MINISTERIO DE TRABAJO, MIGRACIONES Y SEGURIDAD SOCIAL

SERVICIO PÚBLICO DE EMPLEO ESTATAL

FONDO SOCIAL EUROPEO
"El FSE invierte en tu futuro"

PROGRAMA FORMATIVO DE LA ESPECIALIDAD FORMATIVA

GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA

IFCT050PO

PROGRAMAS DE FORMACIÓN DIRIGIDOS PRIORITARIAMENTE A TRABAJADORES OCUPADOS

Noviembre 2018

PROGRAMA DE LA ESPECIALIDAD FORMATIVA:

GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA

DATOS GENERALES DE LA ESPECIALIDAD FORMATIVA

1. Familia Profesional: INFORMÁTICA Y COMUNICACIONES

Área Profesional: SISTEMAS Y TELEMÁTICA

2. Denominación: GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA

3. Código: **IFCT050PO**

4. Objetivo General: Gestionar la seguridad informática en la empresa.

5. Número de participantes: Según normativa, el número máximo de participantes en modalidad presencial es de 30.

6. Duración:

Horas totales: 100 Modalidad: Indistinta

Distribución de horas:

Presencial:..... 100

Teleformación:..... 100

7. Requisitos mínimos de espacios, instalaciones y equipamiento:

7.1 Espacio formativo:

AULA POLIVALENTE:
El aula contará con las instalaciones y equipos de trabajo suficientes para el desarrollo de la acción formativa.
• Superficie: El aula deberá contar con un mínimo de 2m2 por alumno.
• Iluminación: luz natural y artificial que cumpla los niveles mínimos preceptivos.
• Ventilación: Climatización apropiada.
• Acondicionamiento eléctrico de acuerdo a las Normas Electrotécnicas de Baja Tensión y otras normas de aplicación.
• Aseos y servicios higiénicos sanitarios en número adecuado.
• Condiciones higiénicas, acústicas y de habitabilidad y seguridad, exigidas por la legislación vigente.
• Adaptabilidad: en el caso de que la formación se dirija a personas con discapacidad dispondrá de las adaptaciones y los ajustes razonables para asegurar la participación en condiciones de igualdad.
• PRL: cumple con los requisitos exigidos en materia de prevención de riesgos laborales

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 contará con todos los medios y materiales necesarios para el correcto desarrollo formativo.

- Pizarra.
- Rotafolios.
- Material de aula.
- Medios audivisuales.
- Mesa y silla para formador/a.
- Mesas y sillas para alumnos/as.
- Hardware y Software necesarios para la impartición de la formación.
- Conexión a Internet.

En su caso, equipamiento específico necesario para el desarrollo de la acción formativa:

–Periféricos y dispositivos multimedia.

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, tablones, 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 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 cumplimento 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 secuenciase pedagógicamente de tal manera que permiten 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, video, 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. INTRODUCCIÓN A LA SEGURIDAD
1.1. Introducción a la seguridad de información.
1.2. Modelo de ciclo de vida de la seguridad de la información.
1.3. Confidencialidad, integridad y disponibilidad. Principios de protección de la seguridad de la información.
1.4. Políticas de seguridad.
1.5. Tácticas de ataque.
1.6. Concepto de hacking.
1.7. Árbol de ataque.
1.8. Lista de amenazas para la seguridad de la información.
1.9. Vulnerabilidades.
1.10. Vulnerabilidades en sistemas Windows.
1.11. Vulnerabilidades en aplicaciones multiplataforma.
1.12. Vulnerabilidades en sistemas Unix y Mac OS.
1.13. Buenas prácticas y salvaguardas para la seguridad de la red.
1.14. Recomendaciones para la seguridad de su red.

2. POLÍTICAS DE SEGURIDAD.
2.1. Introducción a las políticas de seguridad.
2.2. ¿Por qué son importantes las políticas?
2.3. Qué debe de contener una política de seguridad.
2.4. Lo que no debe contener una política de seguridad.
2.5. Cómo conformar una política de seguridad informática.
2.6. Hacer que se cumplan las decisiones sobre estrategia y políticas.

3. AUDITORIA Y NORMATIVA DE SEGURIDAD.
3.1. Introducción a la auditoría de seguridad de la información y a los sistemas de gestión de seguridad de la información.
3.2. Ciclo del sistema de gestión de seguridad de la información.
3.3. Seguridad de la información.
3.4. Definiciones y clasificación de los activos.
3.5. Seguridad humana, seguridad física y del entorno.
3.6. Gestión de comunicaciones y operaciones.
3.7. Control de accesos.

3.8. Gestión de continuidad del negocio.
3.9. Conformidad y legalidad.

4. ESTRATEGIAS DE SEGURIDAD.
4.1. Menor privilegio.
4.2. Defensa en profundidad.
4.3. Punto de choque.
4.4. El eslabón más débil.
4.5. Postura de fallo seguro.
4.6. Postura de negación establecida: lo que no está prohibido.
4.7. Postura de permiso establecido: lo que no está permitido.
4.8. Participación universal.
4.9. Diversificación de la defensa.
4.10. Simplicidad.

5. EXPLORACIÓN DE LAS REDES.
5.1. Exploración de la red.
5.2. Inventario de una red. Herramientas del reconocimiento.
5.3. NMAP Y SCANLINE.
5.4. Reconocimiento. Limitar y explorar.
5.5. Reconocimiento. Exploración.
5.6. Reconocimiento. Enumerar.

6. ATAQUES REMOTOS Y LOCALES.
6.1. Clasificación de los ataques.
6.2. Ataques remotos en UNIX.
6.3. Ataques remotos sobre servicios inseguros en UNIX.
6.4. Ataques locales en UNIX.
6.5. ¿Qué hacer si recibimos un ataque?

7. SEGURIDAD EN REDES ILANÁMBRICAS
7.1. Introducción.
7.2. Introducción al estándar inalámbrico 802.11 – WIFI
7.3. Topologías.
7.4. Seguridad en redes Wireless. Redes abiertas.
7.5. WEP.
7.6. WEP. Ataques.
7.7. Otros mecanismos de cifrado.

8. CRIPTOGRAFÍA Y CRIPTOANÁLISIS.
8.1. Criptografía y criptoanálisis: introducción y definición.
8.2. Cifrado y descifrado.
8.3. Ejemplo de cifrado: relleno de una sola vez y criptografía clásica.
8.4. Ejemplo de cifrado: criptografía moderna.
8.5. Comentarios sobre claves públicas y privadas: sesiones.

9. AUTENTICACIÓN.
9.1. Validación de identificación en redes.
9.2. Validación de identificación en redes: métodos de autenticación.
9.3. Validación de identificación basada en clave secreta compartida: protocolo.
9.4. Establecimiento de una clave compartida: intercambio de claves Diffie-Hellman.
9.5. Validación de identificación usando un centro de distribución de claves.
9.6. Protocolo de autenticación Kerberos.
9.7. Validación de identificación de clave pública.
9.8. Validación de identificación de clave pública: protocolo de interbloqueo.