593 Digital Publisher
CEIT
ISSN 2588-0705

Estándares de ciberseguridad aplicables a los sistemas informáticos sanitarios para proteger los datos personales

Cybersecurity standards applicable to health IT systems to protect personal data

Cinthya Daniela Salazar-Lazo[1]
Universidad Católica de Cuenca - Ecuador
cdsalazarl12@est.ucacue.edu.ec

Blanca Lucía Avila-Correa[2]
Universidad Católica de Cuenca- Ecuador
blavilac@ucacue.edu.ec

doi.org/10.33386/593dp.2024.1.2156

V9-N1 (ene-feb) 2024, pp 88 - 102 | Recibido: 19 de septiembre del 2023 - Aceptado: 22 de septiembre del 2023 (2 ronda rev.)

1 Como experiencia profesional es de ayudante de desarrollo de Sistemas de gestión de la seguridad de la Información en sistemas sanitarios en instituciones que prestan servicios a entidades gubernamentales.
ORCID: https://orcid.org/0009-0002-0924-416X

2 Soy Docente de la Universidad Católica de Cuenca por casi 25 años. Mi área de conocimiento es la informática. Tengo estudios de cuarto nivel en Gerencia Sistemas y TI en la Universidad de las Américas y en Gestión de Proyectos en la Universidad Católica de Cuenca..
ORCID: https://orcid.org/0000-0002-9273-468X

Cómo citar este artículo en norma APA:

Salazar-Lazo, C., & Avila-Correa, B., (2023). Estándares de ciberseguridad aplicables a los sistemas informáticos sanitarios para proteger los datos personales. 593 Digital Publisher CEIT, 9(1), 88 - 102, https://doi.org/10.33386/593dp.2024.1.2156

Descargar para Mendeley y Zotero

RESUMEN

El avance tecnológico ha permitido gestionar electrónicamente los datos relativos a la salud a través de plataformas y sistemas informáticos para ofrecer a los usuarios mejores servicios sanitarios, no obstante, la protección de datos personales no ha sido considerada de vital importancia en el desarrollo de estos productos de software. El objetivo del presente trabajo es analizar los estándares de ciberseguridad que pueden ser aplicables a los sistemas informáticos para proteger los datos sanitarios de acuerdo con la normativa legal vigente en materia de protección de datos personales en el Ecuador. La investigación tiene enfoque documental descriptivo, en ella se realizó el análisis de los estándares de ciberseguridad y de la Ley Orgánica de Protección de Datos Personales para determinar cuáles pueden ser aplicables en el desarrollo de los sistemas informáticos y cumplir la legislación vigente. La aplicación correcta de estándares de seguridad informática o ciberseguridad minimiza riesgos de vulneración de datos, al mismo tiempo que permite a las entidades sanitarias cumplir la Ley y evitar sanciones.

Palabras clave: informática y desarrollo, protección de datos, derecho de la informática, derecho a la privacidad, servicio de salud.

ABSTRACT

Technological progress has made it possible to electronically manage health-related data through computer platforms and systems to offer users better health services; however, the protection of personal data has not been considered of vital importance in the development of these software products. The objective of this paper is to analyze the cybersecurity standards that can be applicable to computer systems to protect health data in accordance with the current legal regulations on personal data protection in Ecuador. The research has a descriptive documentary approach, in it the analysis of cybersecurity standards and the Organic Law for the Protection of Personal Data was carried out to determine which ones can be applicable in the development of computer systems and comply with current legislation. The correct application of IT security or cybersecurity standards minimizes the risk of data breach, while allowing healthcare entities to comply with the Law and avoid sanctions.

Keywords: informatics and development, data protection, information technology law, right to privacy, health service.

Introducción

Con el constante avance tecnológico de los sistemas de información, la sociedad actual se encuentra más interconectada con el objetivo de obtener servicios o productos; lo que hace habitual compartir datos personales en ámbitos laborales, financieros, académicos, sanitarios, de comunicación, entre otros. De manera similar, se dispone de una variada oferta de sistemas de búsquedas de la información, con distintos nichos y relaciones entre ellos (Codina, 2018, pág. 78).

En nuestras actividades usuales, tales como: utilizar un teléfono inteligente, consumir servicios de geolocalización, realizar transacciones bancarias, registrarse en línea en páginas web, consultar resultados de laboratorio, acceder a servicios de salud por telemedicina, interactuar por medio de domótica en empresas o domicilio, enviar correos electrónicos, iniciar videollamadas y muchas más dejamos huellas electrónicas (Arrieta Cortés, 2011, pág. 5). Todas estas acciones necesitan alimentar con datos a determinados sistemas informáticos. La información procesada siempre queda expuesta a riesgos, lo cual afecta a la gestión organizacional de responsables y encargados del tratamiento de datos, convirtiéndose en un problema potencial que puede perjudicar a los titulares de los datos personales. Con estos antecedentes, proteger la información que se recibe, genera, procesa y se almacena en los sistemas informáticos debe ser una prioridad y una estrategia muy importante, aún más, cuando las plataformas tratan información personal o cualquier otro dato sensible (Pérez, 2022, pág. 105).

