

Protección de Datos, Ciberseguridad y Riesgo Operacional:

Expertos advierten que las nuevas exigencias para el sector salud requieren cambios que van más allá de la tecnología

La adaptación a las nuevas normativas exige revisar procesos, responsabilidades y prácticas de gestión en hospitales y clínicas. Así lo plantearon autoridades, directivos y especialistas de Chile y España durante un encuentro organizado por Eniax en colaboración con Google Cloud y ProSalud Chile, que convocó a cientos de asistentes.

OCTUBRE 2026.- La implementación de las nuevas exigencias de protección de datos y ciberseguridad en salud no depende únicamente de incorporar herramientas tecnológicas. También requiere transformar procesos internos, fortalecer la supervisión de proveedores y preparar a los equipos para responder ante incidentes que puedan afectar la atención de los pacientes. Esta fue una de las principales conclusiones de la [Mesa Ejecutiva del Sector Salud: Protección de Datos, Ciberseguridad y Riesgo Operacional](#), realizada el martes recién pasado en las oficinas de Google en Santiago, donde expertos advirtieron que una eventual postergación de la Ley de Protección de Datos Personales no debería frenar los avances del sector.

El encuentro, organizado por Eniax en colaboración con Google Cloud y ProSalud Chile, se desarrolló en modalidad híbrida, presencial y online, y reunió a 250 asistentes. La jornada convocó a representantes del Consejo para la Transparencia, la Agencia Nacional de Ciberseguridad (ANCI), el Ministerio de Salud y el Centro Nacional en Sistemas de Información en Salud (CENS), además de especialistas jurídicos y tecnológicos, directivos de instituciones sanitarias y un experto internacional conectado desde España.

La discusión se produjo en un escenario marcado por la Ley Marco de Ciberseguridad, que ya establece nuevas responsabilidades para determinados operadores, y la próxima entrada en vigencia de la Ley de Protección de Datos Personales, cuya eventual postergación se encuentra en discusión legislativa. Para las instituciones de salud, ambas normativas plantean desafíos que trascienden la protección de información sensible, al involucrar también la continuidad de los servicios, la seguridad de los pacientes y la responsabilidad sobre los proveedores tecnológicos.

“Chile es uno de los países más digitalizados, especialmente en el área de salud. Pero esa digitalización conlleva no solamente beneficios, sino también riesgos”, señaló Milan Djidara, fundador y CEO de Eniax, durante la apertura. El ejecutivo llamó a mantener la conversación más allá del encuentro, advirtiendo que las instituciones tienen una responsabilidad ética con sus pacientes que no se agota en el cumplimiento de la ley.

En la misma línea, Jean Jacques Duhart, vicepresidente ejecutivo de ProSalud Chile, destacó que el desafío requiere una mirada multidisciplinaria, porque los incidentes tecnológicos pueden afectar no solo la privacidad, sino también la continuidad de la atención clínica y la seguridad de las personas. A su juicio, el sector debe prepararse sin

esperar exclusivamente a las obligaciones legales, fortaleciendo la coordinación y la confianza de los pacientes.

Nuevas normas, brechas pendientes

La conferencia de apertura, moderada por la periodista científica Andrea Obaid, abordó los cambios que introduce el nuevo escenario regulatorio y las dificultades que deberán enfrentar las instituciones para adaptarse.

Natalia González, presidenta del Consejo para la Transparencia, explicó que la nueva legislación establece obligaciones más estrictas, mayores exigencias de rendición de cuentas y un régimen reforzado de protección para los datos de salud. También advirtió sobre los desafíos que enfrenta la puesta en marcha de la nueva Agencia de Protección de Datos Personales, tanto por la conformación de sus autoridades como por los recursos disponibles.

Para González, una eventual postergación podría ofrecer tiempo adicional para resolver parte de estas dificultades, pero también será necesario encontrar un equilibrio entre la protección de los datos sensibles y la posibilidad de continuar desarrollando investigación e innovación sanitaria.

Desde la Agencia Nacional de Ciberseguridad, Juan Ignacio Alarcón, jefe de la División Jurídica, enfatizó la importancia de generar confianza entre reguladores e instituciones para fortalecer la prevención y el reporte de incidentes. “Ante la duda, reporte”, fue su llamado, al explicar que la información entregada por los operadores es fundamental para identificar amenazas y evitar nuevos ataques. Asimismo, recomendó realizar simulacros y contar con procedimientos que permitan responder oportunamente ante una contingencia.

Por su parte, Alejandra García, directora del CENS, planteó que la preparación debe comenzar por identificar qué información sensible manejan las instituciones, quiénes pueden acceder a ella y cómo se controla su uso. También destacó la interoperabilidad como una herramienta para reducir la duplicación de datos y los errores, aunque reconoció las dificultades técnicas y de coordinación que todavía enfrenta su implementación.

José Manuel Villa, encargado de Seguridad de la Información y Ciberseguridad del Ministerio de Salud, reconoció las diferencias de infraestructura y capacidades de protección entre los establecimientos de la red asistencial. En ese contexto, reveló que el Minsal está implementando un Centro de Operaciones de Seguridad (SOC) con capacidades de ciberinteligencia, para anticipar amenazas y detectar posibles filtraciones de información. Asimismo, destacó la necesidad de supervisar los accesos de proveedores externos e incorporar indicadores de gestión que involucren directamente a los equipos directivos en la protección de los sistemas y datos clínicos.

