III. OTRAS DISPOSICIONES

MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

3904 *Resolución de 8 de marzo de 2021, de la Secretaría General de Formación Profesional, por la que se conceden plazas para la realización de cursos en línea para la formación del profesorado que imparte enseñanzas de Formación Profesional.*

El proceso de digitalización progresiva que están experimentado todos los ámbitos de la sociedad, y singularmente los distintos procesos productivos en el marco de una economía industrial y de prestación de servicios globalizada, exigen de las Administraciones públicas una respuesta estratégica que permita a la ciudadanía, con carácter general, y muy especialmente a todos los trabajadores, mantener y mejorar sus competencias acorde con la evolución de los perfiles de los diferentes puestos de trabajo.

El I Plan Estratégico de Formación Profesional del Sistema Educativo 2019-2022, tiene entre sus objetivos diseñar, desarrollar y consolidar un sistema único de Formación Profesional que sitúe a estas enseñanzas como pilar fundamental del desarrollo económico y del bienestar social del país. Este plan consta de nueve ejes que, a su vez, se desagregan en dieciséis objetivos estratégicos y en cuarenta y cinco líneas de actuación. De entre esos ejes cabe destacar el eje 1: Colaboración y participación de las empresas y apertura a los órganos de participación de todos los sectores; el eje 2: Agilización de la respuesta desde la Formación Profesional a las necesidades de cualificación de cada sector productivo; y el eje 7: Formación profesorado de FP asociada a los sectores productivos, como impulsores y determinantes de acciones formativas como la que se convoca mediante la presente resolución.

El Real Decreto 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo, regula en su artículo 27 los cursos de especialización de formación profesional e indica los requisitos y condiciones a que deben ajustarse dichos cursos de especialización. En el mismo artículo se indica que versarán sobre áreas que impliquen una profundización en el campo de conocimiento de los títulos de referencia, o bien, que supondrán una ampliación de las competencias que se incluyen en los mismos. Por tanto, en cada curso de especialización se deben especificar los títulos de formación profesional que dan acceso al mismo.

El Real Decreto 498/2020, de 28 de abril, por el que se desarrolla la estructura orgánica básica del Ministerio de Educación y Formación Profesional, atribuye en su Artículo 5. Secretaría General de Formación Profesional, en el punto m) la coordinación de la red de centros de referencia nacional y la aprobación de sus planes plurianuales de actuación, en colaboración con otras administraciones implicadas.

El Real Decreto 229/2008, de 15 de febrero, por el que se regulan los Centros de Referencia Nacional en el ámbito de la formación profesional, en el punto 3, del artículo 2. Definición, indica que Los Centros de Referencia Nacional podrán incluir acciones formativas dirigidas a estudiantes, trabajadores ocupados y desempleados, así como a empresarios, formadores y profesores, relacionadas con la innovación y la experimentación en formación profesional, vinculadas al Catálogo Nacional de Cualificaciones Profesionales.

La Fundación EOI, F.S.P., fue calificada como Centro de Referencia Nacional mediante el Real Decreto 991/2014, de 28 de noviembre.

La Secretaría General de Formación Profesional conjuntamente con el Centro de Referencia Nacional en Comercio Electrónico y Marketing Digital para la FP han diseñado un curso para la formación del profesorado que imparte enseñanzas de Formación Profesional del Sistema Educativo.

La presente convocatoria de cursos pretende dar respuesta a la necesidad de proporcionar una educación inclusiva y de calidad en el ámbito de la Formación

cve: BOE-A-2021-3904
Verificable en https://www.boe.es

Profesional, de acuerdo con lo previsto en la Ley Orgánica 2/2006 de 3 de mayo, de Educación, cuyo artículo 102 establece la formación permanente como un derecho y obligación de todo el profesorado y una responsabilidad de las Administraciones educativas y de los propios centros y en el que se reconoce, además, la competencia del Ministerio de Educación y Formación Profesional para ofrecer programas de formación permanente de carácter estatal. Para ello, y en virtud de lo expuesto, dispongo:

1. Objeto y finalidad de la convocatoria

1.1 Objeto. La presente resolución tiene como objeto la convocatoria para la adjudicación de las plazas disponibles para los cursos de formación del profesorado de Formación Profesional que realizará la Secretaría General de Formación Profesional, en colaboración con la Fundación EOI, F.S.P.

