LITORALPRESS

Fecha: 21-01-2026
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: Cómo se están adaptando a la Ley Marco de Ciberseguridad los Operadores de Importancia Vital en salud pública

Pág. : 23
Cm2: 643,8
VPE: $ 5.704.686

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

Cómo se están adaptando a la Ley Marco de Ciberseguridad los Operadores de Importancia Vital en salud pública

POR LAURA FLORES

El ciberataque que sufrió el Instituto de Salud Pública en junio del año pasado, y la filtración de 250 GB de información -como fichas clínicas, diagnósticos médicos y resultados de exámenes sensibles- a la Clínica Dávila en diciembre, reactivaron el debate sobre la seguridad informática en el sistema de salud nacional.

El 17 de diciembre, la Agencia Nacional de Ciberseguridad (ANCI, creada bajo la Ley Marco de Ciberseguridad) publicó en el Diario Oficial la lista final del primer proceso de calificación de Operadores de Importancia Vital (OIV), es decir, prestadores de servicios esenciales que dependen de redes informáticas y cuya continuidad operativa es crítica para el funcionamiento del país, y que en caso de infracción, arriesgan multas por hasta 40 mil UTM (unos $ 2.780 millones).

El listado calificó a 114 prestadores institucionales de salud (públicos y privados) y 29 servicios de salud bajo la administración del Estado, los que cuentan con un plazo de 60 días corridos -desde su calificación en el Diario Oficial- para designar un delegado de ciberseguridad responsable de informar incidentes a las autoridades, y a jefes superiores, directores y principales ejecutivos de la organización; e implementar medidas para reducir el impacto y la propagación de incidentes de seguridad informática.

DF se contactó con diferentes hospitales y servicios de salud

- Hospitales y servicios de salud ya están avanzando en la designación de delegados de ciberseguridad, capacitación, protocolos de continuidad operativa y sistemas de monitoreo.

pública calificados como OIV para saber cómo están avanzando y adecuándose para cumplir con los requisitos de la ley.

Servicio de Salud Metropolitano Occidente y Hospital Félix Bulnes

La directora del Servicio de Salud Metropolitano Occidente -y en representación del Hospital Clínico Félix Bulnes-, Daniella Greibe, indicó que tanto el servicio como el hospital ya contaban con avances previos a su calificación como OIV, como políticas de seguridad de la información "por distintas fallas en los sistemas".

Destacó que, además de llevar a cabo capacitaciones internas, implementaron un centro de operaciones de seguridad que va detectando y previniendo cualquier amenaza o ataque a los sistemas de información. "Se conformaron comités de ciberseguridad, que partieron elaborando una política que se difundió entre todos los funcionarios", explicó.

Además, Greibe dijo que crearon un "decálogo" de ciberseguridad con recomendaciones para el personal y que, aunque cuentan con tecnología para "poder cumplir en cierta medida" con la neutralización de los ataques, están "en constante búsqueda de recursos" para avanzar en la actualización de sus sistemas.

Añadió que, a pesar de la falta de recursos "humanos y financieros" para dar cumplimiento a la ley, ya designaron un delegado de ciberseguridad a partir de la reasignación de funciones.

Hospital de Urgencia Asistencia Pública

La jefa del Departamento de Tecnología de la Información del Hospital de Urgencia Asistencia Pública, Susana Avendaño, señaló que ya designaron a un delegado de ciberseguridad, y que conformaron un comité especializado de carácter "preventivo" para dar cumplimiento al Compromiso de Gestión del Minsal (Comges) y los requisitos establecidos en la Ley Marco de Ciberseguridad.

Avendaño afirmó que el hospital ya contaba con políticas y procedimientos de seguridad informática antes de su designación como OIV, como un "plan antidesastres" que contempla protocolos "a ejecutar en caso de ciberataques o daño de servidores" y medidas de acción para restablecer la continuidad de los sistemas.

"En caso de caída de sistemas, el proceso clínico continúa su atención con registro en papel, el cual se respalda en digital una vez restablecidos los mismos. En el caso de la ficha clínica, cabe mencionar que los sistemas son controlados por la empresa que presta el servicio, la que tiene el contrato directamente con el servicio de salud", dijo.

Servicios de Salud Metropolitano Norte y Valparaíso-San Antonio

A través de un comunicado, el Servicio de Salud Metropolitano Norte informó avances en ocho líneas de acción.

Entre ellas, la designación de un *CISO* (sigla en inglés de director de seguridad de la información) y un encargado del Sistema de Gestión de Seguridad de la Información; la realización de respaldos diarios de información clínica y administrativa; campañas de concientización a los usuarios a través de canales oficiales; y monitoreo permanente de sus sistemas a través de inteligencia artificial y generación de alertas tempranas.

Según el documento, el servicio está en "proceso de contratación de un profesional con dedicación exclusiva en ciberseguridad, a nivel de la Unidad de Informática", y llevan actualizadas "en un 80%" sus políticas de seguridad de la información, "en concordancia con las normativas vigentes".

Desde el Servicio de Salud de Valparaíso y San Antonio señalaron por escrito que ya designaron un delegado de ciberseguridad, el que ya está "trabajando de manera coordinada con la Unidad de Seguridad de la Información y Ciberseguridad del Ministerio de Salud".