DIARIO DE CASTILLA Y LEÓN EL MUNDO
El Mundo (Diario de Castilla y León) -Innovadores 04/04/23
Castilla y León
Pr: Semanal (Martes)
Tirada: 9.090
Dif: 6.731
Cod: 155834986
Pagina: 2
Secc: OTROS Valor: 1.150,02 € Area (cm2): 219,6 Ocupac: 24,03 % Doc: 1/1 Autor: Num. Lec: 26924

BLOG
OPINIÓN

La ciberseguridad en los hospitales

JULIO CÉSAR MIGUEL PÉREZ

El 5 de marzo de 2023 el Hospital Clínic de Barcelona sufrió un ciberataque del tipo *ramsomware* que afectó a las tres sedes del hospital y a tres centros de atención primaria.

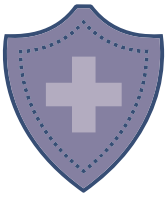
El ciberataque ha supuesto dejar de hacer más de 4.000 análisis de pacientes ambulatorios, más de 300 intervenciones y más de 11.000 visitas de las consultas externas. Se ha confirmado también la exfiltración de datos de los pacientes.

Ciberdelincuentes pertenecientes al grupo Ransonm House penetraron en el sistema del centro hospitalario mediante un ataque *ransomware, a* través del cual obtuvieron los expedientes clínicos de los pacientes y luego cifraron esa información para que no se pudiese acceder a ella.

Exigen un rescate económico de 4,5 millones de euros a cambio de no difundir esa información.

Hay que tener en cuenta que los datos médicos es una información muy sensible que estos ciberdelincuentes pueden usar también para extorsionar individualmente a los pacientes exigiéndoles una cantidad de dinero bajo amenaza de hacer pública información comprometedora.

Estos ataques tienen éxito, esencialmente, porque las administraciones y organismos públicos no tienen la ciberseguridad entre sus prioridades, pese a la ingente cantidad y la sensibilidad de los datos que manejan.



Es común que el personal disponga de equipos informáticos obsoletos, con sistemas operativos que ya no tienen soporte del fabricante y con unas medidas de seguridad totalmente precarias.

La ciberseguridad no es tener un antivirus y ya está. Requiere atender múltiples ámbitos, como es la formación del personal, la protección de los equipos, la gestión de las vulnerabilidades, la detección de las intrusiones, la gestión ágil de los incidentes de seguridad, tener un plan de continuidad, etc.

El Esquema Nacional de Seguridad (ENS) establece las medidas de seguridad que las administraciones y organismos públicos deben implantar de forma obligada en sus sistemas informáticos para garantizar la seguridad de dichos sistemas y, por ende, la seguridad de la información que manejan de los ciudadanos.

De estar plenamente implantado, este tipo de incidentes no se producirían con el impacto y alcance que actualmente tienen, ya que se dispondría de medidas para evitar que se propague y un plan para recuperar las operaciones de forma ágil.

Es necesario impulsar su implantación «real» en todas las administraciones y organismos públicos. Solo así estarán adecuadamente protegidos los datos de todos nosotros.

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