Ciberataques contra la infraestructura de salud. Experiencia internacional

Autor

Juan Pablo Jarufe Bader
Email: jjarufe@bcn.cl
Tel.: (56) 32 226 3173
(56) 22 270 1850

Nº SUP: 139247

Resumen

La Organización Panamericana de Salud, ente regional de la Organización Mundial de la Salud, ha categorizado a la seguridad de la información como "uno de los ocho principios rectores de la transformación digital del sector de la salud".

A su vez, el Banco Mundial recomienda adoptar una serie de medidas para mejorar la resiliencia del sector salud ante ciberataques, entre las que menciona el liderazgo de los Ministerios de Salud y de las autoridades subnacionales, de manera que propongan legislaciones y regulaciones que promuevan prácticas de ciberseguridad en el sector, tanto respecto a los pacientes, trabajadores, proveedores y operadores de la industria; y la consonancia entre la implementación de medidas de ciberseguridad en salud y los llamados Principios de Desarrollo Digital, específicamente el diseño de usuario, el uso de estándares abiertos, el *open data* y *open source*, así como la colaboración internacional.

Por otra parte, la Regla Nro. 71 del Manual de Tallin sostiene que los sistemas y redes computacionales del sector salud deben ser respetados y protegidos frente a posibles ciberataques de cualquier origen. Esta protección cesa en caso de que las redes informáticas de salud, así como las unidades y el transporte médico, sean utilizados para perpetrar actos dañinos contra otras personas, en el contexto de conflictos internos o internacionales, conforme lo recoge la Regla Nro. 73.

Respecto a la penalidad que reciben los ataques contra sistemas de salud a nivel internacional, el artículo 264 numeral 2 de la Ley Orgánica Nro. 10, del Código Penal español, castiga con reclusión de hasta cinco años a quien, por cualquier medio, sin autorización y de manera grave, lesione el funcionamiento de los servicios públicos esenciales o de infraestructuras críticas como las del sector salud.

A lo largo de los últimos cinco años se ha sucedido una serie de ciberataques contra servicios de salud a nivel internacional, como ha quedado en evidencia en países como Alemania, Brasil, España, Estados Unidos, Francia, México y el Reino Unido.

Introducción

El presente documento da cuenta de las medidas sugeridas por diversos organismos multinacionales en materia de ciberataques contra infraestructura hospitalaria, al tiempo de analizar algunos ordenamientos jurídicos que han buscado regular esta materia.

El documento igualmente expone la evidencia más reciente en materia de ciberataques contra los sistemas de salud en el plano internacional.

I. Organismos internacionales y ciberataques contra los sistemas de salud

La Organización Panamericana de Salud (OPS), ente regional de la Organización Mundial de la Salud (OMS), ha categorizado a la seguridad de la información como "uno de los ocho principios rectores de la transformación digital del sector de la salud".

Sobre este punto, la entidad transnacional ha sugerido como líneas de acción (OPS, s/i: 9):

- Presentar instrumentos normativos para regular el tratamiento y acceso a información de salud, en base a los principios de privacidad, confidencialidad y seguridad.
- Enunciar políticas públicas para introducir un plan de seguridad y protección de datos de salud, precisando perfiles de acceso, según las acciones a realizar por el usuario.
- Formar de manera activa a los agentes envueltos en el flujo de información de salud, en lo relativo a pautas de seguridad informática y riesgos asociados.
- Poner en marcha instrumentos de monitoreo, que adviertan ciberincidentes en los mecanismos de información para la salud.
- Implementar instancias de consentimiento informado para ingreso, registro y protección de datos sensibles.
- Hacer operativos servicios centralizados de certificación de seguridad de datos sensibles de salud, a través de tecnologías de certificación de cadena de bloques (*blockchain*).

Por su parte, la Agencia para la Ciberseguridad de la Unión Europea (ENISA) ha estado trabajando desde 2014 con la comunidad de ciberseguridad para el sector salud a través de todo el bloque, con la intención de impulsar la resiliencia del sector, mediante el desarrollo e implementación de un marco regulatorio consistente con principios como el cuidado de la información sensible y la transparencia.

