

Protocolo de Ciberseguridad

Lineamientos Estratégicos
para la Operación Clínica
del Sistema Nacional de Salud

Dirección General de Modernización del Sector Salud



Gobierno de
México

Salud
Secretaría de Salud

Publicado por la Dirección General de Modernización del Sector Salud
1ª edición, 2026
Septiembre, 2026

D.R. Secretaría de Salud.
Agrarismo 227, Piso 2.
Col. Escandón II Secc.
DT. Miguel Hidalgo. C.P. 11800, CDMX.

Hecho en México.
Se permite la reproducción total o parcial, sin fines comerciales, citando la fuente.

Sugerencia de cita:
Protocolo de Ciberseguridad. [Recurso electrónico]. México: Secretaría de Salud, Dirección General de Modernización del Sector Salud; 2026.

Para efectos del presente documento, las referencias y menciones a personas se entenderán realizadas de manera incluyente y no discriminatoria.

DIRECTORIO DE LA SECRETARÍA DE SALUD

Dr. David Kershenobich Stalnikowitz
Secretario de Salud

Lic. Eduardo Clark García Dobarganes
Subsecretario de Integración Sectorial y Coordinación de
Servicios de Atención Médica

Dr. José Enrique Pérez Olguín
Director General de Modernización del Sector Salud

Lic. Efraín Cornejo Romero
Director de Salud Digital

Lic. Francisco Emmanuel Vázquez Repizo
Subdirector de Salud Digital

Dra. Karina Salas Martínez
Enfermera especialista en área normativa

Mtra. María José Manzano Escalón
Jefa de Departamento de Evaluación de Intervenciones en Salud

Lic. Ricardo Serrano Campuzano
Soporte Administrativo

C. Ian Germán Enciso Raya
Servicio Social

Contenido

CAPÍTULO 1	3
Marco General de la Ciberseguridad	3
Definición y Enfoque Operativo	3
Fundamento Legal	4
CAPÍTULO 2	5
Ciberseguridad para las Instituciones Públicas de Salud: Vulnerabilidades y Amenazas	5
Panorama de Riesgos y Amenazas Cibernéticas Activas	5
Desafíos Estructurales del Sistema de Salud	6
Impacto y Afectaciones Operativas	6
CAPÍTULO 3	7
Gobernanza, Factor Humano y Seguridad Técnica en el Ecosistema de Salud Digital	7
Marco de Gobernanza y Distribución de Responsabilidades	7
Seguridad Digital y Control de Acceso	8
Control y Gestión de Datos en Atención a Distancia	9
CAPÍTULO 4	10
Seguridad de la Infraestructura Física y Tecnológica (Seguridad Multicapa)	10
Endurecimiento (Hardening) de Sistemas y Dispositivos	10
Arquitectura de Red y Perímetro Técnico	10
Protección de la Infraestructura Física y Resiliencia	11
CAPÍTULO 5	12
Estándares Internacionales y Cumplimiento Normativo del Sector Salud	12

CAPÍTULO 1

Marco General de la Ciberseguridad

De acuerdo con el Plan Nacional de Desarrollo 2025-2030, el Estado mexicano impulsará la digitalización más ambiciosa de la historia, así como el fortalecimiento de las capacidades institucionales en materia de innovación tecnológica, análisis de datos y ciberseguridad, con el propósito de ofrecer servicios públicos más eficientes, accesibles y seguros para la población.

Conforme al artículo 42 Ter, fracciones VI y XII de la Ley Orgánica de la Administración Pública Federal, corresponde a la Agencia de Transformación Digital y Telecomunicaciones definir los protocolos de seguridad de la información y emitir las normas y lineamientos obligatorios para la Administración Pública Federal.

La ciberseguridad en las instituciones públicas de salud comprende el conjunto de políticas, controles y procesos destinados a salvaguardar la infraestructura y los sistemas que soportan la Salud Digital.