En un segundo panel, especialistas jurídicos y tecnológicos profundizaron en las brechas que persisten en hospitales y clínicas. Entre ellas, el uso de canales informales para compartir información clínica, los controles de acceso insuficientes, la fragmentación de sistemas y la falta de claridad sobre las responsabilidades de los proveedores externos.

Jessica Matus, directora de Privacidad y Protección de Datos de Magliona Abogados, advirtió sobre las dificultades que genera la circulación cotidiana de información médica a través de aplicaciones como WhatsApp y la necesidad de documentar quién accede a las fichas clínicas y con qué propósito. Lizzy Seaman, de Prieto Abogados, subrayó que el desafío no consiste únicamente en conocer las obligaciones legales, sino en hacerlas operativas y generar una cultura de protección de datos en todos los niveles de las organizaciones.

En tanto, Pablo Viollier, de Data Compliance, puso el foco en la creciente dependencia de proveedores tecnológicos, que amplía la exposición de las instituciones y obliga a revisar contratos, responsabilidades y mecanismos de supervisión. Desde la gestión de riesgos, César Pallavicini, de la Alianza Chilena de Ciberseguridad, advirtió que las consecuencias de una falla operacional en salud pueden ir mucho más allá de lo económico. “El riesgo operacional no solo tiene pérdida financiera, puede tener pérdidas humanas”, enfatizó.

La experiencia internacional estuvo representada por Carlos González, delegado de Protección de Datos de la Orden Hospitalaria San Juan de Dios, en España, quien explicó que las certificaciones de seguridad y privacidad no solo permiten acreditar estándares, sino también involucrar a las distintas áreas de una institución. Desde su experiencia, estos procesos contribuyen a que la protección de datos deje de ser una tarea exclusiva de los especialistas informáticos y pase a formar parte de la cultura organizacional.

La continuidad operacional también es clínica

Uno de los momentos centrales de la jornada fue el panel dedicado al riesgo y la continuidad operacional, que reunió a la Dra. María Begoña Yarza, directora del Instituto Nacional del Tórax y exministra de Salud; Claudio García, gerente comercial de Clínica Indisa; y Milan Djidara, y estuvo bajo la moderación de Jean Jacques Duhart.

La doctora Yarza destacó que la digitalización ha mejorado sustancialmente la seguridad de los pacientes al permitir disponer de información clínica, anticipar necesidades y coordinar la atención de personas que requieren seguimiento durante años, muchas de ellas con múltiples enfermedades crónicas.

Sin embargo, esa misma dependencia obliga a prepararse para posibles interrupciones. A partir de su experiencia hospitalaria, relató que han debido realizar simulaciones para enfrentar eventuales caídas de sus sistemas de información, precisamente porque hoy resulta difícil imaginar la operación clínica sin ellos.

“Si esto falla, el primer riesgo son los pacientes, las personas”, advirtió la exministra, quien también defendió la necesidad de contar con planes alternativos que permitan mantener la atención ante contingencias. Además, agregó que las nuevas exigencias regulatorias pueden convertirse en una oportunidad para mejorar la gestión sanitaria. “A mí me gusta esto de que nos pongamos ciertos límites. Porque lo que viene en inteligencia artificial, si no estamos preparados, esto no sé lo que sería”, sostuvo, advirtiendo sobre los riesgos de incorporar nuevas tecnologías sin un marco adecuado.

ENIAX

Para avanzar, propuso fortalecer los espacios de decisión conjunta entre profesionales clínicos, especialistas tecnológicos, equipos jurídicos y directivos, e incorporar la perspectiva de los pacientes en estos procesos.

Desde el sector privado, Claudio García, de Clínica Indisa, identificó dos obstáculos principales para implementar las nuevas exigencias: los costos de inversión y el cambio cultural. Según explicó, la adaptación requiere revisar prácticas habituales, desde el acceso a las fichas clínicas hasta el intercambio de información entre profesionales, además de considerar las diferencias de recursos entre instituciones grandes, medianas y pequeñas.

Djidara, en tanto, advirtió que la digitalización de procesos aislados ha generado sistemas que no siempre se comunican entre sí. A su juicio, el sector necesita avanzar hacia una visión integrada del recorrido del paciente, donde las decisiones tecnológicas respondan a las necesidades clínicas y no únicamente a criterios informáticos o comerciales.

El fundador de Eniax también planteó la necesidad de anticipar dificultades concretas de implementación, como los mecanismos de verificación de identidad de pacientes que realizan gestiones a distancia, y llamó a evitar que las nuevas exigencias terminen obstaculizando el acceso a los servicios de salud.

Al cierre, Duhart enfatizó que el sector debe asumir un papel activo en la discusión sobre cómo implementar las nuevas normativas. “Lo que no podemos hacer es tomar palco y cruzar los dedos para ver qué va a pasar”, señaló, llamando a elaborar propuestas que permitan una transición efectiva, gradual y acorde con la realidad de los prestadores.

La jornada dejó planteado que el principal desafío del sector salud no será únicamente cumplir con nuevas obligaciones legales, sino incorporarlas a la gestión cotidiana de hospitales, clínicas y centros médicos. Un cambio que exige coordinación entre equipos clínicos, directivos, especialistas tecnológicos y proveedores, con un objetivo común: proteger la información de los pacientes sin comprometer la continuidad ni la calidad de su atención.