UNIVERSIDAD PRIVADA DEL NORTE

FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

“MODELO DE CIBERSEGURIDAD PARA EL SECTOR DE SALUD PÚBLICA: 2018-2020”: una revisión de la literatura científica

Trabajo de investigación para optar al grado de:

Bachiller en Ingeniería de Sistemas Computacionales

Autor:

Maylen Alida Alvines Villegas

Asesor:

Mg. Ing. Michael Alejandro Cabanillas Carbonell

Lima - Perú

2020

DEDICATORIA

Esta revisión de la literatura está dedicada a mis padres, mis asesores por apoyarme y guiarme en cada decisión. Enseñarme a ser perseverante y que siempre tenemos que apuntar a más.

Maylen Alida Alvines Villegas

AGRADECIMIENTO

Mi agradecimiento a Dios, a mis padres.

Maylen Alida Alvines Villegas

Tabla de contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Hoy en día la información de diversos centros de salud se ha visto afectada por ciberataques, estos problemas surgen debido a que a que no se cuenta con planes eficientes y consistentes de ciberseguridad. Afectando enormemente a la seguridad nacional, ya que se habla de data personal masiva, financiera e intelectual. En la actualidad se afirma que el sector de salud se sitúa entre los cinco sectores principales que se encuentran expuestos a mayores riesgos de seguridad desde el 2018. Por lo que es de vital importancia tomar medidas para proteger la privacidad datos del personal y del público.

La presente revisión sistemática tiene como objetivo analizar modelos de ciberseguridad aplicado al sector salud pública. En esta revisión se sintetizaron los datos extraídos de 50 artículos, relacionados al tema de ciberseguridad y modelos de ciberseguridad. La búsqueda de la información se realizó en la base de datos de IEEEXLORE, Scopus, WOS y Science Direct. En total se encontró que el 52% de artículos (26) son analíticos y el 48% son descriptivos (24).

La revisión de la literatura científica realizada nos indica que las características básicas que debe presentar un marco de ciberseguridad dirigido al sector de salud pública; entre ellas tenemos: tamaño pequeño a mediano, adaptable, componible y reusable.

PALABRAS CLAVES: Revisión sistemática, salud, seguridad informática, ciberseguridad, ciberataques. .

CAPÍTULO I. INTRODUCCIÓN

En los últimos años, la ciberseguridad ha tomado un gran papel a nivel mundial, para todo tipo de empresas, organizaciones, etc. Debido a la cantidad de datos sin precedentes que estás recopilan, procesan y almacenan en computadoras, celulares y otros dispositivos. Una gran parte de estos datos es información confidencial, ya sea propiedad intelectual, datos financieros, información personal u otro tipo de dato, y el acceso a estos o la exposición no autorizada podrían tener consecuencias negativas. ("¿Qué es la seguridad cibernética?", 2020)

Y es que con el desarrollo de nuevas técnicas y herramientas, los ciberataques han aumentado considerablemente. Este es un problema real, independientemente del tamaño de la empresa u organización, ya que hoy en día las nuevas tecnologías son una de las principales herramientas para llevar a cabo sus funciones. A medida que crece el volumen y la sofisticación de los ataques cibernéticos, las entidades, especialmente aquellas que tienen la tarea de proteger la información relacionada con la seguridad nacional, la salud o los registros financieros; deben tomar medidas para proteger su información comercial y personal confidencial. (it Digital Media Group, 2019)

Uno de los sectores más afectados y vulnerables a los ataques cibernéticos, son los sistemas de salud, por varias razones, una de ellas explicada por Branley & Coventry (2018), es que contienen muchos dispositivos interconectados, desde equipos hospitalarios hasta pacientes de la comunidad con sensores implantables; carecen de normas de seguridad, planes eficientes y consistentes de seguridad en los productos utilizados, además es poco probable que la ciberseguridad sea una prioridad a la hora de comprar un equipo.

Estos fallos tienen profundas consecuencias para los pacientes, tanto en los resultados clínicos, como en la violación de los datos personales, afectando enormemente a la seguridad

nacional, ya que se habla de data personal masiva, financiera e intelectual, lo cual llegaría a eclipsar incluso el terrorismo. Y es que Joaquín Ruiz Díaz (2016), recalca que para los terroristas, el conocimiento y la captura de esta información, constituyen a una amenaza para la sociedad que es necesario prevenir y combatir. Es por esto que para construir un sistema de salud confiable es necesario desarrollar un modelo estándar de ciberseguridad.

Para tener mayor conocimiento del problema, debemos definir el concepto de ataque cibernético. Según Tyas Tunggal. (2020) es cualquier intento de exponer, alterar, desactivar, destruir, robar u obtener acceso no autorizado a un sistema informático, infraestructura, red o cualquier otro dispositivo inteligente. Por otro lado, Bendovschi Andrea (2015), indica que todas las definiciones de ataque cibernético, tienen en común el objetivo de comprometer la confidencialidad, la integridad y la disponibilidad de los datos. La tecnología, trae consigo el progreso del cibercrimen, por lo que las nuevas formas de realizar ataques, llegan a ser aún más difíciles y permanecen sin ser rastreados, desarrollándose continuamente. Otra definición sería la de Repp: "Un proceso/acción, cuyo propósito es capturar el control de la red informática y/o su desestabilización. Como cualquier proceso, un ciberataque se caracteriza por una cierta secuencia de etapas, llamada ciclo de vida." (Repp, 2018). Finalmente, Hannaway y Crootov (2011) expresan que los ataques cibernéticos consisten en cualquier acción realizada para socavar las funciones de una red informática con fines políticos o de seguridad nacional. Puede llevarse a cabo mediante cualquier acción: hackear, bombardear, cortar, infectar, etc.- pero, para que sea un ciberataque, debe tener por objeto socavar o perturbar el funcionamiento de una red informática.

Otro término a definir es el de ciberseguridad, que según el autor Gómez Vieites (2014), en su obra Enciclopedia de la Seguridad Informática, la define como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos

puedan ocasionar daños sobre la información, violar la confidencialidad, autenticidad o integridad, bloquear el acceso de todos los usuarios autorizados al sistema y reducir considerablemente el rendimiento de los equipos.