En este contexto, la transformación digital del Sistema Nacional de Salud requiere consolidar una arquitectura robusta de ciberseguridad que garantice la protección, confidencialidad, integridad y disponibilidad de la información en salud, así como la interoperabilidad segura entre instituciones, plataformas y sistemas digitales. Lo anterior permitirá fortalecer la soberanía tecnológica y de los datos, asegurar el intercambio confiable de información clínica y administrativa, y consolidar la salud digital centrada en las personas, con servicios modernos, coordinados y resilientes frente a riesgos y amenazas del entorno digital.

Definición y Enfoque Operativo

Para efectos de este documento, se adopta la definición oficial establecida en la Política General de Ciberseguridad para la Administración Pública Federal:

“Conjunto de estrategias, procesos, regulación, normas técnicas, controles, herramientas y acciones de cultura y concientización orientadas a proteger los activos, incluyendo la infraestructura tecnológica, redes, sistemas de información, base de datos, datos personales, personas, instalaciones y todo componente en el que se recaba, convierte, almacena, protege, procesa, transmite, usa y recupera información institucional. Su finalidad es establecer, implementar, mantener y mejorar permanentemente la protección de activos contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados, entre otro tipo de acciones que afecten los activos de información protegidos de la APF que ésta gestiona o es responsable. La ciberseguridad contempla mecanismos de prevención, detección, contención, respuesta, recuperación y mejora continua, alineados a estándares nacionales e internacionales.”

Bajo este marco rector, la ciberseguridad en el sector salud no se limita a un enfoque informático estático, opera como el elemento estratégico y transversal para el Sistema Nacional de Salud. Su propósito fundamental es disminuir riesgos y amenazas mediante un modelo dinámico de prevención, detección, contención y resiliencia que garantice la continuidad de los servicios de Atención Médica a Distancia, proteja la soberanía de los datos clínicos de la población y asegure la confianza ciudadana en el ecosistema de Salud Digital.

Fundamento Legal

La obligatoriedad de normar e implementar mecanismos de seguridad digital en las instituciones públicas de salud deriva de un marco de concurrencia y estricta complementariedad institucional entre el ente rector tecnológico y la Secretaría de Salud:

1. **Rectoría Nacional en Ciberseguridad (ATDT):** *Conforme al artículo 42 Ter, fracciones VI y XII de la Ley Orgánica de la Administración Pública Federal, corresponde a la Agencia de Transformación Digital y Telecomunicaciones definir los protocolos de seguridad de la información, así como emitir las normas y lineamientos obligatorios en materia de TIC y seguridad digital para toda la Administración Pública Federal (APF).*
2. **Rectoría Secretaría de Salud:** *Conforme al artículo 39, fracciones I, VI y XIII de la Ley Orgánica de la Administración Pública Federal, en relación con las atribuciones normativas en materia de sistemas informáticos sectoriales, corresponde a la Secretaría de Salud definir las políticas de innovación del Sistema Nacional de Salud, así como emitir las normas, lineamientos y estándares obligatorios en materia de interoperabilidad, tecnologías para la salud, telesalud y el Expediente Clínico Electrónico para todas las instituciones públicas del sector.*

Por lo tanto, este protocolo sectorial no duplica ni sustituye las atribuciones de la ATDT; por el contrario, constituye el instrumento de adopción, implementación operativa y especialización clínica de la Política General de Ciberseguridad dentro del Sistema Nacional de Salud, integrando los componentes, humana y hospitalaria a las directrices emitidas por la Agencia.

CAPÍTULO 2

Ciberseguridad para las Instituciones Públicas de Salud: Vulnerabilidades y Amenazas

La transformación digital de los servicios de salud ha permitido modernizar los procesos de Atención Médica a Distancia, fortalecer la coordinación institucional y ampliar el acceso a servicios mediante el uso de plataformas digitales, sistemas de información, conectividad y herramientas tecnológicas.