Para mitigar los riesgos en los sistemas informáticos existen estándares de seguridad que, si bien es cierto, se encuentran en constante cambio, proporcionan reglas y parámetros para que las organizaciones puedan reglamentar y autorregular su gestión de seguridad de información de forma segura (Velasco Melo, 2008, pág. 34).

La principal preocupación de los titulares de los datos es la gestión de la seguridad de la información, debido a que no se precisan las políticas de protección que las organizaciones poseen para controlar todos los datos apropiadamente. En este sentido, la seguridad de la información debe disponer de tres características básicas, disponibilidad, integridad y confidencial (De La Cruz Rodríguez, Méndez Fernández, & Méndez Fernández, 2023), es decir, que la información se encuentre disponible en cualquier lugar e instante, independiente de donde se haya generado, además que sea completa, fiable, confidencial y con controles de accesos.

Debido a que datos relativos a la salud o datos sanitarios son especialmente sensibles (Abad & Carnicero, 212, pág. 237), es importante asegurar que el tratamiento e intercambio de esta información se produzcan en entornos seguros. Además, debido a que los sistemas de información se comunican entre ellos, se deben garantizar la confidencialidad, seguridad e integridad de los datos sanitarios (Martínez Jara, 2022, pág. 785) en entornos compartidos.

Frente a esta situación, es valioso destacar que los sistemas de información sanitaria deben cumplir con mecanismos que salvaguarden la seguridad de la información a través de estándares de ciberseguridad. En este contexto, la salud electrónica (salud-e) dispone de algunos estándares para utilizarlos en sus sistemas y de modo que cumplan con los requisitos requeridos en la normativa legal. Entre ellos están, por ejemplo, ISO/IEEE 11073, HL7, DoF (Sungkee & Hyoungho, 2018), ISO/IEC 27002 (Velepucha Sánchez, Morales Carrillo, & Pazmiño Campuzano, 2022) o ISO 27001 (Ramos Mamami, Cahuaya Ancco, & Llanqui Argollo, 2023, págs. 98-99).

El Convenio 108 del Consejo de Europa es el instrumento jurídico internacional vinculante de protección de datos personales. Ha sido elaborado documentos de referencia en áreas como la inteligencia artificial, el Big data, los datos relativos a la salud, los medios de la comunicación y la privacidad, gobernanza de internet y el tratamiento de datos personales por las fuerzas y cuerpos de seguridad (Consejo de Europa, 2023).

El convenio 108 ha sido un referente a nivel global para implementar en las legislaciones de cada país las Leyes de protección de datos personales. En Latinoamérica, los países que se han adherido a él son Argentina, México y Uruguay (Consejo de Europa, 2023), disponiendo de políticas gubernamentales para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

En el Ecuador hasta ahora no ha existido legislación especializada en la protección de datos personales para que regule o proporcione normativa en esta materia. En el Registro Oficial Suplemento 459 de 26-may.-2021, la Asamblea Nacional del Ecuador promulga la Ley Orgánica de Protección de Datos personales (Ley de Protección de Datos Personales, 2021), sin embargo, no se encuentra aprobado el Reglamento a la Ley Orgánica de Protección de Datos Personales (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022) y tampoco el país se encuentra adherido al convenio 108. En la presente investigación se analiza la normativa ecuatoriana en materia de protección de datos personales y, de acuerdo con ello, se recomiendan cuáles son los estándares internacionales de ciberseguridad que puedan ser aplicados en el desarrollo de los sistemas informáticos sanitarios ecuatorianos, debido a que, la gran mayoría de desarrolladores y empresas de software nacionales no tienen contemplados en sus procesos de desarrollo los requerimientos que la ley ecuatoriana ha determinado. No se pueden aplicar las recomendaciones para otros países, inclusive en Latinoamérica, porque cada legislación tiene sus propias particularidades.

Método

El presente trabajo de investigación tiene carácter descriptivo documental con diseño bibliográfico en el cual se realizó una revisión de la literatura asociada. Se inició analizando la normativa legal vigente en el Ecuador sobre la materia de protección de datos personales relativos a la salud, contenida específicamente en la Ley de Protección de Datos Personales emitida en 2021, como fuente principal de los requerimientos que los sistemas informáticos sanitarios necesitan para implementar la seguridad informática.

La recopilación de artículos científicos, libros, políticas e información técnica contenida en bases de datos de fuentes de reconocida confiabilidad y en los sitios oficiales de los estándares internacionales de seguridad informática fueron los referentes para determinar cuáles son las características apropiadas para proteger los datos relativos a la salud, según lo establece el marco jurídico ecuatoriano. A través de la investigación documental, realizando el análisis y evaluación de cada estándar de ciberseguridad de acuerdo con sus especificidades, se recomienda cuáles son los posibles estándares aplicables en los sistemas sanitarios con el objetivo de cumplir lo establecido en materia legal ecuatoriana.