La entidad ha abogado por robustecer la capacidad de respuesta de las instituciones de salud del bloque ante ciberataques, por medio del desarrollo de un marco regulatorio, de un sistema de intercambio de información entre los operadores del sector, la creación de CSIRT sectoriales, y la promoción de discusiones, eventos y conferencias para debatir estos temas (ENISA, 2023).

A su vez, el diagnóstico del Banco Mundial remite a un sector de salud crecientemente inserto en las tecnologías digitales, a la vez que expuesto a los riesgos y vulnerabilidades en este ámbito, con consecuencias que pueden afectar a múltiples actores del sector, desde las agencias de salud públicas hasta los propios pacientes, pasando por los institutos de investigación, las compañías farmacéuticas y los proveedores tecnológicos.

Este impacto podría traducirse en retos a la atención de pacientes, un aumento en las tasas de morbilidad y mortalidad, mayores niveles de ansiedad y estrés entre el personal de salud, y una erosión de la confianza en la capacidad del sector para manejar las ciberamenazas y entregar una atención de calidad (*World Bank*, 2023: 1-2).

En consecuencia, el Banco Mundial ha sostenido que, dada la naturaleza crítica de los cuidados de salud para las sociedades modernas, la ubicuidad de las ciberamenazas y las vulnerabilidades del sector, las consecuencias de un ataque de esta índole sobre los pacientes pueden ser catastróficas, lo mismo que los costos para el sector.

Por lo mismo, la entidad recomienda adoptar una serie de medidas para mejorar la resiliencia del sector salud ante ciberataques, entre las que menciona el liderazgo de los Ministerios de Salud y de las autoridades subnacionales, de manera que propongan legislaciones y regulaciones que promuevan prácticas de ciberseguridad en el sector, tanto respecto a los pacientes, trabajadores, proveedores y operadores de la industria; y la consonancia entre la implementación de medidas de ciberseguridad en salud y los llamados Principios de Desarrollo Digital, específicamente el diseño de usuario, el uso de estándares abiertos, el *open data* y *open source*, así como la colaboración internacional (*World Bank*, 2023: 6-7).

El Banco Mundial también ha sugerido que los países implementen Estrategias Nacionales de Ciberseguridad, que contengan una visión, objetivos de alto nivel, principios y prioridades que guíen al Estado en esta materia, a la vez que entreguen a los actores involucrados un marco con tareas, roles, responsabilidades, pasos, programas e iniciativas a asumir. Esta directriz igualmente debiese contener un análisis de riesgos y capacidades en el sector salud, con un alcance tanto nacional como subnacional.

En este sentido, el organismo ha comprometido financiamiento y asistencia técnica a los países que requieran fortalecer su ecosistema de ciberseguridad, a fin de incrementar la ciberresiliencia de sus infraestructuras críticas. Este apoyo se ha traducido en medidas de prevención contra ataques hacia las personas, tecnologías y procesos.

La respuesta ante ciberincidentes ha sido canalizada, además, mediante el funcionamiento a nivel país de equipos de respuesta ante emergencias informáticas (CERT), equipos de respuesta ante incidentes de seguridad (CSIRT) y equipos de respuesta ante incidentes computacionales (CIRT), todos los cuales asumen la tarea de coordinar respuestas ante ciberincidentes, gestionar cibervulnerabilidades, implementar buenas prácticas en conjunto con el sector privado y propiciar la cooperación internacional.

Otra entidad que ha mostrado su preocupación por los ataques cibernéticos sobre el sector salud ha sido el Foro Económico Mundial, instancia independiente que cuenta con un Centro para la Ciberseguridad, encargado de dirigir la acción global contra los desafíos en este ámbito, concertando la participación de actores públicos y privados.

Entre las medidas más específicas que ha adoptado este organismo, se encuentran (*World Economic Forum*, 2023):

- La capacitación en ciberseguridad, a través de instancias como la Alianza Ciberglobal, que busca proveer un entrenamiento libre y accesible a la próxima generación de expertos en ciberseguridad a nivel mundial.
- La construcción de una arquitectura en materia de ciberseguridad, que incremente la resiliencia de los sectores críticos, como energía, industria y salud.
- El desarrollo de instancias como el Consejo para un Mundo Conectado, que ha establecido requerimientos tecnológicos para responder ante ciberamenazas. Una de estas iniciativas es el *Paris Call for Trust and Security in Cyberspace*, que remite al concepto de paz digital global, enfatizando en la importancia de la confianza y la colaboración.