En este contexto, la ciberseguridad se ha convertido en un elemento estratégico indispensable para garantizar la continuidad, seguridad y confiabilidad de los servicios de salud.

Las instituciones públicas del sector salud administran y procesan grandes volúmenes de información sensible y estratégica (expedientes clínicos, datos personales, información epidemiológica y registros administrativos) y dependen de infraestructura tecnológica crítica para la operación de hospitales, laboratorios, de la telesalud, la telemedicina, la salud móvil, los registros médicos o de salud electrónicos, dispositivos portátiles y mecanismos de coordinación. Por ello, proteger estos activos digitales contra las amenazas del ambiente digital es una prioridad de seguridad institucional para salvaguardar la soberanía de los datos de salud del Estado y, principalmente, el derecho a la protección de la salud.

Panorama de Riesgos y Amenazas Cibernéticas Activas

Debido al alto valor de la información clínica y de salud, así como a la importancia crítica de la operación hospitalaria, el sector salud enfrenta un contexto de riesgos creciente. Las principales amenazas técnicas identificadas que pueden vulnerar el ecosistema digital son:

- **Ransomware:** Software malicioso que restringe el acceso a sistemas o información mediante el cifrado de datos, exigiendo un pago para su liberación. En el entorno hospitalario, esto bloquea el acceso inmediato a expedientes clínicos, deteniendo cirugías o consultas programadas.
- **Phishing e Ingeniería Social:** Técnicas de manipulación psicológica dirigidas al personal clínico o administrativo para obtener credenciales de acceso a las redes institucionales mediante correos o mensajes engañosos.
- **Ataques de Denegación de Servicio (DDoS):** Acciones orientadas a saturar los recursos tecnológicos y servidores para impedir el funcionamiento normal de portales médicos, sistemas de citas o plataformas de telemedicina.
- **Vulnerabilidades en Dispositivos Médicos Conectados:** Debilidades en la seguridad de equipos biomédicos interconectados (bombas de infusión, monitores de signos vitales, tomógrafos) que pueden ser explotadas para comprometer su funcionamiento o alterar la información que procesan.
- **Robo y Filtración de Datos Clínicos:** Obtención no autorizada de expedientes y datos de salud con fines de extorsión, venta o espionaje, afectando gravemente la confidencialidad y la privacidad de los pacientes.

Desafíos Estructurales del Sistema de Salud

A las amenazas externas se suman vulnerabilidades internas de carácter estructural que limitan las capacidades de defensa del sector y que deben ser atendidas con urgencia:

- *Heterogeneidad Tecnológica y Rezago:* Coexistencia de plataformas digitales modernas con sistemas e infraestructura obsoleta que ya no reciben parches ni actualizaciones de seguridad por parte de los fabricantes.
- *Brecha de Talento Especializado:* Escasez de personal técnico calificado en seguridad de la información enfocado específicamente en entornos hospitalarios y de salud digital.
- *Limitaciones Presupuestarias:* Restricciones en el gasto público para la adquisición, licenciamiento y mantenimiento de controles avanzados de ciberseguridad.
- *Cultura Digital y Factor Humano:* Falta de concientización sistémica en el personal operativo respecto a la seguridad digital, lo que incrementa el riesgo de errores involuntarios o incidentes provocados por usuarios internos.

Impacto y Afectaciones Operativas

La materialización de cualquiera de estas amenazas no se limita a un fallo informático; genera afectaciones graves en la operación del sector salud, tales como:

1. *Interrupciones críticas en la operación de hospitales, unidades médicas y servicios de urgencias.*
2. *Pérdida de integridad y disponibilidad en la información clínica indispensable para la toma de decisiones médicas.*
3. *Compromiso legal por la filtración de datos personales sensibles.*
4. *Pérdida de confianza ciudadana en las instituciones y plataformas de salud del Estado.*

CAPÍTULO 3

Gobernanza, Factor Humano y Seguridad Técnica en el Ecosistema de Salud Digital

La ciberseguridad en las instituciones públicas de salud comprende el conjunto de políticas, controles y procesos destinados a salvaguardar la infraestructura y los sistemas que soportan la Salud Digital. Conforme al artículo 42 Ter, fracciones VI y XII de la Ley Orgánica de la Administración Pública Federal, corresponde a la ATDT definir los protocolos de seguridad de la información y emitir las normas y lineamientos obligatorios para la Administración Pública Federal (APF).

