EL MUNDO
DIARIO DE CASTILLA Y LEÓN
El Mundo (Diario de Castilla y León) -Innovadores 07/02/23
Castilla y León
Pr: Semanal (Martes)
Tirada: 9.426
Dif: 6.938
Cod: 154283806
Pagina: 3
Secc: OTROS Valor: 1.150,02 € Area (cm2): 219,6 Ocupac: 24,03 % Doc: 1/1 Autor: Num. Lec: 27752

BLOG
OPINIÓN

# *Tendencias de ciberseguridad en 2023*

JULIO CÉSAR MIGUEL PÉREZ

Estimado lector, como ya sabes, la sociedad están inmersa en la digitalización de los procesos. La ciberseguridad se convierte en parte esencial de esta digitalización, pues si los sistemas de información no se protegen de forma adecuada, estaremos exponiendo a las empresas, administraciones y ciudadanos a un alto riesgo de sufrir incidentes con consecuencias desastrosas.

Estas son las principales tendencias en el ámbito de la ciberseguridad para este 2023:

**1. Incremento y sofisticación de los ciberataques**

El *ransomware* continuará evolucionando así como otros los ataques de ingeniería social, que cada vez son más personalizados, efectivos y dañinos. El uso de la Inteligencia Artificial incrementará su precisión.

**2. La Certificación de la ciberseguridad crece exponencialmente**

Cada vez se exige más a las entidades que gestionan información de terceros (por ejemplo, Centros de Proceso de Datos, Administraciones Públicas, empresas que manejan información personal, etc.) que certifiquen la ciberseguridad de sus sistemas a través de las diferentes certificaciones que existen (como la ISO 27001, el Esquema Nacional de Seguridad o TISAX) para dar confianza y tranquilidad a los clientes y ciudadanos de que gestionan de forma apropiada algo tan fundamental en las organizaciones.

**3. El Internet de las Cosas (IoT) lo complica**

Cada vez existen más objetos que se conectan a la red local de la organización o de la casa, como por ejemplo, televisores, electrodomésticos, termostatos, sensores de presencia, detectores de fugas de agua, etc. De cara a ciberseguridad, cualquier dispositivo que se conecte a la red es un vector de entrada de posibles ciberataques y es necesario gestionar adecuadamente la configuración de estos dispositivos e instalar continuamente las actualizaciones de seguridad del fabricante.

**4. El factor humano continua siendo decisivo**

El 95% de los ciberataques se siguen produciendo debido al factor humano. El usuario sigue siendo el eslabón más débil de la cadena de la seguridad. Esto es particularmente crítico en un entorno de trabajo remoto. Por este motivo, durante 2023 existirá un incremento de los ciberataques cuyo vector de entrada sean los propios empleados de las organizaciones. La formación del personal va a ser imprescindible para evitar al máximo que se produzcan. Para ello, las empresas comenzarán a hacer obligatoria la formación en ciberseguridad para todos sus empleados.

Y tu, querido lector, ¿estás «ciberpreparado» para 2023?

---

**Julio César Miguel Pérez** es presidente de AETICAL y CEO de Grupo CFI. http://grupocfi.es.