

FCOI25- SEGURIDAD Y CIVISMO EN EL ENTORNO DIGITAL NIVEL INTERMEDIO

- **FAMILIA**

Formación complementaria

- **DURACIÓN**

40 hores

- **MODALIDAD**

Virtual presencial

- **CURSO**

100% subvencionado

1. ¿A QUIÉN VA DIRIGIDO?

Este curso va dirigido estas personas específicamente mujeres que no hayan finalizados los estudios básicos como la ESO.

Es un curso básico en el cual no pedimos ningún requisito para poder realizarlo pero sí que tenga las habilidades de comunicación lingüística suficiente para cursar el curso.

Tiene un máximo de 40 horas divididas en tres módulos de 15 y 10 horas.

Además podrás obtener conocimientos básicos relacionados con herramientas digitales y al tener esta base podrás pasar al nivel intermedio en el cual podrás continuar formándote cada vez mejor.

El más importante es que para poder cursarlo tienes que estar inscrita en el SOC (Servicio de Ocupación de Cataluña), estés en situación de paro o seas trabajadora en activo.

Finalmente el curso es 100% subvencionado y no tiene ningún coste para la alumna. Ofrecemos un alta calidad en nuestros cursos para dar un buen servicio y conseguir que el alumnado pueda adquirir todos los conocimientos que necesita.

2.CONTENIDOS

MÓDULO DE FORMACIÓN 1: PROTECCIÓN DE SISTEMAS, DISPOSITIVOS Y CONTENIDOS DIGITALES

RESULTADOS DE APRENDIZAJE

CONOCIMIENTOS/CAPACIDADES COGNITIVAS Y PRÁCTICAS

Aplicación y configuración de medidas de protección y seguridad de dispositivos y sistemas digitales

- Contraseñas
- Bloqueo de pantalla
- Protección de la comunicación
- Actualización de las medidas

Aplicación y configuración de medidas de protección y seguridad

- Posibles vías de infección
- Antivirus
- Cortafuegos
- Actualización de las medidas

Aplicación de medidas de seguridad a contenidos digitales

- Sistema automatizado de copias de seguridad
- Protección contra accesos no autorizados

MÓDULO DE FORMACIÓN 2: PROTECCIÓN DE DATOS PERSONALES Y SU PRIVACIDAD

RESULTADOS DE APRENDIZAJE

CONOCIMIENTOS/CAPACIDADES COGNITIVAS Y PRÁCTICAS

Análisis de puntos críticos en la protección de los datos personales

- Exceso de solicitudes de datos personales para utilizar una aplicación.
- Errores en el tratamiento de los datos: finalidades y periodo de almacenamiento
- Sin información disponible sobre el acceso, modificación y eliminación de datos
- No cumplimiento de la normativa de protección de datos
- Tratamiento de datos de menores y colectivos vulnerables
- Propuestas de mejora o actuaciones necesarias

Aplicación del marco normativo para proteger los datos personales y la privacidad en entornos digitales.

- Características del marco normativo
- Formas de aplicación

Aplicación de buenas prácticas de protección de la identidad y privacidad

- Configuración personalizada de la privacidad en las herramientas y entornos digitales
- Permisos de las aplicaciones
- Protección de la privacidad de los contenidos generados.

Ejecución de transacciones electrónicas con seguridad

- Uso de identificaciones personales electrónicas
- Firma digital
- Identificación y actuación de casos sofisticados de suplantación de identidad.

Habilidades de gestión, personales y sociales

- Implicación y demostración de actitudes rigurosas en la detección de puntos críticos en la protección de datos personales y la privacidad.
- Participación en la propuesta de mejoras en la protección de datos personales y la privacidad.
- Responsabilidad en la aplicación del marco normativo para proteger los datos personales y la privacidad en entornos digitales.
- Defensa por la protección de los datos personales de menores y colectivos vulnerables.

MÓDULO DE FORMACIÓN 3: PROTECCIÓN ACTIVA DE LA SALUD, EL BIENESTAR Y EL ENTORNO.

