

Número de control: 20155735

Nombre: Martín Maximiliano Gutiérrez Piñón

Fecha: Domingo, 24 de Agosto de 2025

Actividad: Proyecto final “Ciberseguridad y modelo de negocio orientado a organismos de la salud en México”

Materia: Marco jurídico de la seguridad informática

## Introducción

La digitalización acelerada del sector salud ha transformado la forma en que los hospitales registran, almacenan y comparten información clínica. Historias clínicas electrónicas, sistemas de imagenología, dispositivos médicos conectados y plataformas de telemedicina han mejorado la eficiencia operativa y la calidad de la atención, sin embargo, también se ha ampliado la superficie de ataque y la exposición de datos personales sensibles. En México, estos datos están protegidos por marcos legales como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), además de los derechos ARCO y las Normas Oficiales Mexicanas aplicables al expediente clínico y a los sistemas de información en salud. El incumplimiento no solo implica sanciones y pérdida de confianza, sino riesgos directos para la seguridad del paciente y la continuidad operativa.

La ciberseguridad aplicada en los hospitales y clínicas deja de ser un asunto que debe tomarse a la ligera ya que pueden recibir multas millonarias por no cumplir con el manejo correcto de la información de sus pacientes. Amenazas como el ransomware, phishing, accesos no autorizados y la manipulación de dispositivos del internet de las cosas médicas (IoMT) pueden paralizar servicios críticos, comprometer diagnósticos, y afectar la toma de decisiones médicas. El otro punto es que también la información de los pacientes se cataloga como sensible y pueden utilizarla con fines delictivos hacia la vida personal de los pacientes por eso es necesario la implementación de marcos de seguridad como la ISO 27001 o el NIST.

Este proyecto aborda la problemática desde una perspectiva general donde identificamos amenazas y vulnerabilidades frecuentes en entornos hospitalarios, evalúa brechas respecto a obligaciones legales, buenas prácticas y que propone un plan de ciberseguridad con medidas técnicas y administrativas, así como un programa de capacitación para el personal. La finalidad es proteger la confidencialidad, integridad y disponibilidad de la información clínica y asegurar la continuidad de los servicios de salud, fortaleciendo la confianza de pacientes, profesionales y autoridades en el ecosistema hospitalario.

## Motivos de selección del tema

Cuando comencé con esta materia no conocía las leyes que protegen a la sociedad pero conforme fui avanzando y conociendo mas encontre puntos débiles en el sector salud ya que es un sector bastante olvidado en cuanto a la protección de la información así que decidí realizar un modelo de negocio donde en un futuro yo pueda ofrecer mis servicios a dichas entidades hablándoles sobre la ciberseguridad y auditando sus sistemas como hacker ético, el sector salud es uno de los ámbitos más críticos en cuanto al manejo de información, ya que administra datos sensibles de pacientes como historiales médicos, diagnósticos, tratamientos y datos personales. La digitalización de la información de los servicios de salud, el uso de sistemas electrónicos de historias clínicas y la interconexión de dispositivos médicos hacen que los hospitales se conviertan en objetivos atractivos para ciberataques.  
 La creciente amenaza de ransomware, robo de datos y accesos no autorizados pone en riesgo tanto la seguridad de los pacientes como la continuidad de los servicios hospitalarios.

La ciberseguridad en hospitales es un tema urgente y prioritario, no solo por el cumplimiento de leyes y normativas, sino también por el impacto directo en la vida de las personas ya que un ataque puede paralizar dichos servicios dando inicio a situaciones sociales muy graves.

## Definición y desarrollo del planteamiento del problema

El problema central radica en la falta de preparación y protección adecuada de los sistemas informáticos y físicos de hospitales. Muchas instituciones de salud cuentan con infraestructura tecnológica desactualizada, escasos recursos para invertir en seguridad informática, información sensible en formatos físicos y una baja o nula cultura de prevención por parte del personal.  
Esta situación genera vulnerabilidades que pueden ser explotadas por atacantes, ocasionando

* Filtración de datos personales y médicos.
* Alteración de diagnósticos o historiales clínicos.
* Interrupción de servicios médicos.
* Incumplimiento de normativas como la Ley de Protección de Datos Personales (según el país).