Resultados

Marco Legal

Cualquier tipo de información acerca de una persona está relacionada con la privacidad, por ejemplo, la cédula de identidad, historial crediticio, correo electrónico, datos de salud u otros que sirvan para identificarse (Rivera Barrantes, 2019). En el Ecuador, la Ley Orgánica de Protección de Datos Personales, en adelante LOPDP, define como dato personal al dato que identifica o que sirve para ser identificable a una persona natural, sea o no de una forma directa, (Ley Orgánica de Protección de Datos Personales, 2021); en el Art. 4 del mismo texto hace referencia a los datos relativos a la salud como los datos personales que puedan revelar información del estado de salud de una persona, sea física y mental y en la que también incluye la prestación de servicios sanitarios.

Los artículos 30,31 y 32 de la LOPDP tratan sobre la protección de los datos relativos a la salud en los cuales se especifican las características de seguridad jurídica, acotando la aplicación de medidas técnicas organizativas para tal efecto. Si bien es cierto, no determinan protecciones específicas para sistemas informáticos sanitarios, la información debe ser gestionada apropiadamente de acuerdo con las

herramientas que la tecnología dispone. Entre los lineamientos principales que se proporcionan para el tratamiento luego de la recolección de este tipo de datos son los de seguridad adecuada de los datos, protección contra un tratamiento no autorizado o ilícito, pérdida, destrucción, daño accidental. (Ley Orgánica de Protección de Datos Personales, 2021).

El Art. 37 de la LOPDP determina la seguridad de los datos personales, manifiesta que hay que tener en cuenta el principio de seguridad de datos personales, para lo cual se deben considerar las categorías, volumen o cantidad de datos, seguridad integral, probabilidad de riesgos, entre otros. La normativa también describe otras medidas que se recomiendan para mitigar los riesgos identificados, entre las que describen a la confidencialidad, integridad y disponibilidad, anonimización o seudonimización o cifrado, acceso a datos de forma rápida en caso de incidentes, resiliencia técnica y acogerse a los estándares internacionales para gestionar los riesgos, implementación y manejo de sistemas de seguridad de información.

En la misma legislación ecuatoriana, según el literal *f* del artículo 7 de la Ley Orgánica de Salud, toda persona tiene derecho a tener una historia clínica única (Ley Orgánica de Salud, 2022), la cual, debe contener términos precisos, que sean comprensibles y completos, además de confidenciales. Las características del expediente sanitario descritas en la normativa vigente reflejan que los ciudadanos tienen derecho a la protección de los datos relativos a la salud, por consiguiente, obligan a las instituciones que prestan servicios sanitarios a acoger medidas para proteger sus sistemas informáticos que contienen esta información.

La normativa nacional permite identificar cuáles son los requisitos más relevantes en un sistema de información sanitaria, la confidencialidad, integridad y disponibilidad de la información (Cabrera Peña & Montenegro Jaramillo, 2022, pág. 179). En esa misma línea, y de acuerdo con lo recomendado por la Red Interamericana de Protección de Datos, los sistemas o plataformas informáticas, que gestionen el tratamiento de datos personales, deben cumplir lo prescrito en la legislación del Estado correspondiente (Red Iberoamericana de Protección de Datos, 2016, pág. 30).

Requerimientos de sistemas de información sanitarios

La información no tiene utilidad si es que no se especifica lo que realmente se requiere tratar o procesar (García Ortega, 2023, pág. 3); por lo tanto, para determinar las características de la seguridad en la información que deben poseer los servicios sanitarios y, por consiguiente, los sistemas informáticos que traten datos de salud deben establecerse los factores a proteger.

Es sustancial considerar los aspectos que definen a la seguridad informática; según la norma ISO 27000, encargada de establecer los requisitos y las buenas prácticas para la gestión de las seguridades de la información en las organizaciones, define a la seguridad de la información como la "Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas" (ISO 27000, 2023).

La confidencialidad es entendida como la seguridad o condición de que la información no pude estar disponible para terceros no autorizados, (Vidal Ledo, García Pierrot, & Cazes, 2005). La integridad hace referencia a que la información se encuentre correcta, sin modificaciones y errores; y, la disponibilidad se enfoca en que la información se encuentre disponible a los usuarios o sistemas autorizados (Instituto Nacional de Ciberseguridad España, INCIBE, 2016, pág. 6).

Para lograr el objetivo de proporcionar seguridad a la información, es fundamental disponer de herramientas de gestión estratégica que conduzcan a lograr la protección de la información (Velasco Melo, 2008, pág. 10), por ejemplo, estándares como la ISO 27001 para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) (Blanco & Rojas, 2012, pág. 338) o Health Level Seven

International (HL7).

Estándares de seguridad informática – Sistemas de información sanitarios

Health Level Seven International (HL7)

La Health Level Seven International, en adelante HL7, es una organización fundada en 1987, dedicada a proveer un marco integral y estándares relacionados para el intercambio de información de salud electrónica (HL7 International, 2023), facilitando la interoperabilidad entre aplicaciones informáticas que apoyan los procesos de la atención sanitaria (Socarrás Benitez, Vega Izaguirre, & Afonso Artiles, 2021, pág. 6).

La Organización HL7 crea los estándares de seguridad informática con sus propias siglas HL7, a partir del modelo de referencia OSI (Open Systems Interconnection Model – Interconexión de sistemas abiertos) (Castro Silvestre, Hernández Bravo, Carranza Gómez, & Montero Valverde, 2019).

