



* CIBERATAQUES. CONOCIMIENTO Y BUENAS PRÁCTICAS EN MATERIA DE CIBERSEGURIDAD

* IMPLICACIONES LEGALES DE LOS TRABAJADORES EN EL USO DE LAS TIC EN LAS EMPRESAS

La completa dependencia tecnológica que hoy en día tienen las empresas, en las que se trabaja permanentemente "en la nube", unido al aumento exponencial de los ciberataques y la constante evolución de las técnicas de hacking, han derivado en una de las mayores amenazas y riesgos a las que se enfrentan las empresas. Sin duda alguna, estamos hablando de la que puede ser ya la mayor amenaza de las empresas. El 70% de las empresas afectadas por ciberataques son PYMES, debido a que **éstas parten de cero y sin ninguna preparación.**

Asimismo, la evolución de las tecnologías de la información y la comunicación y la extensión de su uso a través de los servicios y aplicaciones de Internet, como redes sociales, mensajería instantánea o correo electrónico en dispositivos inteligentes, ha llevado a que el uso de la información (datos) de carácter personal, puede dar lugar a la comisión de diversos delitos sin que en ocasiones se llegue a ser consciente de ello.

A esto se suma que cualquier empresa puede ser víctima de una brecha de seguridad en sus sistemas informáticos y sufrir robo de información y datos. El nuevo Reglamento General de Protección de Datos establece sanciones importantes a las empresas por no haber hecho nada para evitarlo (culpabilidad pasiva).

El uso intensivo de Internet ha hecho que proliferen este tipo de conductas, por lo que es necesario proporcionar pautas básicas para evitar ser víctimas o incluso cometer acciones delictivas sin ser consciente de su trascendencia.

LA CIBERSEGURIDAD YA NO ES UN LUJO, ES UNA NECESIDAD.

El Teletrabajo y el papel de la tecnología y la privacidad, ha dotado de mucho más valor y necesidad la prevención de ciberataques.



“La cadena más fuerte siempre se rompe por su eslabón más débil”

DESCRIPCION

Queramos o no, cualquier trabajador de una empresa forma parte del perímetro de seguridad de la compañía. Se pueden tener los sistemas técnicos más avanzados para protegerse de ciberataques, pero si un trabajador hace “click” en el sitio equivocado..... el hacker ha tenido éxito.

Por otro lado cualquier trabajador de la empresa puede estar cometiendo un delito contra la privacidad y protección de datos, sin ser consciente de ello por desconocer las implicaciones legales de lo que está haciendo en su rutina de trabajo diario.

FINALIDAD

Que los trabajadores de la empresa conozcan con detalle todas las amenazas y riesgos para la empresa que se pueden producir a través de un mal uso de sus sistemas informáticos y dispositivos móviles.

Sobre todo conseguir la concienciación de los trabajadores, a través del conocimiento, de que la amenaza existe, y enseñarles las pautas correctas a seguir en su trabajo diario.

A QUIEN VA DIRIGIDO

A todos los trabajadores en general de una empresa, que manejen ordenadores y sistemas informáticos y digitales, así como dispositivos móviles. **Independientemente del puesto y categoría que ocupen.**

PROGRAMA DEL CURSO. (9 horas)

PARTE I

1. Ciberseguridad en las organizaciones. Amenazas y riesgos cibernéticos en las empresas.
2. Principios y actuaciones básicas en materia de Ciberseguridad.
3. Riesgo interno: Las fugas de información
- 4.- Guía de buenas prácticas. Concienciación de que el riesgo existe, y que todos los trabajadores forman parte del perímetro de ciberseguridad de su empresa.

PROGRAMA DEL CURSO.

PARTE II

1. Aspectos legales del uso y securización de las Telecomunicaciones.
2. Marco normativo de la protección de Datos. Lo que deben saber los trabajadores de la LOPDGDD 3/2018 y RGPD 2016/679
3. Los principios relativos al tratamiento de datos.
4. Propiedad Intelectual e industrial en el entorno digital. Códigos de conducta y prevención de delitos cometidos por los trabajadores debido al desconocimiento.

PARTE III

1. Responsabilidad proactiva en materia de Ciberseguridad.
2. Responsabilidad penal de las empresas en Materia de Ciberseguridad. Sanciones.

A CADA PARTICIPANTE SE LE EMITE UN CERTIFICADO DE

“PREVENCIÓN Y CONCIENCIACIÓN BÁSICA EN CIBERSEGURIDAD Y PRIVACIDAD”

Este certificado es válido ante la **AGENCIA ESPAÑOLA DE PROTECCION DE DATOS**, en el caso de que la empresa sufra una brecha de seguridad y robo de información, acreditando que todo el personal ha recibido la formación necesaria, evitando así fuertes sanciones económicas.

El curso se imparte: 6 horas en clase presencial en streaming (Plataforma online) en directo con interacción entre el profesor y alumnos + 3 horas presencial para casos prácticos y resolución dudas en nuestras instalaciones o “in company”.

www.ciberseguridadaragon.com

* WORLD TRADE CENTER Torre Oeste Planta 15. Avda. María Zambrano 31

* PARQUE EMPRESARIAL DE LA EXPO.

Avda. de Ranillas nº 4.

info@ciberseguridadaragon.com

Tlfno: 976 011 435

CURSO BONIFICADO:



Fundación Tripartita
PARA LA FORMACIÓN EN EL EMPLEO