Configuración de dispositivos de redes industriales:

10.1 Configuración de usuarios y/o direcciones *IP* habilitadas a controlar los dispositivos.

10.2 Gestión de actualizaciones del firmware de los dispositivos.

10.3 Copias de seguridad de una configuración deseada y su custodia.

5030. Análisis Forense en Ciberseguridad Industrial

Horas lectivas: 132 horas

Horas de estancia en la empresa: ninguna

Duración total: 132 horas

Equivalencia en créditos ECTS: 11

Resultados de aprendizaje y criterios de evaluación

1. Desarrolla procesos de análisis forense en sistemas de control industrial aplicando metodologías reconocidas.

Criterios de evaluación

1.1 Identifica los dispositivos a analizar para garantizar la preservación de evidencias.

1.2 Utiliza mecanismos y herramientas adecuadas para la adquisición y extracción de las evidencias.

1.3 Realiza análisis de las evidencias de forma manual.

1.4 Realiza análisis de las evidencias mediante herramientas automáticas para dar respuesta a la investigación forense.

1.5 Documenta el proceso de análisis realizado de forma metódica y detallada para garantizar la reproducción de todos los pasos.

1.6 Considera la línea temporal de las evidencias, el mantenimiento de la cadena de custodia y la elaboración de conclusiones a nivel técnico y ejecutivo.

1.7 Comunica las conclusiones del análisis forense realizado a los interlocutores pertinentes.

2. Desarrolla el proceso de análisis forense en sistemas de control y controladores lógicos programables aplicando metodologías reconocidas.

Criterios de evaluación

2.1 Identifica los sistemas de control de supervisión y adquisición de datos (SCADA), sistemas de control distribuido (DCS) y controladores lógicos programables (PLC) a analizar para garantizar la preservación de las evidencias.

2.2 Emplea mecanismos y herramientas adecuadas para la adquisición y extracción de evidencias que garanticen su autenticidad, compleción, fiabilidad y legalidad.

2.3 Analiza las evidencias de forma manual y mediante herramientas automáticas para dar respuesta a investigaciones forenses.

2.4 Documenta el proceso de análisis realizado para garantizar la reproducción de todos los pasos.

2.5 Considera la línea temporal de las evidencias, el mantenimiento de la cadena de custodia y la elaboración de conclusiones a nivel técnico y ejecutivo.

CVE-DOGC-B-24325035-2024

2.6 Comunica formalmente las conclusiones del análisis forense realizado a los interlocutores pertinentes.

3. Desarrolla el proceso de análisis forense en robótica industrial aplicando metodologías reconocidas.

Criterios de evaluación

3.1 Identifica los dispositivos industriales a analizar para garantizar la preservación de las evidencias.

3.2 Utiliza los mecanismos y herramientas necesarios para la adquisición y extracción de evidencias adecuadas que garantizan su autenticidad, completitud, fiabilidad y legalidad.

3.3 Realiza análisis de evidencias de forma manual y mediante herramientas automáticas para dar respuesta a investigaciones forenses.

3.4 Documenta el proceso de análisis realizado de manera metódica y detallada para garantizar la reproducción de todos los pasos.

3.5 Considera la línea temporal de las evidencias, el mantenimiento de la cadena de custodia y la elaboración de conclusiones a nivel técnico y ejecutivo.

3.6 Comunica formalmente las conclusiones del análisis forense realizado a los interlocutores pertinentes.

4. Desarrolla el proceso de análisis forense en dispositivos del Internet de las cosas (IoT), de sectores industriales y otros como los de transporte, salud, construcción etc., aplicando metodologías reconocidas.

Criterios de evaluación

4.1 Identifica los dispositivos a analizar para garantizar la preservación de las evidencias.

4.2 Utiliza los mecanismos y herramientas necesarios para la adquisición y extracción de evidencias adecuadas que garanticen su autenticidad, completitud, fiabilidad y legalidad.

4.3 Realiza análisis de evidencias de manera manual y mediante herramientas automáticas para permitir dar respuesta a investigaciones forenses.

4.4 Documenta el proceso de análisis para garantizar la reproducción de todos los pasos.

4.5 Se considera la línea temporal de las evidencias, el mantenimiento de la cadena de custodia y la elaboración de conclusiones a nivel técnico y ejecutivo.

4.6 Comunica formalmente las conclusiones del análisis forense realizado a los interlocutores pertinentes.

5. Responde ante un incidente de ciberseguridad que afecta a la organización tomando las medidas necesarias.

Criterios de evaluación

5.1 Desarrolla procedimientos de actuación para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales en sistemas de control industrial.

