Relyens lanza su Seguro Ciber, un escudo de protección para las organizaciones sanitarias

- **El sector sanitario se ha convertido en un blanco predilecto para los hackers y eso ha desencadenado un notable aumento en el número de ciberataques.**
- **Esta nueva cobertura asegurará las consecuencias de un incidente que afecte a los sistemas de información de los centros médicos.**
- **Con este seguro, Relyens completa su oferta de servicios enfocados a la ciberseguridad de las instituciones sanitarias.**

Madrid, 5 de octubre de 2023. Relyens, gestor europeo de riesgo sanitario, lanza al mercado español el Seguro Ciber para cubrir las consecuencias y daños causados por una violación de la seguridad de los sistemas informáticos y dispositivos conectados en las redes de los centros sanitarios. Este nuevo producto nace tras el aumento de ciberataques producidos durante los últimos años en el sector médico, que se ha convertido en uno de los objetivos preferidos de *hackers* y grupos criminales que operan a través de la Red.

Este tipo de amenazas afecta a los sistemas de información de las organizaciones sanitarias y pueden derivar en la sustracción de información privada y datos de los pacientes y de los profesionales sanitarios que trabajan en ellos. Además, los ciberataques pueden poner el peligro la salud de las personas ingresadas y bajo atención médica al afectar a los dispositivos conectados.

Relyens, como aseguradora sanitaria, ofrece este nuevo producto para cubrir las posibles consecuencias derivadas de un incidente cibernético, un error de funcionamiento o una violación de la protección de datos en un centro u organización médica.

Una cobertura integral y a medida para protegerse de los ciberataques

El Seguro Ciber que ofrece el Grupo a sus clientes cubre los siguientes aspectos:

- Gastos de asistencia, que incluyen el apoyo en la gestión de la crisis y el pago de honorarios de los expertos y consultores encargados de mitigar la amenaza y sus consecuencias.
- Daños propios originados por el ciberataque, que puede provocar la interrupción parcial o total de la actividad sanitaria hasta restaurar de nuevo los sistemas.
- Indemnizaciones a terceros para restaurar las consecuencias derivadas de un ciberataque o de la violación de la seguridad de la información.

Esta cobertura de Relyens ofrece un servicio de gestión de incidentes disponible 24/7 e incluye el apoyo de expertos de diversos ámbitos, como expertos técnicos en respuesta a incidentes, abogados especializados en procedimientos de gestión de compromiso de datos, servicio de investigación o comunicación de crisis.

Hacia una protección total que mejore la seguridad del paciente

Con este seguro, Relyens completa su oferta de servicios enfocados en la protección en el ámbito de la ciberseguridad y mantiene su apuesta por crear un entorno sanitario de confianza ayudando a profesionales e instituciones sanitarias a crear un mundo más sano y seguro para las personas.

www.relyens.eu / Twitter: @Relyens / Linkedin: Relyens

Acerca de Relyens

Relyens es el grupo mutualista europeo de referencia en seguros y gestión de riesgos al servicio de los profesionales sanitarios y actores territoriales. Para asegurar su actividad y garantizar la calidad de los servicios prestados a pacientes y ciudadanos, Relyens les ayuda a controlar los riesgos relacionados con la prestación de asistencia sanitaria, la gestión del capital humano o la ciberseguridad. Despliega un enfoque global único que combina soluciones de gestión, prevención de riesgos y seguros. El Grupo desarrolla sus actividades en Francia, España, Italia, Alemania y Bélgica con 1.100 empleados, y ha registrado ***1.019,9 millones de euros en primas cobradas y 581,4 millones de euros en volumen de negocios en 2022****. Creado en Lyon hace casi 100 años por y para hospitales, Relyens es empresa con una misión social desde 2021. Su razón de ser es 'Actuar e innovar, junto a quienes trabajan por el interés general, para construir un mundo de confianza'.*

Contacto de prensa

Juan de la Villa - +34 608 48 26 45 - jdelavilla@comunicacionrrpp.es / relyens@comunicacionrrpp.es