De acuerdo lo citado anteriormente, se evidencia el gran riesgo que representan los ataques cibernéticos, Jacqueline Ross (2018), recalca que las amenazas al sector salud son reales, así como la importancia de la protección de la información del paciente, y la importancia de construir una cultura organizacional de seguridad con educación y entrenamiento. Lo cual implica que se deben plantear medidas (como el uso de un software de antivirus, detección de intrusos, antimalware, marcos y estándares) y protocolos para resguardar la seguridad informática. Se debe tener en cuenta que la ciberseguridad se ve condicionada por distintos factores y características del propio sistema y su entorno, por lo que también es necesario contemplar cuestiones como el nivel de centralización / descentralización del sistema, funcionamiento, sensibilidad, evaluación de entorno y el cumplimiento del marco legal vigente (Protección de datos personales, protección de la propiedad intelectual, etc).

Ante lo indicado, se realiza la presente investigación con el fin de responder a la pregunta: ¿Cuáles son las características de modelo de gestión de ciberseguridad para el sector salud pública? Orientado a enfrentar este problema lo que se propone identificar el modelo de ciberseguridad más apto para el sector de salud, que reducirá el riesgo de sufrir ciberataques.

Por lo tanto, el objetivo de estudio buscar las mejores prácticas de seguridad informática aplicado al sector salud pública. En la investigación se han considerado revistas publicadas en el ámbito del continente americano haciendo un análisis exhaustivo del tipo de publicación y revista, diseño de investigación, sector, instrumentos y variables de estudio

CAPÍTULO II. METODOLOGÍA

2.1 Tipo de estudios

La recopilación de las fuentes de información se realizó en los meses de abril a mayo del 2020 sobre estudios relacionados con la investigación "Diseño de un modelo de seguridad para el sector de salud pública". Tomando en consideración los siguientes criterios:

a) Artículos de estudios con información relacionada la ciberseguridad, descripción de componentes de un modelo de ciberseguridad, describir los factores críticos de que un modelo de ciberseguridad debe cumplir. Estos artículos se encontraron en su mayoría en IEEEXPLORE, Scopus, WOS y Science Direct.

b) El periodo de publicación comprende entre los años 2018 -2020, el objetivo principal es hallar información sobre modelos de seguridad informática. Se trabajó con la información de revistas publicadas en los últimos diez años.

c) Para encontrar información relacionada al tema anteriormente señalado, se consideró el título. Se buscó información sobre el tema en cada BD con las siguientes palabras claves:

    a. IEEPLORE: Ciberseguridad, ciberataques, seguridad informática, salud.

    b. Scopus: Ciberseguridad, ciberataques, seguridad informática, salud.

    c. Web of Science: Ciberseguridad, seguridad informática, salud.

    d. Science Direct: Ciberseguridad, ciberataques, salud.

    Según la información adquirida la muestra estuvo conformada por artículos con contenido sobre modelos de seguridad de la información.

Los criterios de inclusión empleados fueron los siguientes: El artículo debe medidas adicionales de ciberseguridad a aplicar en el sector salud, contener información relacionada a modelos de ciberseguridad o modelos de ciberseguridad aplicados al sector de salud, debe contener una breve descripción del modelo y debe describir los puntos claves que debe contener un modelo.

En cuanto a los criterios de exclusión, el artículo no muestra un modelo de ciberseguridad o no contiene información relacionada al tema en revisión.

2.2 Codificación de datos

Luego de seleccionar los artículos más importantes se procedió a clasificarlos (Tabla N°1). Los artículos fueron codificados de acuerdo con las características de las revistas y publicaciones año de publicación, nombre, gestor de base de datos, sector, tipo de estudio, lugar de procedencia, objetivo.

Tabla 1: Características de la unidad de análisis

	Año	Nombre	Gestor	Sector	Tipo de estudio	Lugar de procedencia	Objetivo
1.	2018	Cybersecurity of Healthcare IoT-Based Systems: Regulation and Case-Oriented Assessment	IEEXPLORE	Salud	Descriptivo	Kyiv, Ukraine	Análisis de las normas internacionales sobre seguridad cibernética médica y sanitaria. Proporciona un modelo normativo jerárquico desarrollado de las normas internacionales de seguridad cibernética.
2.	2015	Cyber-Attacks – Trends, Patterns and Security Countermeasures	IEEXPLORE	Empresarial	Analítico	Oxford, United Kingdom	Presenta las contramedidas que las empresas pueden adoptar para garantizar una mayor seguridad que sirva de apoyo en la defensa de su negocio frente a los atacantes desde el punto de vista de la seguridad de la información.
3.	2018	An access control framework for protecting personal electronic health records	IEEXPLORE	Salud	Descriptivo	Mbarara, Uganda	En este documento, los investigadores se basan en los conceptos existentes de los Sistemas de Información Médica y el uso de la Infraestructura de Clave Simétrica para diseñar un marco para el acceso seguro a los registros electrónicos personales de salud.

4.	2018	An integrated methodology for big data classification and security for improving cloud systems data mobility	IEEXPLORE	Todos	Analítico	Alemania	Propone una metodología integrada para clasificar y asegurar grandes datos antes de ejecutar la movilidad, la duplicación y el análisis de los datos.
5.	2018	A Study on Encryption Techniques to Protect the Patient Privacy in Health Care Systems	IEEXPLORE	Salud	Descriptivo	India	En este artículo se revisan los diferentes modelos, esquemas y aplicaciones relacionados con el cifrado de datos y los algoritmos de criptografía propuestos por diferentes investigadores para asegurar los dispositivos médicos de uso inteligente.
6.	2018	Theoretical Aspects of Cyber-atack Modeling	IEEXPLORE	Todos	Analítico	Rusia	El artículo está dedicado al análisis de los datos necesarios para la simulación de ciberataques. El estudio examina el ciclo de vida de un ciberataque, la definición de su firma y los métodos utilizados para implementarla.
7.	2017	Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge?	Science Direct	Salud	Descriptivo	Australia	Comparación y análisis de las normas de controles técnicos de la ISO/CEI 80001 (ISO/CEI 80001-2-2 e ISO/CEI 80001-2-8), identificando las esferas de omisión, cobertura, adición o mejora que pueden repercutir en la eficacia de la

							norma ISO/CEI 80001 para proporcionar una protección eficaz de la ciberseguridad
8.	2018	Cybersecurity in healthcare: A narrative review of trends, threats and ways forward	Science Direct	Salud	Analítico	United Kingdom	Especifica las nuevas leyes y regulaciones para facilitar la superación de las infracciones pueden reducir la confianza de los pacientes, paralizar los sistemas de salud y amenazar la vida humana.
9.	2018	Digital health: Cybersecurity is a value creation lever, not only a source of expenditure	Science Direct	Salud	Analítico	Canada	Describe la importancia de la ciberseguridad en el sector de salud y las tecnologías digitales y como recientes ciberataques que han afectado y perturbado a muchas organizaciones y sistemas de atención de la salud en todo el mundo.
10.	2019	Secure Edge of Things for Smart Healthcare Surveillance Framework	WOS	Salud	Descriptivo	Australia	Introduce un novedoso marco informático de Edge of Things (EoT) para servicios de vigilancia de salud seguros e inteligentes. La Encriptación Totalmente Homomórfica (FHE) preserva la privacidad de los datos y se almacena y procesa dentro de un marco EoT
11.	2019	Adaptive Cybersecurity Framework for Healthcare Internet of Things. International Symposium on	WOS	Salud	Descriptivo	Noruega	Propone el Marco de Ciberseguridad Adaptativa, trabajo que apoya la adaptación dinámica a las amenazas cibernéticas. Además, simulamos y