5.2 Prepara respuestas ciberresilientes para intervenir inmediatamente ante incidentes de ciberseguridad que permitan seguir prestando los servicios de la organización.

5.3 Establece un flujo de toma de decisiones y escalado interno y/o externo adecuados al incidente.

5.4 Lleva a cabo las tareas de restablecimiento de los servicios afectados por el incidente, hasta confirmar la vuelta a la normalidad.

5.5 Documenta las acciones realizadas incluyendo las conclusiones que permitan mantener un registro de lecciones aprendidas.

5.6 Notifica el incidente formalmente a todos los involucrados o afectados: clientes, proveedores, personal interno, medios de comunicación y autoridades competentes en los tiempos adecuados.

5.7 Realiza un adecuado seguimiento del incidente para evitar que una situación similar se repita.

CVE-DOGC-B-24325035-2024

Contenidos (orientativos)

1. Proceso de análisis forense en sistemas de control industrial:

1.1 Principio de Locard.

1.2 Tipos de análisis forenses.

1.3 Cadena de custodia.

1.4 Funciones *Hash*.

1.5 Sistemas de ocultación.

1.6 Volcado de memoria.

1.7 Extracción de evidencias volátiles, no volátiles y en tránsito.

1.8 Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas manuales.

1.9 Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas automatizadas.

1.10 Borrado seguro de soportes.

2. Proceso de análisis forense en sistemas de control y controladores lógicos programables:

2.1 Funciones Hash en sistemas.

2.2 Sistemas de ocultación en sistemas.

2.3 Extracción de evidencias volátiles, no volátiles y en tránsito en sistemas.

2.4 Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas manuales en sistemas.

2.5 Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas automatizadas en sistemas.

2.6 Borrado seguro de sistemas.

3. Desarrollo del proceso de análisis forense en robótica industrial:

3.1 Funciones *Hash* en dispositivos industriales.

3.2 Sistemas de ocultación en dispositivos industriales.

3.3 Extracción de evidencias volátiles, no volátiles y en tránsito en dispositivos industriales.

3.4 Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas manuales en dispositivos industriales.

3.5 Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas automatizadas en dispositivos industriales.

3.6 Borrado seguro en dispositivos industriales.

4. Proceso de análisis forense en dispositivos del Internet de las cosas (IoT), de sectores industriales y otros:

4.1 Funciones *Hash* en dispositivos.

4.2 Sistemas de ocultación de dispositivos.

4.3 Extracción de evidencias volátiles, no volátiles y en tránsito en dispositivos.

4.4 Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas manuales en dispositivos.

4.5 Análisis de evidencias volátiles, no volátiles y en tránsito con herramientas automatizadas en dispositivos.

CVE-DOGC-B-24325035-2024

4.6 Borrado seguro en dispositivos.

5. Respuesta ante un incidente de ciberseguridad:

5.1 Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes.

5.2 Implantar capacidades de ciberresiliencia.

5.3 Tareas de restablecimiento de los servicios afectados por incidentes.

5.4 Documentación y lecciones aprendidas.

5.5 Notificación del incidente.

5.6 Seguimiento del incidente.

5031. Seguridad Integral

Horas lectivas: 132 horas

Horas de estancia en la empresa: ninguna

Duración total: 132 horas

Equivalencia en créditos ECTS: 10

Resultados de aprendizaje y criterios de evaluación

1. Integra las normas y procedimientos de seguridad física en la ciberseguridad en entornos OT identificando los posibles riesgos.

Criterios de evaluación

1.1 Caracteriza el riesgo y la seguridad físicos.

1.2 Describe los fundamentos y herramientas básicas de un esquema de seguridad física.

1.3 Define los conceptos básicos de normas de seguridad física para entornos OT.

1.4 Caracteriza las normas de seguridad física aplicables en función de la actividad a desarrollar.

1.5 Determina los procedimientos de seguridad física en entornos OT que son de aplicación conforme a las normas aplicables.

1.6 Implementa los procedimientos de seguridad física determinados.

1.7 Comprueba que la integración de las normas y procedimientos de seguridad física cumplen con los requisitos de ciberseguridad.

2. Integra las normas y procedimientos de seguridad operacional en la ciberseguridad en entornos OT identificando los posibles riesgos.