Los estándares HL7 se asocian en las siguientes categorías de referencia: a) estándares primarios para la integración, interoperabilidad y cumplimiento de sistemas, b) CDA, arquitectura de documentos clínicos, c) EHR, que proporcionan modelos y perfiles funcionales para la gestión de registros médicos electrónicos, d) FHIR, son recursos rápidos de interoperabilidad sanitaria, e) Versión 2 (V2), es un protocolo de aplicación para el intercambio electrónico de datos en entornos sanitarios, f) Versión 3 (V3), son un conjunto de especificaciones basadas en el Modelo de información de referencia (RIM) de HL7, g) Sintaxis de Arden, es un formalismo para representar el conocimiento clínico procedimental h), CCOW, la especificación de gestión del contexto clínico, i) Modelos de análisis de dominio/paradigma cruzado, j) Dominios clínicos y administrativos, k) Guías de implementación e i) Reglas y referencias (HL7 International, 2023).

Uno de los estándares más destacados a nivel de comunicación de datos entre sistemas de información en salud es el HL7 V2.x (HL7 International, 2023). Los objetivos principales son la gestión de los datos y la interoperabilidad existente entre los sistemas (Perez Vasquez, 2022, pág. 7).

Otro estándar muy importante es el HL7 FHIR, por sus siglas en inglés Fast Healthcare Interoperability Resources, que permite definir el formato de datos y el protocolo de intercambio de información, sin imponer el modo de almacenamiento de los datos. (Jacek Kryszyn, Waldemar T. Smolik, Damian Wanta, Mateusz Midura, & Przemysław Wróblewski, 2023).

Con la misma importancia, el estándar HL7 CDA (Clinical Document Architecture) R2 (Release 2), ha sido creado para el marcado de los documentos o lenguaje de marcas, siendo una forma de codificar un documento, especificando la semántica y estructura de los documentos clínicos con el objetivo de intercambiarlos entre los prestadores sanitarios, es decir, para que sean interoperables entre las diferentes plataformas informáticas, disponiendo de seis características: persistencia, administración, potencial de autenticación, contexto, totalidad y legibilidad humana (Díaz Ordoñez, 2020, pág. 24).

ISO/IEC 27001:2022 — Sistemas de gestión de la seguridad de la información — Requisitos

ISO/IEC27001 es el estándar más conocido mundialmente en cuánto a implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) (International Organization for Standardization, 2022). Pertenece a la familia de las normas ISO/IEC 27000:2018 que proporcionan una descripción de la gestión de seguridad de la información, abordando aspectos de ciberseguridad, protección de la privacidad y seguridad informática (International Organization for Standardization, 2023). Se puede considerar un elemento clave en la gestión de protección de la información (Kitsios, Chatzidimitriou, & Kamariotou, 2023, pág. 3) por medio de implementar buenas prácticas de seguridad informática en una organización. (Ramos Mamami, Cahuaya Ancco, & Llanqui

Argollo, 2023, págs. 98-99)

La ISO/IEC 27001:2022 especifica los requisitos para que se puedan establecer, implementar, mantener y mejorar continuamente un SGSI (Servicio Ecuatoriano de Normalización, 2023). Esta norma contiene requisitos para que los riesgos sean evaluados y que se proporcione un tratamiento adecuado, adaptándose a los requerimientos y necesidades de la organización (International Organization for Standardization, 2022). La norma ISO/IEC 27001 permite reducir cualquier amenaza cibernética (Viguri Cordero, 2021, pág. 10). Estos estándares son aplicados por cualquier tipo de Organización, de cualquier tamaño o actividad, gubernamental o no, entre ellas las sanitarias, que pretenda gestionar la seguridad, como son los datos personales sanitarios.

La norma ISO/IEC 27001:2022 es certificable y dispone de 7 cláusulas de control, las cuales son: Contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora; 22 subcláusulas; y un anexo de referencia de controles de seguridad de la información (International Organization for Standardization, 2022).

ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información

Las normas ISO/IEC 27002 pertenecen a la serie ISO/IEC 27000, descienden de un estándar de seguridad corporativo entregado por Shell al Gobierno Británico a inicios de los años noventa, con el tiempo se convirtió en el estándar británico BS 7799 y se adoptó como ISO/IEC 17799 en el 2000. La norma tuvo una revisión en 2005, y cambió su nomenclatura a ISO/IEC 27002 en 2007 para alinearse con los otros estándares de la serie ISO/IEC 27000 (Motii & Semma, 2017, pág. 1); la última revisión fue en 2022.

Las ISO/IEC 27002 son una serie de principios y directrices para iniciar, determinar, implementar, mejorar y mantener la gestión de TI en cualquier organización; el enfoque dado de esta norma es para controlar el tratamiento de riesgos en un Sistema de Gestión de Seguridad de la Información (Gehrmann, 2012, pág. 73), en adelante SGSI.

Este sistema tiene una orientación sistemática para gestionar y controlar los sistemas de información con el objetivo de precautelar los tres aspectos principales, la confidencialidad, integridad y disponibilidad de la información (Sulistyowati, Handayani, & Suryanto, 2022, pág. 226). En las organizaciones que se encuentren aplicando un SGSI, las ISO/IEC 27002 se utilizan para implementar los requisitos establecidos en las ISO/IEC 27001 (Purba, Purnawan, & Eka Pratama, 2018, pág. 153).