El problema no es solo tecnológico, sino mayormente organizacional y humano, pues la capacitación y concienciación del personal es clave para prevenir incidentes.

### Objetivo general

Implementar planes integrales de ciberseguridad en hospitales para garantizar la protección de la información sensible de los pacientes, el cumplimiento de normativas legales y la continuidad de los servicios médicos.

### Objetivos específicos

1. Analizar las principales amenazas cibernéticas que afectan al sector hospitalario.
2. Identificar vulnerabilidades en la infraestructura tecnológica y en la gestión de la información.
3. Proponer políticas y protocolos de seguridad que incluyan aspectos técnicos, organizacionales y legales.
4. Diseñar un plan de capacitación para el personal hospitalario en materia de ciberseguridad.
5. Evaluar el cumplimiento normativo en relación con la protección de datos sensibles en el ámbito de la salud.
6. Ayudar a este sector tan olvidado y desatendido en cuanto a temas de ciberseguridad dándole un valor invaluable a mi trabajo y dedicación.

## Justificación del proyecto

El presente proyecto se justifica en la necesidad de proteger la información médica y garantizar la seguridad de los pacientes en un entorno cada vez más digital, los hospitales no sólo manejan datos personales de alto valor, sino que además la disponibilidad de sus sistemas informáticos es crítica para la atención médica.  
Una falla en la seguridad puede traducirse en riesgos para la vida de los pacientes, pérdidas económicas y sanciones legales para la institución, además implementar la ciberseguridad fortalece la confianza entre pacientes y hospitales, mejora la resiliencia de la organización y contribuye al cumplimiento legal.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)

Es la norma que regula a los particulares como empresas, asociaciones civiles, organizaciones privadas o personas físicas con actividad profesional deben tratar los datos personales de sus clientes. Su propósito es proteger la privacidad de los individuos y garantizarles el derecho a la autodeterminación informativa. Esta ley es especialmente relevante en el ámbito hospitalario privado, pues la información médica de los pacientes está clasificada como dato sensible, y por lo tanto exige un nivel más alto de protección.

Establece que toda institución debe contar con un aviso de privacidad en el que informe a los titulares para qué se usan sus datos, cómo se almacenan, si se comparten con terceros y qué medidas de seguridad se implementan. Además, obliga a aplicar controles administrativos, físicos y técnicos que eviten el acceso no autorizado o el mal uso de la información. En caso de incumplimiento, contempla sanciones que pueden ir desde multas económicas muy elevadas hasta situaciones penales.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)

Regula el tratamiento de datos personales en instituciones públicas como organismos federales, estatales y municipales, así como partidos políticos, sindicatos y órganos autónomos. Mientras que la LFPDPPP se enfoca en el sector privado, esta ley busca garantizar que el sector público también sea responsable con la información de los ciudadanos.

Su objetivo es asegurar que los datos personales recolectados por entidades gubernamentales se manejen con seguridad, se usen únicamente para las finalidades establecidas y se eliminen cuando ya no sean necesarios. En hospitales públicos esta ley resulta fundamental porque regula cómo se debe conservar y proteger el expediente clínico electrónico de los clientes. También establece sanciones para funcionarios o instituciones que hagan un uso indebido de los datos, reforzando la rendición de cuentas y la transparencia.

Derechos ARCO

Tanto la LFPDPPP como la LGPDPPSO reconocen los llamados Derechos ARCO, que son el núcleo de la protección de datos en México. Se trata del derecho de toda persona a acceder a la información que una institución posee sobre ella, rectificar los datos si son inexactos o están desactualizados, cancelarlos cuando ya no tienen justificación para ser conservados, y oponerse a su uso en situaciones específicas.

En el ámbito hospitalario, los Derechos ARCO garantizan que los pacientes tengan control sobre sus expedientes clínicos y sobre cualquier otro dato personal que se les haya solicitado. Esto implica que un hospital no puede almacenar, usar o transferir información sin el consentimiento del paciente solo en los casos donde la ley está realizando una investigación o algo por el estilo.