Criterios de evaluación

2.1 Caracteriza el riesgo y la seguridad operacionales.

2.2 Describe los fundamentos y herramientas básicas de un esquema de seguridad operacional.

2.3 Define los conceptos básicos de normas de seguridad operacional.

CVE-DOGC-B-24325035-2024

2.4 Caracteriza las normas de seguridad operacional aplicables en función de la actividad a desarrollar.

2.5 Determina los procedimientos de seguridad operacional que son de aplicación al entorno conforme a las normas aplicables.

2.6 Implementa los procedimientos de seguridad operacional determinados.

2.7 Comprueba que la integración de las normas y procedimientos de seguridad operacional cumplen con los requisitos de ciberseguridad.

3. Integra las normas y procedimientos de calidad en la ciberseguridad en entornos OT identificando los posibles riesgos.

Criterios de evaluación

3.1 Define el concepto de riesgo y pérdida que afecta a la calidad.

3.2 Describe los fundamentos y herramientas básicas de un esquema de calidad.

3.3 Define los conceptos básicos relativos a normas de calidad.

3.4 Caracteriza las normas de calidad aplicables en función de la actividad que hay que desarrollar.

3.5 Determina los procedimientos de calidad que son de aplicación al entorno conforme a las normas aplicables.

3.6 Implementa los procedimientos de calidad determinados.

3.7 Comprueba que la integración de las normas y procedimientos de calidad cumplen con los requisitos de ciberseguridad.

4. Aplica medidas de ciberseguridad en los sistemas instrumentados de seguridad (SIS) ajustándose a las normas aplicables.

Criterios de evaluación

4.1 Caracteriza los tipos de fallos y de sistemas instrumentados de seguridad.

4.2 Discrimina entre las diferentes plataformas de tecnologías SIS, seleccionando aquellas que se adecuen a la realidad industrial de la organización.

4.3 Selecciona las normas aplicables en función de la actividad a desarrollar (IEC 61508 o las que eventualmente la sustituyan).

4.4 Determina los niveles de integridad de seguridad de aplicación al entorno conforme a la norma aplicable (IEC 61508 o las que eventualmente la sustituyan).

4.5 Determina las técnicas y medidas de seguridad de los SIS.

4.6 Comprueba que los SIS cumplen con los requisitos de ciberseguridad.

5. Gestiona de forma integral los riesgos de seguridad aplicando metodologías reconocidas.

Criterios de evaluación

5.1 Caracteriza la gestión integral de riesgos.

5.2 Describe las normas, marcos y metodologías de la gestión integral de los riesgos de seguridad.

5.3 Implementa un marco de gestión de riesgos de acuerdo con la normativa aplicable (ISO 31000 o las que, eventualmente, la sustituyan).

5.4 Identifica y evalúa el riesgo de acuerdo con la normativa aplicable (ISO 31000 o las que, eventualmente, la sustituyan).

5.5 Trata, acepta y comunica el riesgo según la normativa aplicable (ISO 31000 o las que, eventualmente, la

CVE-DOGC-B-24325035-2024

sustituyan).

Contenidos

1. Normas y procedimientos de seguridad física en la ciberseguridad en entornos OT:

1.1 Riesgos de seguridad física en un entorno OT.

1.2 Normas de seguridad física aplicables a un entorno OT.

1.3 Integración de la seguridad física en la seguridad OT.

2. Normas y procedimientos de seguridad operacional en la ciberseguridad en entornos OT:

2.1 Riesgos de seguridad operacional con un entorno OT.

2.2 Entornos OT.

2.3 Integración de la seguridad operacional en la seguridad OT.

3. Normas y procedimientos de calidad en la ciberseguridad en entornos OT:

3.1 Riesgos que afecten a la calidad en un entorno OT.

3.2 Normas de calidad aplicables a un entorno OT.

3.3 Integración de la calidad en la ciberseguridad OT.

4. Medidas de ciberseguridad en los sistemas instrumentados de seguridad (SIS):

4.1 Tipologías de fallos y sistemas instrumentados de seguridad.

4.2 Plataformas de tecnologías disponibles para implementar un sistema instrumentado seguro (SIS), y sus requisitos.

4.3 Normativa aplicable (IEC 61508 o las que eventualmente la sustituyan).

4.4 Métodos para determinar los niveles de integridad de seguridad (SIL).

4.5 Técnicas y medidas de seguridad en los SIS.

4.6 Requisitos de ciberseguridad en los sistemas instrumentados de seguridad.

5. Gestión integral de los riesgos de seguridad:

5.1 Marco de Gestión de Riesgos conforme a la normativa aplicable (ISO 31000 o las que eventualmente la sustituyan).

5.2 Identificación, evaluación, tratamiento, aceptación y comunicación del riesgo y vigilancia según la normativa aplicable (ISO 31000 o las que eventualmente la sustituyan).