Comprende objetivos de control y controles a implementar para el cumplimiento de los requisitos identificados a través del análisis o evaluación de los riesgos; otro objetivo es servir como guía práctica del desarrollo de procedimientos de un SGSI (Mendes, L. de Oliveira, & B. F. da Costa, 2013, pág. 74). Cada organización debe establecer cuáles controles debería aplicar de acuerdo con sus requerimientos, no obstante, no se trata de no usarlos, si no de justificar por qué no se los va a incorporar (Rodríguez Arroyo, 2020, pág. 53).

Las ISO/IEC 27002:2022 disponen de 4 cláusulas de control, que se resumen en; controles organizacionales, de personas, físicos y tecnológicos; 93 controles y dos anexos, de uso de atributos y correspondencia de las normas (International Organization for Standardization, 2023).

ISO 27799:2016 Informática de la salud — Gestión de la seguridad de la información en salud utilizando ISO/IEC 27002

La seguridad de la información se obtiene por medio de la implementación de determinados controles, en los que se encuentran las políticas, procesos, procedimientos, estructuras de organización y funciones del software y del hardware (Bozic, 2020, pág. 73).

Digital Publisher CEIT ISSN 2588-0705

El campo de la ciberseguridad a partir de 2012 ha experimentado una gran cantidad de publicaciones, entre las cuales se encuentran normas, reglamentos, leyes y guías de buenas prácticas, además, muchos científicos multidisciplinarios discuten sobre ciberseguridad y ofrecen recomendaciones. Entre las más importantes que se deben consultar son la ISO 27799 (Eichelberg, Kleber, & Kämmerer, pág. 1528).

ISO 27799 es una guía que proporciona información para proteger la confidencialidad, integridad y disponibilidad de los datos personales de salud (Thales group, 2023). Proveen las directrices para apoyar la interpretación y ejecución de las ISO/IEC 27002 en el área sanitaria (Sanchez Henarejos, Fernández Alemán, & Toval Álvarez, 2013, pág. 3).

Según la descripción técnica que hace la International Organization for Standardization, las normas ISO 27799:2016 son aplicables a la información sanitaria desde todas sus aristas, es decir, protege la información sanitaria en cualquiera de sus presentaciones, tales como, imágenes, videos, palabras, números, entre otras; de la misma manera, el medio para almacenarla sea físico o electrónico y medio para trasmitirla, entre los que se citan el fax, de forma manual, correo electrónico o redes informáticas. Es tecnológicamente neutra y no es certificable (Internacional Organization for Standardization (ISO), 2023).

Existen áreas de seguridad que no se encuentran contempladas en la norma, las cuales son la metodología y pruebas estadísticas para la anonimización efectiva y metodologías para implementar la seudonimización de datos personales sanitarios, la calidad de los servicios de las redes y los métodos que se pueden utilizar para medir la disponibilidad de redes utilizadas en sistemas informáticos sanitarios; y, para finalizar, la calidad de datos a diferencia de su integridad (Internacional Organization for Standardization (ISO), 2023).

Las normas ISO 27799:2016 disponen de 14 cláusulas: Políticas de seguridad de la información, Organización de la seguridad de la información, Seguridad de los recursos humanos, Gestión de activos, Control de acceso, Criptografía, Seguridad física y ambiental, Seguridad de las operaciones, Seguridad de las comunicaciones, Adquisición, desarrollo y mantenimiento del sistema, Relaciones con proveedores, Gestión de incidentes de seguridad de la información, Aspectos de seguridad de la información de la gestión de la continuidad del negocio, Cumplimiento; en su parte final dispone de tres anexos: Amenazas a la seguridad de la información en salud, Plan de acción práctico para la implementación de ISO/IEC 27002 en el cuidado de la salud y Lista de verificación para la conformidad con ISO 27799 (Internacional Organization for Standardization (ISO), 2023).

ISO/TC 215 Informática de la salud

Estas normas se aplican en el campo de la informática para poder facilitar la captura, el intercambio y utilización de los datos, la información y los conocimientos relacionados con la salud para respaldar y habilitar todos los aspectos del sistema sanitario. Dispone de 232 normas ISO publicadas y 58 en revisión (Internacional Organization for Standardization, 2023). Las normas tratan diversas temáticas específicas, por ejemplo, dispone del ISO/IEEE 11073-10102:2014 Informática sanitaria. Comunicación de dispositivos médicos en el punto de atención. Parte 10102: Nomenclatura. ECG anotado (Internacional Organization for Standardization, 2023).

Discusión

Los sistemas informáticos gestionan información de diversa índole. El enfoque en la presente investigación ha sido el tratamiento y seguridad de la información de los datos relativos a la salud en los sistemas informáticos sanitarios ecuatorianos, para ello se analizan los requerimientos del marco legal vigente con las características de los estándares citados para determinar el cumplimiento de aplicación o no en estos sistemas.

