***Taller de seguridad informática: Por qué un antivirus no es suficiente***

PROYECTO DE SENSIBILIZACIÓN Y FORMACIÓN EN CIBSERSEGURIDAD Y CONFIANZA EN EL ÁMBITO DIGITAL, EN EL MARCO DEL PROYECTO POCTEP "COMPETIC"

***Objetivo***

La Junta de Castilla y León, a través de la Dirección General de Industria y Competitividad realizará durante los meses de septiembre y octubre una serie de jornadas presenciales sobre ciberseguridad para pymes y autónomos del entorno rural de Castilla y León.

Estos talleres tienen como objetivo exponer y analizar el riesgo del uso de las TICs si no se utilizan de forma segura y formar a empresarios y autónomos principalmente de zonas rurales en materia de ciberseguridad, conociendo los peligros a los que pueden estar expuestos sus negocios y cómo protegerse de estos y de los ciberataques. Especial hincapié se hará en la importancia de proteger la información con la que trabajan las empresas.

***Lugar y fechas***

Carracedelo (LEÓN)

20 de septiembre

Horario: 09:00 – 14:00

Aula de Formación del Centro Innovador Social

C/San Esteban, 2

Además de la sesión presencial, los alumnos recibirán un manual con los contenidos del taller y se les dará acceso a una serie de webinars (videoconferencias) con temática relacionada con los contenidos de las jornadas formativas presenciales.

***Destinatarios principales del proyecto***

Emprendedores, autónomos y personas interesadas del entorno rural

***Contenido del taller***

Este taller consistirá en exponer y analizar los riesgos del uso de las TICs, desde las actuaciones involuntarias de los trabajadores hasta las acciones intencionadas por parte de los ciberdelincuentes y que pueden afectar a los usuarios más vulnerables.

También se formará a los emprendedores, autónomos y microempresas, para mejorar la ciberseguridad de su negocio, para conocer adecuadamente los procesos que pueden ser peligrosos para su empresa y se insistirá en la importancia de proteger la información que las empresas manejan para la prestación de los servicios, y la seguridad de la de la información que se utiliza.

1. Primera parte teórica: La importancia de la seguridad TIC en las pymes

* Conceptos básicos de seguridad
* El valor de la información en la empresa
* Los errores más comunes de seguridad en las pymes
* Identificación de las amenazas (Wi-Fi, web, malware, emails, redes sociales, dispositivos móviles…)
* Buenas prácticas (seguridad física, copias de seguridad, evitar software malicioso y phishing, contraseñas seguras, consejos para acceder a banca electrónica, e-commerce y e-Administración)
* Aspectos legales

1. Segunda parte práctica: Desarrollar un plan de seguridad

* Análisis de casos
* Prospectiva

1. Tercera parte práctica: Ejemplos de buenas prácticas

* En este apartado los participantes también podrán poner sus propios ejemplos para practicar los conocimientos que han adquirido.

***Para más información e inscribirse:***

***Mail:*** *cursos@enclaveformacion.com*

***Teléfono:*** *983140650*

***Inscripciones:*** [*https://www.enclaveformacion.com/ciberseguridad/*](https://www.enclaveformacion.com/ciberseguridad/)