La importancia de la ciberseguridad en la transformación digital en un mundo globalizado.

Hoy en día, **quien no ha digitalizado sus procesos pierde competitividad**.

La realidad en Europa

El 42% de las grandes compañías en Europa están digitalizadas frente al 16% de las PYMES

El 56% de las empresas que desarrollan su actividad en consultoría, IT o servicios de información están altamente digitalizadas

Solo el 6% de los fabricantes de metal y siderúrgicas están digitalizados

Por último, el 53% de las empresas danesas (por citar un ejemplo) están altamente digitalizadas cuando sólo un 8% en Bulgaria y Rumanía alcanzan el mismo nivel de digitalización.

La realidad en España

	Con 10 empleados o menos	Con más de 10 empleados
Disponen de ordenadores	81,92 %	99,16 %
Tiene conexión a internet	78,17 %	98,18 %
Tiene conexión a internet y página web	28,80 %	78,10 %
Utilizan redes sociales	35,20 %	63,03 %
Realizan ventas por comercio electrónico	9,50 %	25,46 %
Realizan compras por comercio electrónico	17,90 %	34,94 %

¿Cómo lo hace Europa?

Promoviendo la inversión en la transformación digital mediante planes de ayuda a la inversión en la digitalización de procesos empresariales e industriales, con fondos que llegan a través de los gobierno nacionales, como el KIT Digital, etc., y otros programas desarrollados desde las regiones con los fondos transferidos.

Potenciando el futuro a través de estos 3 ejes:

Ciberseguridad
Supercomputación
Inteligencia Artificial

¿Cuál es el objetivo de la ciberseguridad?

El principal objetivo de la ciberseguridad es disponer de una serie de medidas técnicas y organizativas para conseguir la protección digital de las personas, de las empresas y de la información que gestionan.

La ciberseguridad protege la información y, por tanto, protege a las personas.

¿Hasta dónde llega la ciberseguridad?

Cibercrimen: engloba las conductas delictivas que se practican mediante el aprovechamiento de la red.

Ciberamenazas: Son las posibilidades de comisión de daños a personas u organismos mediante el uso de Internet.

Ciberespacio: Es aquella realidad simulada implementada dentro de los ordenadores y redes digitales existentes a nivel mundial, siendo un concepto más amplio que el propio Internet.

Ciberdefensa: Se conoce como ciberdefensa al conjunto de acciones de tipo activo, pasivo, proactivo, preventivo y reactivo que se aplican para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición.

Malware: término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, software de rescate, spyware, adware, software de miedo, etc.

Protege la información mediante la ciberseguridad

Asegurando su integridad, disponibilidad y confidencialidad. En definitiva, aumentando su ciberresilicencia frente a posibles amenazas.

Solo en los últimos días…

Un ciberataque a Iberdrola expone los datos de 1,3 millones de clientes

La compañía niega que se hayan comprometido datos financieros ni de consumo de los usuarios, aunque reconoce que sí reveló su nombre, DNI, domicilio y número de teléfono

Más de 200 números de móviles españoles, posibles objetivos de Pegasus

- Según el diario 'The Guardian', estos teléfonos habrían sido seleccionados en 2019
- Estas son las penas de cárcel a las que se enfrentan los espías de Pegasus

Gobierno de Costa Rica sufrió un ciberataque que lo obligó a suspender sus plataformas digitales

El país centroamericano tuvo que deshabilitar varios servicios informáticos del Estado tras confirmar un hackeo en la plataforma digital del Ministerio de Hacienda. El gremio de industriales costarricense señaló que se presentaron perjuicios por el trastorno en aduanas.

El ayuntamiento de Caldes de Montbui, afectado por un ataque informático

• El consistorio está trabajando en la restauración de los servicios municipales

Alertan a las instituciones vascas de un posible ciberataque «inminente»

El Centro Criptográfico Nacional ha notificado a la UPV la venta de datos, claves incluidas, de usuarios de su cuenta corporativa

Gijón sigue recuperando servicios tras el ciberataque

LA VOZ
GIJON

Plaza del Ayuntamiento en Gijón PACO RODRÍGUEZ

A finales de semana se prevé que funcionen de nuevo el registro municipal y las solicitudes de Servicios Sociales y bibliotecas

Cae una banda de ciberdelincuentes que hackeó los gestores de nóminas en instituciones de Granada y Madrid y levantaron más de 53.000 euros