Las organizaciones sanitarias a nivel general, extranjeras o nacionales, públicas o privadas, pequeñas o grandes, custodian información relativa a la salud de sus usuarios, la cual debe ser protegida técnicamente acorde a normas internacionales destinadas para la seguridad de la información. Las tres características esenciales que los sistemas de gestión de la seguridad de la información (SGSI) mantienen como fundamentales y esenciales para tratar la información sanitaria son la confidencialidad, integridad y disponibilidad.

La legislación ecuatoriana se encuentra orientada con los mismos objetivos de protección de los datos personales de acuerdo con los SGSI; la Ley Orgánica de Protección de Datos Personales (LOPDP) expone que, para disminuir los riesgos, especialmente en los datos sanitarios, es necesario considerar algunas características como la protección de la confidencialidad, integridad y disponibilidad, anonimato, resiliencia técnica; así como de acogerse a los estándares internacionales en materia de seguridad.

Considerando la LOPDP en el desarrollo de las aplicaciones informáticas del sector sanitario ecuatoriano, no se ha encontrado evidencia de que estos principios hayan sido implementados en sistema sanitario público o privado alguno. Todavía existe un vago conocimiento de la aplicación de esta normativa como requisito para el desarrollo de software en esta área.

Antes de implementar los principios de seguridad establecidos en la LOPDP en los sistemas informáticos sanitarios en el Ecuador, es necesario analizar el diseño y la arquitectura de software para verificar la factibilidad de ponerlos en práctica. La incorporación de los requerimientos funcionales y no funcionales con las particularidades contempladas en la normativa conlleva en muchos casos a hacer una reingeniería de los sistemas. En el caso de que un sistema legado no permita incorporar estas características, la entidad correspondiente deberá migrar sus sistemas. Estas entidades no solo deben cumplir las exigencias legales, sino que deberán abordar esta responsabilidad desde la perspectiva ética. La protección de información médica no solo es un deber impuesto por la ley, sino también una obligación moral ineludible. La sensibilidad de los datos médicos exige salvaguardar la confidencialidad y la integridad de los datos.

En el mismo orden de ideas, cualquier entidad que disponga de un sistema informático médico que no posea las características que determina la ley puede ser sancionada económicamente por la Autoridad Nacional de Protección de Datos Personales y por las autoridades competentes que correspondan; así mismo, queda expuesta a demandas judiciales por parte de sus usuarios con reparaciones económicas muy altas que pueden comprometer gravemente la estabilidad y continuidad de una organización privada o al Estado si es que son Instituciones públicas.

Por otra parte, es necesario considerar, que a nivel internacional se han desarrollado diversos estándares de ciberseguridad para el tratamiento de la información sanitaria. Las características técnicas de seguridad de la información que han sido descritos se encuentran en algunos estándares, tales como, los Health Level Seven International (HL7), ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO 27799:2016 e ISO/TC 215.

Los estándares HL7, proporcionan modelos para la integración e interoperabilidad entre sistemas abiertos para transmitir los registros médicos electrónicos (EMR). Los protocolos establecidos proporcionan la confidencialidad, integridad y disponibilidad en el intercambio de datos entre las distintas plataformas, proporcionando la seguridad de los datos relativos a la salud. La aplicación de los estándares aumenta la eficiencia de los procesos sanitarios, respaldan efectivamente los datos de aplicación clínica y su debida gestión. Sin embargo, la implementación requiere considerar los costos de inversión y la complejidad técnica que implica la puesta en práctica de protocolos y formatos y semántica de documentos clínicos, del mismo modo, la integración de sistemas

ligados, las actualizaciones, cambios y ajustes de los estándares y los importantes desafíos de seguridad. Según el análisis realizado, los estándares HL7 cumplen con lo exigido en la LOPDP.

Las normas ISO/IEC 27001:2022 analizan los requisitos de seguridad de la información, ciberseguridad y protección de la privacidad de acuerdo con el contexto de la Organización; determina, implementa, mantiene y realiza la mejora continua de un SGSI. Es un estándar muy utilizado debido a que se establece con base a las necesidades y requerimientos de la organización, preservando la conocida triada de la CIA (confidencialidad, integridad y disponibilidad) cumpliendo con lo establecido en la protección de datos personales de salud según el marco jurídico vigente en el Ecuador.

Establecer los lineamientos de buenas prácticas de seguridad en los sistemas sanitarios con base a la normativa ecuatoriana en materia de protección de datos personales es complejo. Hasta el momento, la gran mayoría de desarrolladores de software se han limitado a diseñar e implementar sistemas sanitarios específicos con base a los requerimientos del cliente, aplicando únicamente las directrices tradicionales en temas de ciberseguridad. Por citar un ejemplo, se desarrollan controles de acceso, no obstante, no se consideran generar y poner en marcha algoritmos para anonimizar o seudonimizar los datos como lo determina la Ley.

Los desafíos para implementar sistemas adecuados de gestión de seguridad de la información son considerables, se deben identificar los riesgos a través de un enfoque holístico, es decir, se tienen que examinar leyes, requerimientos, tecnología, personas y políticas para disponer de una excelencia operacional y minimizar los riesgos de la seguridad.

