PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

FACULTAD DE MEDICINA

TRABAJO DE TITULACIÓN

SUBMODALIDAD: CAPITULO DE LIBRO

TEMA:

CIBERSEGURIDAD: LA NECESIDAD DE SEGURIDAD DE LOS DATOS DEL PACIENTE EN AMÉRICA LATINA

PREVIO A LA OBTENCIÓN DEL TITULO DE MAGISTER EN GESTIÓN DE CALIDAD EN SALUD Y SEGURIDAD DEL PACIENTE

DIRECTOR: DR. CAMPOS PROAÑO FERNANDO RAFAEL

AUTOR: OBST. PAREDES HUACA LESLIE ALEJANDRA

QUITO, AGOSTO DE 2024

DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las políticas y manuales de la Pontificia Universidad Católica del Ecuador, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas políticas.

Asimismo, cedo los derechos en línea patrimoniales de mi trabajo de titulación, con fines de difusión pública, además apruebo la reproducción dentro de las regulaciones de la Pontificia Universidad Católica del Ecuador y de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Firma del estudiante: 

Nombre: Paredes Huaca Leslie Alejandra

Cédula: 1004096176

Lugar y fecha: Quito, 26 de Agosto de 2024.

DEDICATORIA

. El desarrollo de este trabajo de investigación está dedicado a Dios, la base sólida en mi vida, porque me ha bendecido cada día, ha sido fiel desde siempre y por su palabra me ha dado fortaleza para continuar en mi vida. También esto es por mi mamá, que siempre me ha enseñado con ejemplo y ha impulsado a crear una mejor versión de mí, al igual le dedico a mi hermanita por ser mi compañera en todas las etapas y a mi esposo por su compañía en este trayecto, cuyo apoyo incondicional me inspira, por depositar su entera confianza en mí y mis capacidades.

Con amor y gratitud.

Alejandra Paredes.

AGRADECIMIENTOS

Gracias a Dios por permitirme realizar otro sueño, gracias a mi mentor el Dr. Fernando Campos por su paciencia y guía continua y gracias a todos los docentes que me enseñaron con amor en cada clase, me infundieron sus grandes conocimientos y me inspiraron a convertirme en un mejor profesional que busca la excelencia.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

No se encuentran elementos de tabla de ilustraciones.

RESUMEN

Gracias a los avances tecnológicos en la industria de la salud, el ciberespacio se utiliza cada vez más como un lugar de encuentro virtual para la interacción social, pero también permite el almacenamiento y uso de grandes cantidades de información, lo que lo convierte en un blanco fácil para los ciberdelincuentes debido al valor y relevancia de esta información sensible. El presente capítulo tiene como propósito indagar sobre la ciberseguridad y la necesidad de seguridad de los datos del paciente en América Latina.

Debido a factores socioeconómicos y educativos, América Latina tiene una brecha digital significativa en comparación con los continentes del "primer mundo". Recibe más de 1.600 ciberataques por segundo, siendo Brasil el que recibe más de la mitad, seguido de México (23%), Colombia (8%) y Perú (6%). Las recomendaciones que los gobiernos pueden implementar para ayudar al sector público y privado a mitigar los riesgos incluyen equipos de respuesta, mecanismos de colaboración, capacitación formal y una mayor inversión en infraestructura digital.

En Ecuador, en 1998, la protección de datos personales no era considerada un derecho fundamental, sino que se implementaba a través de otros derechos civiles, pero en 2021 se aprobó y dio a conocer nuestra primera política de seguridad cibernética con la ayuda del acuerdo ministerial 006-2021 con el objetivo establecer y fortalecer la capacidad del Estado para garantizar la implementación de los derechos humanos y las libertades y proteger los activos legítimos del Estado en el ciberespacio.

ABSTRACT

Thanks to technological advances in the healthcare industry, cyberspace is increasingly used as a virtual meeting place for social interaction, but it also allows for the storage and use of large amounts of information, making it a target. Easy for cybercriminals due to sensitive information. The purpose of this chapter is to investigate cybersecurity: the need for patient data security in Latin America.