Panorama actual de ciberseguridad en hospitales

1. Aumento sostenido de incidentes y ataques

Los ciberataques contra el sector salud han crecido de manera exponencial. En 2022 se reportó un incremento del 74 % en incidentes a nivel global, siendo el mayor aumento entre todas las industrias

En 2024, las cifras alcanzaron niveles alarmantes: en EE.UU., 14 brechas de datos en salud superaron el millón de registros afectados, comprometiendo a casi 70 % de la población

En lo que va del 2025 se investigaron más de 300 incidentes de seguridad hasta mitad de año, una cifra con clara tendencia a superar la de 2024

Un ejemplo reciente ilustrativo es el ataque con ransomware a DaVita, que afectó a 2.7 millones de personas y generó costos operativos estimados en 13.5 millones USD

2. Principales amenazas y vectores de ataque

El Ransomware continúa siendo la amenaza más grave. En 2024, el 67 % de las organizaciones del sector salud sufrieron este tipo de ataque, con costos de recuperación promedio de más de 10 millones de dólares por incidente

Se proyecta que para 2026, más del 40 % de los sistemas de salud en EE.UU. enfrentarán ransomware, y el costo promedio de una brecha podría superar los 12 millones USD

Suministro de ataques (supply chain): el 62 % de las violaciones en el sector salud se originaron por proveedores externos o terceros

Amenazas internas y errores humanos: en 2024, el 70 % de los incidentes relacionados con pérdida de datos en salud fueron originados por actores internos, ya sea por acción maliciosa o por descuido

Dispositivos médicos conectados (IoMT): equipos como marcapasos, bombas de insulina y sensores, con firmware desactualizado o sin cifrado, amplían la superficie de ataque.

Phishing avanzado e inteligencia artificial: se prevé un aumento en el uso de IA para diseñar correos hiper personalizados, difíciles de detectar por filtros tradicionales. Aplicaciones móviles y portales de pacientes: vulnerabilidades en su desarrollo y controles de acceso deficientes representan riesgos significativos

3. Factores estructurales y desafíos internos

Muchas organizaciones trabajan con infraestructura tecnológica antigua o heredada, difícil de parchear y actualizar lo que las hace susceptibles a vulnerabilidades conocidas.

El personal hospitalario a menudo carece de capacitación en ciberseguridad, lo que agrava el riesgo de errores humanos, como caer en phishing o mala gestión de datos

Recortes presupuestarios: se invierte menos del 6 % del presupuesto de TI en seguridad, limitando la implementación de medidas preventivas y de respuesta

El enfoque está más en cumplir con requisitos normativos que en diseñar estrategias de ciberseguridad basadas en evaluación de riesgos reales.

4. Implicaciones y costos asociados

El costo promedio de una brecha en el sector salud fue de 10.93 millones USD en 2023, casi el doble del promedio de otras industrias.

En 2024, el ataque a Change Healthcare expuso 190 millones de registros médicos y representó un costo estimado en más de 3 mil millones USD.

Además de la pérdida económica, los incidentes pueden interrumpir múltiples servicios médicos esenciales y desgastar de cierta manera la confianza de los pacientes en las instituciones. Un ejemplo emblemático fue el ciberataque “WannaCry” del 2017, que provocó cancelaciones masivas de citas y gastos millonarios en el Reino Unido.

5. Respuestas regulatorias y esfuerzos de mitigación

En Europa, la Comisión Europea propuso la creación de un centro paneuropeo de ciberseguridad para hospitales, bajo ENISA, que incluirá un sistema de alerta temprana operativo desde 2026

A nivel global organizaciones independientes promueven marcos como el NIST e ISO 27001, junto con políticas de segmentación de redes, detección continua y programas de entrenamiento al personal.

Impacto de los ciberataques en el sector salud (ejemplos y consecuencias)

La creciente digitalización de los hospitales y sistemas de salud ha hecho que los ciberataques no solo impliquen pérdidas económicas, sino también consecuencias directas en la atención médica y la seguridad de los pacientes. A continuación, se describen algunos de los casos más relevantes a nivel mundial y sus impactos.

1. WannaCry (2017 – Reino Unido, NHS)

El servicio nacional de salud (NHS) del Reino Unido fue una de las víctimas principales del ransomware WannaCry, que infectó más de 200,000 computadoras en 150 países.