Cuando una Organización sanitaria de cualquier tipología o tamaño ha decidido que requiere implementar un sistema de seguridad de la información (SGSI) mediante ISO/IEC 27001:2022 para cumplir con la LOPDP y demás leyes que regulan los servicios sanitarios en Ecuador, debe considerar que la implementación es compleja y requiere un alto nivel de experticia técnica y de gestión, así como los costos y recursos mantenimiento del SGSI. Otro importante desafío que deberán enfrentar es el cambio cultural en entornos en los que la seguridad de los datos no se considera una prioridad, asimismo, la gestión del cambio debida a las modificaciones en los procesos existentes. No menos crucial es enfrentar las amenazas de seguridad que constantemente evolucionan, por lo que mantener el SGSI actualizado es relevante.

Implementar, mantener y mejorar el SGSI con ISO/IEC 27001:2022 en las entidades sanitarias, al igual que en cualquier tipo de organización, requiere enfrentar algunos retos y aplicar buenas prácticas, entre ellas es lograr el compromiso de la alta dirección, identificar, gestionar riesgos, establecer políticas de seguridad, formar y concienciar al personal sobre la seguridad de la información, entre otras.

Las normas ISO 27799:2016 e ISO/TC 215 tratan la Informática de la salud; son normas especializadas en el cumplimiento de los controles de las ISO/IEC 27002:2022 amparados desde las ISO/IEC 27001:2022. Estas normas son utilizadas efectivamente para cumplir con una debida gestión de la información sanitaria, con las características que determina la ley. Son normativas enfocadas a proteger la información sanitaria desde todas las aristas, en otros términos, aplica para todos los formatos disponibles como: videos, imágenes o documentos y en cualquier medio en el que se encuentren almacenados (electrónico o en papel) y, por último, cualquier forma de transmisión, sean estás, redes informáticas, correo y demás. Son tecnológicamente neutrales, lo que permite a los desarrolladores de software la posibilidad de elegir nuevas tecnologías y cumplir con los requisitos de seguridad establecidos previamente. En consecuencia, estos estándares cumplen de igual manera con lo dispuesto en la LOPDP y son aplicables en el desarrollo de sistemas sanitarios en el Ecuador utilizando las ISO/IEC 27002.

Algunos de los beneficios de implementar ISO 27799:2016 son la estandarización de la gestión de la seguridad de la información en el sector sanitario, facilitando la interoperabilidad y el intercambio de datos entre entidades símiles, la protección de información sensible, garantizando la privacidad y confidencialidad, mejora la gestión de riesgos y consecuentemente la confianza de las partes interesadas. Sin embargo, al igual que otros estándares, los desafíos de su implementación se centran en la complejidad técnica y especializada en esta materia.

Complementariamente, la ISO/TC 215 ofrece la colaboración de expertos internacionales para enriquecer la calidad de los estándares y promover el cumplimiento de los controles de las ISO/IEC 27002:2022 amparados desde las ISO/IEC 27001:2022 para garantizar la precisión e integridad de los datos sanitarios. Igualmente, la complejidad técnica, la limitación de recursos, la actualización constante son un desafío que deben considerarse, para alinear puntos de vista y lograr consensos, no es tarea fácil y puede llevar tiempo.

Conclusiones

En relación con la información encontrada en la presente investigación, se ha determinado que los estándares citados ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO 27799:2016 e ISO/TC 215 cumplen con lo dispuesto en la Ley para la protección de datos personales relativos a la salud, y que pueden ser aplicables en el desarrollo de nuevos sistemas informáticos.

Razonablemente, se puede establecer que los sistemas informáticos legados, de acuerdo con su estructura de programación, podrían establecer controles para la seguridad de la información de acuerdo con estas normas, no obstante, debe realizarse un análisis profundo debido a que, en muchos casos, realizar una reingeniería de estos sistemas es imposible, consecuentemente no podrían cumplir con la normativa vigente.

Es importante recomendar a los desarrolladores de software sanitario, que antes de efectuar algún diseño e implementarlo, deben considerar que las políticas legales son requisitos fundamentales para que sus sistemas sean confiables para las partes interesadas, y evitar conflictos jurídicos con sanciones económicas.

Cualquier organización que tenga como finalidad llevar a cabo el tratamiento de datos personales sanitarios debe efectuar un análisis de riesgos de sus sistemas informáticos, concluyendo cuál sería el impacto si las amenazas llegan a concretarse, para reforzar y aplicar las medidas de seguridad pertinentes, considerando como requisitos principales lo instituido en la Ley de protección de datos personales.

Las organizaciones deben estar orientadas a la mejora continua de sus sistemas informáticos, principalmente deben disponer de herramientas que evalúen periódicamente la seguridad de los datos personales sanitarios para minimizar los riesgos que puedan surgir, con el objetivo de dotar de un algo grado de adaptación a los cambios que la Ley y el entorno exigen.

Cumplir con la LOPDP es crucial para garantizar la privacidad y confidencialidad de datos sensibles relacionados con la salud de los ecuatorianos y evitar sanciones legales. Para lograrlo, las entidades de salud deben acoger las buenas prácticas y recomendaciones de al menos uno de los estándares citados en este trabajo.