Los ciberataques aumentaron un 148% el pasado año y las aseguradoras endurecen la suscripción

'**Cyber resilience; 12 key controls to strengthen your security**' es el informe elaborado por **Marsh** donde ofrece 12 pautas de ciberseguridad para logar la resiliencia cibernética y mejorar la asegurabilidad en cualquier organización. Señala la correduría y consultora que los ciberataques crecieron el pasado año un 148% y apunta que ante ello "las aseguradoras están endureciendo las condiciones de suscripción de sus seguros". Añade que el "análisis del entorno operativo cibernético y los controles de riesgo de los solicitantes que piden las aseguradoras son cada vez más exhaustivos".

La empresa eólica Nordex sufre un ciberataque que afecta a sus plantas de Navarra

LOS PIRATAS INFORMÁTICOS ACTUARON ENTRE EL JUEVES 31 DE MARZO Y VIERNES 1 DE ABRIL. TODAVÍA LA COMPAÑÍA ESTÁ ANALIZANDO LA AFECCIÓN DEL PROBLEMA

aeiciberseguridad
Agrupación Empresarial Innovadora CIBERSEGURIDAD y Tecnologías Avanzadas

CYBERSECURITY innovation HUB

¿Qué normativas regulan estas cuestiones?

- Ley 34/2002, de 11 de julio, de servicios a la sociedad de la información y comercio electrónico (LSSICE).
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Directiva del Parlamento Europeo y del Consejo relativa a medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión" (Directiva NIS 2017).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (RGPD)
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

¿A qué se enfrentan las PYMEs?

Ciberataques

Distinto tipo de malware, como:

- Ransomware
- Denegación de Servicio
- Phishing
- Spyware

Sistemas de gestión

Conectividad
Continuidad de negocio
Concienciación
Formación
Relación con proveedores
Relación con clientes
Facturación
Firma electrónica

Entorno Web

Comercio electrónico
Pasarela de pagos
Redes sociales
SSL

LAS PERSONAS.
El eslabón más débil

Teletrabajo

Control de dispositivos móviles
Trabajo en la nube
Acceso a servidores
Wifi
Control de terminales corporativos
Backup

Gestión de la información

RGPD
LSSI
Identidad digital
Reputación online
Fuga de datos
Privacidad

Claves para las PYMEs

1.- Auditoría de Análisis de situación.

¿En qué situación de ciberseguridad está mi empresa?

- Análisis de riesgos y vulnerabilidades ¿A qué riesgos se enfrenta? ¿Cuáles son mis vulnerabilidades?

- Análisis de impacto ¿Cómo afectaría a mi empresa un ataque?

Claves para las PYMEs

2.- Proceso Implantación de Medidas

- **Formación y sensibilización** en temas como: Conceptos de ciberseguridad; Tipos de ciberataques; Efectos de un ciberataque; Cómo prevenir los ataques; Elementos más comunes en ciberseguridad; Gestión de contraseñas; Privacidad; Navegación por la red; Consejos para manejar redes sociales; El trabajo en la nube; Elementos para la protección.

- **Tests de intrusión, test de penetración, ingeniería social** (el firewall humano),….

Claves para las PYMEs

3.- Gestión de incidentes

Si mi empresa sufre un incidente de ciberseguridad:

- recurrir a manual de gestión de incidente, para conocer los pasos a seguir según la tipología del incidente, impacto, riesgo, etc.

- recurrir a nuestro proveedor de confianza o a un experto en ciberseguridad

- escalar el incidente (por ejemplo, si hemos sufrido un ataque, proceder con la denuncia ante la Guardia Civil o Policía Nacional)

Recuerde

LA INFORMACIÓN ES EL ORO DEL SIGLO XXI
Y SOLO HAY DOS TIPOS DE EMPRESAS: LAS QUE HAN SUFRIDO UN CIBERATAQUE Y LAS QUE LO VAN A SUFRIR.

MINIMICE EL IMPACTO, IMPLEMENTANDO MEDIDAS DE CIBERSEGURIDAD QUE ASEGUREN LA PERMANENCIA DE SU NEGOCIO Y SU REPUTACIÓN.

Gracias.

Tomás Castro Alonso
Presidente de AEI de Ciberseguridad y
representante de CyberDIH

presidente@aeiciberseguridad.es