1.2 Finalidad. Esta convocatoria tiene la finalidad de ofrecer un programa de actividades para la formación permanente del profesorado que facilite su actualización técnica, científica, pedagógica y didáctica y, en consecuencia, mejore su desempeño profesional en los ámbitos específicos objeto de la misma.

2. Financiación

2.1 Esta convocatoria no conlleva gastos de formación para los beneficiarios al realizarse en modalidad *e-learning*.

2.2 Los gastos derivados del uso de equipos informáticos personales, así como los de conexión a redes y flujo de datos que pudieran derivarse de la participación en el curso serán asumidos por cada uno de los beneficiarios.

2.3 Esta convocatoria no tiene el carácter de subvención ni supone el derecho a la percepción de ayudas de carácter económico para los beneficiarios.

3. Características de los cursos

3.1 El Ministerio de Educación y Formación Profesional, a través de la Fundación EOI, F.S.P., en su calidad de Centro de Referencia Nacional en Comercio Electrónico y Marketing Digital para la FP organizan un curso de formación destinado a la preparación de profesores de Formación Profesional con atribución docente para impartir los cursos de especialización de Ciberseguridad en entornos de las tecnologías de la información, establecido por el Real Decreto 479/2020, de 7 de abril, y de Ciberseguridad en entornos de las tecnologías de operación establecido por el Real Decreto 478/2020, de 7 de abril.

3.2 El curso de formación consta de tres módulos desarrollados en el anexo I:

– Módulo de Formación 1: Conceptos de Ciberseguridad, con una duración de treinta horas.

– Módulo de Formación 2: Especialidad en Ciberseguridad en entornos de las tecnologías de la información, con una duración de veinte horas.

– Módulo de Formación 3: Especialidad en Ciberseguridad en entornos de las tecnologías de operación, con una duración de veinte horas.

Los tres módulos se realizarán en modalidad *e-learning*, desarrollando el programa que se incluye en el anexo I de la presente resolución de forma secuencial (Módulo de Formación 1, Módulo de Formación 2, Módulo de Formación 3).

3.3 El curso tendrá una duración total de 70 (30+20+20) horas, y se desarrollará entre el 7 de abril y el 15 de julio del año 2021.

3.4 Para atender las posibles cuestiones y dudas planteadas por el alumnado durante el periodo de duración del curso, se habilitará *un sistema* para que las dudas del alumnado sean resueltas por los expertos de la Fundación EOI, F.S.P.

cve: BOE-A-2021-3904
Verificable en https://www.boe.es

4. Requisitos y perfiles de los destinatarios

Podrán solicitar plaza para la realización del curso quienes cumplan las siguientes condiciones:

a) Ser funcionario perteneciente a los cuerpos de Catedráticos de Enseñanza Secundaria, Profesores de Enseñanza Secundaria o Profesores Técnicos de Formación Profesional.

b) Encontrarse en servicio activo en el momento de formalizar la solicitud y mantener dicha condición durante el periodo de realización del curso.

c) Estar impartiendo en el curso 2020-21 módulos profesionales correspondientes a los títulos de Formación Profesional que dan acceso a los cursos de especialización a que se hace referencia en el apartado 3.1 y que se consignan en el Anexo II de la presente convocatoria, con la excepción de los módulos profesionales de Formación y orientación laboral y Empresa e iniciativa emprendedora.

5. Solicitudes, documentación y plazo de presentación

5.1 Solicitud. Los interesados que reúnan los requisitos exigidos en la presente convocatoria deberán solicitarlo mediante el formulario electrónico disponible por Internet en la dirección https://sede.educacion.gob.es/, que podrá ser localizado introduciendo el nombre de la convocatoria en la sección «buscar trámites».