Consecuencias

* Se cancelaron más de 19,000 citas médicas y cirugías.
* Ambulancias tuvieron que ser desviadas a otros hospitales.
* Pérdidas económicas estimadas en 92 millones de libras.
* Se evidenció la vulnerabilidad de sistemas hospitalarios desactualizados y sin parches de seguridad.

2. Change Healthcare (2024 – Estados Unidos)

Una de las empresas más grandes de procesamiento de pagos médicos sufrió un ataque de ransomware que expuso 190 millones de registros de pacientes.

Consecuencias

* Interrupciones masivas en los pagos de seguros médicos.
* Retrasos en tratamientos debido a la imposibilidad de facturar y procesar medicamentos.
* Impacto financiero superior a 3,000 millones de dólares.
* Considerado uno de los peores ciberataques de la historia del sector salud.
* Normativas y marcos regulatorios aplicables: GDPR, HIPAA (en EE.UU.) Ley de Protección de Datos Personales.

3. DaVita (2025 – Estados Unidos)

La empresa de servicios de diálisis fue atacada por un ransomware, comprometiendo los datos de 2.7 millones de pacientes.

Consecuencias

* Exposición de información médica y personal altamente sensible.
* Pérdidas operativas de 13.5 millones de dólares.
* Riesgo de que los atacantes manipulen datos clínicos críticos.

4. Hospital Universitario de Düsseldorf (2020 – Alemania)

Un ataque de ransomware paralizó los sistemas informáticos del hospital.

Consecuencias

* Una paciente que necesitaba atención urgente fue redirigida a otro hospital y falleció durante el traslado.
* Este caso marcó el primer incidente documentado donde un ciberataque hospitalario se relacionó directamente con una muerte.
* El evento llevó a Alemania a reforzar su legislación en ciberseguridad hospitalaria.

5. Ataques a hospitales en España (2025)

Varias comunidades autónomas reportaron ciberataques a infraestructuras críticas, incluidas redes hospitalarias.

Consecuencias

* Interrupciones en consultas externas y sistemas de gestión de citas.
* Aumento de costes de recuperación y presión para invertir en seguridad.
* Refuerzo de la colaboración con la Agencia de Ciberseguridad de la Unión Europea (ENISA).

6. Impacto general en pacientes y operación hospitalaria

* Consecuencias en los pacientes
* Retrasos en diagnósticos y tratamientos.
* Interrupción de cirugías y consultas críticas.
* Exposición de datos médicos sensibles que pueden ser usados para extorsión o fraude.
* Riesgo directo para la vida en casos de atención urgente.

Consecuencias en la operación hospitalaria

* Pérdida de confianza de pacientes y autoridades.
* Incremento de costos operativos por recuperación y demandas legales.
* Paralización de servicios críticos como laboratorios, radiología o administración de medicamentos.
* Cumplimiento forzado de nuevas regulaciones y aumento en primas de seguros cibernéticos.

Modelo general de negocio para ofrecer servicios como freelancer

El modelo de negocio que se plantea busca proporcionar a los hospitales un servicio integral que abarque desde la prevención y monitoreo de amenazas, hasta la respuesta ante incidentes y el cumplimiento normativo. Asimismo, considera la capacitación del personal de salud como un pilar fundamental, ya que la seguridad digital en hospitales depende tanto de la tecnología implementada como de la conciencia y preparación de quienes la operan.

De esta manera, el desarrollo de un modelo de negocio en ciberseguridad hospitalaria representa no solo una oportunidad de emprendimiento, sino también una contribución social al fortalecer la resiliencia del sector salud, proteger la información más sensible de los pacientes y garantizar la confianza en las instituciones médicas frente a los desafíos de la era digital.

## 1. Propuesta de Valor

## Proteger la información sensible de pacientes (historias clínicas, diagnósticos, datos personales y financieros).

## Garantizar la continuidad operativa de los servicios hospitalarios ante ciberataques.

## Cumplimiento de leyes y normativas en México Ley Federal de Protección de Datos Personales, Derechos ARCO, NOMs en salud internacionalmente HIPAA, GDPR.

