OTRAS DISPOSICIONES

DEPARTAMENTO DE EDUCACIÓN

5318

ORDEN de 16 de octubre de 2018, de la Consejera de Educación, por la que se establecen cuatro programas de especialización profesional.

El Estatuto de Autonomía del País Vasco, en su artículo 16, atribuye la competencia propia sobre la enseñanza en toda su extensión, niveles y grados, modalidades y especialidades a la Comunidad Autónoma del País Vasco, sin perjuicio del artículo 27 de la Constitución y Leyes Orgánicas que lo desarrollen, de las facultades que atribuye al Estado el artículo 149.1.30.ª de la misma y de la alta inspección necesaria para su cumplimiento y garantía.

La Ley Orgánica 5/2002, de 19 de junio, de las cualificaciones y de la formación profesional, tiene por finalidad la ordenación de un sistema integral de formación profesional, cualificaciones y acreditación, que responda con eficacia y transparencia a las demandas sociales y económicas a través de las distintas modalidades formativas. También establece que la oferta de formación sostenida con fondos públicos debe favorecer la formación a lo largo de toda la vida y acomodarse a las diferentes expectativas y situaciones personales y profesionales.

En el ámbito laboral, de acuerdo con lo dispuesto en el artículo 12.2 del Estatuto de Autonomía, corresponde a la Administración General de la Comunidad Autónoma del País Vasco la competencia de ejecución de la legislación del Estado, especialmente, en lo que aquí es más relevante, promoviendo la cualificación de los trabajadores y las trabajadoras y su formación integral.

Para mejorar la empleabilidad de las personas, tanto en el corto como en el largo plazo, se va a requerir de nuevas estrategias y mecanismos. Por un lado, incrementando las horas dedicadas a los procesos de adquisición de competencias como única forma de lograr el mayor grado de especialización que demandan ámbitos cada vez más complejos. Por otro lado, la demanda de trabajadoras y trabajadores con una formación y competencias que se ajusten al entorno competitivo actual exige romper con esquemas anteriores y evolucionar desde un modelo formativo orientado al «puesto de trabajo» hacia otro centrado en el «campo profesional». Un cambio de paradigma que coloca a la persona en el centro promoviendo la adquisición o consolidación de competencias técnicas, personales y sociales, que garanticen la polivalencia y funcionalidad necesarias.

El establecimiento de cualificaciones más adecuadas a las necesidades reales del tejido productivo debe permitir, por una parte, adecuar la formación de las personas que estudian formación profesional a las necesidades cada vez más especializadas de las empresas y, por otra, mejorar la cualificación de los trabajadores y las trabajadoras dotándoles de las competencias que demandan los sectores productivos generadores de empleo.

La mejora de la formación profesional, en términos de eficacia, exige una especialización de la oferta y una planificación de la misma más ajustada a las necesidades del mercado laboral, especialmente en aquellos sectores y puestos de trabajo emergentes, que generen más empleo y que sean estratégicos para el futuro de la economía del País Vasco.

La formación profesional se revela, en este contexto, como un elemento clave para facilitar las herramientas que deben dar respuesta a las cualificaciones demandadas por los puestos de trabajo presentes y futuros.

El hecho de que existan numerosas demandas provenientes de los sectores productivos relevantes para la economía origina la necesidad de impulsar la elaboración de unos programas de formación que den respuesta rápida tanto a la adecuación y mejora de la empleabilidad de las personas como a las demandas de mayor especialización del tejido productivo y que puedan ser certificados por la Administración de la Comunidad Autónoma del País Vasco. Estos programas, certificados de esta forma, no darán lugar a un título o certificación académica, certificación profesional o certificación parcial acumulable en tanto que las competencias no estén incluidas en el Catálogo Nacional de Cualificaciones Profesionales.

En el Decreto 32/2008, de 26 de febrero, por el que se establece la ordenación general de la Formación Profesional del Sistema Educativo, modificado por el Decreto 14/2016, de 2 febrero, se establecen los programas de especialización profesional del País Vasco en el ámbito de la formación profesional, así como su reconocimiento y certificación, que acredite su valor dentro del marco normativo vigente.

Es por todo ello que en la Ley 4/2018, de 28 de junio, de Formación profesional del País Vasco, en el capítulo V, se establece el Marco Vasco de Cualificaciones y Especializaciones Profesionales.

Esta Ley regula un marco vasco de cualificaciones y especializaciones profesionales, con objeto de dar respuesta a nuestro mercado de trabajo a través del sistema general de formación profesional. En él se incluirán las certificaciones y acreditaciones propias de los programas de especialización profesional del País Vasco. La Ley de Aprendizaje a lo Largo de la Vida ya establece el sistema de acreditación de las actividades de aprendizaje a través de diferentes vías; en esta ley se trata de complementar aquella regulación con referencia a una de las actividades que se desea promover de forma singular: los programas de especialización en el ámbito profesional, actividades que requieren de un reconocimiento y certificación que reconozca su valor dentro del marco normativo vigente.

Con este referente para su elaboración, se han analizado las demandas de sectores productivos estratégicos en nuestra economía y de esta forma se han definido los programas de especialización profesional que se incluyen en la presente Orden.

Esta Orden viene a completar el catálogo de programas de especialización profesional publicado mediante la Orden de 27 de julio de 2016, de la Consejera de Educación, Política Lingüística y Cultura por la que se establecen siete programas de especialización profesional, así como las condiciones generales para su autorización e impartición, y la Orden de 23 de diciembre de 2016, de la Consejera de Educación por la que se establecen cinco programas de especialización profesional, incorporando cuatro nuevos programas de especialización profesional.

Por todo lo expuesto,

RESUELVO:

Artículo único.– Objeto.

1.– La presente Orden tiene por objeto establecer la estructura de cuatro programas de especialización profesional que se incorporan en los anexos, de acuerdo con lo establecido en el artículo 12 ter del Decreto 32/2008, de 26 de febrero, por el que se establece la ordenación general de la Formación Profesional del Sistema Educativo en el País Vasco.

2.– Los programas de especialización para los que se define su estructura y que se anexan a la presente Orden, se indican en los anexos que se citan a continuación:

Anexo I: Ciberseguridad en pymes.

Anexo II: Inspección de materiales metálicos y uniones soldadas mediante ensayos no destructivos.

Anexo III: Producción integral en líneas de fabricación de productos tubulares.

Anexo IV: Soldadura para la industria aeroespacial.

