



**PROGRAMA FORMATIVO DE LA ESPECIALIDAD FORMATIVA
CIBERSEGURIDAD. SECTOR HOSTELERÍA
IFCT151PO**

PROGRAMAS DE FORMACIÓN DIRIGIDOS PRIORITARIAMENTE A TRABAJADORES OCUPADOS

5 de abril de 2018

**PROGRAMA DE LA ESPECIALIDAD FORMATIVA:
CIBERSEGURIDAD. SECTOR HOSTELERÍA**

DATOS GENERALES DE LA ESPECIALIDAD FORMATIVA

1. Familia Profesional: INFORMÁTICA Y COMUNICACIONES

Área Profesional: SISTEMAS Y TELEMÁTICA

2. Denominación: CIBERSEGURIDAD. SECTOR HOSTELERÍA

3. Código: **IFCT151PO**

4. Objetivo General: Utilizar el conjunto de herramientas, políticas, conceptos y salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios.

5. Número de participantes: -

6. Duración:

Horas totales: 150

Modalidad: Teleformación

Distribución de horas:

Presencial:..... 0

Teleformación:..... 150

7. Requisitos mínimos de espacios, instalaciones y equipamiento:

7.1 Espacio formativo:

Cada espacio estará equipado con mobiliario docente adecuado al número de alumnos, así mismo constará de las instalaciones y equipos de trabajo suficientes para el desarrollo del curso.

7.2 Equipamientos:

Se entregará a los participantes los manuales y el material didáctico necesarios para el adecuado desarrollo de la acción formativa

Las instalaciones y equipamientos deberán cumplir con la normativa industrial e higiénico sanitaria correspondiente y responderán a medidas de accesibilidad universal y seguridad de los participantes. En el caso de que la formación se dirija a personas con discapacidad se realizarán las adaptaciones y los ajustes razonables para asegurar su participación en condiciones de igualdad.

7.2.1 En el caso de formación en modalidad teleformación, se requiere el siguiente equipamiento:

Requisitos técnicos de la plataforma de teleformación y del contenido virtual de aprendizaje para especialidades formativas no dirigidas a la obtención de certificados de profesionalidad en la modalidad de teleformación

1. Requisitos técnicos de la plataforma de teleformación

La plataforma de teleformación que se utilice para impartir acciones formativas no conducentes a la obtención de certificados de profesionalidad deberá reunir los siguientes requisitos técnicos:

- Compatibilidad con los estándares SCORM e IMS.
- Rendimiento, entendido como número de alumnos que soporte la plataforma, velocidad de respuesta del servidor a los usuarios, y tiempo de carga de las páginas Web o de descarga de archivos, que permita:
- Soportar un número de alumnos equivalente al número total de participantes en las acciones formativas que esté impartiendo el centro o entidad de formación, garantizando un hospedaje mínimo igual al total del

alumnado de dichas acciones, considerando un número de usuarios concurrentes del 40% de ese alumnado.

- Disponer de la capacidad de transferencia necesaria para que no se produzca efecto retardo en la comunicación audiovisual en tiempo real, debiendo tener el servidor en el que se aloja la plataforma un ancho de banda mínimo de 100Mbps, suficiente en bajada y subida.
- Funcionamiento 24 horas al día, los 7 días de la semana.
- Compatibilidad tecnológica y posibilidades de integración con cualquier infraestructura informática o sistema operativo, base de datos, navegador de Internet de entre los más usuales o servidor web, debiendo ser posible utilizar las funciones de la plataforma con complementos (plug-in) y visualizadores compatibles. Si se requiriese la instalación adicional de algún soporte para funcionalidades avanzadas, la plataforma debe facilitar el acceso al mismo sin coste.
- Integración de herramientas y recursos necesarios para gestionar, administrar, organizar, diseñar, impartir y evaluar acciones formativas a través de Internet, disponiendo, específicamente, de las siguientes:

Herramientas que faciliten la colaboración y la comunicación entre todos los alumnos, tanto de carácter asíncrono (foros, tabloneros, correo, listas, etc.), como síncrono, (sistema de mensajería, chat, videoconferencia, etc.).

