* ¿TU EMPRESA ES CIBERSEGURA? EL DECÁLOGO DE LA CIBERSEGURIDAD

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 transcendencia.

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

Muestra de forma clara cuales son los riesgos que se están asumiendo con una mala configuración y gestión de los sistemas informáticos desplegados en la empresa u organismo al que pertenece el alumno. Se describen con detalle, uno a uno, los 10 principios que deben regir la política de Ciberseguridad corporativa, haciendo especial hincapié en las configuraciones de seguridad de todos los componentes de la red de la empresa, el irrenunciable compromiso de la Dirección de la empresa con la Ciberseguridad y, sobre todo, con el elemento clave, que no es otro que todas las personas que forman parte de la organización.

FINALIDAD

Enseñar a los alumnos cuales son los riesgos que se están asumiendo con una mala configuración y gestión de los sistemas informáticos desplegados en la empresa u organismo. Informar sobre los diferentes medios informáticos, hardware o software, que permiten un buen control de nuestros activos en cuanto a la seguridad. Asegurar las operaciones, control de accesos a sistemas y aplicaciones, gestión segura de contraseñas, y la prevención a través del eslabón más débil de la cadena, las personas, en todos y cada uno de los niveles de la organización.

La finalidad última del curso es aplicar técnicas y protocolos de seguridad en una empresa, entidad u organismo, y realizar una hoja de ruta de la implantación del protocolo de seguridad en la organización, así como saber cómo actuar en caso de un incidente provocado por un ciberataque.

A QUIEN VA DIRIGIDO

A mandos intermedios y responsables de Áreas o departamentos de una empresa. Directores y General Managers.

Administradores informáticos de las empresas y responsables de back office, y en general para todo aquel trabajador que maneje sistemas, programas y aplicaciones informáticas específicas y críticas en una empresa.

PROGRAMA DEL CURSO. (9 horas)

1. Clasificación de la amenazas.
2. Gestión de los activos
    - Identificación de los activos
    - Clasificación de la información
    - Gestión de soportes
    - Gestión de la configuración

PROGRAMA DEL CURSO.

3. Seguridad de las operaciones

- Procedimientos y responsabilidades
- Instalación de sistemas y aplicaciones
- Análisis de las capacidades de los servidores
- Actualizaciones de seguridad en las aplicaciones
- Gestión y control de sistemas antivirus
- Copias de seguridad
- Gestión de la monitorización
- Gestión segura de las contraseñas

4. Gestión de incidentes.

6. Decálogo de la Ciberseguridad.

El curso se impartirá: 9 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

info@ciberseguridadaragon.com

* WORLD TRADE CENTER Torre Oeste Planta 15. Avda.María Zambrano 31
* PARQUE EMPRESARIAL DE LA EXPO. Avda. de Ranillas nº 4.

Tlfno: 976 011 435

BONIFICADO POR:

Fundación Tripartita
PARA LA FORMACIÓN EN EL EMPLEO