3.– Las condiciones para la impartición de los mismos serán las que se establecen en el artículo 12 ter del Decreto 32/2008, de 26 de febrero, por el que se establece la ordenación general de la Formación Profesional del Sistema Educativo en el País Vasco, así como en la precedente Orden de 27 de julio de 2016, de la Consejera de Educación, Política Lingüística y Cultura por la que se establecen siete programas de especialización profesional, así como las condiciones generales para su autorización e impartición.

DISPOSICIÓN FINAL PRIMERA.– Entrada en vigor.

La presente Orden entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del País Vasco.

DISPOSICIÓN FINAL SEGUNDA.– Recursos.

Contra la presente Orden podrá interponerse recurso potestativo de reposición ante la Consejera de Educación en el plazo de un mes, o recurso contencioso-administrativo ante la Sala de lo Contencioso-administrativo del Tribunal Superior de Justicia del País Vasco en el plazo de dos meses. El plazo para la interposición se contará en ambos casos a partir de la publicación en el Boletín Oficial del País Vasco.

En Vitoria-Gasteiz, a 16 de octubre de 2018.

La Consejera de Educación,
CRISTINA URIARTE TOLEDO.

ANEXO I A LA ORDEN DE 16 DE OCTUBRE DE 2018

PROGRAMA DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN PYMES

A) Datos de identificación.

Denominación: ciberseguridad en pymes.

Código: EP013.

Duración: 900 horas.

B) Perfil profesional.

Competencia general:

Garantizar la seguridad de sistemas y aplicaciones mediante el diseño de código de forma segura, el uso de metodologías y herramientas de seguridad activa e investigación forense, identificando vulnerabilidades y amenazas y definiendo planes estratégicos de ciberseguridad.

Campo profesional:

Esta figura profesional ejerce su actividad en el área de informática de entidades que dispongan de sistemas para la gestión de datos e infraestructura de redes, es decir, hoy en día, cualquier organización. En general, desarrolla su actividad en aquellos departamentos en los que se requiera prevenir y solucionar las posibles vulnerabilidades que se puedan dar.

Las ocupaciones y puestos de trabajo más relevantes son los siguientes:

● Auditor o auditora de seguridad de redes de comunicación y sistemas informáticos.

● Consultor o consultora de LOPD.

● Diseñador o diseñadora y montador o montadora de plataformas seguras.

● Controlador o controladora de sistemas de seguridad en redes industriales.

● Programador o programadora de código seguro.

Competencias técnicas, personales y sociales para su intervención profesional:

a) Desarrollar código de forma segura reconociendo las vulnerabilidades de programación.

b) Crear e implementar aplicaciones libres de vulnerabilidades, utilizando herramientas de seguridad.

c) Utilizar test de intrusión para identificar y localizar potenciales objetivos.

d) Escanear diferentes vulnerabilidades y analizar los resultados elaborando documentos.

e) Aplicar métodos de recogida de evidencias y utilizar técnicas de análisis para su evaluación.

f) Instalar, configurar y usar herramientas de análisis forense para detectar evidencias que se puedan dar en un sistema informático.

g) Configurar y utilizar dispositivos hardware para análisis forense de equipos informáticos.

h) Recuperar información de los artefactos en sistemas operativos propietarios.

i) Elaborar informes forenses a partir de los resultados obtenidos en su análisis.

j) Definir planes estratégicos de ciberseguridad.

k) Implementar y certificar un sistema de gestión de seguridad de la información.

l) Identificar los estándares internacionales de referencia para el gobierno de la seguridad y reconocer la legislación y la reglamentación, tanto nacional como internacional sobre seguridad y protección de datos.

m) Desarrollar las diferentes fases correspondientes a un análisis de riesgo aplicando las metodologías de análisis de riesgos más usadas en la industria de Seguridad de la Información y elaborando un plan para la gestión del riesgo residual resultante del análisis.

n) Aplicar pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático.

o) Implantar mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.

p) Implementar técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.

q) Implementar cortafuegos para asegurar un sistema informático analizando sus presentaciones y controlando el tráfico hacia la red interna.

r) Implementar servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.

s) Implementar soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.

t) Identificar vulnerabilidades y amenazas específicas de los sistemas de control en la industria y localizar buenas prácticas de referencia de reputación internacional.

u) Instalar y desplegar un entorno básico de automatización y control.

v) Identificar sistemas de automatización accesibles desde Internet

w) Explotar vulnerabilidades básicas en sistemas de automatización y control.

x) Interpretar comunicaciones y protocolos industriales.

y) Configurar y desplegar un cortafuegos industrial básico.

z) Proponer distintas tecnologías de ciberseguridad válidas para entornos industriales, así como medidas organizativas o procedimentales para mejorar la seguridad en dichos entornos.

aa) Mediar entre el área de seguridad de TI y el área de automática en una organización.

bb) Desarrollar las fases para la implantación de un Sistema de Gestión de la Seguridad.

cc) Usar sistemas de mejora continua.

dd) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la empresa.

ee) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos relativos a su entorno profesional, gestionando su formación y los recursos existentes para el aprendizaje a lo largo de la vida.

ff) Resolver situaciones o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y del conjunto de miembros del equipo.

gg) Comunicarse con sus iguales, superiores, clientes o clientas y personas bajo su responsabilidad, utilizando vías eficaces de comunicación, transmitiendo la información o conocimientos adecuados y respetando la autonomía y competencia de las personas que intervienen en el ámbito de su trabajo.

hh) Organizar, coordinar o participar en equipos de trabajo con responsabilidad, supervisando el desarrollo del mismo cuando sea necesario, manteniendo relaciones fluidas y asumiendo el liderazgo, así como aportando soluciones a los conflictos grupales que se pudiesen presentar.

C) Formación.

Ámbitos de aprendizajes. Asignación horaria.

1.– Introducción a la ciberseguridad: redes, programación orientada a objetos y seguridad informática: 100 horas.

2.– Programación de código seguro:150 horas.

3.– Seguridad perimetral: 150 horas.

4.– Análisis forense: 100 horas.

5.– Seguridad en sistemas industriales: 150 horas.

6.– Pentesting y auditoría web: 150 horas.

7.– Gestión y gobierno de la seguridad: 100 horas.

– Resultados del aprendizaje del programa:

Responsabilidad y autonomía en la actividad profesional (transversales al programa).

Esta persona asume la responsabilidad de asesorar sobre cómo aplicar las medidas de ciberseguridad en entornos informáticos, poniendo en marcha todos los mecanismos de seguridad a su alcance para evitar vulnerabilidades y, en el caso de que se produjera algún incidente, asegurarse de que producen el menor impacto posible y evitar que se repita. Así mismo, mediará entre las áreas de informática corporativa y de automática de las organizaciones, cuando sea necesario, y supervisará las actividades que el personal de estas lleva a cabo.

