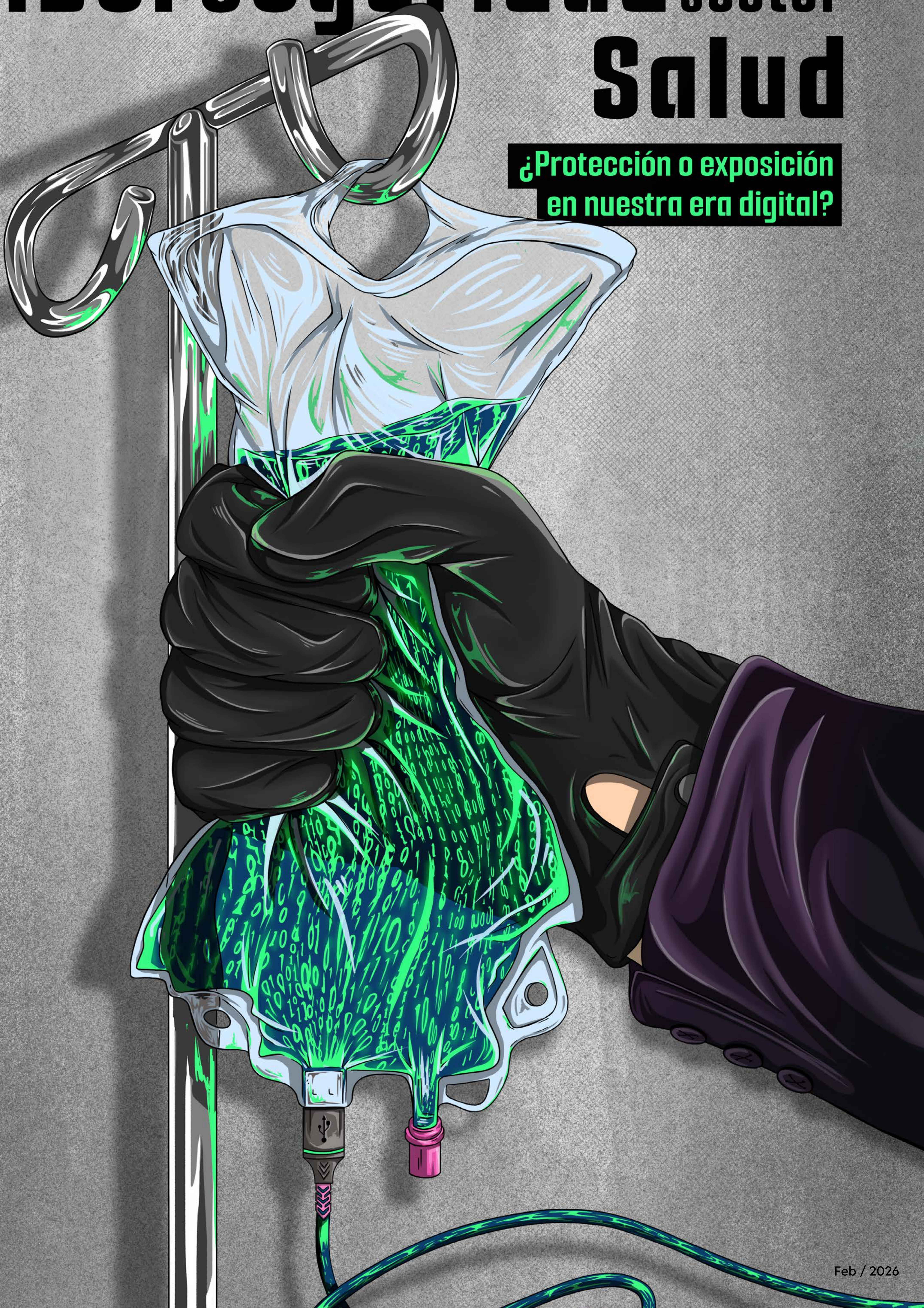
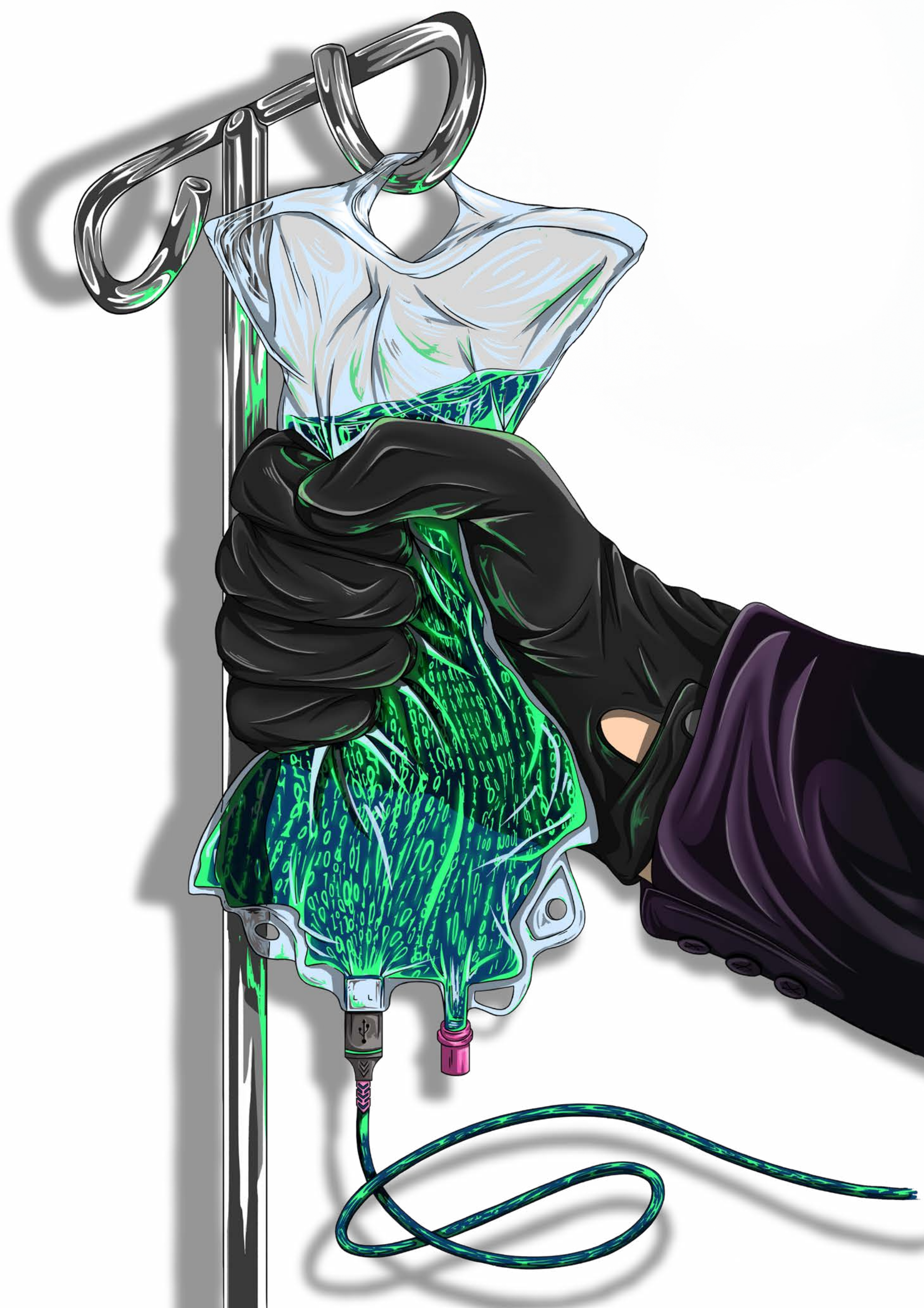