La firma de la solicitud por el/la interesado/a podrá ser efectuada con cualquiera de los sistemas de firma electrónica establecidos en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas o con el Sistema de Identificación Básica habilitado en la Sede Electrónica y enviada por el procedimiento telemático establecido, quedando así presentada a todos los efectos. No serán tenidas en cuenta aquellas solicitudes cumplimentadas por vía telemática que no completen el proceso de presentación estipulado, que permitirá obtener en el área personal el resguardo de solicitud, el cual deberá ser conservado por el/la solicitante para acreditar, en caso de que resulte necesario, su presentación en el plazo y forma fijados.

A los efectos establecidos en el párrafo anterior y en los términos legalmente previstos, la firma electrónica del interesado/a podrá efectuarse mediante la utilización de claves concertadas y/o la aportación de información conocida por ambas partes. El formulario generado por la sede electrónica incluye un número que identifica la solicitud y un resumen digital que garantiza la integridad de la misma. En caso de modificación del impreso oficial, manual o electrónicamente, la solicitud será automáticamente excluida.

De conformidad con lo previsto en el punto 1 del artículo 68 de la Ley 39/2015, de 1 de octubre, si la solicitud de inscripción no reúne los requisitos que señala el artículo 66, y en su caso, los que señala el artículo 67 u otros exigidos por la legislación específica aplicable, se requerirá al interesado para que, en un plazo de 10 días hábiles, subsane la falta o acompañe los documentos preceptivos, con indicación de que, si así no lo hiciera, se le tendrá por desistido de su petición, previa resolución que deberá ser dictada en los términos previstos en el artículo 21.1 de la citada ley.

Las notificaciones se realizarán por el sistema de notificación por comparecencia electrónica, previsto en el artículo 41, de la Ley 39/2015, de 1 de octubre, a través de la sede electrónica de este Ministerio que los solicitantes han utilizado para su petición, surtiendo ésta todos los efectos de notificación practicada a partir de la fecha de dicha publicación.

5.2 Documentación. El formulario de solicitud deberá ir acompañado de certificación expedida por el Secretario del Centro Educativo en el que el docente se halle prestando servicios durante el curso académico 2020/2021, con el visto bueno del Director o, en su caso, de certificación expedida por el Servicio de Inspección Educativa, en la que se haga constar la impartición efectiva de docencia durante el curso 2020/2021 en alguno de los ciclos formativos recogidos en el Anexo II de la presente convocatoria. Dicho documento podrá seguir el modelo recogido en el anexo III.

cve: BOE-A-2021-3904
Verificable en https://www.boe.es

La documentación indicada deberá, en caso de disponer de los originales en papel, digitalizarse mediante un procedimiento de escaneado y entregarse en formato PDF en la sede electrónica, durante el proceso de confección y presentación de la solicitud.

La Secretaría General de Formación Profesional podrá solicitar, en cualquier momento del procedimiento administrativo, los originales en papel a través de los cuales se generaron todos los archivos electrónicos incorporados a la solicitud, con el fin de contrastar su validez y concordancia. En el caso de que los originales sean electrónicos, la Secretaría General de Formación Profesional podrá comprobar su autenticidad por medio de la verificación de la firma o firmas electrónicas y el fechado electrónico de tales originales, no siendo necesaria la aportación de original en papel alguno.

El Ministerio de Educación y Formación Profesional se reserva el derecho de actuar legalmente contra aquellos que modificasen o alterasen aquellos documentos originales para generar los archivos electrónicos en la solicitud.

5.3 Plazo de presentación. Desde el día 15 de marzo de 2021 hasta el día 23 de marzo de 2021.

La información sobre esta convocatoria se encontrará a disposición de los interesados en la sede electrónica ubicada en https://sede.educacion.gob.es y en http://www.todofp.es.

6. Criterios de adjudicación de las plazas

6.1 El número de plazas disponibles se establece por cupos proporcionales para cada Comunidad Autónoma en función de su plantilla docente de Formación Profesional, garantizando una distribución homogénea de beneficiarios de la acción formativa en el conjunto del Estado.