– Asociados al ámbito 1: Introducción a la ciberseguridad: redes, programación orientada a objetos y seguridad informática.

– Destrezas y habilidades a adquirir.

1.– Integrar ordenadores y periféricos en redes cableadas e inalámbricas, evaluando su funcionamiento y prestaciones.

Criterios de evaluación:

a) Se han identificado los estándares para redes cableadas e inalámbricas.

b) Se ha utilizado el sistema de direccionamiento lógico IP para asignar direcciones de red y máscaras de subred.

c) Se han configurado adaptadores de red cableados e inalámbricos bajo distintos sistemas operativos.

2.– Administrar las funciones básicas de un router estableciendo opciones de configuración para su integración en la red.

Criterios de evaluación:

a) Se han utilizado distintos métodos para acceder al modo de configuración del router.

b) Se han configurado rutas estáticas.

c) Se han identificado los archivos que guardan la configuración del router y se han gestionado mediante los comandos correspondientes.

d) Se han utilizado los comandos proporcionados por el sistema operativo del router que permiten hacer el seguimiento de posibles incidencias.

e) Se ha descrito las capacidades de filtrado de tráfico.

f) Se han utilizado comandos para gestionar listas de control de acceso ACL.

3.– Configurar redes locales virtuales identificando su campo de aplicación.

Criterios de evaluación:

a) Se han implementado VLANs.

b) Se han configurado enlaces troncales.

c) Se ha utilizado un router o switch multilayer para interconectar diversas VLANs.

d) Se han configurado conmutadores para trabajar de acuerdo con los protocolos de administración centralizada.

e) Se ha monitorizado la red mediante aplicaciones basadas en protocolo SNMP.

4.– Adoptar pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.

Criterios de evaluación:

a) Se han descrito las diferencias entre seguridad física y lógica.

b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.

c) Se han valorado las ventajas que supone la utilización de sistemas biométricos.

d) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.

e) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral especialmente en sistemas conectados a redes públicas.

5.– Implantar técnicas seguras de acceso remoto a un sistema informático interpretando y aplicando el plan de seguridad.

Criterios de evaluación:

a) Se han clasificado las zonas de riesgo en un sistema, según criterios de seguridad perimetral.

b) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.

c) Se ha implementado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.

d) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.

6.– Implementar cortafuegos para asegurar un sistema informático analizando sus prestaciones y controlando el tráfico hacia la red interna.

Criterios de evaluación:

a) Se han descrito las características, tipos y funciones de los cortafuegos.

b) Se han clasificado los niveles en que se realiza el filtrado de tráfico.

c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.

d) Se han configurado filtros en el cortafuegos a partir de un listado de reglas de filtrado.

e) Se han revisado los registros de sucesos del cortafuegos.

7.– Escribir y probar programas sencillos aplicando los fundamentos de la programación orientada a objetos.

Criterios de evaluación:

a) Se han identificado los fundamentos de programación orientada a objetos.

b) Se han instanciado objetos a partir de clases predefinidas.

c) Se han utilizado métodos y propiedades de los objetos.

d) Se han escrito llamadas a métodos estáticos.

e) Se han utilizado parámetros en las llamadas a métodos.

f) Se han incorporado y utilizado librerías de objeto.

g) Se han utilizado constructores.

8.– Desarrollar programas organizados en clases aplicando los principios de programación orientada a objetos.

Criterios de evaluación:

a) Se han identificado la sintaxis, estructura y componentes de una clase.

b) Se han definido clases.

c) Se han creado constructores.

d) Se han desarrollado programas que implementan y utilizan objetos de las clases creadas.

e) Se han utilizado mecanismos para controlar la visibilidad de las clases y sus miembros.

f) Se ha definido el concepto de herencia.

g) Se han definido y utilizado clases heredadas.

h) Se han creado y utilizado métodos estáticos.

i) Se han creado y utilizado librerías de clases.

j) Se han creado y definido interfaces.

9.– Desarrollar programas aplicando características avanzadas de los lenguajes orientados a objetos.

Criterios de evaluación:

a) Se han identificado los conceptos superclase y subclase.

b) Se han diseñado y aplicado jerarquías de clases.

c) Se han probado y depurado las jerarquías de clases.

d) Se han realizado programas que implementan y utilizan jerarquías de clases.

– Conocimientos (100 horas).

Redes cableadas e inalámbricas:

● Configuración de direcciones IP y máscaras subred.

● Configuración de adaptadores de red cableados e inalámbricos bajo distintos sistemas operativos.

● Configuración de dispositivos de interconexión en redes cableadas e inalámbricas.

Configuración y administración básica del router:

● Diferentes métodos de acceso al router.

● Comandos para la configuración y administración del router. Configuración de rutas estáticas.

● Comandos para el seguimiento de incidencias y monitorización del estado del router.

● Configuración de filtros de tráfico del router.

● Gestión de listas de control de acceso (ACL).

Redes virtuales:

● Implementación de VLANs.

● Diagnóstico de incidencias en VLANs.

● Configuración de enlace troncal entre dispositivos.

● Configuración de router o switch multilayer para interconectar diversas VLANs.

● Protocolos de VLANs.

● Monitorización de la red mediante aplicaciones basadas en el protocolo SNMP.

Pautas de seguridad informática:

● Principales causas de vulnerabilidad y su origen.

● Políticas de contraseña.

● Seguridad física y seguridad lógica.

Técnicas de acceso remoto. Seguridad Perimetral:

● Zonas de riesgo de un sistema informático.

● Implantación de un servidor como pasarela de acceso a la red interna.

● Configuración de métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.

● Protocolos seguros de comunicación.

Instalación y configuración de cortafuegos:

● Planificación de la instalación de cortafuegos.

● Configuración de filtros en un cortafuegos a partir de un listado de reglas de filtrado.

● Diagnósticos sobre posibles problemas.

Utilización de objetos:

● Características de los objetos y de las clases.

● Propiedades o atributos de los objetos.

● Concepto de método.

● Control de acceso a los miembros de una clase.

● Concepto de método estático.

● Parámetros y valores devueltos. Librerías de objetos.

● Concepto de constructor.

● Destrucción de objetos y liberación de memoria.

Desarrollo de clases:

● Concepto de clase. Estructura y miembros de una clase.

