MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL

SERVICIO PÚBLICO DE EMPLEO ESTATAL SEPE

FONDO SOCIAL EUROPEO
El FSE invierte en tu futuro

PROGRAMA FORMATIVO

SEGURIDAD EN SISTEMAS INFORMÁTICOS CON IBM

Marzo 2021

DATOS GENERALES DEL CURSO

1. Familia Profesional: INFORMÁTICA Y COMUNICACIONES (IFC)

Área Profesional: SISTEMAS Y TELEMÁTICA

2. Denominación: SEGURIDAD EN SISTEMAS INFORMÁTICOS CON IBM

3. Código: IFCT31

4. Nivel de cualificación: 3

5. Objetivo general:

Administrar la seguridad de la empresa en los entornos TI con los diferentes productos de IBM, habilitando acciones programadas para la gestión centralizada de perfiles de usuarios, acceso a aplicaciones, eventos de seguridad y detectores de intrusiones y amenazas (tanto internas como externas) para evitar daños en los sistemas informáticos y robo de datos confidenciales.

6. Prescripción de los formadores:

6.1. Titulación requerida:

Titulación universitaria u otros títulos equivalentes, o capacitación profesional equivalente acreditada por el fabricante.

6.2. Experiencia profesional requerida:

El formador deberá estar homologado como instructor en la correspondiente especialidad de la tecnología específica del fabricante y contar con las certificaciones vigentes.

Tener experiencia acreditable de al menos 12 meses en la ocupación relacionada con la especialidad.

6.3. Competencia docente:

Será necesario tener experiencia metodológica o experiencia docente. Los formadores deberán contar con formación metodológica, o experiencia docente contrastada superior a 800 horas, durante los dos últimos años, relacionadas con la familia de Informática y Comunicaciones.

7. Criterios de acceso del alumnado:

7.1. Nivel académico o de conocimientos generales:

Título de FP Grado superior en informática.

Cuando el aspirante al curso no posea el nivel académico indicado, demostrará conocimientos suficientes a través de una prueba de acceso.

Se requiere inglés a nivel de lectura y conocimientos en administración y seguridad de sistemas informáticos.
Todos los aspirantes al curso deberán demostrar sus conocimientos a través de una prueba de nivel

8. Número de alumnos:

Máximo 25 participantes para cursos presenciales.

9. Relación secuencial de módulos:

- Módulo 1: Fundamentos de Seguridad en IT .
- Módulo 2: Administración del IBM Security Directory Server.
- Módulo 3: Gestión de accesos IT con ISAM.
- Módulo 4: Gestión de identidades IT con ISIM.
- Módulo 5: Gestión de la información y eventos de seguridad con QRADAR.
- Módulo 6: Gestión de Sistemas de protección de bases de datos de IBM(Guardium).

10. Duración:

Horas totales: 255 horas

Distribución horas:

- Presencial: 255 horas
- Teleformación: 0 horas
- A distancia convencional: 0 horas

11. Requisitos mínimos de espacios, instalaciones y equipamiento.

11.1. Espacio formativo:

- Aula de Informática: Superficie: 45 m^2 para grupos de 15 alumnos (3 m^2 por alumno).

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.

11.2. Equipamiento:

Los equipos tendrán unas características equivalentes a las enumeradas a continuación, consideradas siempre como mínimas:

- 16 ordenadores (15 alumnos y 1 profesor) con las siguientes características mínimas:
  - Procesador Intel Pentium D 3,2 GHz
  - 16 GB de RAM
  - Disco duro SATA 160 GB
  - Tarjeta de red 10/100/1000 Mbps
  - Tarjeta gráfica 256 Mb. PCIe
  - Tarjeta de sonido
  - Lector grabador de DVD
  - Teclado
  - Ratón
  - Monitor color 17”
- Impresora laser con conexión a red.
- Software específico del fabricante para la impartición del curso: Las licencias de los productos estarán disponibles por parte del GTP. Sólo las Familias de Productos de Software IBM especificadas en la Propuesta para las cuales el GTP ha obtenido las licencias apropiadas a partir de la Fecha de Inicio del Servicio están cubiertas bajo la misma.
- 16 licencias de Sistema Operativo: Windows 7 (64-bit) o similar
- 1 Licencia de Sistema Operativo de Red.
- Acceso a Internet
- 16 licencias del software ofimático necesario para la impartición del curso.
- 16 licencias de servidor de un software antivirus.
- Pantalla y cañón de proyección.

A los alumnos se le proporcionará la documentación oficial de IBM necesaria para la impartición del curso.

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.

12. Evaluación del aprendizaje

Se llevará a cabo una evaluación continua y sistemática durante el proceso de aprendizaje y al final del mismo para comprobar si los alumnos han alcanzado los objetivos establecidos en cada módulo y, por consiguiente, han realizado el curso con el aprovechamiento requerido.

13. Certificación oficial del fabricante

La ejecución y financiación del programa formativo incluye la presentación de los alumnos que han realizado el curso con aprovechamiento a los exámenes para obtener la certificación oficial del fabricante, que gestionará el centro y que en ningún caso supondrá coste alguno para el alumno.

En concreto, para esta acción formativa estan vinculados los siguientes exámenes de certificación oficial de IBM, o los que los sustituyan y estén vigentes en el momento de su impartición.

- C1000-026 - IBM Security QRadar SIEM V7.3.2 Fundamental AdministrationTest
- C2150-609 - IBM Security Access Manager V9.0 Deployment
- C2150-606 IBM Certified Administrator - Security Guardium V10.0

14. Requisitos oficiales de los centros

El centro deberá acreditar que se encuentra autorizado por el fabricante para poder impartir adecuadamente cursos de formación con certificación oficial del mismo. Para la impartición de esta especialidad formativa el Centro ha de ser un GTP (Global Training Providers) de IBM o un partner de un GTP.