Marco de Gobernanza y Distribución de Responsabilidades

Para asegurar la adecuada coordinación institucional con la ATDT y dar estricto cumplimiento a los mandatos normativos vigentes, se establece la siguiente estructura de gobernanza para el sector salud:

- *Vigilancia y Auditoría Central:* La ATDT, mantiene la facultad exclusiva de vigilar el cumplimiento de la Política General, así como de realizar evaluaciones, auditorías técnicas y requerimientos de información.
- *Alineación Sectorial y Plazos Técnicos:* En consistencia con el Artículo Tercero Transitorio del Acuerdo por el que se emite la Política General de Ciberseguridad para la APF, la Secretaría de Salud y las instituciones del sector adaptarán de forma progresiva sus esquemas de riesgo y arquitecturas lógicas a los lineamientos técnicos, criterios de cumplimiento y formatos oficiales que la ATDT emitirá en un plazo no mayor a 180 días naturales contados a partir del inicio de vigencia de dicha Política.
- *Estructura de Enlace Institucional:* De conformidad con el Artículo Cuarto Transitorio del citado Acuerdo, la Secretaría de Salud y las entidades que integran el Sistema Nacional de Salud formalizarán la designación del Titular Institucional en Materia de Ciberseguridad y de su respectivo Auxiliar dentro del plazo establecido de 60 días naturales. Dichos nombramientos se notificarán por escrito a la ATDT para habilitar los canales oficiales de coordinación operativa y gestión conjunta de incidentes.

Gestión del Factor Humano y Cultura de Prevención

El personal de salud es el eslabón principal en la cadena de seguridad en el entorno clínico. La gestión del factor humano se abordará bajo los siguientes criterios:

- *Capacitación Obligatoria en Ingeniería Social:* Todo el personal médico, de enfermería y administrativo deberá cursar programas anuales de concientización orientados a la identificación de técnicas de manipulación como Phishing, Spear Phishing, Vishing y

Smishing (suplantación de autoridades sanitarias o proveedores de insumos médicos), reduciendo el riesgo de acceso no autorizado a través del engaño.

- **Prevención de Errores Involuntarios:** *Establecimiento de guías operativas estandarizadas en consultorios, laboratorios y áreas de urgencias que eliminen la improvisación en el uso de los sistemas de información hospitalaria. Se implementarán mecanismos de doble verificación para acciones críticas como la exportación masiva de datos o la modificación de privilegios de acceso.*
- **Cultura de Reporte No Punitivo:** *Implementación de canales de comunicación directa y confidencial para que el personal reporte de inmediato sospechas de brechas de seguridad o errores operativos involuntarios, priorizando la contención del riesgo y la resiliencia colectiva sobre la sanción disciplinaria.*

Seguridad Digital y Control de Acceso

El acceso a los expedientes clínicos y sistemas institucionales se regirá por políticas estrictas de control de identidad:

