



Ciberseguridad para empresas

Ciberseguridad para empresas

Duración: 60 horas

Precio: euros

Modalidad: e-learning

Metodología:

El Curso será desarrollado con una metodología a Distancia/on line. El sistema de enseñanza a distancia está organizado de tal forma que el alumno pueda compatibilizar el estudio con sus ocupaciones laborales o profesionales, también se realiza en esta modalidad para permitir el acceso al curso a aquellos alumnos que viven en zonas rurales lejos de los lugares habituales donde suelen realizarse los cursos y que tienen interés en continuar formándose. En este sistema de enseñanza el alumno tiene que seguir un aprendizaje sistemático y un ritmo de estudio, adaptado a sus circunstancias personales de tiempo

El alumno dispondrá de un acceso a una plataforma de teleformación de última generación con un extenso material sobre los aspectos teóricos del Curso que deberá estudiar para la realización de pruebas objetivas tipo test. Para el aprobado se exigirá un mínimo de 75% del total de las respuestas acertadas.

El Alumno tendrá siempre que quiera a su disposición la atención de los profesionales tutores del curso. Así como consultas telefónicas y a través de la plataforma de teleformación si el curso es on line. Entre el material entregado en este curso se adjunta un documento llamado Guía del Alumno dónde aparece un horario de tutorías telefónicas y una dirección de e-mail dónde podrá enviar sus consultas, dudas y ejercicios El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá del tipo de curso elegido y de las horas del mismo.

Profesorado:

Nuestro Centro fundado en 1996 dispone de 1000 m2 dedicados a formación y de 7 campus virtuales.

Tenemos una extensa plantilla de profesores especializados en las diferentes áreas formativas con amplia experiencia docentes: Médicos, Diplomados/as en enfermería, Licenciados/as en psicología, Licenciados/as en odontología, Licenciados/as en Veterinaria, Especialistas en Administración de empresas, Economistas, Ingenieros en informática, Educadores/as sociales etc...

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas de las siguientes formas:

- Por el aula virtual, si su curso es on line
- Por e-mail
- Por teléfono

Medios y materiales docentes

-Temario desarrollado.

-Pruebas objetivas de autoevaluación y evaluación.

-Consultas y Tutorías personalizadas a través de teléfono, correo, fax, Internet y de la Plataforma propia de Teleformación de la que dispone el Centro.

Titulación:

Al finalizar el curso obtendrás un certificado de realización y aprovechamiento del curso según el siguiente modelo:



Requisitos previos:

No hay requisitos previos ni profesionales ni formativos

Salidas profesionales:

Esta formación está encaminada a obtener una mejor cualificación y competencia profesional.

Programa del curso:

OBJETIVOS 42020 CIBERSEGURIDAD PARA EMPRESAS ? Objetivo principal: Proporcionar a los participantes los conocimientos y herramientas para la gestión de ciberincidentes y ciberataques dentro del entorno digital empresarial, al igual que el uso seguro de herramientas de Inteligencia Artificial, comprendiendo los riesgos, buenas prácticas y medidas de seguridad necesarias para una navegación, comunicación y trabajo seguro en Internet. ? **Objetivos secundarios:** Comprender la evolución de la digitalización y su impacto en la privacidad, la seguridad en Internet y la legislación vigente en ciberseguridad e Inteligencia Artificial. Aprender a configurar y proteger dispositivos como ordenadores, móviles y tablets mediante antivirus, copias de seguridad y otras medidas de seguridad esenciales. Adoptar buenas prácticas de seguridad digital, incluyendo la actualización de sistemas operativos, la configuración segura del WiFi y el uso responsable de navegadores e Inteligencia Artificial.

Identificar y prevenir amenazas digitales como virus, phishing, spyware, ataques por ingeniería social, keyloggers y otros tipos de malware, así como conocer herramientas de protección como firewalls y antivirus. Aprender a detectar nuevos ataques y fraudes de 2025. Protegerse en entornos digitales sensibles, incluyendo compras en línea, operaciones bancarias, teletrabajo seguro y la prevención del fraude en empresas. El curso incluye material educativo adicional para reforzar el aprendizaje, entre los que se encuentran: ? 45 vídeos explicativos ? 18 guías descargables ? 11 supuestos prácticos ? Glosario de términos y bibliografía especializada Este contenido complementario permitirá a los participantes profundizar en cada tema y aplicar los conocimientos adquiridos en situaciones reales.

ÍNDICE 42020 CIBERSEGURIDAD PARA EMPRESAS TEMA 1 LA ERA DIGITAL ? Pandemia y digitalización ? Privacidad y seguridad en Internet ? Legislación en ciberseguridad ? Inteligencia Artificial TEMA 2 PRIMEROS PASOS EN INTERNET ? El ordenador personal y su configuración básica ? Antivirus básicos gratuitos ? Las copias de seguridad ? Protección de tablets, móviles y otros dispositivos vulnerables TEMA 3 BUENAS PRÁCTICAS EN SEGURIDAD ? Sistemas operativos ? Windows. Importancia de las actualizaciones ? WiFi. Ventajas e inconvenientes ? Los navegadores ? Uso seguro de Inteligencia Artificial TEMA 4 VIRUS Y ANTIVIRUS ? Qué es un virus. Clasificación ? Medios de infección más importantes: - Correo electrónico - - Cd's, DVD, USB Webs y enlaces ? Antivirus, uso eficaz ? AVG Antivirus Free: Una alternativa libre TEMA 5 TRABAJAR CON SEGURIDAD ? E-commerce y compras seguras - - - Medios de pago seguros Información sobre los comercios seguros Gestiones bancarias y otras operaciones delicadas Fraude y estafas ? Teletrabajo seguro - Métodos de acceso en remoto TEMA 6 LA COMUNICACIÓN SEGURA ? Gmail, la opción más segura ? Cuidado con los documentos adjuntos ? Spam y protección ante posibles virus ? Ransomware ? Filtros antispam ? Phishing ? Keyloggers ? PC Zombies TEMA 7 CORTAFUEGOS O FIREWALL ? Definición y uso eficaz del Firewall ? Configuración y testeo ? Zone Alarm TEMA 8 CIBERATAQUES ? Clasificación de los ciberincidentes según ENISA ? Gestión de ciberincidentes ? Ataques a contraseñas ? Ataques por ingeniería social ? Ataques a las conexiones ? Ataques por malware ? Nuevos ataques con IA ? Medidas de protección TEMA 9 PROGRAMAS ESPÍA ? Spyware, qué es y cómo actúa ? Cómo detectarlo ? Eliminar un programa espía TEMA 10 CIBERAMENAZAS EN LA EMPRESA ? Ingeniería social ? Correo electrónico ? Principales fraudes ? Recomendaciones de seguridad ANEXO ? Glosario de términos ? Bibliografía ? Supuestos prácticos