MÓDULOS FORMATIVOS

Módulo nº 1

Denominación: FUNDAMENTOS DE SEGURIDAD EN IT

Objetivo: Conocer la terminología y fundamentos básicos de la seguridad, así como las diferentes herramientas y protocolos.

Duración: 20 horas.

Contenidos teórico-prácticos:

- Conceptos generales de seguridad.
- Shell Linux.
- TCP/IP. Análisis de los diferentes Logs y su monitorización.
- Ataques web y ataques de “fuerza bruta”.
- Uso de SE - Linux y otras herramientas.

Módulo nº 2

Denominación: ADMINISTRACIÓN DEL IBM SECURITY DIRECTORY SERVER

Objetivo: Gestionar y administrar el IBM Directory Server para un rápido desarrollo y despliegue de aplicaciones Web, incluyendo funciones de gestión, replicación y seguridad.

Duración: 30 horas

Contenidos teórico-prácticos:

- Introducción.
- Conceptos y gestión de datos de directorio
- Seguridad
- Directorios distribuidos
- Actuación
- Determinación de problemas

Módulo nº 3

Denominación: GESTIÓN DE ACCESOS IT CON ISAM

Objetivo: Gestionar el ISAM (anteriormente llamado, IBM Tivoli Access Manager, para e-business), solución de autenticación de registro de usuario escalable y centralizado tanto en autorización como de la web; incluyendo la parte del ISAM para móviles aplicando políticas de acceso para la web y aplicaciones móviles

Duración: 45 horas

Contenidos teórico-prácticos:

- Propósito y componentes de IBM Security Access Manager para Web
- Uso del dispositivo Web Gateway
- Autenticación y autorización de proxy inverso
- Creación de usuarios, grupos, listas de control de acceso y directivas de objetos protegidos
- Introduction a Security Access Manager for Mobile
- Instalación de Security Access Manager para dispositivos virtuales móviles
- Configuración de Security Access Manager para dispositivos virtuales móviles
- Creación de políticas de acceso
- Configuración de la seguridad móvil
- Creación de directivas de acceso basadas en el contexto.

Módulo nº 4

Denominación: GESTIÓN DE IDENTIDADES IT CON ISIM

Objetivo: Gestionar las identidades dentro de una compañía, utilizando para ello la solución propuesta por IBM, ISIM (IBM Security Identity Manager).

Duración: 40 horas

Contenidos teórico-prácticos:

- Introducción a IBM Security Identity Manager 6.0
- Planificación de una implementación de IBM Security Identity Manager
- Instalación de IBM Security Identity Manager 6.0
- Gestión de la organización
- Gestión de usuarios y gestión de roles
- Alimentos de identidad
- Servicios y políticas.
- Recursos de aprovisionamiento
- Flujos de trabajo.
- Control de acceso
- Gestión del ciclo de vida
- Auditoría e informes
- Personalización
- Determinación de problemas.

Módulo nº 5

Denominación: GESTIÓN DE LA INFORMACIÓN Y LOS EVENTOS DE SEGURIDAD CON QRADAR

Duración: 65 horas

Objetivo: Instalar y gestionar el programa QRadar SIEM.

Contenidos teórico-prácticos:

- Introducción a IBM Security QRadar SIEM
- Cómo QRadar SIEM recopila datos de seguridad
- Utilización del panel QRadar SIEM
- Investigación de un delito que es provocado por eventos
- Investigar los hechos de un delito
- Uso de perfiles de activos para investigar los delitos
- Investigación de un delito que es provocado por flujos
- Uso de reglas y bloques de construcción
- Creación de informes QRadar SIEM
- Realización de filtrado avanzado
- Uso de tolos administrativos.
- Creación de la jerarquía de red
- Herramientas de administración actualizadas
- Administrar usuarios
- Gestión de datos
- Recopilación de registros y registros de flujo
- Recopilación de registros de registro de Windows
- Gestión de fuentes de registro personalizadas
- Uso de reglas
- Creación de reglas
- Gestión de falsos positivos
- Uso de Reference Maps en las reglas.
- Introducción a IBM Security Network Protection.
- Instalación y Gestión del aparato.
- Configuración de la directiva de acceso a la red.
- Configuración de la política de prevención de intrusiones.

- Uso de alertas y eventos.
- Ajuste de reglas de política de acceso a redes y comportamiento de prevención de intrusiones.
- Captura de tráfico de red.
- Control del acceso de usuarios.
- Inspeccionar el tráfico cifrado SSL.
- Implementación de reglas SNORT.
- Configuración de la protección avanzada contra amenazas.
- Integración con QRadar SIEM.
- Supervisión de los datos del evento.

Módulo nº 6

Denominación: GESTIÓN DE SISTEMAS DE PROTECCIÓN DE BASES DE DATOS DE IBM (GUARDIUM)

Duración: 55 horas

Objetivo: Configurar Guardium V11, para descubrir, clasificar, analizar, proteger y controlar el acceso a datos confidenciales, evaluando vulnerabilidades y supervisando la actividad de los datos y archivos.Crear informes, auditorías, alertas, métricas y procesos de supervisión del cumplimiento de la política de seguridad de la empresa.

Contenidos teórico-prácticos:

- Guardium: Introducción y Arquitectura.
- Interfaz de usuario y gestión de accesos.
- Gestión de Grupos.
- Vista del sistema y gestión de datos
- Gestión de políticas
- Auditoría, Descubrimiento y Evaluación de vulnerabilidades.
- Consultas e informes personalizados
- Automatización del flujo de trabajo para el cumplimiento de las políticas de seguridad.
- Monitoreo de la actividad de archivos.