CIBERSEGURIDAD ARAGON

CURSO DE CIBERSEGURIDAD Y PRIVACIDAD ESPECÍFICO PARA HOSPITALES, CLÍNICAS Y CENTROS MÉDICOS.

LOS HOSPITALES Y CENTROS MÉDICOS, COMO TODAS LAS ORGANIZACIONES MODERNAS, TIENEN UNA DEPENDENCIA ABSOLUTA DE LOS SISTEMAS INFORMÁTICOS PARA TODAS SUS ACTIVIDADES, TANTO ADMINISTRATIVAS COMO CLÍNICAS.

ESTAMOS HABLANDO DE ORGANIZACIONES MUY COMPLEJAS, QUE TRABAJAN 24 h x 7 x 365 , CON MULTITUD DE SISTEMAS QUE NECESITAN CONECTARSE ENTRE SÍ, A LO QUE HAY QUE AÑADIR LAS PIEZAS MÁS VALIOSAS PARA LOS CIBERDELINCUENTES, " LA INFORMACIÓN CLÍNICA DE LOS PACIENTES".

Los ataques de hackers a Hospitales y Clínicas que se han conocido recientemente pueden ser catastróficos para un hospital. No solo por la disrupción de su operatividad o la incapacidad de contar con la información esencial del paciente, que ya supone una situación de caos, sino también por el coste económico que supone restaurar sistemas y copias de seguridad, así como el daño reputacional que el Centro atacado puede sufrir a partir de estos hechos y por la pérdida de los historiales clínicos de sus pacientes.

***Ciberataques, Hackers, robos de información**, e **implicaciones legales en el uso de los datos personales de los pacientes**, encuentran un fácil campo de cultivo en los hospitales y Centros Sanitarios debido al desconocimiento generalizado de estos riesgos por parte de los médic@s, enfermer@s y el personal de administración.*

LA CIBERSEGURIDAD YA NO ES UN LUJO, ES UNA NECESIDAD.

Un Colegio o Centro Educativo puede disponer de los sistemas técnicos más avanzados, pero si un trabajador por desinformación hace "click" en el sitio equivocado.....

"La cadena más fuerte siempre se rompe por su eslabón más débil"

LOS RIESGOS A LOS QUE SE ENFRENTAN LOS HOSPITALES, CLÍNICAS Y CENTROS MÉDICOS.

En los Hospitales y Centros Sanitarios **la prioridad** ha de referirse a **la seguridad del paciente,** tanto por la confidencialidad de sus datos como por el correcto funcionamiento de los equipos médicos, Si nos planteamos los **perjuicios** derivados de un fallo de seguridad causante de averías e inutilización de uno o varios equipos, hay que tener en cuenta, **en primer lugar**, la integridad física del paciente debido al fallo ocurrido, o la integridad y confidencialidad de los datos de éste. **En segundo lugar,** las responsabilidades legales derivadas del ciberincidente y las consecuencias de éste, y **en tercer lugar,** los costes económicos originados para solucionar la avería ocasionada, así como el tiempo de inactividad por la inutilización de los equipos.

El nuevo Reglamento General de Protección de Datos establece **sanciones importantes** a las empresas y entidades privadas por no haber hecho nada para prevenir este tipo de incidentes. Es lo que denomina **culpabilidad pasiva**.

FINALIDAD

Queramos o no, cualquier trabajador de un Hospital y de cualquier Centro Sanitario (Médic@s, enfermer@s, auxiliares y personal de dirección y administración) forma parte del perímetro de seguridad del Centro, incluso cuando se conecta desde su casa con su ordenador portátil, o utiliza su pendrive particular en los ordenadores del propio Centro Sanitario.

Asimismo, el uso de la información (datos) de carácter personal, como son los historiales clínicos de los pacientes, al no constituir la actividad principal del personal sanitario, en numerosas ocasiones genera dudas sobre la interpretación y aplicación de su regulación, y puede llegar a dar lugar a la comisión de diversos delitos sin que en la gran mayoría de las ocasiones se llegue a ser consciente de ello.

Por estas razones, la finalidad del curso es que el personal de los Centros Sanitarios conozcan con detalle todas las amenazas, riesgos y delitos que se pueden producir a través de un mal uso de sus sistemas informáticos y dispositivos móviles. Y Sobre todo conseguir la concienciación del personal sanitario, a través del conocimiento, de que la amenaza existe, y enseñarles las pautas correctas a seguir en su trabajo diario.

A QUIEN VA DIRIGIDO

A todo el personal sanitario, desde médicos a auxiliares, así como al equipo directivo del Centro Sanitario y al personal de administración, que utilicen cualquier tipo de sistema informático, tanto fijo como en dispositivos móviles.

A CADA PARTICIPANTE SE LE EMITE UN CERTIFICADO DE "PREVENCIÓN Y *CONCIENCIACIÓN BÁSICA EN CIBERSEGURIDAD Y PRIVACIDAD*"

Este certificado es válido ante la **AGENCIA ESPAÑOLA DE PROTECCION DE DATOS**, en el caso de que la empresa sufra una brecha de seguridad y robo de información, acreditando que todo el personal ha recibido la formación necesaria, evitando así fuertes sanciones económicas.

PROGRAMA DEL CURSO. (9 horas)

PARTE I. CIBERSEGURIDAD

1. Ciberseguridad en las organizaciones. Amenazas y riesgos cibernéticos en Hospitales y Centros Sanitarios.
2. Principios y actuaciones básicas en materia de Ciberseguridad.
3. Riesgo interno: Las fugas de información. Los "diamantes" en los Centros Sanitarios: Los historiales clínicos.

4.- Guía de buenas prácticas. Concienciación de que el riesgo existe, y que todos los trabajadores forman parte del perímetro de ciberseguridad de su empresa.

5.- Responsabilidad penal de las entidades en Materia de Ciberseguridad. Sanciones.

PROGRAMA DEL CURSO.

PARTE II. PRIVACIDAD

1. Conceptos básicos de los datos de carácter personal. Aspectos diferenciales al trabajar con historiales clínicos.
2. Principales novedades del Reglamento General de Protección de Datos que afectan al Sector Sanitario.
3. Seguridad, privacidad y confidencialidad de la información médica del paciente.
4. Decálogo para un correcto uso de los datos de carácter personal en los Centros Sanitarios.

El curso se imparte: 6 horas en clase presencial en streaming (Plataforma online) en directo con interacción entre el profesor y alumnos + 3 horas presencial para casos prácticos, tutorización y resolución dudas en nuestras instalaciones o "in company".

www.ciberseguridadaragon.com

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

info@ciberseguridadaragon.com

Tlfno: 976 011 435

CURSO BONIFICADO

Fundación Tripartita
PARA LA FORMACIÓN EN EL EMPLEO