



IFCT135PO CIBERSEGURIDAD PARA USUARIOS 10 HORAS

Modalidad: teleformación

FORMACIÓN PROGRAMADA
2020

¿QUÉ ES EL CRÉDITO FORMATIVO?

La **Formación Programada**, también conocida como Formación Bonificada, tiene como objetivo ofrecer a los trabajadores una formación que responda a las necesidades de sus puestos de trabajo para poder actualizar sus conocimientos o desarrollar nuevas competencias laborales, con lo que esto supone para la productividad general de la empresa.

Las empresas disponen de un crédito de formación para todo el año calculado a partir del número de empleados/as. Este crédito se hace efectivo una vez finalizada la acción formativa mediante la aplicación de **bonificaciones a la cotización de la Seguridad Social**.

La cuantía no consumida a final de año se considerará desestimada por las empresas, y se perderá.

Desde BETAFORMACIÓN, Entidad Organizadora reconocida por la [Fundación Tripartita](#) y con más de 30 años de experiencia en la formación y la gestión de subvenciones **queremos ayudarles:**

- Informándoles del importe máximo subvencionado para invertir en formación.
- Asesorándoles de forma personalizada y en busca de la máxima optimización para su empresa.
- Ofreciéndoles una formación de calidad adaptada a sus necesidades.

VENTAJAS DE ELEGIR BETA FORMACIÓN



- ✓ Más de 30 años como entidad organizadora y gestora de la formación programada
- ✓ Trabajamos con grupos reducidos y personalizados
- ✓ Cursos 100% bonificables en las cuotas de la S.S
- ✓ Material didáctico actualizado, orientado a la formación continua y adaptado a las necesidades de la empresa
- ✓ Cursos tutorizados por expertos en la materia
- ✓ Entrega de diploma para acreditar la adquisición de competencias profesionales
- ✓ Herramientas digitales para un aprendizaje donde y cuando el alumnado quiera

Si esta formación no es de tu interés
contáctanos y preparemos tu curso a medida

OBJETIVOS DEL CURSO

- Conocer y asimilar los conceptos de seguridad en los sistemas de información, en base a la sociedad de la información.
- Estudiar los principales riesgos de seguridad, tipos de vulnerabilidades, fallos de programa, programas maliciosos, etc.
- Saber aplicar los principales estándares y buenas prácticas en materia de seguridad en sistemas de información.
- Conocer los conceptos entorno a la ciberseguridad.
- Analizar e identificar las amenazas más frecuentes en los sistemas de información.
- Estudiar los principales estándares que rigen la ciberseguridad.
- Comprender el significado e importancia de la criptografía.
- Estudiar los conceptos entorno al software dañino.
- Clasificar el tipo de software dañino basándonos en las características que presenta.
- Conocer la ingeniería social y las redes sociales.
- Estudiar y conocer los mecanismos y sistemas de seguridad de las redes inalámbricas.
- Configurar la seguridad de la red inalámbrica.
- Conocer los mecanismos y sistemas de seguridad.
- Exponer diferentes medidas de protección para el acceso a los recursos y comunicaciones.
- Seguir unas correctas políticas de seguridad para poder establecer comunicaciones seguras.
- Estudiar las principales medidas de seguridad frente a código malicioso.

CONTENIDOS

10 horas

Unidad didáctica 1. Introducción a la seguridad en sistemas de información.

- 1.1. Conceptos de seguridad en los sistemas.
- 1.2. Clasificación de las medidas de seguridad.
- 1.3. Requerimientos de seguridad en los sistemas de información.

Unidad didáctica 2. Ciberseguridad.

- 2.1. Concepto de ciberseguridad.
- 2.2. Amenazas más frecuentes a los sistemas de información.
- 2.3. Tecnologías de seguridad más habituales.
- 2.4. Gestión de la seguridad informática.

Unidad didáctica 3. Software dañino.

- 3.1. Conceptos sobre software dañino.
- 3.2. Clasificación del programa malicioso.
- 3.3. Amenazas persistentes avanzadas.
- 3.4. Ingeniería y redes sociales.

Unidad didáctica 4. Seguridad en redes inalámbricas.

Unidad didáctica 5. Herramientas de seguridad.

- 5.1. Medidas de protección.
- 5.2. Control de acceso de los usuarios al sistema operativo.
- 5.3. Gestión segura de comunicaciones, carpetas y otros recursos compartidos.
- 5.4. Protección frente a código malicioso.



PASOS A SEGUIR

Paso 1

Contrato de adhesión a la agrupación de empresas, firmado y sellado.

Cumplimentar la FICHA DE DATOS de la empresa.

Una vez tramitado esto en la plataforma de la Fundación Tripartita, informaremos a la empresa del crédito disponible para el actual ejercicio económico.

Paso 2

Rellenar la ficha de datos de los participantes, adjuntar las cabeceras de las nóminas del último mes y firmar el modelo de necesidades.

Paso 3

Una vez aceptadas las propuestas económica y formativa, pasaremos a notificar el inicio de la acción formativa, en la plataforma de la Fundación Tripartita, para ello deberéis de adjuntar: la propuesta económica, la propuesta formativa el calendario, y el documento de presentación del curso, firmados y sellados.

Además de cumplimentar el documento que acredite las horas de formación que se llevarán a cabo dentro de la jornada laboral.



CONFÍAN EN BETA





BETA FORMACIÓN

C/ Tirant lo Blanc nº26

46900

Torrent, Valencia

[Tel. 961 571 010](tel:961571010)

info@betaformacion.com



¡A 5min de la parada de metro Torrent Avinguda!

www.betaformacion.com