		Medical Information and Communication Technology					evaluamos el marco usando la teoría de juegos evolutivos.
12.	2019	Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector	WOS	General	Analítico	Reino Unido	Realiza un estudio empírico de la viabilidad y aplicación de la técnica de seguridad de la información sobre las causas de los errores humanos básicos (IS-CHEC), que es una adaptación para la seguridad de la información de la técnica de evaluación y reducción de los errores humanos (HEART).
13.	2018	Cybersecurity for Medical Devices.	IEEXPLORE	Salud	Descriptivo	Estados Unidos	Se aplica un marco de seguridad de los programas informáticos, utilizar los diez principios rectores para el diseño de programas informáticos seguros, realizar pruebas exhaustivas y aplicar un proceso sólido de gestión de riesgos para garantizar que la confidencialidad, la integridad y la disponibilidad de los dispositivos médicos, los datos médicos, las redes informáticas y los servicios médicos no sean perjudiciales.
14.	2018	Cybersecurity in Hospitals: A Systematic, Organizational Perspective. Journal of Medical Internet Research	WOS	Salud	Analítico	Estados Unidos	El propósito es desarrollar una perspectiva sistemática y organizativa para estudiar la dinámica del desarrollo de la capacidad en materia de seguridad cibernética en los hospitales y la forma en que esa dinámica organizativa interna

							interactúa para formar un sistema de seguridad cibernética hospitalaria en los Estados Unidos.
15.	2019	Health care and cybersecurity: Bibliometric analysis of the literature	Science Direct	Salud	Analítico	Estados Unidos	El objetivo de este estudio fue proporcionar una visión general de la literatura en la intersección de la seguridad cibernética y la prestación de atención de la salud.
16.	2018	Continuous and transparent access control framework for electronic health records: A preliminary study	WOS	Salud	Analítico	Malasya	Esta investigación propone un continuo y marco transparente de control de acceso basado en un estudio preliminar.
17.	2018	Cybersecurity and the Medical Device Product Development Lifecycle	WOS	Salud	Descriptivo	Reino Unido	En esta contribución se examinan las orientaciones relativas a la seguridad cibernética de los dispositivos médicos dentro del ciclo de vida del desarrollo de los productos.
18.	2018	An Overview of Cybersecurity Regulations and Standards for Medical Device Software	WOS	Salud	Analítico	Austria	En este documento se examinan los reglamentos y normas de seguridad cibernética vigentes para los programas informáticos de dispositivos médicos establecidos por los organismos gubernamentales y los organismos que desarrollan normas industriales e internacionales
19.	2018	A review of health impact assessment frameworks	Science Direct	Salud	Analítico	Reino Unido	Examinar los numerosos marcos de HIA de manera sistemática y comparativa

20.	2018	Cybersecurity Education and Training in Hospitals	WOS	Salud	Descriptivo	Finlandia-Hungría	Este documento presenta el trabajo en curso en el campo de la desarrollar la educación y la capacitación en materia de seguridad cibernética en los hospitales. El Marco Educativo de Resistencia Proactiva (Prosilience EF) es una respuesta al desafío específico de la Comisión Europea de "concienciar" y la elaboración de planes de capacitación sobre la ciberseguridad en los hospitales.
21.	2018	Cybersecurity: A Real Threat to Patient Safety.	Science Direct	Salud	Analítico	Estados Unidos	Describe la importancia de la seguridad de la paciencia y la amenaza real que representan los ciberataques
22.	2018	Cyber Vulnerabilities on Smart Healthcare, Review and Solutions	WOS	Salud	Analítico	Malasia	Analizar los problemas que las personas podrían estar enfrentando relacionados con cuestiones de seguridad en sus hogares inteligentes e iniciar un debate sobre cómo los dispositivos de asistencia sanitaria que vienen en un paquete por los futuros hogares son vulnerables a los ataques cibernéticos que resultarán en violaciones de datos
23.	2018	The evolving state of medical device cybersecurity	WOS	Salud	Analítico	Estados Unidos	Este artículo ofrece una instantánea actual del estado evolutivo de la ciberseguridad de los dispositivos médicos a lo largo del ciclo de vida del producto, incluidos los problemas que

							impiden la seguridad de los dispositivos médicos y las iniciativas actuales para fomentar la ciberseguridad de los dispositivos médicos.
24.	2018	Ransomware in healthcare facilities : The future is now	WOS	Salud	Analítico	Estados Unidos	Examinamos el alcance de las recientes infecciones de software de rescate en entornos sanitarios, las responsabilidades de riesgo y los costes asociados a dichas infecciones, y las posibles tácticas de mitigación de riesgos.
25.	2018	Cybersecurity for critical infrastructures: Attack and defense modeling	IEEXPLORE	Salud	Descriptivo	Irlanda, Estados Unidos	EI presente documento se informa de un estudio exhaustivo sobre la ciberseguridad de las infraestructuras críticas. Se propone un marco de seguridad para el control de supervisión y la adquisición de datos con los siguientes cuatro componentes principales
26.	2018	Standards for Medical Device Cybersecurity in 2018	WOS	Salud	Descriptivo	Estados Unidos	Describe los estándar adecuados a aplicar en los equipos médicos
27.	2019	Authentication and Secure Key Management in E-Health Services: A Robust and Efficient Protocol Using Biometrics	IEEXPLORE	Salud	Descriptivo	Estados Unidos	Se ha propuesto un protocolo robusto y eficiente de autenticación basado en la biometría y de acuerdo con las claves para los servicios de salud electrónica