6.2 Las plazas disponibles para cada Comunidad Autónoma serán adjudicadas a los candidatos de la misma que cumplan los requisitos por riguroso orden de petición.

6.3 Las plazas libres no adjudicadas en el cupo de cada Comunidad Autónoma serán redistribuidas con los mismos criterios de proporcionalidad entre el resto de Comunidades Autónomas.

7. Ordenación e instrucción del procedimiento de concesión de las ayudas

7.1 El órgano concedente será la Secretaría General de Formación Profesional.

7.2 El órgano de instrucción será la Subdirección General de Ordenación e Innovación de la Formación Profesional, a la que se autoriza para aplicar y desarrollar lo dispuesto en la presente Resolución.

7.3 Comisión de selección. Para la selección de candidatos y adjudicación de plazas se constituirá una Comisión que estará integrada por los siguientes miembros:

– El Subdirector General de Ordenación e Innovación de la Formación Profesional, que actuará como presidente.

– Un funcionario de la Subdirección General de Ordenación e Innovación de la Formación Profesional, designado por el Subdirector General, con nivel de Jefe de Área o similar, que actuará como vocal.

– Un funcionario del Gabinete Técnico de la Secretaría General de Formación Profesional, designado por el Director del Gabinete Técnico, que actuará como vocal.

– Un asesor técnico docente de la Subdirección General de Ordenación e Innovación de la Formación Profesional, designado por el Subdirector General, que actuará como vocal.

– Un funcionario de la Subdirección General de Ordenación e Innovación de la Formación Profesional, con nivel de Jefe de Servicio o similar, designado por el Subdirector General, que actuará como secretario.

cve: BOE-A-2021-3904
Verificable en https://www.boe.es

8. Criterios de valoración y adjudicación de plazas

8.1 Criterios de valoración. Al no existir criterios de baremación susceptibles de valoración mediante fórmula o juicio de valor, la propuesta de adjudicación realizada por la comisión de selección atenderá al cumplimiento estricto de los criterios de distribución y requisitos establecidos en los apartados 4 y 6 de esta resolución.

8.2 Adjudicación de las plazas. La comisión de selección realizará un informe, que contendrá el listado de candidatos propuestos, así como la correspondiente lista de reserva, que se confeccionará con los candidatos no seleccionados ordenados por riguroso orden de inscripción.

9. Resolución de la convocatoria

9.1 La competencia para resolver corresponde a la persona titular de la Secretaría General de Formación Profesional, de conformidad con el artículo 5 del Real Decreto 498/2020, de 28 de abril, por el que se desarrolla la estructura orgánica básica del Ministerio de Educación y Formación Profesional, así como con la Orden EFP/43/2021, de 21 de enero, sobre fijación de límites para la administración de determinados créditos para gastos y de delegación de competencias, que dictará la resolución de concesión.

9.2 La resolución de concesión contendrá la relación de candidatos seleccionados, así como la lista de candidatos en reserva para cubrir las plazas que pudieran quedar vacantes como consecuencia de renuncia u otras causas.

9.3 La resolución de concesión será publicada en el «Boletín Oficial del Estado», y se dará publicidad de la misma en el portal TodoFP (www.todofp.es).

10. Renuncias

El plazo de presentación de renuncia voluntaria se deberá formular en el plazo de cinco días hábiles, a partir de la publicación de la resolución de adjudicación, y se formalizará a través de la sede electrónica del Departamento en el formulario de solicitud de renuncia voluntaria que en la misma figura al efecto.

11. Obligaciones de los beneficiarios

Los beneficiarios de estos cursos estarán obligados a:

a) Aceptar todas las bases de esta convocatoria y realizar el curso concedido de acuerdo con las normas fijadas en esta.

b) Someterse a las actuaciones de comprobación y control que realice la Subdirección General de Ordenación e Innovación de la Formación Profesional, así como cumplimentar los documentos que, al efecto, les sean requeridos.