Ciberseguridad^{en} sector Salud

¿Protección o exposición
en nuestra era digital?





Ciberseguridad en sector salud, ¿Protección o exposición en nuestra era digital?

La era digital ha generado avances significativos en el sector salud, potenciando el modelo tradicional de atención a los pacientes. Aun sin tratarse siempre de tecnologías sofisticadas, estas herramientas han permitido mejorar de forma notable los procesos. Hoy, hablar de agendamiento de citas mediante portales web, consultas de telemedicina con médicos especialistas y plataformas que centralizan la información de los pacientes (desde datos demográficos y resultados de exámenes médicos hasta la construcción constante de la historia clínica) equivale a hablar de servicios básicos que las personas esperan recibir de las entidades prestadoras de salud.

Sin embargo, nos encontramos ante un escenario en el que, aun cuando el negocio no tenga un componente tecnológico como parte de su núcleo, debe empezar a escalar su capacidad para resguardar, garantizar y proteger la información sensible que administra.

Entendiendo este contexto, no resulta lejano pensar que un incidente de ciberseguridad en una entidad que presta servicios de salud —como la interrupción de procesos quirúrgicos programados, el bloqueo de acceso a historias y exámenes clínicos, la afectación en la entrega de medicamentos o la exposición de información de las personas— pueda derivar en escenarios críticos que afectan directamente la salud y la integridad del paciente.

Principales retos que se asumen al concentrar datos y servicios que pueden afectar la integridad de las personas

Los principales retos implican que las compañías de salud desarrollen mesas de trabajo que logren integrar visiones holísticas ya que el componente tecnológico no es el único que enfrenta grandes retos:

Recientemente, IBM publicó el estudio “Healthcare Industry Attack Trends 2024”, centrado en EE. UU., en el que concluye que las pérdidas pueden ascender a miles de millones de dólares. Un ataque de ransomware, por ejemplo, puede comprometer procesos de facturación, autorizaciones y la prescripción de medicamentos.