## Reducción de riesgos legales, financieros y reputacionales.

## Capacitación al personal de salud para crear una cultura de ciberseguridad.

## Servicios adaptados al tamaño del hospital desde clínicas pequeñas hasta grandes hospitales.

## 2. Segmentación del mercado

Es necesario segmentar el mercado para poder enfocarnos en un solo sector y de esta manera hacer lo mejor que podemos.

## Hospitales públicos y privados.

## Clínicas especializadas (laboratorios, oncología, cardiología, etc.).

## Centros de diagnóstico e institutos de investigación médica.

## Gobiernos y dependencias de salud.

## Empresas de seguros de salud que buscan proteger la información de sus asegurados.

## 3. Canales de Distribución

## Contacto directo con directores de TI y administradores hospitalarios.

## Alianzas con colegios médicos y asociaciones hospitalarias.

## Marketing digital B2B (LinkedIn, webinars, ferias de salud).

## Distribuidores de software/hardware médico que integren la ciberseguridad como valor agregado.

## Consultorías presenciales y servicios remotos en la nube.

## 4. Relación con los Clientes

## Consultoría personalizada y diagnósticos de seguridad.

## Contratos de mantenimiento y monitoreo continuo (SLA – Service Level Agreement).

## Soporte 24/7 para incidentes críticos.

## Capacitación constante al personal médico y administrativo.

## Reportes periódicos de cumplimiento y métricas de seguridad.

5. Fuentes de Ingreso

* Consultorías iniciales (evaluación de riesgos y auditorías).
* Venta de paquetes de servicios (firewalls, cifrado, segmentación de red, respaldo en la nube).
* Planes de suscripción mensual/anual para monitoreo y respuesta a incidentes.
* Capacitación y certificación interna del personal hospitalario.
* Integración de soluciones de terceros (antivirus corporativo, SIEM, EDR) con margen de ganancia.
* Proyectos a medida (cumplimiento con HIPAA o ISO 27001).

6. Actividades Clave

* Auditorías de seguridad y pruebas de penetración en sistemas hospitalarios.
* Monitoreo 24/7 de redes hospitalarias y sistemas médicos.
* Gestión de vulnerabilidades y actualización de sistemas.
* Implementación de protocolos de respaldo y recuperación ante desastres (DRP).
* Entrenamiento en ciberseguridad para médicos, enfermeros y administrativos.
* Cumplimiento normativo en salud digital.

## 8. Socios Clave

## Proveedores de tecnología (Cisco, Fortinet, Palo Alto, CheckPoint).

## Empresas de cloud computing (AWS, Azure, Google Cloud).

## Fabricantes de dispositivos médicos IoT (para parches de seguridad).

## Asociaciones médicas y colegios de salud (para acceso a clientes).

## Aseguradoras de salud (que incentivan a hospitales a proteger datos).

9. Estructura de Costos

* Infraestructura tecnológica (equipo para realizar auditorías).
* Gastos en certificaciones y capacitaciones constantes.
* Marketing y relaciones comerciales.
* Seguro de responsabilidad cibernética.
* Costos operativos de soporte 24/7.
* Traslados en vehículo

Mucha de la información y documentos solicitados aquí adelante no los tienen o nunca los han creado por lo que es parte de nuestro trabajo realizarlos ya que precisamente para eso se estaría realizando la auditoría.

1. Documentación legal y normativa

* Políticas internas de seguridad de la información: reglamentos del hospital sobre uso de sistemas, contraseñas, accesos, dispositivos, etc.
* Aviso de privacidad del hospital (conforme a la LFPDPPP o LGPDPPSO).
* Consentimientos informados de pacientes sobre el tratamiento de datos personales y médicos.
* Contratos con proveedores de TI y terceros (ej. servicios en la nube, mantenimiento de software o hardware), para verificar cláusulas de seguridad y confidencialidad.
* Cumplimiento normativo: leyes aplicables (LFPDPPP, LGPDPPSO, Ley General de Salud, Normas Oficiales Mexicanas sobre expediente clínico electrónico como la NOM-024-SSA3-2012).