28.	2019	E-Health and Privacy: Risks, Opportunities and Solutions	IEEXPLORE	Salud	Descriptivo	Turquía	Se aborda el marco de las tecnologías de la información y las comunicaciones, se examinan los estudios propuestos en la literatura considerando los posibles riesgos y oportunidades y, por último, se han presentado al lector las precauciones/sugerencias futuras.
29.	2019	Safety and Security Architecture Analyses Framework for the Internet of Things of Medical Devices	IEEXPOLRE	Salud	Desrciptivo	Alemania	Desarrolla un meta-modelo para estandarizar las arquitecturas de seguridad de la IO. Utilizado para identificar los puntos débiles de la arquitectura con la ayuda de nuestro marco de análisis durante la fase de diseño.
30.	2018	Ensuring Privacy and Security in E-Health Records	IEEXPLORE	Salud	Analítico	India, Jordan, Taiwan	Propone un enfoque eficiente para preservar la identidad y también proteger la privacidad de los datos clínicos utilizando un esquema de cifrado muy eficaz. Además, se examinó un marco de autorización utilizando un acceso de diversos grados
31.	2018	Framework for Accessibility Evaluation of Hospital Websites	IEEXPLORE	Salud	Descriptivo	Ecuador, España	Este estudio describe los problemas de accesibilidad a la web identificados en 22 sitios web de hospitales según el ranking de Webometrics. En el proceso de evaluación se aplicó un marco para ayudar en la evaluación de

							los sitios web propuestos por el World Wide Web Consortium
32.	2018	Measuring attitude towards personal data for adaptive cybersecurity	WOS	Salud	Analítico	China, Reino Unido	El objetivo de la investigación es desarrollar una escala de medición fiable para cuantificar y comparar las actitudes hacia los datos personales que se puedan incorporar a los modelos de investigación del comportamiento de la ciberseguridad.
33.	2018	A New Framework for Detecting Insider Attacks in Cloud-Based E-Health Care System	IEEXPLORE	Salud	Descriptivo	Nigeria	Propone un nuevo marco para la detección de ataques internos en el sistema de salud basado en la nube, utilizando la técnica de extracción de marcas de agua y de detección de registros.
34.	2018	The Future of Health Care Cybersecurity	WOS	Salud	Analítico	Estados Unidos	Toma conciencia del daño potencial que la falta de importancia al proceso de BON puede causar. Es vital que los organismos reguladores tomen medidas para proteger los datos privados de sus licenciatarios y, en última instancia, del público.
35.	2020	Medical device cybersecurity—At the convergence of CE and IT	IEEXPLORE	Salud	Analítico	Estados Unidos	Proporciona una comprensión básica de los retos a los que se enfrenta la industria de la salud en general y ofrece una visión general de las principales prácticas que pueden aplicarse a corto plazo para mitigar el problema así como, a largo

							plazo, para obtener dispositivos médicos mejores, más seguros y más seguros.
36.	2019	Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices − A Review	IEEXPLORE	Salud	Analítico	Pakistan, Estados Unidos, Reino Unido	En este trabajo, estudiamos las vulnerabilidades de seguridad presentes en los dispositivos médicos de última generación estudiando las pruebas de seguridad y los ataques demostrados por los investigadores en más de cien dispositivos.
37.	2020	Security Architecture Framework for Internet of Things (IoT)	IEEXPLORE	General	Descriptivo	Estados Unidos	Este trabajo propone un novedoso marco de arquitectura de seguridad para la IO.
38.	2018	Medical Device Security in the IoT Age	IEEXPLORE	General	Descriptivo	Estados Unidos	El análisis de este documento se centrará en las cuestiones inherentes al actual proceso de descubrimiento, la actualización y la aplicación de parches a los procesos de software vulnerables, las responsabilidades de los fabricantes y las posibles soluciones provisionales para los proveedores de servicios de salud que pueden ayudar a identificar los riesgos mientras esperamos los cambios en los actuales procesos de la FDA y proporcionar las medidas que los proveedores de servicios de salud pueden tomar en el ínterin para proteger sus redes.

39.	2018	A Review of Standards with Cybersecurity Requirements for Smart Grid	Science Direct	General	Descriptivo	Polonia	El presente documento se analizan las relaciones entre las normas para comprender dónde se superponen o complementan las normas y dónde son completamente independientes
40.	2018	Cybersecurity Vulnerability Mitigation Framework through Empirical	Science Direct	General	Descriptivo	Estados Unidos	En este documento se presenta la arquitectura detallada de la metodología mejorada de análisis de la brecha prioritaria (EPGA) de CyFEr y su aplicación a los LCR.
41.	2019	Medical Device Vulnerability Mitigation Effort Gap Analysis Taxonomy	Science Direct	Salud	Descriptivo	Estados Unidos	Revisa la literatura de los últimos cinco años con el objetivo de identificar la cantidad de esfuerzo que han aportado cinco partes asociadas de dispositivos médicos: Autoridad, Dispositivo Fabricantes, instalaciones de atención médica, organizaciones de normas y academia
42.	2018	Cyber-analytics: Modeling factors associated with healthcare data breaches	Science Direct	Salud	Descriptivo	Estados Unidos	El propósito de este estudio fue desarrollar un modelo de factores asociados con las violaciones de los datos de salud
43.	2019	A fraud detection approach with data mining in health insurance	Science Direct	Salud	Analítico	Sudáfrica y Turquía	Sobre la base de unos pocos casos que se sabe o se sospecha que son fraudulentos, la técnica de detección de anomalías calcula la probabilidad o la posibilidad de que cada registro sea fraudulento

							analizando las reclamaciones de seguros anteriores.
44.	2019	Applying public health strategies to the protection of cyberspace	Science Direct	Salud	Analítico	Estados Unidos	Este documento presenta una estrategia para la salud en el ciberespacio que se inspira en construcciones e iniciativas en el ámbito de la salud pública.
45.	2019	Biosecurity risk mapping and gap analysis in South East Asia	Science Direct	General	Analíico	Bélgica y Singaput	En el presente documento se describen los resultados del Proyecto 62, que consistió en el levantamiento de mapas y la evaluación de riesgos de bioseguridad en el Asia sudoriental
46.	2019	Authentication and Secure Key Management in E-Health Services: A Robust and Efficient Protocol Using Biometrics	IEEXPLORE	General	Analítico	Pakistan	Se ha propuesto un protocolo robusto y eficiente de autenticación basado en la biometría y de acuerdo con las claves para los servicios de salud electrónica. Además, se ha demostrado mediante análisis formales e informales que el sistema propuesto es de probada seguridad.
47.	2019	E-Health and Privacy: Risks, Opportunities and Solutions	IEEXPLORE	Salud	Descriptivo	Turquía	Aborda el marco de las tecnologías de la información y las comunicaciones, se han examinado los estudios propuestos en la literatura considerando los posibles riesgos y oportunidades y, por último, se han presentado al lector las precauciones/sugerencias futuras.