12. Certificaciones

A los profesores participantes se les expedirá, una vez finalizados los mismos, un certificado por el número de horas de formación correspondientes a cada Módulo de Formación completo que se haya cursado con evaluación positiva, de acuerdo con la Orden EDU/2886/2011, de 20 de octubre, por la que se regula la convocatoria, reconocimiento, certificación y registro de las actividades de formación permanente del profesorado, siempre que reúnan los requisitos en ella establecidos. Para obtener la certificación, es prescriptivo que los participantes superen las actividades que se determinen en cada uno de los módulos de formación y cumplimenten la documentación que, a estos efectos, les será facilitada a la finalización del curso.

cve: BOE-A-2021-3904
Verificable en https://www.boe.es

13. Recurso

Contra la presente Resolución se podrá interponer recurso de alzada en el plazo de un mes, de acuerdo con lo establecido en los artículos 121 y 122 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

14. Efectos y publicidad

La presente convocatoria se regirá por las normas específicas contenidas en esta Resolución, que entrará en vigor el día siguiente de su publicación en el «Boletín Oficial del Estado».

Madrid, 8 de marzo de 2021.–La Secretaria General de Formación Profesional, Clara Sanz López.

ANEXO I

Contenidos

Módulo de Formación 1: Conceptos de ciberseguridad

Objetivo. Adquirir conocimientos generales que permitan al profesor tener un conocimiento global y actualizado del campo de la ciberseguridad y verificar su relación con la protección de la información y los sistemas de control industrial, obteniendo los conocimientos generales a aplicar en las organizaciones y empresas para proteger la información y los dispositivos de producción empresarial.

Duración: Treinta horas.

Conocimientos/capacidades cognitivas y prácticas:

– Conocer los conceptos generales de ciberseguridad y su relación con la seguridad (una hora):

- Definición y alcance de la ciberseguridad.
- Áreas de actuación de la ciberseguridad.
- Ubicación de la ciberseguridad.
- Dimensiones de la seguridad y garantías que ofrece.
- Protección de la información.
- Cibercriminales: un mercado en crecimiento.

– Concienciación en ciberseguridad (dos horas):

• Actividades de concienciación en la empresa: (Empleados, equipo directivo, equipos técnicos (desarrolladores, administradores de sistemas), actividades de concienciación a clientes.

• Phishing ético.

– Gobierno de la seguridad de la información (tres horas):

- Organización de seguridad en una empresa.
- Causas de los ataques en la empresa.
- Pilares de una estrategia de ciberseguridad.
- Proceso de gestión de riesgos.
- Roles en ciberseguridad.

o El rol del CISO y el desarrollo de su función.
o Coordinación de la seguridad en la empresa.
o Las tres líneas de defensa.
o Red Team, Blue Team, Purple Team.
o Ciberseguro: opción para gestionar riesgos.

cve: BOE-A-2021-3904
Verificable en https://www.boe.es

- Marcos de referencia en gestión de la ciberseguridad (ISO 27032, NIST).
- Marcos de gestión de riesgos (ISO 27005, NIST SP 800 30).
- Requisitos legales (RGPD, PSD2, HIPAA).

– Distinguir las amenazas y vulnerabilidades reconociendo sus efectos en los sistemas (seis horas):

- Categorías de los ciberataques.
- Ataques para obtener información.
- Ataques a nivel de red.
- Ataques de monitorización.
- Ataques de autenticación.
- Ataques de denegación de servicio.
- Ingeniería social (phishing, fraude al CEO, suplantación de identidad, etc.).
- Tipos de Malware: (virus, gusano, troyano, ransomware, etc.).
- Ataques DoS y DDoS.
- APTs.
- Botnets.
- Seguridad en el perímetro de las redes.
- Riesgos de terceros: el control de la cadena de suministro.