2. Documentación técnica de infraestructura

* Inventario de activos de TI: servidores, estaciones de trabajo, laptops, dispositivos médicos conectados (IoMT), redes, firewalls, routers, switches y todo lo relacionado con TI.
* Diagramas de red y arquitectura tecnológica: segmentación de redes, interconexiones entre áreas administrativas, médicas y de pacientes.
* Listado de sistemas críticos: expediente clínico electrónico, sistemas de laboratorio, radiología, farmacia, control de citas, facturación.
* Configuraciones de seguridad de firewalls, IDS/IPS, VPNs, routers, switches y servidores.
* Registros de actualizaciones y parches de sistemas operativos, bases de datos y aplicaciones hospitalarias.
* Documentación de respaldos (backups): políticas, periodicidad, ubicación y pruebas de recuperación.

3. Documentación de gestión y procesos

* Política de control de accesos: roles de usuario, privilegios, cuentas administrativas, usuarios externos (proveedores, médicos residentes).
* Registros de accesos y logs de sistemas: quién accedió, desde dónde y cuándo.
* Procedimientos de manejo de incidentes de seguridad: bitácoras de incidentes pasados, reportes de respuesta, planes de mejora.
* Plan de continuidad del negocio y recuperación ante desastres: cómo se mantiene la operación en caso de un ciberataque o caída de sistemas.
* Capacitaciones al personal: evidencias de programas de concientización en ciberseguridad para médicos, administrativos y técnicos.

## 4. Documentación clínica relacionada con TI

## Gestión del expediente clínico electrónico: reglas de acceso, tiempos de conservación, cifrado, interoperabilidad con otros sistemas.

## Uso de dispositivos médicos conectados (IoT e IoMT): manuales de seguridad, protocolos de comunicación, actualizaciones de firmware.

## Interconexión con terceros: laboratorios externos, aseguradoras, farmacias, etc.

## Con toda esta documentación podrás

## Verificar el cumplimiento legal (LFPDPPP, LGPDPPSO, NOMs).

## Identificar riesgos técnicos (red, servidores, dispositivos médicos).

## Evaluar procesos de gestión y cultura organizacional en torno a la seguridad.

## En un hospital, además de revisar servidores y redes, debemos poner especial atención en los dispositivos médicos conectados (monitores, bombas de infusión, equipos de imagenología), porque son una puerta de entrada muy usada en ataques recientes.

Protección legal del prestador de servicios

Cuando se ofrecen este tipo de servicios no solo debemos crear documentos para nuestros clientes potenciales también es necesario que tu como freelancer te protejas ya que estas realizando auditorías de ciberseguridad donde puedes provocar daños colaterales a la estructura de red, al software o puntos finales, tu como freelancer debes limitar tus auditorias, establecer tiempos, costos, que documentos vas a entregar al cliente y el cómo vas a realizar la auditoría, en pocas palabras es necesario que todo lo que vayas a realizar vaya documentado y firmado para evitar problemas legales hacia tu persona.

Para realizar una auditoría de ciberseguridad en un hospital, se necesitan documentos técnicos como administrativos y legales ya que se trata de una institución que maneja información sensible de salud (datos personales sensibles).

El alcance específico de las pruebas se definirá en un documento anexo denominado “Scope of Work (SOW)”, el cual detalla:

* Sistemas, redes y aplicaciones autorizadas para pruebas.
* Tipos de pruebas permitidas (ej. pentesting, revisión de configuraciones, simulaciones de phishing, etc.).
* Métodos prohibidos (ej. ataques de denegación de servicio salvo autorización expresa).
* Horarios autorizados para la ejecución de las pruebas.

Uno de los documentos más importantes es el contrato de prestación de servicios o contrato de auditoría. Este documento establece formalmente la relación entre ambas partes, definiendo con claridad el alcance de la auditoría, las áreas y sistemas que serán evaluados y aquellos que quedan fuera del análisis. Además, debe especificar la duración del proyecto, las fases de ejecución, los entregables esperados, los honorarios y la forma de pago. Incluye también cláusulas de limitación de responsabilidad, de manera que quede constancia de que no eres responsable de fallas no detectadas, daños derivados de sistemas defectuosos o incidentes fuera de tu control.