Due to socioeconomic and educational factors, Latin America has a significant digital divide compared to the "first world" continents, receiving more than 1,600 cyber-attacks per second, with Brazil receiving more than half, followed by Mexico (23%) , Colombia (8%) and Peru (6%). Recommendations that governments can implement to help the public and private sector mitigate risks include response teams, collaboration mechanisms, formal training and increased investment in infrastructure.

In Ecuador, in 1998, the protection of personal data was not considered a fundamental right, but was implemented through other civil rights, but in 2021 our first cybersecurity policy was approved and announced with the help of the ministerial agreement 006-2021 with the objective of establishing and strengthening the capacity of the State to guarantee the implementation of human rights and freedoms and protect the legitimate assets of the State in cyberspace.

.

1. INTRODUCCIÓN

El avance imparable en la tecnología, la propagación de sus funciones de facilitar los procesos de interacción y organización de la información personal y empresarial, abre muchas oportunidades para que los delincuentes encuentren formas de obtener datos confidenciales de los usuarios, como contraseñas bancarias y correos electrónicos, mediante la instalación de malware en computadoras, teléfonos móviles o cualquier otro dispositivo (HERNÁNDEZ, CERQUERA, & VANEGAS, 2015).

La transformación de los sistemas de salud en una época digital es una oportunidad no solo para simplificar el acceso a los pacientes, sino que abre la posibilidad a la investigación y búsqueda de nuevos tratamientos. Sin embargo, para asegurar su efectividad es importante implementar políticas de ciberseguridad para la protección de los datos de los pacientes.

En el sector de la salud no solo es importante solo proteger la información como hacer el bien, sino que esto va más allá, implicando espacios éticos y legales.

En 2019, el uso de tecnología en la industria de la salud aumentó durante la pandemia de Covid-19, y la salud fue uno de los sectores más afectados. En 2020, las filtraciones de datos en EE. UU. aumentaron un 55%, el 67% de las cuales fueron incidentes de seguridad cibernética. Cabe mencionar que los costos financieros de los ciberataques son importantes, oscilando entre 3,86 y 7,13 millones de dólares durante el año 2020 en EE.UU.

Según la (OPS, 2023) “Adoptar instrumentos regulatorios en materia de procesamiento y protección de información sensible de salud, así como lineamientos y estándares internacionales de seguridad para sistemas de información centrados en el paciente”. La consumación de estos sistemas debe respetar los derechos relacionados con la salud que equilibre la necesidad de acceso a los datos y la privacidad.

En América Latina la seguridad de la información tiene grandes desafíos en el ciberespacio, debido a que los ataques prosperan más rápido que la capacidad de gestión de los gobiernos, siendo así que en América Latina apenas se encuentran el proceso de desarrollo de estatutos relacionados con la ciberseguridad (Aguilar, 2020).

2. METODOLOGÍA

Investigación bibliográfica que incluye de manera exclusiva datos abiertos y/o públicos.

3. DESARROLLO

3.1 GENERALIDADES EN CIBERSEGURIDAD

Las nuevas tecnologías nos han permitido un crecimiento exponencial a nivel social debido a sus múltiples beneficios, entre ellos el acceso a la información en corto tiempo y con un costo mínimo, el contacto interpersonal con cualquier parte del mundo debido a la inmediatez de las comunicaciones pero a su vez ha supuesto problemas de seguridad las cuales son aprovechadas por ciberdelicuentes, por lo cual los usuarios deben tomar ciertas precauciones al usar el mundo digital (Telefónica, 2016).

En la actualidad, los incidentes en Internet se han convertido en parte del día a día de gobiernos, empresas y en el sistema sanitario. Desde hace unos años atrás el sistema sanitario ha comenzado a instaurar un proceso de innovación digital que demanda el uso de las nuevas tecnologías, donde se ve expuesto al sinnúmero de amenazas que debe manejar con el fin de proteger la información de los usuarios, pero a su vez tener fácil acceso a la información. Por lo cual es de vital importancia contar con un sistema de gestión de seguridad.

