Consultoría
Formación
Innovación

Usuario Seguro de Sistemas Informáticos

"Una formación imprescindible para utilizar sistemas informáticos e Internet de forma segura"

Incluye material de referencia en formato papel

PIDE MÁS INFORMACIÓN

info@grupocfi.es
www.formacioncfi.es

Usuario Seguro de Sistemas Informáticos

La tecnología e Internet se han convertido en herramientas imprescindibles para los trabajadores de cualquier empresa, independientemente de su tamaño o actividad.

Sin embargo, cada ordenador, cada tableta y cada móvil en la entidad es un vector de riesgo si el usuario que lo utiliza no conoce los riesgos que existen en Internet y cómo protegerse de ellos.

Cada vez se producen más delitos en Internet (ciberdelitos) que afectan tanto a los usuarios como a las empresas (fraudes, estafas, robo de datos y de dinero, etc.). En todos ellos existe un elemento común: un usuario que no ha sido formado adecuadamente.

Este curso va a capacitar al trabajador para que utilice de forma segura los sistemas y dispositivos informáticos de la empresa, así como los servicios disponibles en Internet (correo, navegación, etc.).

¿A quien va dirigido?

A directivos, mandos intermedios y profesionales que utilizan ordenadores, tabletas o móviles y acceden a Internet.

Requisitos previos
Ninguno

Forma y lugar de impartición
Online

Duración
60 horas

Titulación
Usuario Seguro de Sistemas Informáticos

¿Qué vas a aprender?

En este curso te enseñamos, de forma muy sencilla y con un lenguaje comprensible los riesgos que existen en los dispositivos tecnológicos y en Internet, así como a protegerte de ellos.

En concreto, aprenderás:

- Las amenazas y riesgos que existen en Internet y cómo protegerte de ellos
- A trabajar con ordenadores, tabletas y móviles de forma segura.
- Cómo manejar y proteger los datos personales.
- Las técnicas de ingeniería social y engaños más comunes.

Al finalizar este curso, el usuario estará formado para utilizar de forma segura ordenadores, tabletas y smartphones así como los servicios de Internet (navegación, correo, buscadores, etc.).

Métodología

Este curso es totalmente Online basado en vídeos. A través de vídeos el formador transmite sus conocimientos al alumno de forma dinámica y eficiente.

¡Bienvenido a la formación audiovisual interactiva!

Formación en vídeos

Dentro del aula de teleformación el alumno accede a las decenas de vídeos que componen el curso y a través de los cuáles el formador desarrolla su contenido. Esta es la forma más eficiente de impartir formación online, puesto que el alumno puede ver el vídeo las veces que desee hasta comprender lo explicado.

También se dispone de material descargable en otros formatos, como PDF o Word.

Aula de teleformación

Disponemos de un completo aula de teleformación en Internet a través del cuál el alumno realiza el curso, sigue su evolución, realiza consultas al tutor, etc.

Este aula es totalmente compatible con PC, Mac, tabletas y dispositivos móviles que dispongan de conexión a Internet.

Material didáctico

Una vez matriculado, el alumno recibirá en su domicilio el material didáctico en soporte papel.

Tutorización

El alumno está en todo momento acompañado por su tutor, que seguirá la evolución de su aprendizaje y resolverá las dudas que se le planteen.

Temario

El contenido del curso está repartio en 12 módulos de aprendizaje:

1. **Fundamentos de la Ciberseguridad.** Usuarios, terminología y tipos de ataques.
2. **Seguridad en el Sistema Operativo.** Vulnerabilidades, ataques de configuración, contraseñas y seguridad Física.
3. **Código Malicioso.** Virus, gusanos, troyanos y rootkits. Como detectarlos y eliminarlos.
4. **Seguridad en las Redes Wifi.** Seguridad y amenazas.
5. **Seguridad en la navegación.** Transacciones online, Cookies y Privacidad.
6. **Seguridad en el Correo Electrónico.** Spam, phishing, envío de datos sensibles por email, etc.
7. **Seguridad en los dispositivos móviles.** Instalación de App´s, vulnerabilidades, privacidad y seguridad.
8. **Otras Amenazas en Internet.** Redes Sociales, P2P, buscadores y servicios en la nube.
9. **Ingeniería Social y Robo de Identidad.** Técnicas de ingeniería social basadas en humanos y máquinas.
10. **Copias de Seguridad y Recuperación de Datos.** Planificación y recuperación de datos.
11. **Cifrado de Datos.** Tipos de Herramientas para cifrar.
12. **Seguridad y Datos Personales.** Medidas de seguridad, niveles y principios.

Los módulos incluyen ejercicios y cuestionarios de autoevaluación

opiniones

"Me ha parecido muy creativa la forma de impartir el curso. Divertido y dinámico"

María Isabel Tejo. Madrid

"Me parace muy bueno el método utilizado y las herramientas"

Manuel Joarex. Valencia

"Una formación muy práctica y útil"

Guillermo Marco. Valencia

Temario detallado

1. Fundamentos de la ciberseguridad

1.1 Los usuarios y los sistemas de información.
1.2 Terminología empleada.
1.3 Elementos de la seguridad de la información.
1.4 Amenazas y retos en la seguridad de la información.
1.5 Los hackers y sus efectos.
1.6 Tipos de ataques.

2. Seguridad en el sistema operativo

2.1 El sistema operativo.
2.2 Vulnerabilidades y parcheo del sistema operativo.
2.3 Ataques por mala configuración.
2.4 Contraseñas.
2.5 Seguridad física.

3. Codigo malicioso

3.1 El código malicioso.
3.2 Virus y gusanos.
3.3 Troyanos.
3.4 Rootkits.
3.5 Detección del código malicioso.
3.6 Recomendaciones de seguridad.