48.	2018	Safety and security architecture analyses framework for the internet of things of medical devices	IEEXPLORE	Salud	Descriptivo	Alemania	Este artículo desarrolla un enfoque de análisis de seguridad y protección que incluye un meta-modelo estandarizado y un marco de seguridad y protección de la IO que comprende un lenguaje de análisis personalizable.
49.	2018	Ensuring privacy and security in E-health records	IEEXPLORE	Salud	Analítico	Taiwan	En este estudio, hemos implementado el esquema AT&T para manejar el mecanismo de control de acceso de los datos de los pacientes.
50.	2019	A Study on Security Trend based on News Analysis	IEEXPLORE	General	Analítico	Taiwan	Esta investigación facilita a los administradores de la seguridad cibernética el ahorro de tiempo para leer a través de múltiples sitios web de noticias sobre seguridad cibernética y organizar eventos a partir de sus memorias u otros registros, mejorando así la capacidad de las empresas para protegerse activamente contra posibles ataques cibernéticos.

CAPÍTULO III. RESULTADOS

Del total de artículos arrojados por las bases de datos: IEEXPLORE, Science Direct y Web of Science, aplicando los criterios de inclusión y de exclusión, se eliminaron artículos duplicados y poco relevantes para la revisión sistemática, Lo cual nos da, un total de 50 artículos originales en el periodo de tiempo de 2018 a 2020, distribuidos así: IEEXPLORE, 23 artículos; Sciencedirect, 13 artículos y Web of Science, 14 artículos, como se demuestra en la Figura 1. Dichos artículos provienen de diversos países, en su mayoría de Estados Unidos, Reino Unido, Alemania, etc.

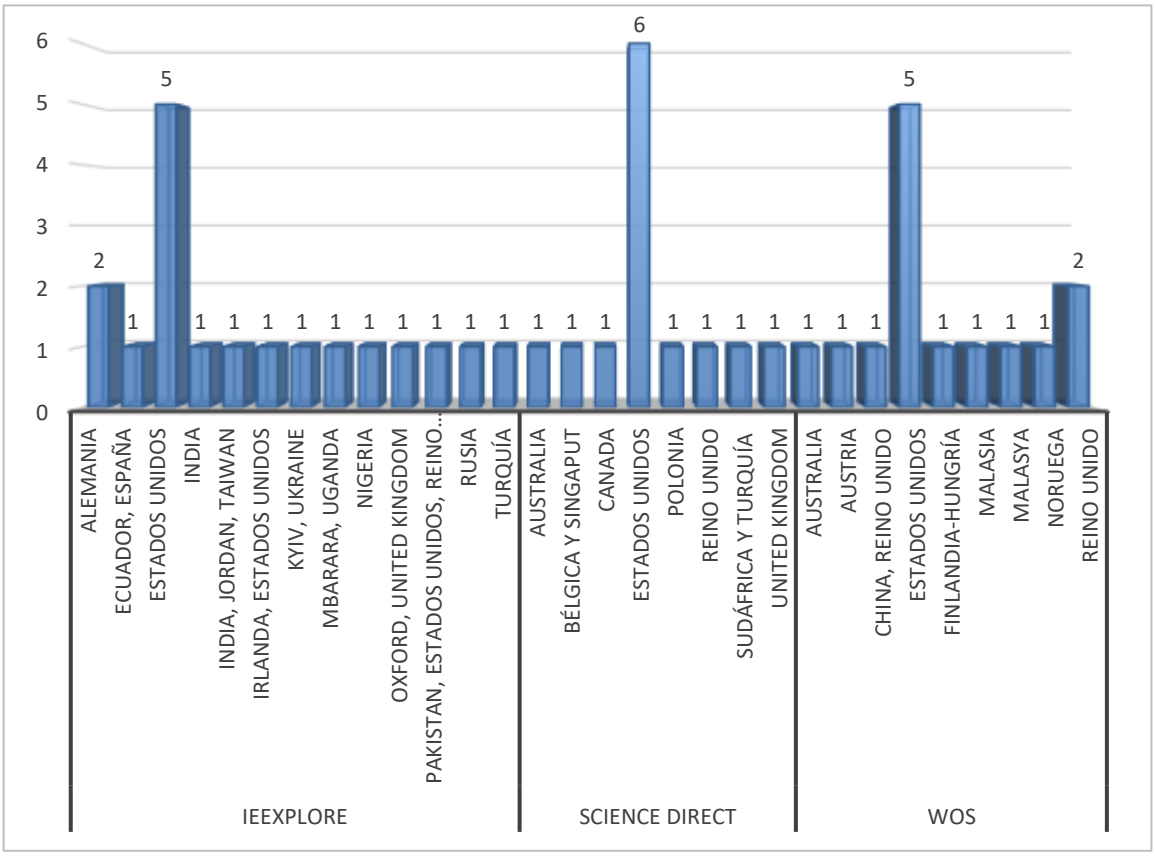

Ilustración 1: Artículos según el país y la BD

Se muestra una relación más detallada en la Figura 2.

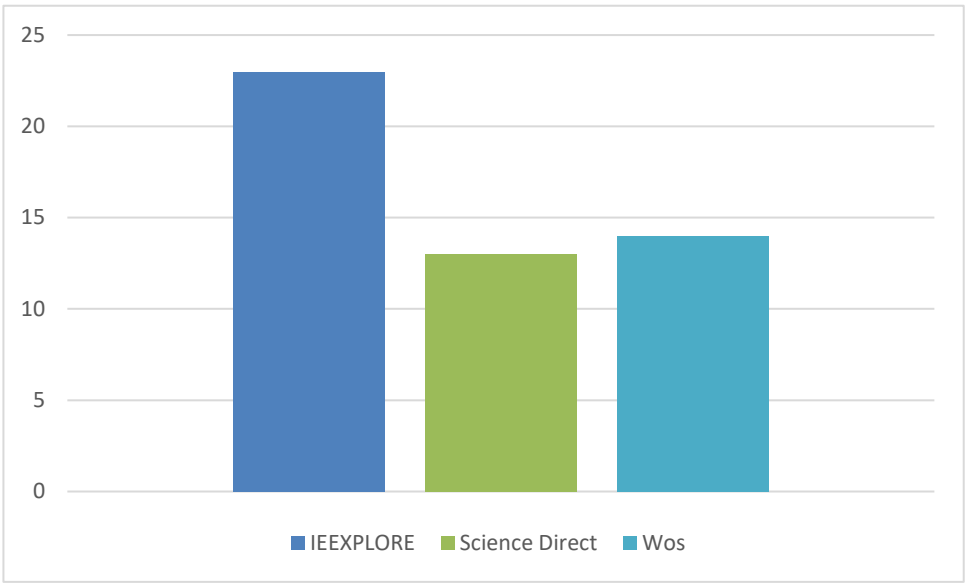

Ilustración 2: Número de artículos según la BD

Finalmente se puede visualizar en la Figura 3 que el 52% son artículos analíticos y el 48% son artículos descriptivos.