El acuerdo de confidencialidad, conocido como NDA por sus siglas en inglés, es otro elemento esencial. Este documento protege tanto al hospital como a ti al comprometerse a mantener en secreto toda la información a la que tengas acceso, incluyendo expedientes médicos, datos administrativos y credenciales de sistemas. También delimita excepciones, por ejemplo información que ya sea pública o que deba compartirse por requerimientos legales, y establece la vigencia de la confidencialidad, que suele prolongarse varios años después de concluida la auditoría.

Adicionalmente se recomienda contar con una carta de delimitación de responsabilidades, la cual deja constancia de las actividades específicas que realizarás y aquellas que no forman parte de tu labor. Este documento aclara que tu trabajo consiste en identificar riesgos, evaluar vulnerabilidades y recomendar medidas correctivas, sin garantizar la invulnerabilidad total de los sistemas. Con ello se reduce el riesgo de que se no atribuyan responsabilidades por incidentes que estén fuera de tu alcance profesional.

Es igualmente indispensable obtener una autorización escrita del hospital, firmada por la gerencia o el responsable de TI. Esta autorización sirve como prueba de que tienes el consentimiento formal para acceder a sistemas y redes, incluyendo pruebas de penetración y revisión de información sensible. Contar con esta autorización protege tu actuación legal frente a cualquier reclamación futura por parte de la institución o de terceros.

Se recomienda que como freelancer considere un seguro profesional de errores y omisiones (E&O insurance), que brinda cobertura ante posibles demandas derivadas de errores accidentales durante la auditoría, como interrupciones temporales de sistemas críticos.

En conjunto, estos documentos contrato de prestación de servicios, acuerdo de confidencialidad, carta de delimitación de responsabilidades, autorización del hospital y el seguro profesional constituyen la base legal y profesional que te permite actuar con seguridad y formalidad como auditor de ciberseguridad en hospitales. Su correcta redacción y firma previa al inicio de la auditoría protegen tu reputación, reducen riesgos legales y establecen un marco claro de responsabilidades y expectativas con la institución contratante.

## Conclusiones

La ciberseguridad en hospitales no es un lujo, sino una necesidad crítica para garantizar la seguridad de los pacientes y el funcionamiento del sistema de salud. La implementación de un plan integral de protección informática permite reducir riesgos, cumplir con la normativa legal y aumentar la confianza de la sociedad en los servicios hospitalarios.  
 Si bien existen limitaciones presupuestarias y de personal, la inversión en seguridad digital representa un beneficio a largo plazo, tanto en la protección de datos sensibles como en la continuidad de la atención médica. El futuro de la salud depende de sistemas tecnológicos seguros, resilientes y confiables.

Me gusto mucho esta materia porque aprendí bastante sobre las leyes que hablan de protección de datos y ciberseguridad que existen en México y en el mundo, antes de esta materia yo creía que no existían leyes establecidas en México o que no estaban tan bien definidas pero ahora veo que el problema no es que las leyes no existan lo que a estado pasando es que las empresas y las personas ignoramos demasiado este tema y no le damos la importancia necesaria, es decir, si ocurre un incidente de ciberseguridad muchas empresas no actúan legalmente solo hacen intentos de mitigación pero no documentan, no siguen un plan, no tienen playbooks y un sin fin de problemas más.

Nosotros como sociedad no tenemos conocimiento sobre el tema y no sabemos a dónde acudir cuando nuestra información tiene una exfiltración. Con la investigación de este proyecto me doy cuenta que uno de los mayores problemas es que muchas empresas buscan fortalecer sus sistemas dejando de lado la capacitación de su personal, el talento humano no es el eslabón más débil si no el más descuidado, el olvidado y el más atacado.

Referencias

[revistahospitalaria.org](http://revistahospitalaria.org/)

[computerweekly.com](http://computerweekly.com/)

Rubrik 2024

The Wall Street Journal

Reuters

[hipaatimes.com](http://hipaatimes.com/)

[scnsoft.com](http://scnsoft.com/)

[scnsoft.com](http://scnsoft.com/)

SharkStriker

[disolutions.net](http://disolutions.net/)

[www.elsevier.com](http://www.elsevier.com/)

[disolutions.net](http://disolutions.net/)

[www.elsevier.com](http://www.elsevier.com/)

[scnsoft.com](http://scnsoft.com/)

The Wall Street Journal

[revistahospitalaria.org](http://revistahospitalaria.org/)

El País