4. Seguridad en las redes wifi

4.1 Redes wifi.
4.2 Proceso de asociación a una red wifi.
4.3 Seguridad en las redes wifi.
4.4 Amenazas para las redes wifi.
4.5 Buetooth y amenazas.

5. Seguridad en la navegación

5.1 La navegación por Internet.
5.2 Vulnerabilidades y descarga de ficheros.
5.3 Datos personales.
5.4 Cookies y privacidad.
5.5 Seguridad en las transacciones online.
5.6 Recomendaciones de seguridad.

6. Seguridad en el correo electrónico

6.1 El correo electrónico.
6.2 Código malicioso en el correo electrónico.
6.3 Spam.
6.4 Phising.
6.5 Envío de datos sensibles por email.

7. Seguridad en los dispositivos móviles

7.1 Las plataformas móviles.
7.2 Vulnerabilidades.
7.3 Privacidad.
7.4 Seguridad.
7.5 Instalación de Apps.
7.6 Recomendaciones de seguridad.

8. Otras amenazas en internet

8.1 Las redes sociales.
8.2 Las redes P2P.
8.3 Los buscadores.
8.4 Servicios en la nube.
8.5 La responsabilidad de los usuarios.

9. Ingenieria social y robo de identidad

9.1 La ingeniería social.
9.2 Técnicas basadas en humanos.
9.3 Técnicas basadas en máquinas.
9.4 El robo de identidad.
9.5 Problemas de la ingeniería social.
9.6 Recomendaciones de seguridad.

10. Copias de seguridad y recuperación de datos

10.1 Las copias de seguridad.
10.2 Copias de seguridad locales.
10.3 Copias de seguridad online.
10.4 Planificación de las copias de seguridad.
10.5 Restaurado de los datos.
10.6 Recomendaciones de seguridad.

11. Cifrado de datos

11.1 El cifrado de datos.
11.2 Tipos de cifrado.
11.3 Cifrado de discos y archivos.
11.4 Cifrado de comunicaciones.
11.5 Firma digital.
11.6 Ataques al cifrado.

12. Seguridad y datos personales

12.1 Los datos personales.
12.2 Principios de la protección de datos personales.
12.3 Los derechos ARCO.
12.4 Niveles de seguridad.
12.5 Medidas de seguridad para ficheros automatizados.
12.6 Medidas de seguridad para fichero manuales.

Autor del curso

JULIO CÉSAR MIGUEL PÉREZ

Emprendedor y Experto en Privacidad y Ciberseguridad

EXTRACTO DE SU FORMACIÓN

Computer Hacking Forensic Investigador by EC-Council (CHFI)

EC-Council Certified Security Analyst (ECSA)

Certified Ethical Hacker by EC-Council (CEH)

APEP Certified Privacy (ACP). Consultor Perfil Tecnológico y Jurídico

Experto en Seguridad de la Información por AENOR

Auditor de Sistemas de Gestión de Seguridad de la Información por AENOR (ISO 27001)

Especialista Implantador de Sistemas de Gestión de Seguridad de la Información por AENOR (ISO 27001)

Especialista Implantador de Planes de Continuidad de Negocio por AENOR (ISO 22301)

Experto en Coaching por la Universidad Camilo José Cela

Certificación Train the Trainer por T. Harv Eker y Blair Singer

Twitter: @juliocesarlopd

Blog: juliocesarmiguel.com

Con una **experiencia de más de 10 años** dedicados al mundo de la protección de datos, la seguridad de la información y la ciberseguridad, Julio César ha pasado por todas las etapas de un profesional que ama su carrera, le gustan los retos y dispone de un amplio bagaje a sus espaldas: **consultor, auditor, formador, escritor y, por último, autor de cursos.**

Su gran experiencia le ha permitido d**esarrollar una metodología de consultoría propia,** que combina la máxima calidad con la optimización del tiempo empleado.

Su **formación multidisciplinar, además,** le permite **combinar** de forma óptima sus conocimientos en **seguridad de la información con el cumplimiento de la normativa de protección de datos y la LSSI** para que sus alumnos aprendan a gestionar a seguridad de la información y la ciberseguridad en concurrencia con el cumplimiento normativo.

Es **fundador y Director de Grupo CFI,** empresa especializada en ofrecer formación, servicios y software para los profesionales de la LOPD, la LSSI y la CIBERSEGURIDAD.

Julio César ha **dirigido el desarrollo de LOPD Manager®,** la plataforma más rápida para implantar y gestionar la LOPD. Esta plataforma es utilizada, a nivel nacional, por más de 500 profesionales de la privacidad.

También ha dirigido el desarrollo de **LSSI Manager®,** una plataforma especializada para profesionales de la LSSI y única en España.

Es autor del libro **"Protección de Datos y Seguridad de la Información",** publicado por la Editorial Ra-Ma y que actualmente se encuentra en su **4ª edición.**

Ha obtenido el título de **Experto en Coaching** por la **Universidad Camilo José Cela**, así como la **Certificación Train the Trainer** de la mano de T. Harv Eker y Blair Singer. Esta formación le ha servido para **optimizar el diseño** de los **cursos que imparte incorporando técnicas de aprendizaje acelerado,** de forma que sus alumnos obtengan los **máximos resultados en el menor tiempo.**

"Si de verdad quieres aprender algo, has de experimentarlo por ti mismo"

Consultoría
Formación
Innovación

Construyendo Futuro Informático S.L.
Avda. Madrid 10, 34004 Palencia
Telféfono: 901 001 802 Fax: 901 001 805
info@grupocfi.es www.formacioncfi.es