Los procesos de actualización de equipos y tecnologías no suelen tener tiempo favorables que logren disminuir de manera temprana la exposición. Gran parte de los hospitales usan equipos y sistemas operativos antiguos que son difíciles de actualizar y que compromete la disponibilidad en la prestación de servicios

IoT y avances tecnológicos ahora permiten controlar de manera remota y automatizada dispositivos médicos como monitores, bombas de presión, resonadores sumando directamente a la superficie de ataque al ser humano y generando riesgos que pueden causar la muerte de los pacientes.

Las regulaciones a nivel global se centran en garantizar la protección de la información relacionada con datos privados y sensibles. De allí surgen marcos normativos más estrictos, como HIPAA, que añade una capa adicional de exigencia en la protección de datos, los cuales pueden incluir información clínica, demográfica, financiera y otra información altamente sensible de los pacientes.

Entendiendo el gran reto ¿Dónde deberían enfocarse las estrategias en las empresas de salud?

Desarrollar una cultura proactiva en la gestión y monitoreo del riesgo cibernético, entendiendo que cualquier evento puede comprometer de manera directa la integridad de los pacientes.

Vinculación de personal experto en la gestión de riesgos que permitan la construcción de estrategias aterrizadas a la realidad de sus compañías.

Segmentación y reducción de la superficie de ataque si se utilizan equipos que pueden tener versiones no tan recientes de software y que por requerimientos de negocio no es viable generar procesos de actualización rápidos e inmediatos.

Planes de continuidad de negocio que puedan ser activados y escalables sin generar una gran codependencia tecnológica habilitando de manera inmediata canales tradicionales de comunicación, estableciendo procesos no tan complejos que permitan canalizar y responder a las necesidades de los pacientes.

Apoyo por parte de los gobiernos en la creación de herramientas que permitan guiar y robustecer las capacidades de respuesta de las entidades prestadoras de servicios de salud, reafirmando el compromiso con la vida de los ciudadanos.

Para el sector salud, la ciberseguridad debe entenderse como un elemento que forma parte de la esencia del negocio, directamente ligado al bienestar del paciente. Sobre las organizaciones recae la responsabilidad de implementar controles técnicos, promover la concientización y construir un ambiente de control que sea sostenible en el tiempo.

Si lo pensamos con detenimiento, la relación con cada paciente es de largo plazo, debido a la cantidad de información sensible que se custodia y que, probablemente, deberá protegerse durante toda la vida de esa persona. En última instancia, se trata de comprender que el negocio gira en torno a crear y mantener la oportunidad constante de salvar vidas.

Ataques a entidades del sector salud

Grupo Fleury (Red de laboratorios y diagnóstico)

Brasil

Junio de 2021

Ataque de ransomware (REvil) que obligó a apagar sistemas internos; el portal web y el agendamiento de exámenes quedaron fuera de servicio, interrumpiendo la atención y poniendo en riesgo grandes volúmenes de datos personales y médicos de pacientes.

Ministerio de Salud de Brasil (ConecteSUS)

Brasil

Diciembre de 2021

Ransomware atribuido al grupo Lapsus\$: caída de los sitios del Ministerio y de la app ConecteSUS; los atacantes afirmaron haber exfiltrado y borrado alrededor de 50 TB de datos, incluyendo información de vacunación COVID-19 y certificados digitales.

Keralty (incluye EPS Sanitas y Colsanitas)

Colombia

Noviembre de 2022

Ransomware atribuido al grupo RansomHouse; afectó servidores, portales web y sistemas de agendamiento. Hubo suspensión parcial de operaciones, largas filas y demoras superiores a 12 horas para recibir atención médica en varios centros asistenciales.

Instituto Oncológico Fundación Arturo López Pérez (FALP)

Chile

Diciembre de 2021

Ataque de ransomware del grupo INC Ransom, considerado el primer caso documentado de este grupo contra el sector salud en Chile. Dejó inoperativos el sitio web, el portal de pacientes “Mi FALP” y el sistema de reservas médicas durante varias semanas, afectando tratamientos oncológicos críticos.

Ministerio de Salud de la Nación (MinSal)

Argentina

Junio de 2024

Ataque de ransomware que cifró datos críticos y paralizó sistemas del Ministerio durante varias semanas. Los atacantes exigieron un rescate en criptomonedas; el incidente impactó la continuidad de servicios de salud y la gestión de información sanitaria a nivel país.



KERBEROS

MANAGING GENERAL AGENCY

www.kerberosre.io