En estos tiempos de desarrollo de las redes informáticas, los llamados ciberdelincuentes siguen avanzando rápidamente en las tecnologías y métodos desarrollados para violar los sistemas de seguridad, debido a que los sistemas son inexpertos, estos se aprovecharían de las instituciones y su pausada resolución de problemas debido a la falta de preparación en esta nueva problemática (Gamón, 2017).

Desde el avance aligerado del internet, también surge el otro lado de la moneda y de ahí nuevos términos como cibercrimen, ciberdelito o ciberdelincuencia que

describe generalmente actividades ilegales en el ciberespacio y tiene cuatro características específicas que lo menciona (Subijana, 2008) “se cometen fácilmente; requieren escasos recursos en relación al perjuicio que causan; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma; y se benefician de lagunas de punibilidad que pueden existir en determinados Estados, los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas”.

Es así, que debemos conocer que la seguridad de la información es un proceso integral que permite salvaguardar la identificación y gestión de la información y a su vez los riesgos que puede estar contrapuesta.

Como define (Solleiro, Castañón, Guillén, Hernández, & Solís, 2022) a la ciberseguridad es un conjunto de servicios, estrategias, mecanismos y políticas que garantizan que el funcionamiento del sistema informático sea seguro, en otras palabras: es un conjunto de tecnologías y métodos para la protección de ciberataques. Los ciberataques que es la entrada de virus que causan la pérdida de información y alteran el buen funcionamiento del sitio web.

En términos de salud, el papel de las TIC (Tecnologías de la información y las comunicaciones) es muy importante para hacer que los servicios de salud sean accesibles a la población desatendida en áreas remotas del país y hacer que estos servicios sean más eficientes, ya que ayuda a brindar a los pacientes una comunicación efectiva, acceso a la información y una nueva consulta dentro del tiempo correcto lleva la experiencia de especialistas a regiones remotas con la ayuda de la telemedicina, mejorando la eficiencia de la prestación de servicios relacionados.

Las tecnologías digitales pueden ayudar a incrementar los servicios de salud para los grupos poblacionales más vulnerables, por lo que es necesario atraer el desarrollo de capital humano e infraestructura que permitan el uso de tecnologías digitales de manera inclusiva, ética y segura. En este contexto, la seguridad de la información es un principio fundamental (OPS, 2023).

Es por ello, que la OPS menciona “Adoptar instrumentos regulatorios en materia de procesamiento y protección de información sensible de salud, así como lineamientos y estándares internacionales de seguridad para sistemas de información centrados en el paciente” (OPS, 2023). La consumación de estos sistemas debe respetar los derechos relacionados con la salud que equilibre la necesidad de acceso a los datos y la privacidad.

Es así que se creó un instrumento como es la auditoría forense, esto es una herramienta para mejorar los procesos existentes, detectar y prevenir actividades sospechosas y encontrar los elementos necesarios para mejorar (HERNÁNDEZ, CERQUERA, & VANEGAS, 2015). De tal manera que cuando existe un hecho, se convierte en medida de detección para futuramente evitar que estos errores.

Es importante comprender cómo identificar y abordar los diversos escenarios que pueden ocurrir en las organizaciones de atención médica y comprender las herramientas de auditoría forense utilizadas para identificar y evaluar los riesgos del fraude cibernético financiero común.

En Ecuador, según el Ministerio de Telecomunicaciones, en el 2021, la primera política de seguridad cibernética fue aprobada mediante Acuerdo Ministerial no. 006-

2021, que reevaluará la capacidad de cerrar brechas y aprovechar oportunidades actuales y futuras en el marco de la cuarta revolución industrial (MINTEL, 2022).