– Comprender los mecanismos de defensa a implementar en las redes privadas (5,5 horas):

- Defensa en profundidad y la DMZ.
- Antimalware.
- IPS/IDS.
- Segregación de redes.
- Firewalls.
- Protocolos de comunicación seguros.
- Cifrado de las comunicaciones.
- Contraseñas.
- El control de acceso.
- Controles para definir una red segura.
- Sistemas de detección de ataques.
- Recuperación de los sistemas ante un ciberataque.
- SIEM.
- Seguridad en redes WIFI y dispositivos inalámbricos.
- Biometría y autenticación fuerte o de doble factor.
- Sistemas anti-DDoS.
- Bastionado/Hardenizado.
- Gestión de Vulnerabilidades y parcheado de sistemas.

– Comprender los mecanismos de protección de la información (seis horas):

- Descubrimiento de la información (Estado estructurado/no estructurado) (almacenada/comunicada/en uso).
- Clasificación de información.
- Etiquetado de información.
- Herramientas de control de acceso a la información (IRM).
- Herramientas de prevención de fuga de información (DLP).
- Medidas de protección: (Control de acceso, cifrado, pseudo-anonimización, ofuscación, control de la integridad).
- Métodos de copia de seguridad.
- La restauración de los datos.

cve: BOE-A-2021-3904
Verificable en https://www.boe.es

– Gestión de identidades (1,5 horas):

- Identificación, autenticación y autorización, no repudio.
- Sistemas biométricos.
- Identidad digital.

– Conocer los servicios que se implementan en la nube (2,5 horas):

- Cloud computing.
- IaaS, PaaS y SaaS
- Servicios de Seguridad en la nube.

– Casos de uso de aplicación práctica (a seleccionar entre los siguientes) (2,5 horas):

- Mapeo de Puertos.
- Ataques a Protocolos Inalámbricos (WiFi y Bluetooth).
- Detección y Prevención (IDS/IPS).
- Gestión de Información y Eventos de Seguridad (SIEM).
- Vectores de Infección.
- Captura de Información (Stealers y Keyloggers).
- Troyanos de Acceso Remoto Fijo/Móvil (RATs).
- Disuasión y Honeypots.
- Herramientas de Ingeniería social.

Módulo de Formación 2: Especialidad ciberseguridad en entornos de las tecnologías de la información

Objetivo: Identificar las necesidades de protección y seguridad a implementar en las organizaciones; comprender y desarrollar las dimensiones de seguridad que dotan de protección a la información y a los recursos que conforman la intranet empresarial; detectar y desarrollar las necesidades de procedimientos y buenas prácticas de ciberseguridad a utilizar en la explotación y mantenimiento técnico de los recursos de las tecnologías de información de las organizaciones; y adquirir los conocimientos para la gestión eficiente de la ciberseguridad en las organizaciones con la finalidad de poder diseñarla y aplicarla.

Duración: Veinte horas.

Conocimientos/Capacidades cognitivas y prácticas:

– Conocer las formas de implementar la seguridad digital (dos horas):

- Peligros latentes en las redes.
- Ataques a la información digital.
- Servicios de seguridad.
- Equipos de respuesta ante emergencias de Ciberseguridad (CERT/CSIRT).
- El Centro de Operaciones de Ciberseguridad (SOC).
- Open Source Intelligence (OSINT).
- Inteligencia de fuerzas humanas (HUMINT).

– Aplicar los controles de ciberseguridad a en las empresas para mejorar la protección de la información (una hora):

- Desarrollo de los controles fundamentales a establecer en una organización.
- Protección del puesto de trabajo.
- El acceso remoto y el teletrabajo.
- El escritorio virtual.

– Comprobar la importancia de la política de seguridad en una organización (una hora):

- El plan director de seguridad.
- Políticas de seguridad dirigidas a los componentes de la empresa.

cve: BOE-A-2021-3904
Verificable en https://www.boe.es

– Identificar las formas de protección de activos (dos horas):

- Protección de datos.
- Protección de las interconexiones.
- El cortafuegos.
- Criptografía.
- Enmascaramiento.
- Gestión de las claves.