Asimismo, el concepto de seguridad articulado se sostiene sobre el modelo de "*Zero trust*", que opera sobre el principio de nunca confiar y siempre verificar. En otras palabras, el acceso a los recursos e información nunca debe ser asumido como seguro, aun dentro del perímetro de red. Esta noción se aplica sobre usuarios, infraestructura, redes, carga de trabajo e información, generando un ambiente que ayudaría a construir resiliencia contra ciberataques contra el sector salud.

Esta modalidad implica la puesta en marcha de sistemas continuos de verificación de identidades en tiempo real, que permitan ir consolidando una cibercultura entre las organizaciones del sector salud.

La Cruz Roja Internacional también ha abogado por la construcción de un espacio humanitario digital seguro y confiable, que permita cautelar la información operacional y los datos de las personas.

Esto último ha cobrado mayor relevancia tras el ataque a los servidores de este organismo en enero de 2022, que vulneró la confidencialidad de los datos de 500 mil personas atendidas por los servicios de esta entidad y de su homóloga islámica, la Media Luna Roja. Esta intrusión está referida en particular a los servicios de restablecimiento del contacto entre familiares separados a causa de conflictos internacionales, violencia, desastres naturales y flujos migratorios (Cruz Roja Internacional, 2022).

Finalmente, es dable relevar el régimen regulatorio introducido por el Manual de Tallin, que establece normas sobre resiliencia y respuesta ante ciberataques.

En concreto, la Regla Nro. 70 establece que el personal médico, las unidades de salud y el transporte médico deben ser respetados y protegidos de cualquier ciberataque, tanto en contextos de conflictos nacionales como internacionales, a partir del despliegue de fuerzas militares con capacidad para defender áreas hospitalarias contra ciberactivistas.

La Regla Nro. 71, en tanto, sostiene que los sistemas y redes computacionales del sector salud deben ser respetados y protegidos frente a posibles ciberataques de cualquier origen; mientras la Regla Nro. 72 llama a visibilizar la identificación de computadores que formen parte de las operaciones médicas, incluyendo marcas electrónicas.

Esta protección cesa en caso de que las redes informáticas de salud, así como las unidades y el transporte médico, sean utilizados para perpetrar actos dañinos contra otras personas, en el contexto de conflictos internos o internacionales, conforme lo recoge la Regla Nro. 73 (*Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2017: 204-210).

II. Regímenes sancionatorios contra ciberataques a los sistemas de salud

Respecto a la penalidad que reciben los ataques contra sistemas de salud a nivel internacional, el artículo 265 del *Decreto-Lei* Nro. 2.848 castiga en Brasil con pena de reclusión de uno a cinco años y multa, a cualquier persona que atente contra la seguridad de servicios de utilidad pública, como los de agua, luz, calor o de otra índole. Esta sanción puede ser aumentada entre un tercio y la mitad, si el infractor incurre en la sustracción de material esencial para el funcionamiento de servicios vitales (*Decreto-Lei Nro. 2.848*, 1940).

En la legislación española, en tanto, el artículo 264 numeral 1 de la Ley Orgánica Nro. 10, del Código Penal, castiga con reclusión de entre seis meses y tres años a quien, “por cualquier medio, sin autorización y de manera grave, borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave” (Ley Orgánica Nro. 10, del Código Penal, 1995).

El siguiente numeral incrementa la penalidad hasta por cinco años y multa del tanto al décuplo del perjuicio ocasionado, en caso de que esta acción hubiese lesionado de manera grave el funcionamiento de los servicios públicos esenciales o de infraestructuras críticas como las del sector salud, que pusieran en peligro la seguridad del Estado, de la Unión Europea o de otro país del bloque.

Asimismo, el artículo 349 de la norma castiga con penas de prisión de entre seis meses y dos años, además de inhabilitación especial de entre tres y seis años para ejercer cargos públicos, a quienes contravengan las disposiciones de seguridad vigentes, poniendo en riesgo la vida, la integridad física o la salud de las personas.

Por último, el artículo 573 considera como delito terrorista cualquier acción grave contra la vida, la integridad física o la salud pública, entre otros bienes colectivos.