Las amenazas en Ecuador incluyen ataques cibernéticos a nuestra infraestructura crítica digital (ICD), nuestra infraestructura técnica obsoleta, los altos costos de adquisición de tecnología y los marcos legales y regulatorios obsoletos nos dejan a todos vulnerables.

3.2 LA CIBERSEGURIDAD EN SALUD

La tecnología ha cambiado muchos campos y la atención sanitaria no es una excepción. Desde la gestión de registros de pacientes hasta la telemedicina y la inteligencia artificial en el diagnóstico, las TIC (Tecnologías de la Información y la Comunicación) desempeñan un papel clave a la hora de optimizar los servicios, mejorar los resultados del tratamiento y garantizar la seguridad del paciente (Cervera & Goussens, 2024).

La conexión inalámbrica permite la interacción e integración con computadoras, ventiladores, bombas de medicamentos, entre otros dispositivos involucrados en la atención médica, permitiendo la recopilación de información importante para el manejo y toma de decisiones en cuanto a la salud del paciente, mayores opciones de tratamiento y monitoreo continuo (Cartwright, 2023).

Sin embargo, a medida del crecimiento de la implementación de estas tecnologías, aumenta también amenazas frente a la integridad de la información del paciente, como registros médicos, resultados de pruebas y datos personales, debido que es extremadamente valiosa en el mercado negro digital. Los ciberdelincuentes

pueden utilizar esta información para cometer fraude, extorsión o venderla a terceros, con consecuencias catastróficas que amenazan la privacidad del paciente, la integridad de los datos médicos y, en última instancia, la vida (Cervera & Goussens, 2024). Los principales ataques que ponen en riesgo los sistemas de salud son el phishing, el ransomware y el malware. El phishing es un tipo de estafa por internet, en la que a través de correos electrónicos maliciosos, llamadas telefónicas o mensajes de texto enviados por atacantes como parte de una técnica de ingeniería social engaña a las víctimas para que revelen información privada o comercial. De modo similar el ransomware es un programa malicioso que cifra los archivos de una víctima y reclama un desembolso para descifrarlos. La nota de rescate suele indicarle al usuario cómo pagar el rescate y descifrar sus archivos. Mientras que el malware es un tipo de software creado particularmente para dañar o inhabilitar computadoras y sistemas informáticos. Se utiliza para sustraer información personal, suprimir archivos o tomar el control de un ordenador, se distribuye a través de archivos adjuntos de correo electrónico o descargas de sitios web no fiables (Meneses, 2022).

A causa de la pandemia por COVID-19 la mayoría de las personas tomaron la opción del teletrabajo, incluyendo al personal de salud, los cuales operan sistemas altamente sensibles, muchos de ellos sin medidas de seguridad sobre la red, siendo así un blanco fácil para grupos o individuos que buscan causar daño buscando su propio beneficio o ventaja estratégica, consiguiendo ganancias financieras en ataques a las instituciones de salud.

Según (Cervera & Goussens, 2024) constan distintas formas de infringir los cimientos básicos a través de los diferentes sistemas informáticos como la historia

clínica electrónica del paciente, los dispositivos de monitorización de los mismos o las diferentes aplicaciones de salud, asimismo, el personal sanitario o de gestión no siempre está adecuadamente capacitado en buenas prácticas de ciberseguridad, lo que crea múltiples puntos de entrada para posibles ataques.

El acoger una historia clínica electrónica donde se registran desde datos demográficos hasta detalles financieros y de seguros de vida y seguridad social, además del uso de dispositivos médicos con red de internet es una oportunidad para los hackers para acceder a los sistemas hospitalarios con el fin de obtener información sanitaria protegida con fines financieros, políticos o de otro tipo (Cartwright, 2023).

La filtración de datos confidenciales o el secuestro de sistemas pueden comprometer la privacidad del paciente y la atención médica. Para contrarrestar esta amenaza, se requieren fuertes medidas de ciberseguridad como medida defensiva (Cervera & Goussens, 2024).