● Herramientas de definición de los atributos y control de acceso.

● Herramientas de declaración de métodos y argumentos.

● Herramientas de diseño de constructores.

● Encapsulación y visibilidad.

● Concepto de herencia.

● Concepto de clase heredada.

Desarrollo de clases avanzadas:

● Jerarquía de clases: superclase y subclases.

● Concepto de polimorfismo.

● Constructores y destructores de subclases. Acceso de métodos de la superclase. Redefinición de métodos de la superclase.

– Asociados al ámbito 2: programación de código seguro.

– Destrezas y habilidades a adquirir.

1.– Crear aplicaciones libres de vulnerabilidades para evitar ataques externos.

Criterios de evaluación:

a) Se ha efectuado el control de acceso a recursos.

b) Se han analizado errores de inyección tanto en el servidor como en el cliente.

c) Se han identificado diferentes protocolos de autenticación.

d) Se han creado, renovado y destruido sesiones de usuario durante la ejecución de la aplicación.

e) Se han explorado las vulnerabilidades de un sistema que permite al atacante fijar el identificador de sesión.

f) Se ha realizado una correcta gestión de las sesiones.

g) Se ha verificado la identidad digital del remitente frente a una comunicación o acceso a un recurso o funcionalidad.

2.– Implementar aplicaciones que envíen la información cifrada.

Criterios de evaluación:

a) Se han aplicado técnicas que tratan sobre la protección o el ocultamiento de la información frente a observadores no autorizados a partir de una clave secreta.

b) Se ha preservado la privacidad de las comunicaciones escritas garantizando que solo quien esté autorizado podrá leer el mensaje original.

c) Se ha garantizado la autenticidad y veracidad de los datos recogidos en el certificado digital expedido.

3.– Desarrollar aplicaciones evitando fuga de datos.

Criterios de evaluación:

a) Se ha controlado la autorización insuficiente.

b) Se han reducido los ataques mediante asignación de roles a los datos y funcionalidades de la aplicación.

c) Se ha utilizado un control de acceso basado en roles.

d) Se han realizado comprobaciones de control de acceso, basadas en la lógica del negocio.

e) Se ha aplicado un mecanismo de control de autorización en el lado del servidor.

f) Se ha asegurado que los mensajes de error solo muestran la información deseada.

g) Se han validado las entradas que controla el usuario.

4.– Aplicar herramientas de seguridad para desarrollo seguro basadas en la normativa vigente.

Criterios de evaluación:

a) Se ha identificado el nivel de riesgo de una aplicación y se ha mapeado con un nivel de riesgo Application Security Verification Standard (ASVS).

b) Se han definido los requisitos de seguridad basados en los requisitos ASVS en función del nivel de identificado.

– Conocimientos (150 horas).

Técnicas de programación segura:

● Principios básicos de seguridad en programación.

● Errores de inyección tanto en servidor, como en cliente.

● Autenticación de protocolos basada en formulario.

● Control de acceso declarativo y programático.

● Gestión de control de sesiones.

● Prevención de fuga de datos.

Implementación de aplicaciones:

● Herramientas específicas de criptografía: técnicas de protección de la información mediante encriptación.

● Certificados digitales para la autenticidad y veracidad de datos recogidos.

● Protocolos de seguridad para permitir que las aplicaciones puedan transmitir la información de manera segura.

● Firmas digitales para garantizar la autenticidad e integridad de un documento generado por medios electrónicos y transmitido a través de medios digitales.

Fuga de datos:

● Técnicas de control de autorización insuficiente.

● Revelación de información en mensajes de error.

● Path transversal.

Normativas vigentes:

● OWASP Top 10 Riesgos de seguridad en aplicaciones web.

● OWASP Application Security Verification Standard (ASVS).

● Security Verification Standard (ASVS).

● Niveles de confianza en la seguridad de aplicaciones web: planificación, definición de requisitos a nivel de riesgo, diseño para un nivel de riesgo, implementación, verificación.

– Asociados al ámbito 3: seguridad perimetral.

– Destrezas y habilidades a adquirir.

1.– Adoptar medidas para asegurar la comunicación en redes públicas, asegurando la identidad de los interlocutores.

Criterios de evaluación:

a) Se han definido los principios y objetivos de la seguridad en los sistemas informáticos.

b) Se han establecido protocolos para garantizar la confidencialidad e integridad de la información.

c) Se han establecido diferentes herramientas de gestores de contraseña.

d) Se han utilizado técnicas de cifrado, firmas electrónicas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.

e) Se han utilizado técnicas de autenticidad, confidencialidad e integridad de la información.

2.– Diseñar e implantar un modelo de seguridad perimetral en un sistema informático.

Criterios de evaluación:

a) Se han identificado diferentes escenarios a la hora de establecer un modelo de seguridad perimetral.

b) Se han configurado y utilizado distintos tipos de cortafuegos.

c) Se han configurado las políticas y reglas de filtrado de un cortafuegos, auditando los registros de sucesos.

d) Se han configurado de forma segura servidores y servicios sobre la DMZ.

3.– Configurar e implementar un Proxy.

Criterios de evaluación:

a) Se han definido los distintos funcionamientos que tienen proxy.

b) Se han configurado y utilizado los distintos tipos de proxy.

4.– Implantar sistemas de autenticación y gestión de identidades en sistemas de acceso remoto.

Criterios de evaluación:

a) Se han definido políticas y procedimientos de seguridad para los procesos de autenticación.

b) Se han identificado protocolos seguros de comunicación y sus ámbitos de utilización.

c) Se han configurado servidores RADIUS para la autenticación remota de usuarios.

d) Se ha implementado el acceso remoto a la red interna mediante conexiones VPN.

e) Se han establecido sistemas de autenticación de dos factores.

5.– Implantar un sistema SIEM (Security Information and Event Management).

Criterios de evaluación:

a) Se han identificado y calificado los eventos de amenazas.

b) Se han implementado las directivas de uso de las aplicaciones.

c) Se han analizado y documentado los distintos eventos registrados.

– Conocimientos (150 horas).

Seguridad en la información:

● Gestores de contraseña.

● Confidencialidad, integridad de la información.

● Aplicación de criptografía a la seguridad de la información.

● Técnicas para el cifrado de la información confidencial.

● Autenticidad.

● Aplicación firma digital.

● Certificados digitales. Gestor de PKI. PKCS.

● Protocolos de revocación: CLR, OCSP.

Seguridad perimetral:

● Diseño y definición de modelos para el establecimiento del perímetro de seguridad.