Respecto al paradigma mexicano, los artículos 84 y 85 de la Ley Federal de Ciberseguridad castigan con entre seis y veinte años de reclusión, más una multa de entre cinco mil y veinte mil unidades de medida, a quienes dañen, alteren u obstaculicen por cualquier medio "el normal funcionamiento de los sistemas informáticos, electrónicos o telemáticos de las instituciones que componen el sistema financiero, las infraestructuras críticas de la información y los sistemas gubernamentales" (Ley Federal de Ciberseguridad, 2023).

A su vez, el artículo 86 sanciona con entre ocho y 25 años de cárcel, más multas de entre ocho mil y veinte mil unidades de medida, a quienes obtengan de manera ilegal, o bien dañen parcial o totalmente la información de sistemas informáticos de las entidades que conforman las infraestructuras críticas de la información.

III. Ciberataques a infraestructura hospitalaria

En cuanto a la evidencia más reciente de ciberataques contra los sistemas de salud a nivel internacional, es posible dar cuenta de una serie de incidentes en una diversidad de países, como se repasa a continuación.

En el caso de Alemania, la policía lanzó en 2020 una investigación por homicidio, luego de que una mujer muriera durante un ciberataque contra el Hospital Universitrio de Düsseldorf, que desactivó los sistemas computacionales del recinto. La paciente, que recibía tratamiento vital, debió ser trasladada a otro nosocomio, en Wuppertal, a treinta kilómetros de distancia, falleciendo durante ese trayecto ("*BBC News*", 2020).

Brasil ha sido otro país blanco de ciberincidentes sobre el ámbito de la salud. Al respecto, en 2021 el ministerio del ramo debió desactivar el sistema de gestión *online* de vacunas contra el "COVID-19", tras haber sufrido dos ataques sucesivos, con apenas cuatro días de diferencia entre sí.

Los ataques fueron reivindicados por la organización "*Lapsus$ Group*", que borró datos necesarios para certificados de vacunación digital, causando daños que retrasaron la restitución de los sistemas del Ministerio de Salud.

Estos incidentes se suman al error involuntario de un funcionario ministerial, que en noviembre del año pasado filtró los datos de 16 millones de pacientes con COVID-19, incluyendo hojas de cálculos con nombres de usuarios, contraseñas y claves para acceder a diversas cuentas gubernamentales y a las fichas de los pacientes ("*CPO Magazine*", 2021).

En cuanto a España, cabe recordar el reciente ciberataque contra el Hospital Clínic de Barcelona, que supuso el bloqueo de archivos digitales, la suspensión y rezago de cientos de procedimientos clínicos, junto con el secuestro de datos (*ransomware*) con la información clínica de miles de pacientes ("El Economista", 2023).

De forma análoga, en agosto pasado el Hospital Waterbury, de los *Prospect Medical Holdings*, sufrió un ciberataque que obligó a clausurar las unidades de urgencias y otros servicios sanitarios críticos.

El apagón informático que sobrevino puso en peligro la seguridad de los datos del nosocomio, así como las operaciones a pacientes hospitalizados y ambulatorios. De hecho, la intrusión obligó al cierre del servicio de urgencias y a la postergación de cirugías electivas hasta nuevo aviso ("*Deutsche Welle*", 2023).

En la misma línea, en diciembre de 2022 el hospital francés de Corbeil-Essonnes, en las cercanías de París, tuvo que cancelar tres operaciones intensivas y otras tantas del área neonatal, debiendo trasladar seis pacientes a otros centros de salud, tras ser impactado por un ciberataque que le tomó al recinto varias semanas antes de volver a su normal funcionamiento.

Dicha vulneración informática fue seguida por la amenaza de un grupo de *hackers*, en cuanto a publicar información confidencial de pacientes y personal médico en la "*dark web*", si no recibían un millonario pago ("France 24", 2022).

El Departamento de Salud de Irlanda, con más de 4.500 servidores de salud, también se vio comprometido con un ciberataque en mayo de 2021, que generó la postergación de diversos servicios médicos ("*BBC News*", 2021).

De acuerdo al estudio "*Cyber Security Report 2023*", en tanto, los ciberincidentes sobre el sector salud mexicano experimentaron un alza del 74% entre 2021 y 2022, con un total de 1.463 intentos de ciberataques a hospitales, clínicas e instalaciones de investigación durante el año pasado.