Según (O'brien, 2020) la industria sanitaria de EE.UU. se encuentra a la cabeza del resto de otras industrias, las filtraciones de datos cuestan un promedio de 7,13 millones de dólares, un 84 % más que el promedio mundial.

Además de los costos financieros, tiene impactos directos e indirectos en la prestación de servicios de salud en la población, como el 12 de mayo de 2017, un ataque de ransomware WannaCry afectó a 230.000 sistemas en más de 150 países incluido Reino Unido, lo que costo al Servicio Nacional de Salud casi £92 millones, donde la población tuvo reducción de acceso a la atención médica, citas médicas y cirugías canceladas, incluso cierre de departamentos de emergencias (Salud, 2018).

3.3 CIBERSEGURIDAD EN SALUD EN LATINOAMÉRICA

La ciberseguridad en países de primer mundo está muy avanzada, pero en el caso de América Latina y el Caribe se encuentra en las primeras etapas de establecimiento de ENCS (Estrategias Nacionales de Ciberseguridad) y desarrollo de capacidades cibernéticas para contrarrestar las amenazas en el ciberespacio (Aguilar, 2020). Por lo que demanda un marco normativo y políticas públicas con lineamentos claro sobre la protección de información.

En América Latina existe una brecha digital bastante importante que se basa en factores socioeconómicos, educativos y según su ubicación geográfica, superar dicha brecha requiere inversiones en infraestructura, servicio de internet, educación y capacitación en el manejo de destrezas ineludibles para gozar de los beneficios de las tecnologías digitales.

América Latina y el Caribe es una de las regiones con mayor incidencia de ciberataques, debido a los bajos niveles de defensa, recibiendo más de 1600 ciberataques por segundo. Equipo de respuesta, mecanismo de cooperación, educación formal y mayor inversión son algunos de los pasos que pueden tomar el gobierno para ayudar al sector privado a mitigar los riesgos, Brasil recibe más de la mitad de los ciberataques, seguido de México (23%), Colombia (8%) y Perú (6%) (Schwartz, Contreras, & Botting).

Según datos proporcionados por la Unión Internacional de Telecomunicaciones en 2013, América Latina divide a los países en cuatro grupos según sus niveles de conectividad. El primer grupo de países con una conectividad superior al 55% es Chile y Argentina; el segundo nivel es con Colombia, Venezuela, Brasil y Panamá con 45% a

55% de conectividad; el tercer grupo lo componen México, Ecuador, Perú y Bolivia. Las tasas de conexión oscilan entre el 35% y el 45%, mientras que Cuba, Nicaragua y otros países centroamericanos están por debajo del 35% (Martin, 2015).

Por lo que es de vital importancia abordar el tema de privacidad y seguridad de los datos, América Latina se ha quedado rezagada con respecto a otras regiones en este sentido de fortalecer la protección de datos y las medidas de seguridad, ya que es esencial para generar confianza y promover la adopción de tecnologías de salud digital.

En enero de 2015, en relación con el desarrollo de Internet en los países del Caribe y América Latina, la Organización de Estados Americanos propuso un plan de seguridad de red para las regiones antes mencionadas. Con su ayuda, intente formular una política integral de ciberseguridad (HERNÁNDEZ, CERQUERA, & VANEGAS, 2015).

3.4 CIBERSEGURIDAD EN ECUADOR

En Ecuador, las tecnologías digitales son esenciales para fortalecer las empresas, los servicios públicos y la administración pública en interés de los ciudadanos. Sin embargo, trae consigo la inseguridad tecnológica por lo que existe la necesidad de ejecutar estrategias para optimizar la seguridad cibernética.

En los estados democráticos pertenecientes de la Comunidad Andina como es el caso de Ecuador, en el proceso de constitucionalización de los derechos fundamentales ha incluido el derecho a la protección de los datos personales en respuesta a los avances tecnológicos (Ordóñez, 2017).