- *Es obligación estricta e intransferible de cada profesional de la salud iniciar sesión de manera individual al comenzar sus actividades de atención médica a distancia y cerrarla manualmente de forma inmediata al apartarse de la estación de trabajo, al concluir una consulta o al realizar el cambio de turno operativo. Si bien los sistemas informáticos dispondrán de mecanismos complementarios de bloqueo automático de pantalla por inactividad, este control no exime al personal de su responsabilidad individual. Cada usuario será legal y administrativamente responsable de cualquier registro, modificación o consulta de datos clínicos que se efectúe bajo su cuenta única mientras esta permanezca abierta.*
- *Implementación gradual y obligatoria de esquemas de autenticación multifactor que combinen contraseñas seguras con códigos de verificación o mecanismos biométricos. Para el acceso a los expedientes clínicos y plataformas del sector, se priorizará la alineación con los estándares internacionales vigentes, garantizando la plena interoperabilidad y compatibilidad con Llave MX, la herramienta centralizada de identidad digital del Gobierno de México. Esto asegurará que la validación de la identidad del personal de salud se realice de manera única, segura y vinculada a la Clave Única de Registro de Población (CURP), mitigando los riesgos de suplantación o accesos no autorizados a datos personales sensibles.*
- *Queda estrictamente prohibido conectar dispositivos personales (celulares, dispositivos de almacenamiento no autorizados) a las estaciones de trabajo. Asimismo, se exigirá el uso de filtros de privacidad en monitores de áreas de alto flujo para asegurar la confidencialidad visual frente a pacientes o personal ajeno.*

Control y Gestión de Datos en Atención a Distancia

Para garantizar el intercambio seguro de datos clínicos y evitar amenazas de exposición de datos personales sensibles durante las interacciones de telemedicina:

- *Todos los datos de salud que se transmitan o almacenen a través de plataformas de telesalud y salud móvil deberán ser cifrados en tránsito (utilizando protocolos seguros como TLS 1.3) y en reposo (mediante algoritmos avanzados como AES-256).*
- *Las bases de datos con expedientes clínicos electrónicos deberán implementar Controles de Acceso Basados en Roles (RBAC) o bien, asegurar que el personal operativo solo visualice la información estrictamente necesaria para la Atención Médica a Distancia*
- *El acceso del personal de salud a las plataformas de atención médica a distancia se realizará de forma obligatoria a través de la e.firma. Al estar vinculada directamente a la Clave Única de Registro de Población (CURP), esta herramienta es el mecanismo oficial para dar certeza jurídica y definir la responsabilidad legal de los profesionales en cada acto clínico digital. Esto garantiza la validez de los registros, recetas e interconsultas emitidas a distancia, protegiendo los derechos del paciente y del personal de salud ante el Sistema Nacional de Salud.*

CAPÍTULO 4

Seguridad de la Infraestructura Física y Tecnológica (Seguridad Multicapa)

La protección del ecosistema de salud digital del Sistema Nacional de Salud requiere trascender la capa lógica y consolidar una arquitectura técnica robusta, redundante y resiliente. La infraestructura tecnológica debe basarse bajo un enfoque de seguridad multicapa, garantizando la continuidad operativa de la Atención Médica a Distancia y la protección de los activos frente a vulnerabilidades críticas.

Endurecimiento (Hardening) de Sistemas y Dispositivos

El fortalecimiento de los activos tecnológicos frente a mecanismos de ataque se ejecutará conforme a los siguientes criterios técnicos:

- **Servidores y Estaciones de Trabajo:** Se aplicarán plantillas de configuración segura (hardening) restrictivas. Esto incluye la deshabilitación obligatoria de servicios, puertos y protocolos innecesarios, la eliminación de cuentas por defecto y la restricción absoluta de privilegios de administrador en los equipos periféricos y terminales de consulta externa.
- **Dispositivos Médicos e Interconectados:** Las instituciones públicas del Sistema Nacional de Salud adoptarán como marco de referencia progresivo los criterios del estándar UL 2900 para la evaluación de vulnerabilidades en equipamiento biomédico interconectado (tales como bombas de infusión, tomógrafos, ventiladores y monitores de signos vitales) antes de su integración a las redes institucionales. Se promoverá, en coordinación con los organismos competentes, que las nuevas adquisiciones de tecnología hospitalaria consideren esquemas de mitigación de riesgos técnicos, el cambio obligatorio de credenciales de fábrica y el aislamiento de su firmware mediante firmas criptográficas.