● Configuración de políticas y reglas de filtrado de cortafuegos.

● Configuración seguro de servidores y servicios sobre la DMZ. Cortafuegos de contención y bastión.

● Acceso seguro a los distintos servidores de la DMZ.

● UTM: Forward, Reverse, Transparent, Cache, Proxies.

Instalación y configuración de servidores Proxy:

● Instalación y configuración de un servidor web-proxy-cache.

● Utilización del servidor proxy para establecer restricciones de acceso web.

● Realización de pruebas de funcionamiento del proxy y monitorización de su actividad.

● Pruebas de acceso desde los clientes al proxy. Configuración de un proxy en modo transparente y modo inverso.

Implantación de técnicas de acceso remoto:

● Políticas y procedimientos de seguridad para los dispositivos de autenticación.

● Autenticación de dos factores. Utilización de tarjetas criptográficas. Sistemas de Single Sign On (SSO).

● Autenticación remota de usuarios, servidores RADIUS.

● Acceso remoto a la red interna mediante conexiones VPN (túnel).

● Comunicación segura a servidores internos a través de conexiones IPSEC (CSP/HA).

● Establecimiento de túneles cifrados para conexiones entre delegaciones.

Implantación de un sistema SIEM en máquinas virtuales:

● Teoría básica de eventos: SIM, SEM.

● Análisis y normalización de eventos.

● Agregación de eventos. Gestión de log y procedimientos de actuación.

● Monitorización, documentación y respuesta ante incidentes de seguridad y amenazas.

– Asociados al ámbito 4: análisis forense.

– Destrezas y habilidades a adquirir.

1.– Reconocer las etapas en que se efectúa el análisis forense e identificar las distintas fases de recogida de evidencias.

Criterios de evaluación:

a) Se han definido conceptos generales sobre el análisis forense.

b) Se han detallado los requisitos de investigación forense.

c) Se ha detallado la información previa a la solicitud de orden de registro.

d) Se ha descrito el modo de entrada al lugar del registro.

e) Se ha especificado la fase de desprecintado y clonado.

2.– Clonar dispositivos de almacenamiento de datos a través de aplicaciones software y equipos hardware.

Criterios de evaluación:

a) Se han utilizado bloqueadores de escritura en distintos dispositivos de almacenamiento de datos.

b) Se han duplicado discos en diferentes soportes.

c) Se ha verificado la integridad de las copias mediante distintos procesos.

3.– Analizar imágenes de disco a través de diferentes herramientas.

Criterios de evaluación:

a) Se ha establecido la diferencia entre espacio sin alojar y espacio slack en el sistema de ficheros.

b) Se han recuperado ficheros borrados.

c) Se han analizado archivos y metadatos.

4.– Capturar información volátil en RAM y analizar procesos en ejecución.

Criterios de evaluación:

a) Se han efectuado volcados de memoria.

b) Se ha analizado la memoria en caliente.

c) Se han identificado y analizado procesos en ejecución.

5.– Recuperar información de los artefactos de sistemas operativos propietarios.

Criterios de evaluación:

a) Se ha detallado la estructura del registro.

b) Se ha examinado el registro de forma on-line y off-line.

c) Se han utilizado diferentes herramientas de análisis del registro.

d) Se ha analizado el diseño y la estructura de carpetas para el análisis de evidencias.

e) Se han analizado los ficheros Hive de registro.

f) Se han analizado ficheros de registro de eventos.

g) Se han analizado ficheros de historial de navegación.

h) Se han analizado ficheros de actividad de perfiles de usuario y sistema.

– Conocimientos (100 horas).

Etapas del análisis forense:

● Etapas: adquisición, análisis, presentación y línea de tiempo.

● Consideraciones previas a la adquisición.

● Orden de volatilidad. Requisitos de investigación forense: aceptabilidad, integridad, credibilidad, relación causa-efecto, repetible y documentada.

Recogida de evidencias:

● Información previa a la solicitud de orden de registro.

● Entrada al lugar del registro.

● Desprecinto y clonado.

Clonado de dispositivos:

● Bloqueadores de escritura hardware/software.

● Obtención de copias bit a bit o a través de imágenes de disco.

● Conceptos sobre discos, particiones y archivos.

● Verificación de la integridad de la copia (procesos hash).

Análisis de imágenes:

● Sistema de ficheros. Espacios sin alojar y espacios slack.

● Recuperación de ficheros borrados.

● Análisis de datos y metadatos.

Análisis de RAM:

● Volcados de memoria. Análisis en caliente.

● Análisis de procesos en ejecución.

Recuperación de información de los artefactos de SO propietarios:

● Estructura del registro. Análisis of-line y on-line del registro.

● Herramientas de análisis del registro.

● Carpetas y archivos más relevantes para el análisis forense.

● Análisis e información de usuario: correo electrónico, historial de navegación, historial de búsquedas, historial de actividad y de ejecución de programas.

– Asociados al ámbito 5: seguridad en sistemas industriales.

– Destrezas y habilidades a adquirir.

1.– Analizar los aspectos básicos de la ciberseguridad industrial, identificando la normativa y buenas prácticas existentes, diferenciando entre un entorno OT y un entorno IT y entendiendo los principales ciberataques que han afectado a grandes empresas industriales de todo el mundo.

Criterios de evaluación:

a) Se ha definido la ciberseguridad industrial.

b) Se ha identificado qué limitaciones tienen los sistemas de automatización y control, en contraste con los sistemas de información, a la hora de implantar contramedidas de seguridad.

c) Se han identificado las prioridades de ciberseguridad en un entorno industrial.

d) Sobre un diagrama de red empresarial se ha identificado qué es el entorno OT y qué el IT.

e) Se ha diferenciado entre regulación de seguridad y buenas prácticas de seguridad.

f) Se ha descrito el alcance de la Ley de Protección de Infraestructuras Críticas y el Real Decreto que la desarrolla, y dónde encontrar información sobre ella.

g) Se han identificado las buenas prácticas IEC 62443 y CCN-STIC, los documentos que las componen y su ámbito de aplicación.

h) Se han identificado los principales ataques sufridos por compañías industriales en el mundo, incluyendo Stuxnet, Duqu, Night Dragon, Flame, Shamoon, Havex/Energetic Bear, Sandworm.

i) Se han extraído «lecciones aprendidas» de los principales ataques presentados.

2.– Recrear un entorno industrial básico, instalando y configurando al menos un autómata simulado y un software de supervisión y control remoto.