– Identificar las necesidades para diseñar y asegurar la disponibilidad de la información (una hora):

- Clasificar la información empresarial.
- El almacenamiento seguro de la información.
- La eliminación de los datos y el borrado seguro.
- Conservación de la información.
- El almacenamiento extraíble.

– Entender la utilidad de los planes de continuidad de negocio en la empresa (dos horas):

- El análisis de impacto (BIA) y gestión de riesgos.
- Conceptos sobre la continuidad:

o Período máximo tolerable de interrupción (MTPD).
o Punto objetivo de recuperación (RPO).
o Tiempo objetivo de recuperación (RTO).

- El plan de continuidad de negocio y estrategias de continuidad:

o Personal.
o Instalaciones.
o Tecnología.
o Información.
o Proveedores.

- El plan de contingencia.
- El plan de recuperación de desastres.

– Conocer la utilidad de la correlación de eventos en la prevención e investigación de incidentes (tres horas):

- Eventos y tipos.
- Eventos de los sistemas de seguridad.
- Criticidad de los eventos.
- Tratamiento de los eventos para su automatización.
- Correlación de eventos, casos de uso.
- Análisis de comportamiento.
- IoC: indicadores de compromiso.
- Soluciones de automatización. El SIEM.
- Sistemas de Respuesta. El EDR.

– Reconocer las formas de aplicar la seguridad en las redes inalámbricas y dispositivos móviles (una hora):

- Metodologías de seguridad y ataques wireless.
- La conexión inalámbrica y las redes.
- Medidas de seguridad en el router.
- Amenazas en los terminales móviles.
- Estrategia de uso de los dispositivos de los empleados (BYOD).

cve: BOE-A-2021-3904
Verificable en https://www.boe.es

– La auditoría de Ciberseguridad (dos horas):

- Proceso de auditoría.
- Requerimientos de auditorías.
- Matriz de aplicabilidad.
- Marcos de control.
- Elaboración de informes de auditoría.

– Análisis forense y custodia de evidencias digitales (2,5 horas).
– Casos de uso de aplicación práctica (a seleccionar entre los siguientes) (2,5 horas):

- Configuración de un Firewall.
- Protección de Datos en MongoDB.
- Almacén de Claves.
- Túnel IPsec.
- Túnel VPN.
- Montaje de un NAS securizado.
- Cifrado y enmascaramiento de datos.

Módulo de Formación 3: Especialidad ciberseguridad en entornos de las tecnologías de operación

Objetivo: Identificar las necesidades de protección y seguridad a implementar en los procesos de producción empresarial y los sistemas de control industrial o SCI; detectar y desarrollar la implementación necesaria en los SCI para asegurar los procesos industriales; desarrollo de procedimientos y buenas prácticas de ciberseguridad a utilizar en la explotación de los SCI y en el mantenimiento técnico de los recursos de las tecnologías de operación o TO; y adquirir los conocimientos para la gestión eficiente de la ciberseguridad en las organizaciones industriales con la finalidad de diseñarla y aplicarla.

Duración: Veinte horas.

Conocimientos/Capacidades cognitivas y prácticas:

– Comprobar la importancia de la política de seguridad industrial en una organización (dos horas):

- Entender el concepto de Internet de las Cosas (IoT).
- Las políticas de seguridad en el entorno industrial.
- Riesgos de seguridad.
- Recomendaciones de seguridad.
- El plan director de seguridad.

– Conocer las formas de implementar la seguridad industrial (dos horas):

- Peligros latentes en las redes.
- Ataques a la información digital.
- Servicios de seguridad.
- Infraestructuras críticas. LPIC y su desarrollo.
- Centro de seguridad industrial.

– Identificar las formas de protección de activos en entornos SCI (Sistemas de control industrial) (una hora):

- Protección de datos.
- Protección de las interconexiones.
- El cortafuegos.
- Criptografía.
- Gestión de las claves.
- Qué ofrecen los fabricantes SCI.

cve: BOE-A-2021-3904
Verificable en https://www.boe.es

– Conocer la ciberseguridad asociada a las comunicaciones inalámbricas en entornos industriales (tres horas):

- Tecnologías inalámbricas en los SCI.
- Características de seguridad de las tecnologías.
- Análisis de la seguridad en las tecnologías inalámbricas.
- Protocolos de comunicación en las redes inteligentes:

  - Comparativa de protocolos.
  - PRIME.
  - Meters and More.
  - G-3-PLC.
  - OSGP.
  - DLMS/COSEM.
  - IEEE 1901.