RESULTADOS DE APRENDIZAJE

CONOCIMIENTOS/CAPACIDADES COGNITIVAS Y PRÁCTICAS

Utilización de medidas de ergonomía

- Conocimiento de las medidas de ergonomía
- Resoluciones a los problemas más comunes

Identificación y actuación ante los riesgos para la salud

- Desconexión digital
- Conductas adictivas
- Mal uso / abuso
- Medidas para prevenir los riesgos

Identificación y actuación de los principales peligros asociados a contenidos digitales

- Detección de contenidos perjudiciales
- Detección de malas conductas por parte otros usuarios
- Acciones de bloqueo
- Denuncia en las redes sociales
- Protocolos en el caso de menores y colectivos vulnerables.
- Configuración de sistemas de control parental

Aplicación de medidas activas de protección del medio ambiente

- Reparación
- Reutilización y reciclaje
- Ahorro energético

Habilidades de gestión, personales y sociales

- Compromiso en la aplicación de medidas de ergonomía de las personas de su entorno.
- Conciencia de los riesgos para la salud asociados al uso de las tecnologías digitales.
- Responsabilidad en el consumo sostenible de la tecnología digital aplicando medidas de reutilización, reparación, reciclaje...
- Implicación ante los peligros asociados a determinados contenidos digitales.
- Demostración de Compromiso en la configuración de sistemas de control parental y protección digitales para menores y colectivos vulnerables.

MÓDULO DE FORMACIÓN 4: ESTRATEGIAS DE GESTIÓN DE LA IDENTIDAD Y PERFILES DIGITALES Y ACTUACIÓN CÍVICA

RESULTADOS DE APRENDIZAJE

CONOCIMIENTOS/CAPACIDADES COGNITIVAS Y PRÁCTICAS

Aplicación de estrategias por la optimización de su impronta y reputación digital

- Mantenimiento y protección de los perfiles y/o cuentas de usuario/a.
- Compilación de evidencias
- Egosurfing
- Integración de la identidad digital en un portafolio sitio web personal

Aplicación y promoción de actuaciones cívicas en el entorno digital

- Uso de licencias y sistemas de atribución según los objetivos.
- Gestión adecuada de críticas y conflictos en espacios sociales digitales.
- Contraste de las noticias engañosas o de la información no verídica

Habilidades de gestión, personales y sociales

- Demostración de una actitud responsable en los derechos de propiedad intelectual cuando se utilizan contenidos digitales.
- Desarrollo de actitudes de flexibilidad para promover la convivencia en el entorno digital.
- Asimilación de la importancia del mantenimiento y la cura de la impronta y reputación digital.
- Demostración de una actitud de compromiso y respeto con la difusión de versiones verdaderas de las noticias engañosas o de la información no contrastada.

3. METODOLOGÍA

La adquisición de competencias digitales requiere de una metodología de aprendizaje muy práctica, aprendiendo haciendo y detectando los propios errores o problemas.

El rol de la persona formadora es de acompañamiento y guía en el proceso de resolución de dudas y problemas, facilitando al estudiante busca su propia solución. También la persona formadora tiene que promover un rol activo y participativo del alumnado facilitando espacios de interacción y comunicación dentro de la plataforma de teleformación.

Las competencias digitales son logradas plenamente cuando las desvinculamos de programas o aplicaciones concretas, por lo tanto hay que globalizar el uso de tecnologías digitales ofreciendo variedad de aplicaciones y buscando los parámetros comunes en las herramientas con las mismas funcionalidades.

4. EVALUACIÓN

- La evaluación tendrá un carácter teórico-práctico y se realizará de forma sistemática y continúa, durante el desarrollo de cada módulo y al final del curso.
- Puede incluir una evaluación inicial y de carácter diagnóstico para detectar el nivel de partida del alumnado.
- La evaluación se llevará a cabo mediante los métodos e instrumentos más adecuados para comprobar los diversos resultados de aprendizaje, y que garanticen la fiabilidad y validez de la misma.
- Cada instrumento de evaluación se acompaña de su correspondiente sistema de corrección y puntuación en el que se explicita, de forma clara e inequívoca, los criterios de medida para evaluar los resultados logrados por los alumnos.
- La puntuación final lograda se expresa en términos de Apto/No apto.
- La evaluación incluye un caso práctico por módulo y un cuestionario final sobre los contenidos del curso.