Criterios de evaluación:

a) Se ha simulado un autómata mediante una Raspberry Pi3 y el software necesario.

b) Se ha cargado una lógica de control básica al autómata.

c) Se ha instalado y configurado un software SCADA/supervisión básico.

d) Se han conectado el software de supervisión y el autómata.

e) Se ha comprobado que el software de supervisión es capaz de ver en tiempo real las variables del autómata y de almacenar sus valores en una base de datos de históricos.

3.– Analizar las características de los distintos componentes industriales, incluyendo PLCs, RTUs, PCs industriales, SIS, SCADA, DCS, MES, etc., así como su lugar en el ámbito de la automatización, su funcionamiento y vulnerabilidades.

Criterios de evaluación:

a) Se ha descrito el lugar de los sistemas ICS dentro del ámbito de los sistemas OT.

b) Se han identificado las diferencias funcionales y tecnológicas en los distintos niveles de automatización.

c) Se han presentado los componentes transversales para el control local: sensores, actuadores, servos y variadores, PLCs, RTUs, PCs industriales y DCS.

d) Se han presentado los sistemas de control por supervisión: DCS, SCADA, historizadores, etc.

e) Se han presentado los sistemas que automatizan y controlan la seguridad (safety) en entornos industriales, así como las versiones híbridas de control y seguridad.

f) Se han presentado otros componentes de automatización y control sectoriales: robots, CNCs, contadores inteligentes, MES, etc.

g) Se han presentado las principales vulnerabilidades que afectan a todos los componentes presentados.

4.– Utilizar herramientas básicas de explotación de vulnerabilidades desde sistemas de automatización y control, particularmente Shodan y Kali-Moki.

Criterios de evaluación:

a) Se ha explicado Shodan, en qué consiste y cómo utilizarlo.

b) Se ha realizado una demostración práctica del uso de Shodan: localización de objetivo y prueba de acceso.

c) Se han identificado las herramientas para descubrimiento de hosts, puertos abiertos, servicios publicados y versiones del servicio.

d) Se ha utilizado JohnTheRipper para romper contraseñas en un sistema de automatización y control.

e) Se ha utilizado Metasploit para explotar una vulnerabilidad en un equipo industrial.

5.– Analizar los aspectos básicos de comunicaciones industriales, los principales protocolos de comunicaciones utilizados (ModBUS, BACnet, Profinet, etc.), su funcionamiento y vulnerabilidades.

Criterios de evaluación:

a) Se han explicado los conceptos de tiempo real, comunicaciones conmutadas y serie.

b) Se han identificado los paradigmas de cliente-servidor y publicación-suscripción, comunicaciones asíncronas, por paso de testigo, etc.

c) Se ha explicado el funcionamiento de los protocolos ModBUS, BacNet y Profinet.

d) Se han explicado los aspectos básicos de seguridad de los protocolos anteriores.

e) Se han presentado las arquitecturas de red típicas (e inseguras) en entornos industriales.

6.– Realizar ataques a comunicaciones y componentes industriales mediante las herramientas presentes en la distribución Kali-Moki o similares.

Criterios de evaluación:

a) Se ha capturado e interpretado tráfico industrial mediante Wireshark y/o TCPDump.

b) Se ha usado TCPReplay para inyectar tráfico en una red industrial.

c) Se han utilizado ModScan, MBTGet para manipular registros en un autómata.

d) Se ha utilizado Metasploit para lanzar un ataque de «pivoting» en una red de control mal diseñada y modificar los parámetros de control de un autómata.

7.– Proponer contramedidas técnicas, incluyendo diodos de datos, cortafuegos industriales, sistemas de detección de intrusiones, así como organizativas, incluyendo segmentación, auditorías sin riesgo, y procedimientos de uso seguro de medios móviles y extraíbles.

Criterios de evaluación:

a) Se ha explicado la necesidad tanto de medidas técnicas como organizativas.

b) Se han presentado los diodos de datos y/o pasarelas unidireccionales y sus diferencias con los cortafuegos.

c) Se han presentado los cortafuegos con capacidades industriales, incluyendo los conceptos DPI y robustez industrial.

d) Se han presentado los sistemas de detección de intrusiones en el ámbito industrial, incluyendo las técnicas de DPBI.

e) Se han explicado las buenas prácticas de segmentación y segregación de comunicaciones industriales.

f) Se han explicado los principios básicos de las auditorías libres de riesgo en entornos industriales.

g) Se han propuesto buenas prácticas para el uso seguro de medios móviles y dispositivos extraíbles, como dispositivos USB, portátiles, móviles, PDAs, etc.

8.– Desplegar y configurar un cortafuegos industrial Modbus.

Criterios de evaluación:

a) Se han presentado las nociones básicas de IPTables.

b) Se ha presentado el módulo Modbus.

c) Se han configurado reglas de filtrado en comandos de lectura y escritura sobre direcciones de memoria en un PLC que se comunica por Modbus/TCP.

d) Se ha comprobado con un autómata y las herramientas MBTget y ModScan el correcto funcionamiento del cortafuegos industrial.

– Conocimientos (150 horas).

Conceptos básicos de Infraestructuras industriales:

● Regulación y buenas prácticas de seguridad industrial: ley PIC, CCN-STIC, IEC 62443. OT vs IT: objetivos de seguridad y limitaciones.

● Principales ataques, grupos criminales y lecciones aprendidas: Stuxnet, Duqu, Night Dragon, Flame, Shamoon, Energetic Bear, Sandworm.

Recreación del entorno industrial:

● Instalación y configuración de un PLC simulado.

● Instalación y configuración de un SCADA básico.

● Configuración conectividad entre PLC y SCADA.

Componentes industriales:

● Introducción a los sistemas de control industrial.

● Sistemas de control local: sensores, actuadores, servos y variadores, PLCs, RTUs, PCs industriales y DCS.

● Aspectos clave, puntos fuertes y puntos débiles. SCADA: funciones, arquitectura y componentes.

● Sistemas de seguridad, sistemas de seguridad instrumentados (SIS) y sistemas integrados de control y seguridad (ICSS).

● Otros sistemas específicos sectoriales: CNC, contadores inteligentes, robots, MES, etc.

Herramientas de explotación de vulnerabilidades en sistemas de automatización y control industrial:

● Shodan: propósito y uso. Distribución.

● Kali-Moki: herramientas para atacar sistemas de automatización y control a nivel de host.

● Uso de JohnTheRipper.

● Uso de Metasploit.

Aspectos básicos sobre comunicaciones industriales:

● Conceptos del tiempo real y de comunicaciones conmutadas y serie.