– Saber obtener y gestionar un inventario de activos en sistemas de control industrial o SCI (dos horas):

- Tipos de implementación de inventarios en SCI.
- Gestión de los activos.
- Herramientas para el inventario de activos en un SCI.
- Fases en la creación de un inventario en el SCI.
- Mantenimiento de inventarios.

– Configurar mecanismos de protección en SCI (dos horas):

- Arquitectura base de sistemas de control.
- Arquitectura de seguridad para sistemas de control.
- Diseño de redes en los SCI.
- Tecnologías de monitorización en el SCI.
- Soluciones tecnológicas.
- Virtual patching.

– Habilitar accesos seguros a los dispositivos de campo industrial (dos horas):

- Niveles de red.
- Segmentación de red.
- Arquitectura de acceso local seguro.
- Arquitectura de acceso remoto a la red industrial.
- Mecanismos de seguridad.

– Desarrollar técnicas de detección y gestión de incidentes en entornos SCI (una hora):

- Clasificación de ciberincidentes.
- Gestión de incidentes de ciberseguridad.
- Procedimiento de actuación.

– Comprender los procedimientos del análisis forense en SCI (1,5 horas):

- Modelado de ataques.
- Proceso del análisis forense.
- Herramientas de análisis forense.
- Análisis forense de un malware.

cve: BOE-A-2021-3904
Verificable en https://www.boe.es

– Entender la utilidad de los planes de continuidad de negocio en entornos SCI (una hora):

- El análisis y gestión de riesgos.
- El plan de continuidad de negocio.
- El plan de contingencia.
- La auditoría de seguridad.
- El plan de recuperación de desastres.

– Casos de uso de aplicación práctica (a seleccionar entre los siguientes) (2,5 horas):

- Gestión de activos mediante RFID.
- Monitorización de Redes Industriales.
- Configuración de T-Pot industrial.
- Securización de MQTT (MOSQUITTO).
- Análisis Forense con Volatility.
- Maqueta securizada de una Smart Factory.
- Bus de Campo PROFINET securizado.

ANEXO II

Ciclos formativos que dan acceso a los cursos de especialización de Ciberseguridad en entornos de las tecnologías de operación establecido por Real Decreto 478/2020, de 7 de abril, y de Ciberseguridad en entornos de las tecnologías de la información establecido por el Real Decreto 479/2020, de 7 de abril

– Técnico Superior en Administración de Sistemas Informáticos en Red.
– Técnico Superior en Desarrollo de Aplicaciones Multiplataforma.
– Técnico Superior en Desarrollo de Aplicaciones Web.
– Técnico Superior en Sistemas de Telecomunicaciones e Informáticos.
– Técnico Superior en Mantenimiento Electrónico.
– Título de Técnico Superior en Sistemas Electrotécnicos y Automatizados.
– Título de Técnico Superior en Mecatrónica Industrial.
– Título de Técnico Superior en Automatización y Robótica Industrial.
– Título de Técnico Superior en Sistemas de Telecomunicaciones e Informáticos.

ANEXO III

Certificación de servicios prestados

D./D.ª ....., en calidad de Secretario/a del centro educativo ....., certifica que D./D.ª ....., con DNI ....., presta servicios como profesor/a en este centro durante el curso académico 2020/2021, impartiendo los módulos profesionales de ....., correspondientes al ciclo de grado superior ....., dentro de las enseñanzas de Formación Profesional del sistema educativo.

En ....., a .....

Firma del Secretario/a Sello del Centro V.º B.º Director/a.

cve: BOE-A-2021-3904
Verificable en https://www.boe.es