En Ecuador, el primer camino hacia el reconocimiento de un derecho constitucional a la protección de datos personales fue la reforma constitucional de 1996, que modificó la Constitución de 1976 para incluir garantías legales de protección de datos personales (Naranjo, 2017), cabe mencionar que la protección de datos personales no se consideró un derecho fundamental, sino que se lograría a través de otros derechos civiles.

En el año 2008, la constitución reconoce el derecho autónomo de la protección de datos personales desde una perspectiva europea, estableciendo que:

"El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley" (Constitución de la República del Ecuador, 2008).

Además, se determinó que los datos personales son bienes legítimos protegidos y deben ser tratados conforme a los principios de licitud y únicamente para los fines para los cuales fueron obtenidos.

Sin embargo, cabe mencionar que debido a la disposición constitucional la definición del perfil aún no se ha determinado, deja muchos límites a la interpretación. Asimismo, el texto constitucional no define disposiciones preventivas y no especifica reglas para el tratamiento de datos personales ya sea en organismos estatales o privados, organismos estatales u organismos internacionales (Rosas & Pila, 2023).

En 2018 se desarrolló el programa "Gobierno Abierto" como parte del Plan Nacional de Gobierno Electrónico para el periodo 2018-2021, en el cual la protección

de la información y datos personales se incluye en la estrategia número 3, donde la misión principal es desarrollar una norma jurídica que constituya la base para instaurar el sistema de protección de este derecho.

Además, en el año 2021, en el “Plan Ecuador Digital 2021”, en el marco de la línea de trabajo “Ecuador eficiente y ciberseguro”, reconoce que abordar temas de ciberseguridad y protección de datos personales es fundamental para proteger a los ciudadanos de las ciber amenazas, al tiempo que promueve el desarrollo económico. Como parte de esta última herramienta, el Gobierno de Ecuador se comprometió a desarrollar un Proyecto de Ley Orgánica de Protección de Datos Personales, el cual fue discutido y aprobado por la Asamblea Nacional.

En mayo de 2021, en el Registro Oficial Suplemento 459, se publicó la Ley Orgánica de Protección de Datos Personales, con el objetivo de garantizar el ejercicio del derecho fundamental a la protección de datos personales (Rosas & Pila, 2023). Es decir, La Ley de Protección de Datos tiene como objetivo proteger los datos personales de los ciudadanos ecuatorianos y garantizar su derecho a acceder a esta información y tomar decisiones relevantes. Esta ley regula y determina los principios, derechos, obligaciones y mecanismos de protección pertinentes.

De la misma manera, en 2021, se aprobó y publicó nuestra primera política de seguridad cibernética mediante Acuerdo Ministerial 006-2021, su propósito es construir y fortalecer las capacidades del Estado para garantizar el ejercicio de los derechos y libertades humanos y proteger los activos legítimos del Estado en el ciberespacio. Reconociendo la necesidad de que los grupos de interés fortalezcan su capacidad para

identificar, gestionar, abordar y mitigar los riesgos de seguridad cibernética (Información, 2022).

Dentro de los principios rectores de la Estrategia Nacional de Ciberseguridad, que sirven como guía para orientar las acciones de los actores nacionales con el fin de salvaguardar la soberanía del estado esta “Salvaguardar los derechos digitales” de las personas donde es importante mencionar la protección de los datos personales y privacidad, la confidencialidad, integridad y disponibilidad de la información.

En Ecuador, según los datos del Ministerio de Gobierno menciona que los delitos cibernéticos más comunes son el fraude informático, robo de identidad y la violación de datos personales. Sin embargo, Ecuador está trabajando para mejorar su capacidad para combatir el cibercrimen a través de la cooperación internacional. Actualmente está en transcurso de adhesión al Convenio de Budapest sobre la Ciberdelincuencia, la cual ayudará a ajustar la legislación nacional, mejorar los métodos de investigación y fortalecer la cooperación con otros países. Ecuador es miembro de la Organización de Policía Criminal Americana y de Interpol, lo que asevera el intercambio de información en tiempo real.