5.3 Normativa de Ciberseguridad Industrial. Normativa NIST SP800-X, NERC-ZIP, IEC 62443, BSI-100 o las que eventualmente la sustituyan.

C080. Proyecto de Ciberseguridad en Entornos de las Tecnologías de Operación

Horas lectivas: 126 horas

Horas de estancia en la empresa: ninguna

CVE-DOGC-B-24325035-2024

Duración total: 126 horas

Resultados de aprendizaje y criterios de evaluación

1. Identifica necesidades del sector productivo, relacionándolas con proyectos tipo que las puedan satisfacer.

Criterios de evaluación

1.1 Clasifica las empresas del sector por sus características organizativas y el tipo de producto o servicio que ofrecen.

1.2 Caracteriza las empresas tipo, indicando la estructura organizativa y las funciones de cada departamento.

1.3 Identifica las necesidades más demandadas en las empresas.

1.4 Valora las oportunidades de negocio previsibles en el sector.

1.5 Identifica el tipo de proyecto requerido para dar respuesta a las demandas previstas.

1.6 Determina las características específicas requeridas en el proyecto.

1.7 Determina las obligaciones fiscales, laborales y de prevención de riesgos, y sus condiciones de aplicación.

1.8 Identifica posibles ayudas o subvenciones para la incorporación de las nuevas tecnologías de producción o de servicio que se proponen.

1.9 Elabora el guion de trabajo que se seguirá para la elaboración del proyecto.

2. Diseña proyectos relacionados con las competencias expresadas en el curso de especialización, incluyendo y desarrollando las fases que lo componen.

Criterios de evaluación

2.1 Recopila información relativa a los aspectos que serán tratados en el proyecto.

2.2 Realiza el estudio de viabilidad técnica del proyecto.

2.3 Identifica las fases o partes que componen el proyecto y su contenido.

2.4 Establece los objetivos que se pretenden conseguir, identificando su alcance.

2.5 Prevé los recursos materiales y personales necesarios para realizarlo.

2.6 Realiza el presupuesto económico correspondiente.

2.7 Identifica las necesidades de financiación para la puesta en marcha del proyecto.

2.8 Define y elabora la documentación necesaria para su diseño.

2.9 Identifica los aspectos que se tienen que controlar para garantizar la calidad del proyecto.

3. Planifica la ejecución del proyecto, determinando el plan de intervención y la documentación asociada.

Criterios de evaluación

3.1 Secuencia las actividades ordenándolas en función de las necesidades de desarrollo.

3.2 Determina los recursos y la logística necesarios para cada actividad.

3.3 Identifica las necesidades de permisos y autorizaciones por llevar a cabo las actividades.

3.4 Determina los procedimientos de actuación o de ejecución de las actividades.

3.5 Identifica los riesgos inherentes a la ejecución, definiendo el plan de prevención de riesgos y los medios y los equipos necesarios.

CVE-DOGC-B-24325035-2024

3.6 Planifica la asignación de recursos materiales y humanos, y los tiempos de ejecución.

3.7 Elabora la valoración económica que da respuesta a las condiciones de la puesta en práctica.

3.8 Define y elabora la documentación necesaria para la ejecución.

4. Define los procedimientos para el seguimiento y control en la ejecución del proyecto, justificando la selección de variables e instrumentos utilizados.

Criterios de evaluación

4.1 Define el procedimiento de evaluación de las actividades o de las intervenciones.

4.2 Define los indicadores de calidad para realizar la evaluación.

4.3 Define el procedimiento para la evaluación de las incidencias que puedan presentarse durante la realización de las actividades, su posible solución y registro.

4.4 Define el procedimiento para gestionar los posibles cambios en los recursos y en las actividades, incluyendo el sistema de registro.

4.5 Define y elabora la documentación necesaria para la evaluación de las actividades y del proyecto.

4.6 Establece el procedimiento para la participación en la evaluación de los usuarios o clientes y elabora los documentos específicos.

4.7 Establece un sistema para garantizar el cumplimiento del pliego de condiciones del proyecto cuando este existe.

Contenidos

Les determina el centro educativo.

(24.325.035)