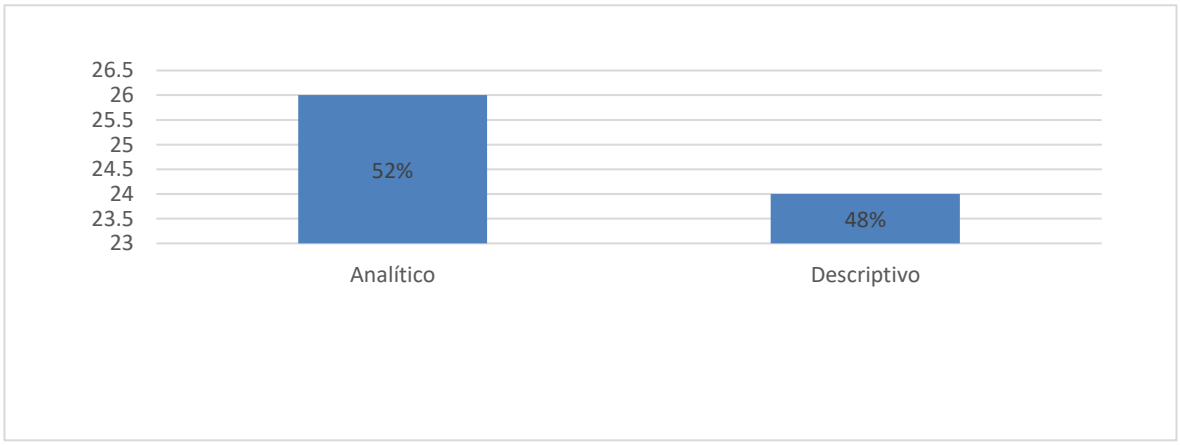

Ilustración 3: Análisis de artículos

Culminada la búsqueda en las bases de datos, se procedió a la selección de artículos, en 4 fases: Identificación, se hace el recuento de artículos obtenidos y se eliminan los duplicados; Evaluación, resultados excluidos por título y resumen; Elegibilidad, artículos eliminados al no abordar análisis de modelos de seguridad, estudios pilotos o estudios descriptivos y qué marcos de ciberseguridad están basados en prácticas aceptadas; Inclusión, finalmente 45 artículos incluidos en la revisión sistemática. Todo el proceso de selección durante las correspondientes fases queda detallado en la Figura 4.

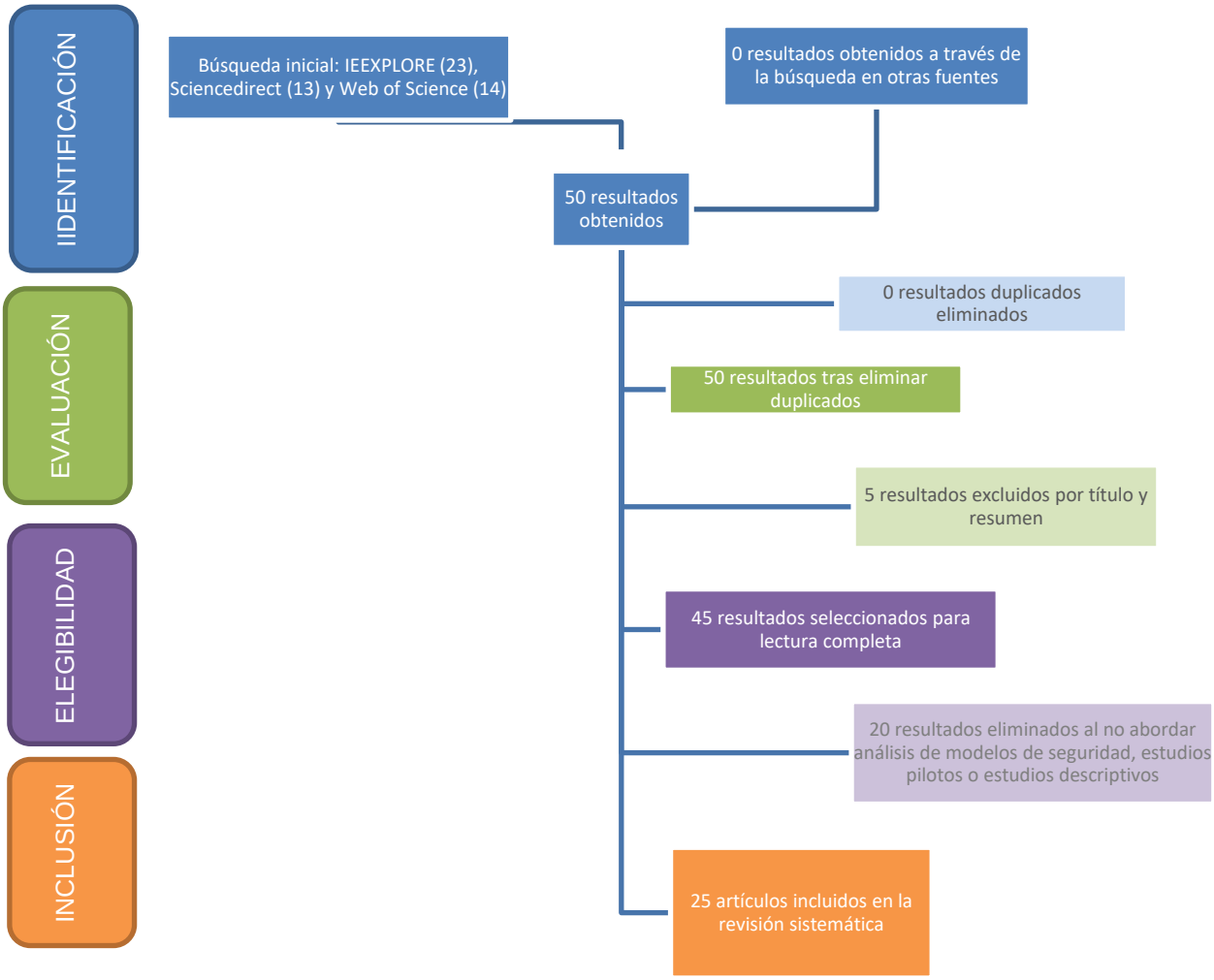

Ilustración 4: Diagrama de flujo

Estructura de un marco de seguridad

Para proteger sus activos, el sector de salud necesita implementar marcos dinámicos, adaptables, robustos, capaces de detectar una amplia variedad de amenazas y tomar decisiones inteligentes en tiempo real. En la literatura revisada, se encontraron 3 estructuras apropiadas, La tabla 2 indica los mejores frameworks encontrados, también, se identificó el público objetivo de cada uno.