El informe también identificó como grupos reconocidos de *ransomware* contra instalaciones médicas, a entidades como "*Lock Bit*", "*BlackCat*", "*Cuba*", "*Zepelín*", "*Conti*" y "*Hive*" ("El Financiero", 2023).

Finalmente, los ciberdelincuentes del ya mencionado grupo "*BlackCat*" atacaron en julio del presente año el *Barts Health NHS Trust*, consorcio responsable de cinco hospitales británicos. La banda cibercriminal amenazó con revelar documentos confidenciales del personal de los centros médicos asociados, incluyendo correos, reportes financieros y datos de tarjetas de crédito (*Cybersecurity Connect*, 2023).

Referencias

"*BBC News*". (2020, septiembre 18). *Police launch homicide inquiry after German hospital hack*. Disponible en: https://www.bbc.com/news/technology-54204356.

"*BBC News*". (2021, mayo 20). *Cyber-attack on Irish health service 'catastrophic'*. Disponible en: https://www.bbc.com/news/world-europe-57184977.

"*CPO Magazine*". (2021, diciembre 21). *Health Ministry of Brazil Hit by Two Ransomware Attacks in One Week; Vaccination Data Stolen & Taken Offline*. Disponible en: https://www.cpomagazine.com/cyber-security/health-ministry-of-brazil-hit-by-two-ransomware-attacks-in-one-week-vaccination-data-stolen-taken-offline/.

Cruz Roja Internacional. (2022, enero 26). Ciberataque contra el CICR: qué sabemos. Disponible en: https://www2.cruzroja.es/-/ciberataque-contra-el-cicr-que-sabemos.

Cybersecurity Connect. (2023, julio 14). *UK hospital cyber attack affects 2.5m*. Disponible en: https://www.cybersecurityconnect.com.au/critical-infrastructure/9318-uk-hospital-cyber-attack-affects-2-5m.

Decreto-Lei Nro. 2.848. (1940, diciembre 7). Disponible en: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm.

"*Deutsche Welle*". (2023, agosto 5). Ciberataque obliga a cerrar varios hospitales en EE.UU. Disponible en: https://www.dw.com/es/ciberataque-obliga-a-cerrar-varios-hospitales-en-eeuu/a-66446426.

"El Economista". (2023, abril 28). Los ciberataques al sector sanitario se disparan un 650%. Disponible en: https://www.eleconomista.es/salud/noticias/12211068/03/23/los-ciberataques-al-sector-sanitario-se-disparan-un-650.html.

"El Financiero". (2023, mayo 3). Sector salud en la mira de los 'hackers': Reportan 74 por ciento de incremento de ciberataques. Disponible en: https://www.elfinanciero.com.mx/empresas/2023/05/03/sector-salud-en-la-mira-de-los-hackers-reportan-74-por-ciento-de-incremento-de-ciberataques/.

ENISA. (2023, septiembre 1). *Health sector*. Disponible en: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health.

"*France 24*". (2022, diciembre 5). *French hospital suspends operations after cyber attacks*. Disponible en: https://www.france24.com/en/france/20221205-french-hospital-suspends-operations-after-cyber-attacks.

Ley Federal de Ciberseguridad. (2023, abril 25). Disponible en: https://www.diputados.gob.mx/LeyesBiblio/iniclave/65/CD-LXV-II-2P-292/02_iniciativa_292_25abr23.pdf.

Ley Orgánica Nro. 10, del Código Penal. (1995, noviembre 23). Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444.

OPS. (s/i). Seguridad de la Información: ocho principios rectores de la transformación digital del sector salud. Disponible en: https://iris.paho.org/bitstream/handle/10665.2/57372/OPSEIHIS230016_spa.pdf?sequence=1.

Tallinn Manual on the International Law Applicable to Cyber Warfare. (2017). Disponible en: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf.

World Bank. (2023, septiembre 1). *Cybersecurity in Health*. Disponible en: https://documents1.worldbank.org/curated/en/099081723223525669/pdf/P17507500a843000d099250f19a00b04019.pdf.

World Economic Forum. (2023, mayo 5). *Healthcare cyber attacks are on the rise: Here's why zero trust will prevent care disruptions*. Disponible en: https://www.weforum.org/agenda/2023/05/cyber-attacks-on-healthcare-rise-zero-trust/.