

Curso de ciberseguridad para empresas

Temario

- 110.1 Introducción a la ciberseguridad (Definiciones básicas)
- 110.2 Ciberdelincuencia, la realidad (Por qué nos debe importar)
- 110.3 Contraseñas ridículas (¿A eso le llaman contraseñas?)
- 110.4 Contraseñas a prueba de bomba (Credenciales infranqueables)
- 110.5 Dónde guardar las contraseñas (Deja de apuntar las contraseñas)
- 110.6 Redes trampa y cómo evitarlas (No es oro todo lo que reluce)
- 110.7 Redes virtuales Privadas (VPN) (Navegación segura y anónima)
- 110.8 Cómo navegar seguros (Abre los ojos)
- 110.9 Ingeniería social ¿de qué hablamos? (Técnicas que intentan manipularte)
- 110.10 Ceguera por falta de atención (Los ciberdelincuentes quieren distraerte)
- 110.11 Phishing (Pesca indiscriminada)
- 110.12 Spear phishing (Pesca con arpón)
- 110.13 Whaling (Caza de ballenas o peces gordos – Fraude del CEO)
- 110.14 Vishing (Estafas por teléfono)
- 110.15 Smishing (Estafas por SMS)
- 110.16 Qrishing (Estafas con códigos QR)
- 110.17 Warshipping (Amenazas ocultas en el correo postal)
- 110.18 Baiting (Ganchos y cebos con trampa)
- 110.19 Malware (Diseñado para dañar)
- 110.20 Ransomware (Pagar por algo que es tuyo)
- 110.21 Blackmail porno o sextorsión (Si no quieres que se vea, no lo hagas)
- 110.22 Mirando por encima del hombro (Las paredes oyen)
- 110.23 Rebuscando en la basura (La basura que uno tira es el tesoro de otro)
- 110.24 Fugas de información (Cómo eliminar las brechas de seguridad)
- 110.25 Tratamiento de la información (Errores frecuentes)
- 110.26 Cuidado con los metadatos (No reveles todo lo que sabes)
- 110.27 Correo no deseado (Practica el sentido común)
- 110.28 Resumen del curso (Repaso de todo lo aprendido)

Examen fin de curso interactivo en directo con todos los alumnos (presencial y videoconferencia) | Examen tipo test para modalidad eLearning

Para quiénes es este curso

Este curso de ciberseguridad está dirigido a todo tipo de empleados de todo tipo de empresas y organizaciones, sin necesidad de que se tenga un nivel mínimo de conocimientos informáticos.

Objetivos de este curso

- Concienciar de la importancia de estar en guardia para hacer frente al cibercrimen.
- Conocer las principales amenazas que utilizan los piratas informáticos para evitar su éxito.
- Localizar las señales de advertencia para evitar el daño antes de que esté hecho.
- Detener con éxito los ataques más frecuentes que producen la mayoría de los problemas más graves.
- Crear entornos seguros de trabajo para trabajar con confianza y tranquilidad.
- Saber aplicar los principales estándares y procedimientos en materia de ciberseguridad.
- Gestionar de forma eficaz y eficiente todas las contraseñas y evitar errores frecuentes en su uso.
- Conocer los signos de los ataques de phishing para evitar el robo de información y las pérdidas económicas.
- Estar al tanto de las estafas de ingeniería social que se aprovechan del comportamiento humano.

Detalles del curso

- Duración: **4 horas**
- Todas las modalidades (presencial, videoconferencia y eLearning)
- Curso audiovisual interactivo (presencial y videoconferencia)
- Documentación del curso en PDF
- Diploma y titulación del centro
- Posibilidad de realizar pruebas pentesting para detectar vulnerabilidades de los empleados
- Este curso para empleados puede adaptarse a las necesidades de cada empresa

Curso bonificable 100%

Fundación Estatal
PARA LA FORMACIÓN EN EL EMPLEO



Más información o solicitudes de presupuesto:

[Info@qualitalent.com](mailto:info@qualitalent.com)

Tel. (+34) 858 959 765