Herramientas de desarrollo, gestión e integración de contenidos.

Herramientas de seguimiento formativo, control del progreso del alumnado y evaluación del aprendizaje.

Herramientas de administración y gestión del alumnado y de la acción formativa.

- Disponer del desarrollo informático a través del cual el Servicio Público de Empleo de la Administración Competente, de manera automática, realice el seguimiento y control de las acciones formativas impartidas, conforme al modelo de datos y protocolo de transmisión establecidos en el anexo II y en la página web de dicho organismo, a fin de auditar la actividad de los centros y entidades de formación y evaluar la calidad de las acciones formativas.

Para poder realizar tal seguimiento, el Servicio Público de Empleo de la Administración Competente, con la periodicidad que determine, se conectará automáticamente con las plataformas de teleformación, por lo que las mismas deberán contar con los desarrollos informáticos que posibiliten tales acciones de seguimiento (protocolo de conexión SOAP).

Sin perjuicio de lo anterior, y de cara al seguimiento puntual de las acciones formativas de certificado de profesionalidad que se impartan, será preceptivo proporcionar al Servicio Público de Empleo de la Administración Competente una dirección (con sus correspondientes credenciales) de acceso a la plataforma, con permiso de administrador, pero sin posibilidad de modificar datos.

- Niveles de accesibilidad e interactividad que como mínimo cumplan las prioridades 1 y 2 de la Norma UNE 139803:2012 o posteriores actualizaciones, según lo estipulado en el Capítulo III del Real Decreto 1494/2007, de 12 de noviembre.

– El servidor de la plataforma de teleformación ha de cumplir con los requisitos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, por lo que el responsable de dicha plataforma ha de identificar la localización física del servidor y el cumplimiento de lo establecido sobre transferencias internacionales de datos en los artículos 33 y 34 de dicha Ley Orgánica y en el Título VI del Reglamento de desarrollo de la misma, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

- Incluir la imagen institucional del Servicio Público de Empleo de la Administración Competente y de las entidades que él designe, con las pautas de imagen corporativa que se establezcan.

– Disponibilidad de un servicio de atención a usuarios que proporcione soporte técnico y mantenga la infraestructura tecnológica y que, de forma estructurada y centralizada, atienda y resuelva las consultas e incidencias técnicas del alumnado. El servicio, que deberá estar disponible para el alumnado desde el inicio hasta la finalización de la acción formativa, deberá mantener un horario de funcionamiento de mañana y de tarde, tendrá que ser accesible mediante teléfono y mensajería electrónica y no podrá superar un tiempo de demora en la respuesta superior a 2 días laborables.

2. Requisitos técnicos del contenido virtual de aprendizaje.

Para garantizar la calidad del proceso de aprendizaje del alumnado, el contenido virtual de aprendizaje de las especialidades formativas no dirigidas a la obtención de certificados de profesionalidad mantendrá una estructura y funcionalidad homogénea, cumpliendo los siguientes requisitos:

- Como mínimo, ser los establecidos en el correspondiente programa formativo que conste en el fichero de especialidades formativas previsto en el artículo 20.3 del Real Decreto 395/2007, de 23 de marzo y esté asociado a la especialidad formativa para la que se solicita inscripción.
- Estar referidos tanto a los conocimientos como a las destrezas prácticas y habilidades recogidas en los objetivos de aprendizaje de los citados programas formativos, de manera que en su conjunto permitan conseguir los resultados de aprendizaje previstos.
- Organizarse a través de índices, mapas, tablas de contenido, esquemas, epígrafes o titulares de fácil discriminación y secuenciarse pedagógicamente de tal manera que permitan su comprensión y retención.
- No ser meramente informativos, promoviendo su aplicación práctica a través de actividades de aprendizaje (autoevaluables o valoradas por el tutor-formador) relevantes para la práctica profesional, que sirvan para verificar el progreso del aprendizaje del alumnado, hacer un seguimiento de sus dificultades de aprendizaje y prestarle el apoyo adecuado.
- No ser exclusivamente textuales, incluyendo variados recursos (necesarios y relevantes), tanto estáticos como interactivos (imágenes, gráficos, audio, vídeo, animaciones, enlaces, simulaciones, artículos, foro, chat, etc.) de forma periódica.
- Poder ser ampliados o complementados mediante diferentes recursos adicionales a los que el alumnado

pueda acceder y consultar a voluntad.