3.5 CASOS REALES

La industria de la salud representa un papel esencial en el bienestar de la sociedad, es un sector crítico, tiene información sensible y además datos de pacientes, lo que la convierte en un objetivo ideal para los ataques, especialmente el ransomware, que se centra en interrupciones del servicio que afectan en gran medida a la sociedad y, por lo tanto, son un problema urgente de abordar.

Pero los ciberataques no son nuevos hoy en día, los registros muestran que Estados Unidos sufrió un gran ataque en 2019. La compañía de seguros Change Healthcare (Nashville, EE. UU.) Es responsable de gestionar los pagos e ingresos entre pacientes, profesionales y proveedores de servicios médicos e intercambiar información médica. Sufrió un ataque cibernético, lo que generó un caos en la atención médica, ya que se vio afectado el acceso a los registros médicos, la información de las farmacias, la dispensación de medicamentos y más. Sin embargo, los ciberdelicuentes ganaron 22 millones de dólares en Bitcoin a costa de afectar redes en salud (Cacho, 2024).

Otro caso es el de Francia. En 2019, se produjeron cortes informáticos en 120 hospitales de todo el país, incluido el Hospital Central Sud-Franceline (CHSF), lo que provocó el aplazamiento de miles de operaciones en todo el país, incluso en uno de los hospitales más grandes de Francia. El CHSF tiene una capacidad de 1.000 camas, donde afectó no solo al software empresarial del hospital, sino que también las admisiones y el almacenamiento de pacientes, incluidas las imágenes médicas; y los ciberdelincuentes exigieron 10 millones de dólares por claves para desbloquear los sistemas hospitalarios (Otero, 2022).

Otro caso reciente fue en el Hospital Clínic de Barcelona (España) donde el centro emitió un comunicado en julio de 2023 confirmando la filtración de registros de atención clínica y de investigación (Barcelona, 2023). Donde varios datos del sistema fueron secuestrados y luego amenazados con ser vendidos a terceros exigiendo un rescate para paralizarlos, provocando cortes generalizados del sistema y varios cierres

del sistema, además de interrupciones de procedimientos e intervenciones específicos en los pacientes.

Además, la primera muerte registrada en el Hospital Universitario de Düsseldorf (Alemania) se produjo como consecuencia de un ataque de ransomware cuando el paciente no pudo adquirir el ingreso que necesitaba. A la luz de todo lo sucedido, es importante construir una cultura de ciberseguridad en la atención sanitaria.

4. CONCLUSIONES Y RECOMENDACIONES

La seguridad del ecosistema cibernético global no puede garantizarse ni gestionarse unilateralmente y requiere cooperación a nivel nacional, regional e internacional para ampliar su alcance e impacto.

En Latinoamérica, la mayoría de los países tienen o están estableciendo algún tipo de agencia de privacidad y protección de datos, pero ninguno tiene aún los recursos para responder a los ataques cibernéticos antes de que acontezcan.

América Latina y el Caribe deben promover el desarrollo de ciencias aplicadas que ayuden a amparar los intereses locales y regionales, y desarrollar legislaciones para regular las actividades cibernéticas públicas y privadas.

Debido al presupuesto actual y la insuficiencia de recursos humanos especializados en ciberseguridad en los organismos, se necesita construir metódicamente una cultura de ciberseguridad, desde cero, educación al personal de salud sobre la ciber conciencia.

Es fundamental que los profesionales de la salud sean conscientes de la ciberseguridad y comprendan que incluso con los mejores sistemas de ciberseguridad implementados, aún pueden ser vulnerables a ataques de phishing que pueden comprometer el sistema del hospital y todos los dispositivos conectados.

Debido a la falta de educación a la ciudadanía y falta de cultura a proteger su información personal, han sido expuestos como víctimas para delitos cibernéticos,

permitiendo el acceso fácil a sus datos personales. Es importante concienciar y entender la importancia de proteger los datos personales en la red y promover el desarrollo de destrezas de los usuarios para gestionar adecuadamente su privacidad en el ciberespacio.

