

GUÍA DIDÁCTICA

FORMACIÓN EN CIBERSEGURIDAD



INTRODUCCIÓN

Bienvenido/a al curso de Ciberseguridad.

En **AMALTEA** valoramos y reconocemos el esfuerzo que suponen los estudios a distancia, por lo que tratamos de hacer la experiencia on-line lo más intuitiva y sencilla posible.

La presente guía está diseñada para **acompañarte y orientarte sobre los contenidos** e instrucciones que deberás desarrollar durante el curso virtual.

Lee atentamente las **pautas y orientaciones** de la Guía y, para cualquier inquietud y/o orientación sobre el desarrollo del curso, **comúnicate con el tutor o tutora** del campus, a través del sistema de mensajería interna.

CONTENIDOS DEL CURSO

Este curso online de Ciberseguridad y protección de la información permitirá al personal de la organización adquirir los conocimientos y habilidades necesarios para reconocer, prevenir y actuar frente a las amenazas digitales más frecuentes. A través de píldoras formativas y microlearnings, se abordarán los conceptos clave de la seguridad informática, la identificación de ataques y malware, el uso seguro de redes y dispositivos, y la aplicación de buenas prácticas de protección de datos. También se profundizará en la normativa vigente –como el RGPD, la LOPDGDD, el Real Decreto-ley 12/2018 y la Directiva NIS2– para comprender las obligaciones legales y éticas que garantizan la seguridad de la información.



CONTENIDOS DEL CURSO

CAPÍTULO 1. INTRODUCCIÓN A LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS

1. Conceptos de seguridad
2. Clasificación de las medidas de seguridad
 - 2.1. Según el recurso a proteger
 - 2.2. Según el momento de su puesta en marcha
 - 2.3. Según el tipo de elemento a proteger
3. Requerimientos de seguridad
 - 3.1. Principales características
 - 3.2. Otras características
 - 3.3. Tipos de ataques

CAPÍTULO 2. CIBERSEGURIDAD

1. Conceptos de ciberseguridad
2. Amenazas más frecuentes a los sistemas de información
 - 2.1. Síntomas de equipo infectado
3. Tecnologías de seguridad más habituales
4. Gestión de la seguridad informática
 - 4.1. Políticas de seguridad
5. Otros conceptos sobre seguridad informática
 - 5.1. Spam
 - 5.2. Phishing



CONTENIDOS DEL CURSO

CAPÍTULO 3. SOFTWARE

1. Conceptos sobre software dañino
2. Clasificación del software dañino
 - 2.1. Virus
 - 2.2. Gusanoso worm
 - 2.3. Bombas lógicas
 - 2.4. Troyanos
 - 2.5. Spyware
 - 2.6. Keylogger
 - 2.7. Adware
 - 2.8. Zombie
 - 2.9. Exploit
 - 2.10. Ransomware
 - 2.11. Otros malware
3. Amenazas persistentes y avanzadas
4. Ingeniería social y redes sociales

CAPÍTULO 4. HERRAMIENTAS DE SEGURIDAD

1. Medidas de protección
2. Control de acceso
 - 2.1. Permisos de los usuarios y de las usuarias
 - 2.2. Registro de usuarios/as
 - 2.3. Autenticación de usuarios/as
3. Gestión segura
 - 3.1. Gestión de carpetas compartidas en Red
 - 3.2. Tipos de accesos a carpetas compartidas
 - 3.3. Compartir impresoras
4. Protección frente a código malicioso
 - 4.1. Antivirus
 - 4.2. Cortafuegos (firewall)
 - 4.3. Antimalware

LAS ACTIVIDADES

El curso de Ciberseguridad es **totalmente virtual**. Todas las actividades se pueden desarrollar en cualquier horario, desde cualquier ordenador con acceso a Internet, desde cualquier lugar.

TIEMPO ASIGNADO

Las actividades y contenidos están diseñadas para que se desarrollen en aproximadamente **50h horas**, por lo que sugerimos hacer una planificación personal para cumplir con los objetivos del curso.

MATERIALES DIDÁCTICOS

Para el desarrollo del Curso usted necesitará trabajar con un ordenador con acceso a Internet, y requerirá disponer de un visor de documentos en PDF (en caso de no disponer de un programa instalado podrá descargarse una versión gratuita en el apartado Enlace a recursos de Software: Adobe Acrobat Reader).

Los materiales didácticos están disponibles en el Aula Virtual y le permitirán obtener información pertinente al desarrollo de los contenidos, ejercicios de auto evaluación, le servirán de guía y orientación en el desarrollo de las actividades del Curso.

LOS MEDIOS

El curso se desarrollará utilizando los módulos de la plataforma moodle, permitiendo una comunicación virtual permanente a través de:

- **Foro General del Aula**, que permite el intercambio asincrónico del grupo sobre un tema compartido.
- **Novedades del Docente**, para las comunicaciones realizadas por el profesorado.

EVALUACIÓN DEL CURSO

Al final de cada uno de los módulos se realizarán **cuestionarios de autoevaluación** que serán de obligado cumplimiento para poder pasar al siguiente módulo.

El alumnado dispondrá únicamente de **2 intentos para resolver cada cuestionario**, con tiempo **ilimitado**. Se escogerá el intento con mayor puntuación.

Al final del curso se realizará un **examen final**, de obligado cumplimiento, con los contenidos de todos los módulos, de un único intento con una limitación temporal de **2 horas**.

La **nota final** se corresponderá con la **media** de todas las **puntuaciones** de cada **módulo** (80%) y el **examen final** (20%).

No es necesario aprobar ambas partes, pero se requerirá de una **puntuación** de al menos **4** para poder hacer media. Se considerará **superado** el curso cuando se obtenga una **nota media igual o superior a 5**.

La superación del curso supondrá la obtención de un **certificado acreditativo** de superación y aprovechamiento del curso.

Para aquellas personas que no hayan alcanzado la puntuación mínima se valorará hacer una **convocatoria de gracia**, en función de la justificación y progresión del alumno/a en cuestión.