– Dar lugar a resúmenes o síntesis y a glosarios que identifiquen y definan los términos o vocablos básicos, relevantes o claves para la comprensión de los aprendizajes.

– Evaluar su adquisición durante o a la finalización de la acción formativa a través de actividades de evaluación (ejercicios, preguntas, trabajos, problemas, casos, pruebas, etc.), que permitan medir el rendimiento o desempeño del alumnado.

8. Requisitos necesarios para el ejercicio profesional:

(Este epígrafe sólo se cumplimentará si existen requisitos legales para el ejercicio de la profesión)

9. Requisitos oficiales de los centros:

(Este epígrafe sólo se cumplimentará si para la impartición de la formación existe algún requisito de homologación / autorización del centro por parte de otra administración competente.

10. CONTENIDOS FORMATIVOS:

1. CONCEPTOS BÁSICOS DE CIBERSEGURIDAD

1.1. El valor de la información

1.2. Hackers y ciberdelincuentes

1.3. Seguridad por defecto

1.4. Políticas y procedimientos

1.5. Delitos informáticos

1.6. Código de derecho de ciberseguridad

2. AMENAZAS, VULNERABILIDADES Y RIESGOS

2.1. Tipos de Amenazas.

2.2. Tipos de vulnerabilidades.

2.3. Vulnerabilidades de IoT

2.4. Ingeniería Social

2.5. Malware

2.6. Virus

2.7. Troyanos

2.8. Gusanos

2.9. Spyware

2.10. Ransomware

2.11. PUPs

2.12. Key Loggers

2.13. Bots.

3. ATAQUES A CREDENCIALES

3.1. Demostración práctica del robo de credenciales de usuario

3.2. Almacenamiento de credenciales

3.3. Passwords en Windows

3.4. Credenciales en caché

3.5. Contramedidas

4. DOS/DDOS

4.1. Características

4.2. Motivación

4.3. Víctimas

4.4. Ejemplos

4.5. Contramedidas

5. OTROS RIESGOS

5.1. Webcam

5.2. Estafas telefónicas

5.3. Dispositivos USB

5.4. Seguridad física

6. MEJORAR LA SEGURIDAD. PARTE I

6.1. Password

6.2. Ataques por e-mail (pishing)

6.3. Seguridad en el navegador

6.4. Seguridad Wireless

6.5. VPN

6.6. Seguridad DNS

6.7. Usuarios predeterminados

6.8. Actualizaciones

6.9. Antivirus

6.10. Firewalls (cortafuegos)

6.11. Sentido Común

7. MEJORAR LA SEGURIDAD. PARTE II

7.1. Seguridad por defecto y/o por diseño

7.2. Sistemas actualizados

7.3. Control de accesos

7.4. Gestión segura de contraseñas

7.5. Antimalware.

- 7.6. El correo electrónico
- 7.7. Navegación Segura
- 7.8. Aplicaciones de confianza.
- 7.9. Copias de seguridad
- 7.10. Destrucción segura
- 7.11. Necesidades específicas en IoT
- 7.12. Necesidades específicas en Cloud.
- 7.13. Sistemas operativos de confianza (TOS)
- 8. REACCIÓN FRENTE UN INCIDENTE
- 8.1. Detección
- 8.2. Análisis
- 8.3. Evaluación
- 8.4. Clasificación de los incidentes de seguridad
- 8.5. Priorización
- 8.6. Reacción