Tabla 2: Estructuras de marco de ciberseguridad

Nombre	**Funciones**	**Componentes**	**Descripción**	**Dirigido a**	**Fuente**
NIST CSF	1. Identificar 2. Proteger 3. Detectar 4. Responder 5. Recuperar	1. Núcleo 2. Niveles de implementación 3. Los perfiles	Gestiona y reporta el riesgo de ciberseguridad tanto internamente como externamente. De misma forma, ayuda a identificar y priorizar acciones para reducir el riesgo	Organizaciones de cualquier industria o multinacionales, mayormente con sede en Estados Unidos.	(Lechner 2017)
HITRUST CSF	1. Armonizar los requisitos de cumplimiento 2. Proporcionar detalles específicos	1. Dominio 2. Control family 3. Requeriment statements	Normaliza los requisitos de seguridad de las organizaciones de atención de la salud, entre otros. Proporciona dirección	Organizaciones del sector de salud u otras.	(Gourisetti, Mylrea, and Patangia 2020)

	sobre cómo se implementan los controles.		de la seguridad, adaptada a las necesidades de la organización.		
ISO/IEC Standards	1. Establecer 2. Implantar 3. Mantener 4. Mejorar	1. Seguridad física y ambiental 2. Control de acceso y gestión de acceso 3. Prácticas de seguridad informática 4. Criptografía 5. Seguridad de las comunicaciones 6. Gestión de incidentes y cumplimiento	Se orienta a la gestión de la seguridad de alto nivel y a la guía de aplicación que acepta las mejores prácticas de la industria en materia de ciberseguridad	Organizaciones multinacionales de cualquier tamaño	(Lechner 2017)

Impacto de características en los frameworks

A partir de la Tabla 1, se evidencia que los frameworks de menor tamaño son más reutilizables y fáciles de combinar, a diferencia de los frameworks de mayor tamaño, los cuales tienen menor probabilidad de ser reutilizados y son difcíciles de combinar.

En cuanto al control de aplicaciones, si se lleva un control parcial, se evidencia que son más componibles y, por consiguiente, más reutilizables. Sin embargo, si se lleva un control total de aplicaciones, se evidencia todo lo contrario.

Finalmente, el beneficio de concepto de roles, facilita a gran escala la reutilización y hace el framework mucho más flexible, haciéndolo más aplicable a los frameworks de mayor tamaño. Por lo que para los marcos pequeños, se recomienda omitir los roles, debido a que estos beneficios no se hacen evidentes. Dicho impacto de características se evidencia en la Tabla 3.

//////////////////	Componible	Reusabilidad	Flexibilidad
Mayor	SF, PAC	SF, PAC	-
Menor	LF, PAC	LF, FAC	RM

Leyenda	
Small framework	SF
Larger framework	LF
Partial app control	PAC
Full app control	FAC
Rol modeling	RM

Tabla 3: Impacto de caracteristicas en el framework

CAPÍTULO IV. CONCLUSIONES

La revisión de la literatura científica realizada nos indica que las características básicas que debe presentar el marco de ciberseguridad dirigido al sector de salud es que debe: ser componible y reusable, por lo tanto, según la tabla 3, este debe ser de tamaño pequeño a mediano; ayudar a eliminar las ineficiencias y superposiciones creadas al tratar de demostrar el cumplimiento de múltiples normas reglamentarias; adaptarse para reflejar su nivel de madurez. En cuanto a estructura se debe seguir la de HITRUST CSF, ya que como se evidencia en la Tabla 2 es altamente adaptable en la industria de salud, sobre todo la estadounidense

Se recomienda en primera instancia tomar un test online, para poder determinar el nivel de riesgo en el que se encuentra (identificando las amenazas de ciberseguridad), realizar un inventario de las vulnerabilidades de todos los dispositivos poseídos por el centro de salud y finalmente consultar con un equipo de especialistas en cibernética para profundizar en las medidas de seguridad cibernética y marcos de seguridad que deberían aplicarse.

Las limitaciones presentadas son las siguientes:

- No todos los modelos de ciberseguridad mencionados son de licenciamiento libre
- No se podrá realizar pruebas en el área real de modelos de seguridad seleccionados.

REFERENCIAS

¿Qué es la seguridad cibernética?. (2020). Retrieved 30 May 2020, from https://www.secureweek.com/que-es-la-seguridad-cibernetica/

Ruiz Diaz, J. (2016). Ciberamenazas: ¿El terrorismo del futuro? [Ebook] (1st ed.). España: IEEE. Retrieved from http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

It Digital Media Group. (2020). Crecen los ataques cibernéticos, especialmente los destinados a IoT. Retrieved 9 May 2020, from https://www.ittrends.es/seguridad/2019/03/crecen-los-ataques-ciberneticos-especialmente-los-destinados-a-iot

Tyas Tunggal, A. (2020). ¿What is a Cyber Attack?. Retrieved 29 April 2020, from https://www.upguard.com/blog/cyber-attack

Hathaway, Oona & Crootof, Rebecca & Levitz, Philip & Nix, Haley & Nowlan, Aileen & Perdue, William & Spiegel, Julia. (2011). The Law of Cyber-Attack. California Law Review. 100.

Gómez Vieites, A. (2011). Enciclopedia de la Seguridad Informática. (2nd ed.). Madrid, España: Ra-Ma.

Ross, J. (2018). Cybersecurity: A Real Threat to Patient Safety. Journal Of Perianesthesia Nursing Supports Open Access, (32), 370-372.

Repp, P. (2018). Theoretical Aspects of Cyber-atack Modeling. 2018 International Russian Automation Conference (RusAutoCon). Perm, Rusia

Strielkina, Anastasiia & Illiashenko, Oleg & Zhydenko, Marina & Uzun, Dmytro. (2018) Cybersecurity of Healthcare IoT-Based Systems: Regulation and Case-Oriented

Assessment. Kharkiv, Ukraine.

Bendovschi, Andreea (2018) Cyber-Attacks – Trends, Patterns and Security Countermeasures. Oxford, United Kingdom.