● Los paradigmas de cliente-servidor y publicación-suscripción, comunicaciones asíncronas y por paso de testigo.

● El funcionamiento de los protocolos ModBUS, BacNet y Profinet.

● Los aspectos básicos de seguridad de los protocolos anteriores.

● Arquitecturas de red típicas (e inseguras) en entornos industriales.

Ataques basados en red y protocolos industriales:

● Uso de Wireshark y/o TCPDump para comunicaciones industriales.

● Uso de TCPReplay para la inyección de tramas de protocolos industriales.

● Uso de MBTGet y ModScan.

● Uso de Metasploit en ataques de pivoting.

Contramedidas técnicas y buenas prácticas organizativas:

● Definición y complementariedad de medidas tanto técnicas como organizativas.

● Diodos de datos y/o pasarelas unidireccionales y sus diferencias con los cortafuegos.

● Cortafuegos con capacidades industriales: DPI y robustez industrial.

● Sistemas de detección de intrusiones en el ámbito industrial: DPBI. Buenas prácticas de segmentación y segregación de comunicaciones industriales.

● Principios básicos de las auditorías libres de riesgo en entornos industriales.

● Buenas prácticas para el uso seguro de medios móviles y dispositivos extraíbles, como dispositivos USB, portátiles, móviles, PDAs, etc.

Cortafuego industrial Modbus:

● El módulo Modbus de IPTables. Reglas de filtrado en comandos de lectura y escritura para Modbus/TCP.

● Uso de herramienta MBTget y ModScan para comprobar el correcto funcionamiento de un cortafuegos Modbus.

– Asociados al ámbito 6: pentesting y auditoría web.

– Destrezas y habilidades a adquirir.

1.– Analizar diferentes fases dentro de una auditoría de seguridad.

Criterios de evaluación:

a) Se han definido los principios y objetivos de una auditoría de seguridad.

b) Se han establecido las distintas modalidades de hacking.

c) Se han establecido diferentes tipos de test. Test de intrusión y análisis de vulnerabilidades.

d) Se han identificado las utilidades y requisitos en los test de intrusión y análisis de vulnerabilidad.

e) Se han definido las distintas fases de una auditoría de seguridad.

f) Se han definido los distintos estándares para la auditoría de seguridad.

2.– Recoger, agrupar y evaluar una serie de evidencias de los sistemas auditados.

Criterios de evaluación:

a) Se han utilizado inteligencia de fuentes abiertas.

b) Se han utilizado las distintas herramientas de reconocimiento o búsqueda de información.

c) Se han recogido, agrupado y evaluado evidencias.

d) Se han escaneado e identificado los distintos servicios.

e) Se han configurado de forma segura servidores y servicios.

1.– Comprobar si un sistema o una web es débil aprovechando alguna vulnerabilidad, e intentar realizar una intrusión en el mismo.

Criterios de evaluación:

a) Se han definido las distintas acciones en el análisis de vulnerabilidad y explotación.

b) Se han analizado las vulnerabilidades, indicando si el sistema o la web es débil.

c) Se han definido las distintas acciones en la explotación de vulnerabilidad.

d) Se han explotado las vulnerabilidades en distintos entornos, utilizando distintas herramientas.

3.– Comprobar si una aplicación para telefonía móvil es segura o no.

Criterios de evaluación:

a) Se han hecho análisis estáticos de la aplicación en lado cliente.

b) Se han analizado las comunicaciones.

c) Se ha analizado dinámicamente su comportamiento.

d) Se ha analizado del lado servidor.

4.– Elaborar un informe detallado de vulnerabilidades.

Criterios de evaluación:

a) Se han descrito las fases para escribir el informe.

b) Se han definido las acciones de recopilación de la información obtenida.

c) Se ha plasmado la información obtenida de las pruebas realizadas.

d) Se ha realizado un informe de los hallazgos, conclusiones y recomendaciones.

e) Se han reportado y documentado las vulnerabilidades.

f) Se han definido distintos recursos para minimizar los principales ataques de vulnerabilidad.

– Conocimientos (150 horas).

Auditoría de seguridad:

● Principios y objetivos de una auditoría de seguridad.

● Clasificación y tipificación de vulnerabilidades.

● Fases de una auditoría de seguridad.

● Tipos de test: test de intrusión y análisis de vulnerabilidades.

● Estándares para la auditoría de seguridad.

Procesos de la auditoría:

● Inteligencia de fuentes abiertas. Escaneo de puertos.

● Fingerprinting de aplicaciones y sistemas (móviles, webs, dispositivos de red...).

Búsqueda y explotación de vulnerabilidades:

● Clasificación de vulnerabilidades y ataques.

● Herramientas de ataque, métodos de explotación.

● Herramientas de pentesting.

● Auditoría de distintos sistemas operativos y servicios.

● Auditoría de aplicaciones web.

Aplicaciones para móviles:

● Análisis estáticos de la aplicación en lado cliente.

● Análisis de comunicaciones.

● Análisis dinámico de su comportamiento.

● Análisis del lado servidor.

Informes de vulnerabilidades:

● Herramientas de documentación. Formato y estructura del informe.

● Plan de acción.

● Detalles de la vulnerabilidad.

– Asociados al ámbito 7: gestión y gobierno de la seguridad.

– Destrezas y habilidades a adquirir.

1.– Analizar la legislación y estándares actuales de gestión y gobierno de la seguridad.

Criterios de evaluación:

a) Se han identificado los conceptos relativos a la seguridad y su gestión.

b) Se han identificado los puntos críticos para la implantación de un gobierno de la seguridad (definición de la política de la seguridad, organización de la seguridad, enfoque orientado a la gestión de riesgos y procesos de mejora continua).

c) Se han identificado los principales actores de desarrollo de normas (ISO, NIST,...) y sus normas asociadas como la ISO 2700x, COBIT, ISO 22301, PCI DSS, ENS, LOPD, así como su interrelación y complementación.

d) Se ha localizado y consultado la normativa y buenas prácticas del gobierno de la Ciberseguridad existentes.

2.– Implementar las fases de un sistema de gestión de seguridad de la información.

Criterios de evaluación:

a) Se han establecido las fases y actividades necesarias para la implantación del gobierno de la seguridad (SGSI).

b) Se han analizado los procesos, metodologías y herramientas que deberán usarse para la implantación del gobierno de la seguridad.

c) Se han identificado los procesos y actividades necesarios para el desarrollo de una evaluación de seguridad y definición de planes de ciberseguridad.

d) Se han identificado y usado sistemas de mejora continua (PDCA) para implementar un Gobierno de Seguridad basados en las mejores prácticas de la Industria.

e) Se han identificado las principales metodologías de análisis de riesgo y sus principales fases de análisis.

