

---

# PlantaDoce.

---

Entorno

## Ciberseguridad en salud: una brecha que cuesta 325 euros anuales al ciudadano

Los expertos alertan del número de ataques cibernéticos en el sector como consecuencia del avance de las nuevas tecnologías médicas y la interconectividad.

---

Albert Cadanet  
8 mar 2019 - 04:57

### Ciberseguridad en salud: una brecha que cuesta 325 euros anuales al ciudadano

El negocio de la salud, en alerta por la llegada de más ataques informáticos. Según el informe *Cost of Data Breach Study*, elaborado por el instituto Ponemon de Estados Unidos, la industria sanitaria genera los costes más elevados en materia de prevención en la red. Durante los últimos cuatro años, las acciones emprendidas en términos de ciberseguridad han supuesto un gasto medio de 369 dólares (325 euros) por ciudadano.

En paralelo, el estudio *2019 Global healthcare outlook*, realizado por Deloitte advierte que el número de ataques a través de Internet seguirá aumentando. “El legado del Wannacry continúa resonando, y los criminales cibernéticos planean ejecutar un mayor número de ataques cada vez más sofisticados”, apunta Deloitte.

En este sentido, el sector de la salud se presenta como una presa idónea. “El volumen de los datos en los sistemas sanitarios es muy valioso y la demanda por programas interconectados sigue incrementándose”, señala el informe. A pesar de todo, la consultora lamenta que “muchas organizaciones siguen sin estar preparadas para hacer frente a estos ataques”.

**La relevancia de los datos médicos y la apuesta por la interconectividad en salud convierte al sector en un blanco perfecto**

---

# PlantaDoce.

---

Según otro informe publicado por Deloitte, titulado *Medtech and the Internet of Medical Things*, el **67% de los fabricantes de productos médicos reconocieron que la probabilidad de sufrir al menos un ciberataque “es elevada”**, un porcentaje que era del 56% en el momento en el que se preguntaba a los proveedores de tecnología.

**Por otra parte, sólo el 17% de los fabricantes y el 15% de los proveedores admitieron que están tomando las precauciones suficientes para prever este tipo de ataques.**

Además, “los inversores claves de cada sociedad no tienen un gran conocimiento de los riesgos que existen dentro de su organización”, añade el informe de Deloitte.

La firma consultora calcula que, en los últimos años, las brechas en el sector de la salud han afectado a un total de 79 millones de personas en todo el mundo. “A pesar de las iniciativas gubernamentales para mejorar en seguridad, el valor de los datos también se incrementa y, con ello, el crimen en la red”, concluye el documento.

## **Deloitte señala que los ataques cibernéticos en la industria sanitaria han afectado a 79 millones de personas en los últimos años**

Como complemento a estos archivos, la multinacional Accenture publicó otro estudio en 2017, bautizado como *Cost of cyber crime study*, donde se especificaban los tipos de ataques más frecuentes en el campo de la salud. Estos son el *phishing* (una técnica en que el *hacker* se hace pasar por una persona o empresa para adquirir información confidencial) y el ataque de denegación de servicio (que imposibilita el acceso de usuarios legítimos a una red).

**La recomendación que emite Deloitte para la prevención de estos percances se centra en la figura de los empleados.** “Ya que muchos trabajadores de la Administración y los hospitales pueden carecer de conciencia para la gestión financiera y operativa teniendo en cuenta los riesgos cibernéticos, la educación del personal debe ser una parte importante de toda gestión de riesgos”, insiste la consultora.