Arquitectura de Red y Perímetro Técnico

- **Segmentación Estricta de Redes (VLANs):** Las redes hospitalarias deberán estructurarse en zonas lógicas aisladas. Se prohíbe de manera tajante que los dispositivos médicos conectados y los sistemas de Expediente Clínico Electrónico (ECE) compartan segmento de red con los accesos públicos de Wi-Fi o las redes administrativas generales. Esta separación es crítica para reducir las amenazas en caso de una intrusión.
- **Firewalls de Nueva Generación (NGFW) e IDS/IPS:** Se implementarán firewalls perimetrales avanzados en cada unidad hospitalaria y centro de datos. Los Sistemas de Detección y Prevención de Intrusiones (IDS/IPS) deberán estar configurados para identificar y bloquear patrones de tráfico anómalos en tiempo real, vinculando las alertas lógicas con protocolos de reacción inmediata.
- **Gestión del Ciclo de Vida y Parcheo:** Se mantendrá un inventario automatizado y auditable de activos tangibles. Queda prohibido el uso de sistemas informáticos en

"Sombra Tecnológica" (Shadow IT). La atención a vulnerabilidades críticas o de "día cero" (0-day) en sistemas de soporte vital o bases de datos clínicas se gestionará con atención inmediata. Ante la emisión de alertas oficiales por la autoridad competente, se implementarán de forma prioritaria controles de mitigación compensatorios para aislar el riesgo, programando la aplicación definitiva del parche de seguridad bajo un protocolo controlado que garantice la continuidad y seguridad de la Atención Médica a Distancia.

Protección de la Infraestructura Física y Resiliencia

- **Centros de Datos Locales y Periféricos:** Las áreas que albergan servidores hospitalarios y almacenamiento analítico contarán con control de acceso físico biométrico obligatorio, sistemas de videovigilancia de circuito cerrado (CCTV) con retención de grabaciones por un mínimo de 90 días, y mecanismos especializados de supresión de incendios no destructivos (gases limpios), así como control estricto de temperatura y humedad.
- **Redundancia Energética y de Conectividad:** Para garantizar la continuidad de la Atención Médica a Distancia ante fallas técnicas o desastres naturales, cada unidad hospitalaria de segundo y tercer nivel deberá contar con enlaces de conectividad redundantes (físicos y satelitales) y Sistemas de Alimentación Ininterrumpida (UPS) acoplados a plantas de energía de emergencia, capaces de soportar la operación de los sistemas críticos por un mínimo de 24 horas.
- **Estrategia de Respaldo 3-2-1:** Es obligatorio implementar políticas de respaldo automatizadas y cifradas para los datos de salud. Se mantendrán 3 copias de seguridad de los expedientes clínicos, guardadas en 2 soportes de almacenamiento distintos (p. ej., local y nube institucional), y al menos 1 copia plenamente fuera de línea (offline / air-gapped), garantizando la restauración inmediata de la operación ante ataques de ransomware sin ceder a extorsiones.
- **Plan de Continuidad de Operaciones (BCP):** Cada unidad médica del Sistema Nacional de Salud dispondrá de protocolos claros de actuación para el retorno temporal, ordenado y seguro a procesos manuales (en papel) ante una caída total o falla grave de los sistemas digitales, asegurando que bajo ninguna circunstancia se interrumpa la Atención Médica a Distancia ni se comprometa la seguridad del paciente.

