

(IFCT050PO) Gestión de la seguridad informática en la empresa



Área: Formación en tecnologías de la información y comunicación

Modalidad: Teleformación

Duración: 80 h

Precio: 600.00€

[Curso Bonificable](#)

[Contactar](#)

[Recomendar](#)

 [Tienda online](#)

[Matricularme](#)

OBJETIVOS

1. Gestionar la seguridad informática en la empresa.

OBJETIVOS ESPECÍFICOS

1. Aprender los principios y el ciclo de vida de la seguridad de la información.
2. Conocer las políticas de seguridad y las tácticas de ataque.
3. Saber qué es un hacker y un árbol de ataque.
4. Conocer las amenazas y vulnerabilidades de seguridad típicas.
5. Reflexionar sobre las buenas prácticas, las salvaguardas y las recomendaciones para la seguridad de red.
6. Conocer la importancia de las políticas de seguridad.
7. Saber qué debe contener una política de seguridad.
8. Aprender lo que no debe contener una política de seguridad.
9. Aprender a conformar una política de seguridad.
10. Reflexionar sobre la importancia de que se cumplan las decisiones sobre estrategia y políticas.
11. Saber qué es un sistema de gestión de seguridad de la información (SGSI).
12. Aprender el ciclo de mejora continua de un SGSI.
13. Conocer los activos de seguridad de un SGSI.
14. Aprender los controles más importantes de un SGSI.
15. Conocer las estrategias de seguridad más utilizadas.
16. Aprender qué es una red informática.
17. Saber realizar un inventario de red.
18. Conocer la exploración y el reconocimiento de red.
19. Aprender a limitar las posibilidades de éxito de un hacker.
20. Conocer cómo se realiza una evaluación de seguridad.
21. Aprender la clasificación de los ciberataques.
22. Conocer los ciberataques remotos y los locales.
23. Saber qué hacer ante un ciberataque.
24. Conocer el estándar 802.11 y sus topologías.
25. Reflexionar sobre la seguridad en las redes inalámbricas abiertas.

EMAIL: info@mferrerconsultores.com

TELÉFONO: 635952170

<https://www.mferrerconsultores.com>

26. Conocer los mecanismos de cifrado y las vulnerabilidades de estos.
27. Conocer la criptografía y el criptoanálisis.
28. Aprender qué es el cifrado y el descifrado.
29. Conocer el cifrado de una sola vez y la criptografía clásica.
30. Conocer la criptografía moderna.
31. Reflexionar sobre claves públicas, privadas y sesiones.
32. Conocer la validación de identificación en redes.
33. Aprender los métodos de autenticación básicos.
34. Conocer el intercambio de claves Diffie-Hellman.
35. Aprender qué es un centro de distribución de claves y Kerberos.
36. Conocer la validación de identificación de clave pública y el protocolo de interbloqueo.

CONTENIDOS

Unidad 1: Introducción a la seguridad.
Unidad 2: Políticas de seguridad.
Unidad 4: Estrategias de seguridad.
Unidad 5: Exploración de las redes.
Unidad 6: Ataques remotos y locales.
Unidad 7: Seguridad en redes inalámbricas.
Unidad 8: Criptografía y criptoanálisis.
Unidad 9: Autenticación.

MATERIALES

Toda la documentación necesaria para la realización del curso se encuentra en la plataforma de teleformación pero se entregarán documentación de ayuda y complementaria al alumno si el formador así lo requiere.

METODOLOGIA

La actividad tutorial será bidireccional, es decir, tanto el alumno se puede poner en contacto con el tutor para solventar dudas o dificultades como el tutor con el alumno para establecer un contacto directo con él, comprobar su nivel de progreso en el estudio, su grado de motivación y su situación personal en relación con su participación en la acción formativa.

Las características de la metodología de este tipo de acciones formativas son:

Total libertad de horarios para realizar el curso desde cualquier ordenador con conexión a Internet, **sin importar el sitio desde el que lo haga**. Puede comenzar la sesión en el momento del día que le sea más conveniente y dedicar el tiempo de estudio que estime más oportuno.

En todo momento contará con un **asesoramiento de un tutor personalizado** que le guiará en su proceso de aprendizaje, ayudándole a conseguir los objetivos establecidos.

Hacer para aprender, el alumno no debe ser pasivo respecto al material suministrado sino que debe participar, elaborando soluciones para los ejercicios propuestos e interactuando, de forma controlada, con el resto de usuarios.

EMAIL: info@mferrerconsultores.com

TELÉFONO: 635952170

<https://www.mferrerconsultores.com>



El aprendizaje se realiza de una manera amena y distendida. Para ello el tutor se comunica con su alumno y lo motiva a participar activamente en su proceso formativo. Va controlando su progreso a través de diversos ejercicios como por ejemplo test de autoevaluación.

Los contenidos del curso se actualizan para que siempre respondan a las necesidades reales del mercado. El departamento multimedia incorpora gráficos, imágenes, videos, sonidos y elementos interactivos que complementan el aprendizaje del alumno ayudándole a finalizar el curso con éxito.

REQUISITOS

Los requisitos técnicos mínimos son:

Navegador Microsoft Internet Explorer 5.5 o superior, con plugin de Flash, cookies y JavaScript habilitados.

No se garantiza su óptimo funcionamiento en otros navegadores como Firefox, Netscape, Mozilla, etc.

Resolución de pantalla de 800x600 y 16 bits de color o superior.

Procesador Pentium II a 300 Mhz o superior.

32 Mbytes de RAM o superior.

CONTROLES APRENDIZAJE

Se llevará a cabo una **evaluación continua**, con el seguimiento a través de las tutorías que van haciendo los profesores, para comprobar si ha habido un aprovechamiento real del curso. Para ello, el alumnado deberá realizar todos los ejercicios que acompañan a los contenidos del curso (evaluaciones, autoevaluaciones, cuestionarios, ejercicios prácticos, etc.) para evaluar que van consiguiendo los contenidos adecuados.

De igual modo, se realizará una **evaluación final**, donde el alumno deberá de responder adecuadamente al examen de evaluación final que será corregido automáticamente una vez realizado.

Plazos de realización:

Evaluación continua: con objeto de garantizar el máximo aprovechamiento del curso, se recomienda al alumnado que entregue los ejercicios prácticos, autoevaluaciones, cuestionarios a lo largo del curso.

Evaluación final: se recomienda que se realice una vez finalizado todo el curso, es decir, el último día del mismo, para poder responder adecuadamente a las preguntas que se indiquen.

Evaluación continua: durante todos los días del curso.

Evaluación final: un día después de la finalización del curso.

EMAIL: info@mferrerconsultores.com

TELÉFONO: 635952170

<https://www.mferrerconsultores.com>