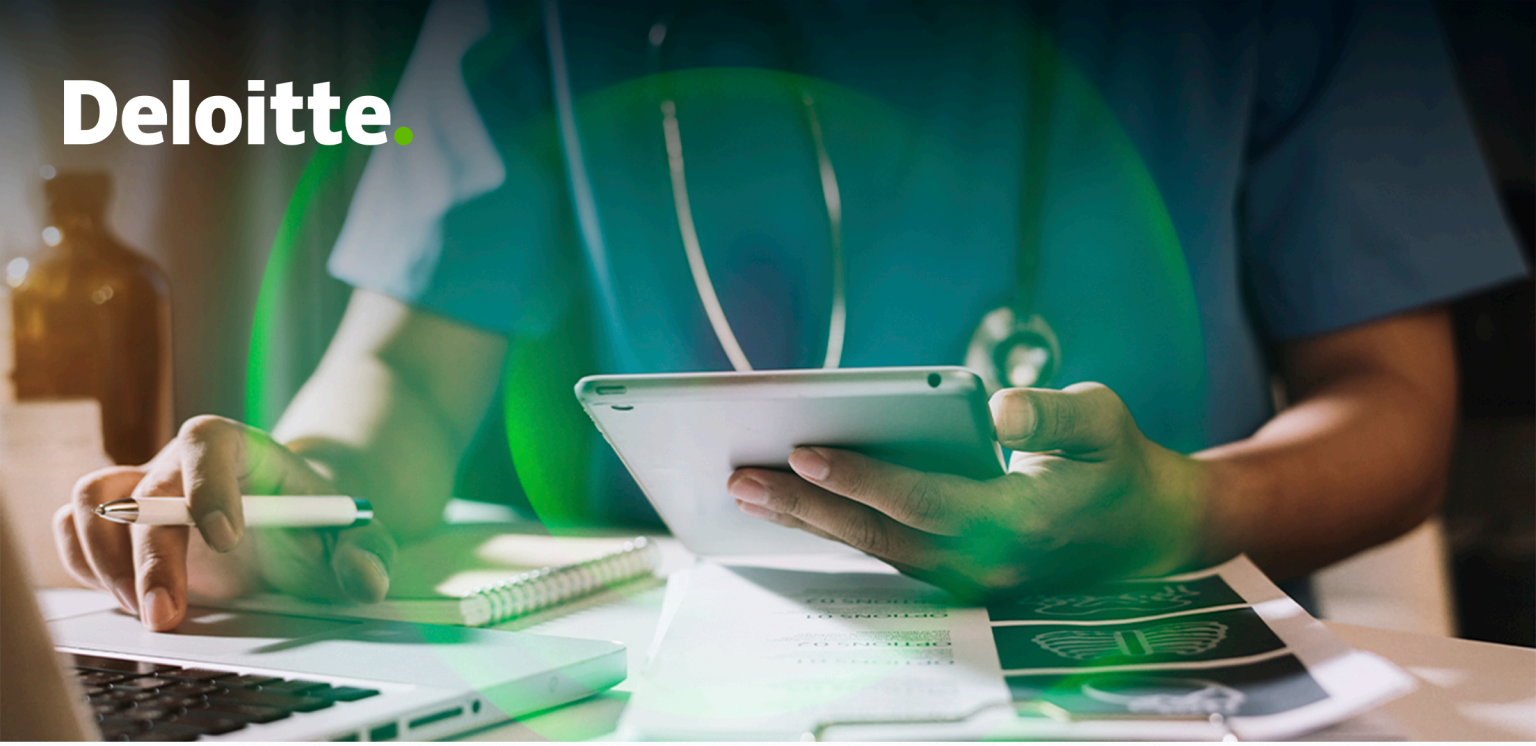

Director en el área Cyber de Deloitte entrega claves de la evolución y futuro de la ciberseguridad en el sector Salud

René Martínez tuvo una destacada participación en la Primera Jornada Chilena de Ciberseguridad en Salud, organizada por la UNAB, Universidad de los Andes, Centro de Extensión del Senado y Biokacking Village.

Con el objetivo de ahondar en los alcances, impacto y desafíos que conlleva la ciberseguridad en el sector de la Salud, se realizó la Primera Jornada Chilena de Ciberseguridad en Salud en el campus Casona de Las Condes de la UNAB.

En la ocasión, Marco Antonio Álvarez, presidente del Directorio de la Alianza Chilena de Ciberseguridad, hizo referencia a un reciente estudio de Deloitte que grafica el alto valor de una copia electrónica de una ficha clínica, superior al de una tarjeta de crédito. Los ciberdelincuentes pueden sacarle cientos de dólares por la relevancia de sus datos. "Así, los desafíos surgen en la sensibilidad de los datos de salud. Hacemos un llamado para continuar avanzando y contar con una institucionalidad robusta en materia de ciberseguridad; avanzar en material legislativa que nos permita ser un país más seguro", señaló.

Por su parte, Víctor Torres Jeldes, Superintendente de Salud del Gobierno de Chile, enfatizó en que la ciberseguridad debe ser una prioridad, considerando que el sector sanitario es cada vez más vulnerable por la falta de cultura de ciberseguridad y el déficit de profesionales capacitados que incrementan la brecha.

"El sector se ha vuelto sumamente atractivo, debido al valor que tiene el robo de datos clínicos y financieros de las personas que se atienden en el sistema. Es fundamental que como país comprendamos que no solo debemos preocuparnos de la protección de los datos clínicos, sino también de garantizar y contemplar una inversión permanente en la actualización y mantención de la funcionalidad de la infraestructura crítica", precisó.

En tanto, René Martínez, Director en el área Cyber de Deloitte, se refirió a la evolución y futuro de la ciberseguridad en la Salud en Chile. "Tenemos que tomar la ciberseguridad más en serio. El 74% de los incidentes de ciberseguridad son producto de la ingeniería social y el 84% de los usuarios reutiliza sus contraseñas. No podemos confiar la seguridad en nuestros pacientes, clientes, colaboradores ni proveedores. Hoy existen 15 billones de dispositivos IoT médicos en el mundo y los dispositivos IoMT representan un gran riesgo. Tenemos que ser conscientes de los riesgos, prepararse, saber qué hacer y tener capacidades de detección temprana y respuesta, pues entre la identificación de un incidente y su contención pueden pasar meses", explicó.

Por último, el especialista enfatizó que el perímetro de ciberseguridad se ha eliminado y que la confianza se establece y verifica en cada sesión. **"La Salud es un ecosistema vivo, interconectado y en constante aprendizaje; la innovación y el futuro de la Salud, así como de la ciberseguridad, vendrán de la mano de la colaboración",** concluyó.