Izaara, Ambrose Atuheire & Ssembatya, Richard & Kaggwa, Fred (2018) An Access Control Framework for Protecting Personal Electronic Health Records. Kampala, Uganda: Mbarara University of Science and Technology

Hababeh, Isamil & Gharaibeh, Ammar & Nofal, Samer & Khalil, Issa (2018) An Integrated Methodology for Big Data Classification and Security for Improving Cloud Systems Data Mobility

Khandare, Laxman & Sreekantha,Desai (2019) A Study on Encryption Techniques to Protect the Patient Privacy in Health Care Systems. Pune, India: Institute of Technology.

Anderson, Scott & Williams, Trish (2018) Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge?.Australia: Flinders University.

Coventry, Lynne & Branley Dawn (2018) Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. United Kingdom: Northumbria University.

Alami, Hassane & Gagnon, Marie-Pierre & Ag Ahmed, Mohamed Ali & Fortin, Jean-Paul (2018) Digital health: Cybersecurity is a value creation lever, not only a source of expenditure. Canada: Université Laval.

Alabdulatif, Abdulatif, Ibrahim Khalil, Xun Yi, and Mohsen Guizani. 2019. "Secure Edge of Things for Smart Healthcare Surveillance Framework." IEEE Access 7(c):31010–21.

Boudko, Svetlana, and Habtamu Abie. 2019. "Adaptive Cybersecurity Framework for Healthcare Internet of Things." International Symposium on Medical Information and Communication Technology, ISMICT 2019-May(1):1–6.

Coban, Cigdem, and Mehmet Fatih Tuysuz. 2019. "E-Health and Privacy: Risks, Opportunities and Solutions." UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering 554–59.

Evans, Mark, Ying He, Leandros Maglaras, Iryna Yevseyeva, and Helge Janicke. 2019. "Evaluating Information Security Core Human Error Causes (IS-CHEC) Technique in Public Sector and Comparison with the Private Sector." International Journal of Medical Informatics 127(January):109–19.

Hegde, Vaishali. 2018. "Cybersecurity for Medical Devices." Proceedings - Annual Reliability and Maintainability Symposium 2018-Janua:1–6.

Jalali, Mohammad S., and Jessica P. Kaiser. 2018. "Cybersecurity in Hospitals: A Systematic, Organizational Perspective." Journal of Medical Internet Research 20(5):e10059.

Jalali, Mohammad S., Sabina Razak, William Gordon, Eric Perakslis, and Stuart Madnick. 2019. "Health Care and Cybersecurity: Bibliometric Analysis of the Literature." Journal of Medical Internet Research 21(2).

Jayabalan, Manoj, and Thomas Oadaniel. 2018. "Continuous and Transparent Access Control Framework for Electronic Health Records: A Preliminary Study." Proceedings - 2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2017 2018-Janua:165–70.

Jones, Richard W., and Konstantinos Katzis. 2017. "Cybersecurity and the Medical Device Product Development Lifecycle." Pp. 76–79 in Studies in Health Technology and Informatics. Vol. 238.

Lechner, Nadica Hrgarek. 2017. "An Overview of Cybersecurity Regulations and Standards for Medical Device Software." Central European Conference on Information and Intelligent Systems 237–49.

Mehmood, Zahid, Anwar Ghani, Gongliang Chen, and Ahmed S. Alghamdi. 2019. "Authentication and Secure Key Management in E-Health Services: A Robust and Efficient Protocol Using Biometrics." IEEE Access 7:113385–97.

Mindell, J. S., A. Boltong, and I. Forde. 2008. "A Review of Health Impact Assessment Frameworks." Public Health 122(11):1177–87.

Nevmerzhitskaya, Julia. 2018. "Cybersecurity Education and Training in Hospitals." 2048–52.

Rauscher, Julia, and Bernhard Bauer. 2018. "Safety and Security Architecture Analyses Framework for the Internet of Things of Medical Devices." 2018 IEEE 20th International Conference on E-Health Networking, Applications and Services, Healthcom 2018 3–5.

Safavi, Seyedmostafa, Ahmad Moaaz Meer, Ed Keneth Joel Melanie, and Zarina Shukur. 2019. "Cyber Vulnerabilities on Smart Healthcare, Review and Solutions." Proceedings of the 2018 Cyber Resilience Conference, CRC 2018 1–5.

Schwartz, Suzanne, Aftin Ross, Seth Carmody, Penny Chase, Steve Christey Coley, Julie Connolly, Cathy Petrozzino, and Margie Zuk. 2018. "The Evolving State of Medical Device Cybersecurity." Biomedical Instrumentation and Technology 52(2):103–11.

Spence, Nikki;, David; P. Paul III, and Alberto Coustasse. 2018. "Ransomware in Healthcare Facilities : The Future Is Now." Academy of Business Research, Fall 2017 Conference 1–14.

Ten, Chee Wooi, Govindarasu Manimaran, and Chen Ching Liu. 2010. "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling." IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans 40(4):853–65.

Yuan, Sean, Anura Fernando, and David C. Klonoff. 2018. "Standards for Medical Device Cybersecurity in 2018." Journal of Diabetes Science and Technology 12(4):743–46.

Acosta-Vargas, Patricia, Tania Acosta, and Sergio Lujan-Mora. 2018. "Framework for

Accessibility Evaluation of Hospital Websites." 2018 5th International Conference on EDemocracy and EGovernment, ICEDEG 2018 9–15.

Vora, Jayneel, Prit Italiya, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, M. S. Obaidat, and K. F. Hsiao. 2018. "Ensuring Privacy and Security in E-Health Records." CITS 2018 - 2018 International Conference on Computer, Information and Telecommunication Systems 1–5.

Issues, Legal, and Surrounding Licensure. 2018. "The Future of Health Care Cybersecurity." Journal of Nursing Regulation 8(4):S29–31.

Nevmerzhitskaya, Julia. 2018. "Measuring Attitude towards Personal Data for Adaptive Cybersecurity." WOS.

Okikiola, Folasade Mercy. 2018. "A New Framework for Detecting Insider Attacks in Cloud-Based E-Health Care System." IEEE Access.

Wirth, Axel, and Stephen L. Grimes. 2020. Medical Device Cybersecurity—At the Convergence of CE and IT. Second Edi. Elsevier Inc.

Yaqoob, Tehreem, Haider Abbas, and Mohammed Atiquzzaman. 2019. "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices-A Review." IEEE Communications Surveys and Tutorials 21(4):3723–68.

Izaara, Ambrose Atuheire, Richard Ssembatya, and Fred Kaggwa. 2019. "An Access Control Framework for Protecting Personal Electronic Health Records." 2018 International Conference on Intelligent and Innovative Computing Applications, ICONIC 2018 1–6.