CAPÍTULO 5

Estándares Internacionales y Cumplimiento Normativo del Sector Salud

La estrategia de ciberseguridad para las instituciones públicas del Sistema Nacional de Salud adopta y se alinea formalmente con los principales marcos de referencia y estándares internacionales, dotando de rigor técnico, metodológico y legal a todas sus operaciones:

Estándar / Marco de Referencia	Ámbito de Aplicación Específico en el Entorno Clínico
ISO/IEC 27001	Sistema de Gestión de Seguridad de la Información (SGSI). Define los requisitos para establecer, implementar, mantener y mejorar continuamente los controles de seguridad institucionales (Confidencialidad, Integridad y Disponibilidad).
ISO 27799	Gestión de la seguridad de la información en el sector salud utilizando ISO/IEC 27002. Proporciona directrices específicas para proteger la confidencialidad, integridad y disponibilidad de los datos de salud e historiales clínicos de los pacientes.
ISO/IEC 27017 e ISO/IEC 27018	Controles de seguridad para servicios en la nube y protección de datos personales (PII) en nubes públicas, esenciales para el almacenamiento seguro de los expedientes clínicos electrónicos centralizados.
UL 2900	Marco de referencia técnico para la evaluación de vulnerabilidades de software y pruebas de penetración en dispositivos médicos conectados. Su adopción en el entorno clínico será gradual y coordinada con las instituciones del sector para fortalecer la seguridad analítica en áreas críticas.
FIDO2 y WebAuthn	Estándares de autenticación criptográfica de clave pública que eliminan el uso de contraseñas vulnerables, base tecnológica del esquema nacional LlaveMx para el acceso del personal de salud.

Bibliografía y documentos de consulta

Agencia de Transformación Digital y Telecomunicaciones. (s.f.). *Ciberseguridad*. Gobierno de México. <https://www.gob.mx/atdt/agendas/ciberseguridad>

Agencia de Transformación Digital y Telecomunicaciones. (2026a). *Plan Nacional de Ciberseguridad 2025–2030*. Gobierno de México. https://www.portal.atdt.gob.mx/wp-content/uploads/2026/01/Plan_Nacional_de_Ciberseguridad-2.pdf

Agencia de Transformación Digital y Telecomunicaciones. (2026b). *Plan Nacional de Infraestructura Digital para México*. Gobierno de México. https://www.portal.atdt.gob.mx/wp-content/uploads/2026/04/Plan_Nacional_Infraestructura_Digital_MX.pdf

Agencia de Transformación Digital y Telecomunicaciones. (2026c). *Política de Ciberseguridad para la Administración Pública Federal*. Gobierno de México. https://www.archivos.atdt.gob.mx/storage/app/media/Politica_de_Ciberseguridad_APF.pdf

Banco Interamericano de Desarrollo [BID]. (2022). *Protegiendo la salud digital: Una guía de ciberseguridad en el sector de salud*. <https://publications.iadb.org/en/publications/spanish/viewer/protegiendo-la-salud-digital-una-guia-de-ciberseguridad-en-el-sector-de-salud.pdf>

Centro de Estudios Superiores Navales [CESNAV]. (2018). *Ciberseguridad: desafíos y oportunidades para México* (Documento de análisis No. 48-18). https://cesnav.uninav.edu.mx/cesnav/ININVESTAM/docs/docs_analisis/da_48-18.pdf

Comisión Europea. (2022). *European action plan for cybersecurity in hospitals and healthcare providers*. Dirección General de Redes de Comunicación, Contenido y Tecnologías. <https://digital-strategy.ec.europa.eu/es/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers>

Consejo de la Unión Europea. (s.f.). *Ciberseguridad: protección de las redes y sistemas de información en la UE*. <https://www.consilium.europa.eu/es/policies/cybersecurity/#research>

Craig, D., Diakun-Thibault, N., y Purse, R. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *National Institutes of Health*. <https://pmc.ncbi.nlm.nih.gov/articles/PMC9543401/>

Departamento de Seguridad Nacional [DSN]. (s.f.). *El Consejo de Seguridad Nacional*. Gobierno de España. <https://www.dsn.gob.es/es/estructuras-de-seguridad-nacional/el-consejo-de-seguridad-nacional>



Gobierno de
México

Salud

Secretaría de Salud