5. BIBLIOGRAFÍA

Aguilar, J. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. *Revista de Estudios en Seguridad Internacional, 6*(2), 17-43. doi:http://dx.doi.org/10.18847/1.12.2

Barcelona, C. (2023). *Clinic Barcelona*. Obtenido de https://www.clinicbarcelona.org/ca/premsa/ultima-hora/ciberatac-a-lhospital-clinic-barcelona

Cacho, J. M. (2024). *Medium*. Obtenido de https://medium.com/@CuraeSalud/el-ciberataque-al-sistema-m%C3%A9dico-de-ee-uu-m%C3%A1s-grave-de-su-historia-8369a8869c90

Cartwright, A. J. (2023). El elefante en la habitación: la ciberseguridad en la atención sanitaria. *Revista de monitorización clinica y computación*, 1123-1132. Obtenido de https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10123010/#

Cervera, A., & Goussens, A. (2024). Ciberseguridad y uso de las TIC en el Sector Salud. *Elsevier*. Obtenido de https://www.sciencedirect.com/science/article/pii/S0212656723002871?via%3Dihub

Constitución de la República del Ecuador. (2008).

Gamón, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *R e vista Latinoamericana de Estudios de Seguridad*.

HERNÁNDEZ, L., CERQUERA, J., & VANEGAS, J. (2015). RIESGOS PRESENTES EN LOS CIBERATAQUES: UN ANÁLISIS A PARTIR DE HERRAMIENTAS DE AUDITORÍA FORENSE. *Pensamiento Republicano*.

Información, M. d. (2022). ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR. *MINTEL*. Obtenido de https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Martin, E. (24 de 06 de 2015). *ee.es.*

Meneses, N. (30 de 11 de 2022). *El Pais*. Obtenido de https://elpais.com/economia/formacion/2022-11-30/phishing-malware-o-ransomware-el-reto-de-formar-en-ciberseguridad-tras-la-pandemia.html

MINTEL. (2022). Estrategia nacional de Ciberseguridad del Ecuador. *Ministerio de Telecomunicaciones y Sociedad de la Información*.

Naranjo, L. (2017). El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador. *Revista de Derecho*(27). Obtenido de https://revistas.uasb.edu.ec/index.php/foro/article/view/501/488

O'brien, S. (23 de 09 de 2020). *Cyber Segurity Briefing*. Obtenido de https://cybersecureforum.co.uk/briefing/average-cost-of-data-breach-in-healthcare-industry-hits-7-13-million/

OPS. (2023). *Iris.paho.org.* Obtenido de https://iris.paho.org/bitstream/handle/10665.2/57372/OPSEIHIS230016_spa.pdf?sequence=1&isAllowed=y

Ordóñez, L. (2017). La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración. *Revista de Derecho, 27*.

Otero, C. (2022). *MeriStation*. Obtenido de https://as.com/meristation/2022/08/25/betech/1661418240_192302.html

Rosas, G., & Pila, G. (2023). LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR. *Revista Internacional de Cultura Visual*.

Salud, E. N. (12 de 10 de 2018). *National Health Executive*. Obtenido de https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled

Schwartz, A., Contreras, B., & Botting, A. (s.f.). *Duke University.* Obtenido de https://www.latamciso.com/Report2023SPA.pdf

Solleiro, J., Castañón, R., Guillén, Á., Hernández, T., & Solís, N. (2022). */www.redinnovagro.in.* Obtenido de https://www.redinnovagro.in/pdfs/cyber.pdf

Subijana, I. (2008). EL CIBERTERRORISMO: UNA PERSPECTIVA LEGAL Y JUDICIAL. *Eguzkilore*, 171. Obtenido de https://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf

Telefónica, F. (2016). *otech.uaeh.edu.mx.* Obtenido de https://otech.uaeh.edu.mx/site/cdn/assets/Microsites/iot/docs/Ciberseguridad.pdf