3.– Implementar metodologías y técnicas de análisis de riesgos.

Criterios de evaluación:

a) Se han identificado las principales metodologías de análisis de riesgos de la industria.

b) Se ha desarrollado un análisis de riesgos completo, desde la identificación inicial de activos hasta la obtención del resultado final del riesgo actual (residual).

c) Se ha elaborado un Plan de Gestión del riesgo residual

4.– Implementar medidas de seguridad para la protección de la información de carácter personal y elaborar los procedimientos necesarios para el cumplimiento de la normativa vigente de protección de datos.

Criterios de evaluación:

a) Se han revisado los principales artículos de la Ley Orgánica de Protección de Datos (LOPD) y el Reglamento General de Protección de Datos, haciendo especial hincapié en las novedades que aporta el RGPD.

b) Se ha elaborado un Documento de Seguridad.

c) Se han elaborado los procedimientos que tanto la LOPD como el RGPD identifican como necesarios:

○ Clausulas informativas.

○ Contratos con terceros.

○ Ejercicio de derechos de los interesados.

d) Se han identificado las principales medidas de seguridad a aplicar en función del nivel de los datos de carácter personal a proteger.

– Conocimientos (100 horas).

Estándares y normativas de seguridad:

● Conceptos y aproximación: enfoque de la gestión del riesgo. Dimensiones de la ciberseguridad. Definición e implantación del Gobierno y Organización de la Seguridad. Otros factores críticos de éxito.

● Principales organismos, estándares y normativas de seguridad: organismos: ISO, ISACA, NIST. Principales normativas y estándares. Estándares: ISO27002, COBIT 5.0, ITIL, NIST 800. ISO 27002:2013.

● Código de Buenas Prácticas: introducción. Dominios ISO 27002:2013 Detalle de sus controles.

● Organización de la seguridad. Cumplimiento y auditoría.

Implantación y gobierno de la seguridad:

● Ciclo de vida: Plan, Do, Check, Act: fases para el desarrollo de un SGSI; requisitos documentales en el desarrollo de un SGSI.

Análisis de Riesgos:

● Conceptos, terminología y definiciones.

● Identificación y repaso de metodologías, principalmente, MAGERIT.

● Elaboración del análisis de riesgos.

● Obtención del riesgo final.

● Elaboración del Plan de Gestión del riesgo.

Protección de la Información de carácter personal:

● Conceptos, terminología y definiciones.

● Artículos clave de la LOPD y el RGPD.

● Elaboración de un Documento de Seguridad.

● Elaboración de cláusulas informativas.

● Procedimientos de ejercicio de derechos de los afectados.

● Contratos con terceros.

● Medidas de seguridad aplicables.

D) Títulos asociados al programa.

● Técnico Superior en Administración de Sistemas Informáticos en Red.

● Técnico Superior en Desarrollo de Aplicaciones Web.

● Técnico Superior en Desarrollo de Aplicaciones Multiplataforma.

Así mismo, de manera excepcional y previa autorización de la Viceconsejería de Formación Profesional, también podrán participar en estos programas de especialización, profesionales con al menos 3 años de experiencia que sean propuestos para ello por las empresas colaboradoras en la impartición del programa.

E) Sector económico y demandantes.

Cualquier sector económico cuya actividad requiere de una infraestructura de red.

Los demandantes podrían ser empresas que se dedican al desarrollo del software, a la gestión y supervisión de las infraestructuras de red y en general, cualquier empresa que quiera proteger su información. Empresas que, para lograr los objetivos de su negocio, precisan de sistemas de automatización y control industrial, incluyendo robots, máquina-herramienta, autómatas, controladores, software de supervisión y control (p. ej. SCADA, DCS, MES), etc.

F) Requisitos del profesorado e instructores.

Apartado 1.– Especialidades del profesorado y atribución docente en los ámbitos de aprendizaje del programa de especialización profesional.

El profesorado del centro de formación deberá poseer los requisitos regulados para alguna de las especialidades que a continuación se indican:

Ámbitos de aprendizaje. Especialidades del profesorado.

1.– Introducción a la ciberseguridad: redes, programación orientada a objetos y seguridad informática. Profesor Técnico o Profesora Técnica de Formación Profesional:

● Sistemas y aplicaciones informáticas.

Profesor o Profesora de Enseñanza Secundaria:

● Informática.

2.– Programación de código seguro: Profesor Técnico o Profesora Técnica de Formación Profesional:

● Sistemas y aplicaciones informáticas.

Profesor o Profesora de Enseñanza Secundaria:

● Informática.

3.– Seguridad perimetral: Profesor Técnico o Profesora Técnica de Formación Profesional:

● Sistemas y aplicaciones informáticas.

Profesor o Profesora de Enseñanza Secundaria:

● Informática.

4.– Análisis forense: Profesor Técnico o Profesora Técnica de Formación Profesional:

● Sistemas y aplicaciones informáticas.

Profesor o Profesora de Enseñanza Secundaria:

● Informática

5.– Seguridad en sistemas industriales: Profesor Técnico o Profesora Técnica de Formación Profesional:

● Sistemas y aplicaciones informáticas.

Profesor o Profesora de Enseñanza Secundaria:

● Informática.

6.– Pentesting y auditoría web: Profesor Técnico o Profesora Técnica de Formación Profesional:

● Sistemas y aplicaciones informáticas.

Profesor o Profesora de Enseñanza Secundaria:

● Informática.

7.– Gestión y gobierno de la seguridad: Profesor Técnico o Profesora Técnica de Formación Profesional:

● Sistemas y aplicaciones informáticas

Profesor o Profesora de Enseñanza Secundaria:

● Informática.

Apartado 2.– El profesorado deberá de acreditar haber recibido formación específica en temas de ciberseguridad para los módulos requeridos en este curso de especialización (Programación de código seguro, Seguridad perimetral, Análisis forense, Seguridad en sistemas industriales, Pentesting y auditoría web y Gestión y gobierno de la Seguridad).

Apartado 3.– Requisitos de experiencia y formación del personal instructor aportado por la empresa.

En relación con el personal instructor aportado por la empresa o empresas participantes en la formación, deberá tener una experiencia laboral en actividades relacionadas con el perfil del programa de al menos 3 años, o acreditar una formación relacionada con los resultados de aprendizaje del programa de al menos, 5 años.