La aplicación de los estándares internacionales de ciberseguridad para la protección de datos relativos a la salud es esencial para garantizar la seguridad, confidencialidad, disponibilidad y privacidad de la información; proporcionan confianza, previenen incidentes de seguridad a través de la gestión de riesgos de seguridad y consienten el cumplimiento regulatorio.

Referencias bibliográficas

Abad, I., & Carnicero, J. (212). Intercambio internacional de información clínica. En S. E. Caribe, *Manual de Salud electrónica para directivos de servicios y sistemas de salud* (pág. 414). Nueva York: Naciones

Unidas.

Arrieta Cortés, R. (2011). *Reflexiones Sobre el Uso y Abuso de los Datos Personales en Chile.* Santiago de Chile, Chile: Andros Impresores. Recuperado el 23 de Junio de 2023, de www.consejotransparencia.cl/wp-content/uploads/estudios/2018/01/reflexiones_sobre_el_uso_y_abuso_de_los_datos_personales_en_chile.pdf

Asamblea Nacional del Ecuador. (26 de Mayo de 2021). *Ley de Ptotección de Datos Personales.* Quito: Asamble Naciona del Ecuador. Recuperado el 12 de Marzo de 2023, de https://www.asambleanacional.gob.ec/es/multimedios-legislativos/63464-ley-organica-de-proteccion-de-datos

Asamblea Nacional del Ecuador. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES.* Quito. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Asamblea Nacional del Ecuador. (2022). *Ley Orgánica de Salud (Última Reforma 29-04-2022)* (Última Reforma: Segundo Suplemento del Registro Oficial 53, 29-04-2022 ed.). Quito: Asamblea Nacional. Obtenido de http://biblioteca.defensoria.gob.ec/handle/37000/3426

Blanco, O., & Rojas, D. (2012). *Manual de salud electrónica para directivos de servicios y sistemas de salud.* Santiago de Chile: Publicación de las Naciones Unidas.

Bozic, V. (2020). Managing information security in healthcare. *Smart Cities and Regional Development Journal, 4*(2), 63-83. doi:https://doi.org/10.25019/scrd.v4i2.72

Cabrera Peña, K. I., & Montenegro Jaramillo, Y. A. (05 de 2022). Protección de Datos Personales en el Marco de la COVID-19: el Caso de CoronApp en Colombia. *The Law, State and Telecommunications Review, 14*(1), 179. doi:doi.org/10.26512/lstr.v14i1.39063

Castro Silvestre, L., Hernández Bravo, J., Carranza Gómez, J., & Montero Valverde, J. (2019). Propuesta de una Aplicación Web para la administración y manejo del historial clínico electrónico (HCE) en el sector salud, utilizando el estándar HL7 para la interoperabilidad. *Memorias del Congreso Internacional de Investigación Academia Journals Puebla 2019*, *11*, págs. 369-. Puebla. Recuperado el 21 de 06 de 2023, de https://eds-s-ebscohost-com.vpn.ucacue.edu.ec/eds/detail/detail?vid=0&sid=b8262874-11e4-4a2f-9c7d-0ffc514ccc5e%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1lZHMtbGl2ZQ%3d%3d#AN=140500802&db=edb

Codina, L. (2018). Sistemas de búsqueda y obtención de informacion: componentes y evolución. *Anuario Think EPI, 12*, 77-82. doi:https://doi-org.vpn.ucacue.edu.ec/10.3145/thinkepi.2018.06

Consejo de Europa. (2023). *https://www.coe.int*. Recuperado el 11 de 9 de 2023, de https://www.coe.int/es/web/data-protection/convention108/parties

De La Cruz Rodríguez, G., Méndez Fernández, R. A., & Méndez Fernández, A. C. (30 de 03 de 2023). Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática. *Revista Innovación y Software, 4*(1), 4. Recuperado el 6 de 7 de 2023, de https://revistas.ulasalle.edu.pe/innosoft

Díaz Ordoñez, P. E. (2020). *Desarrollo de un Prototipo de Framework para brindar seguridad en la confidencialidad de la información en el estándar HL7 CDA R2.* Medellín, Colombia. Recuperado el 10 de 06 de 2023, de hdl.handle.net/20.500.12622/4462.

Eichelberg, M., Kleber, K., & Kämmerer, M. (s.f.). Cybersecurity in PACS and Medical Imaging: an Overview. *Journal of Digital Imaging, 33*(6), 1527–1542. doi:doi.org/10.1007/s10278-020-00393-3

García Ortega, B. (16 de 07 de 2023). *upv.es.*

Obtenido de Introducción a la gestión de la información y del conocimiento en la empresa: https://riunet.upv.es/bitstream/handle/10251/184851/Garcia%20-%20Introduccion%20a%20la%20gestion%20de%20la%20informacion%20y%20del%20conocimiento%20en%20la%20empresa.pdf?sequence=1

Gehrmann, M. (julio-diciembre de 2012). Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations. *NAVUS - Revista de Gestão e Tecnologia, 2*(2), 66-77. Obtenido de www.redalyc.org/articulo.oa?id=350450810007

HL7 International. (2023). *HL7 International*. Recuperado el 21 de Junio de 2023, de http://www.hl7.org/implement/standards/index.cfm?ref=nav

Instituto Nacional de Ciberseguridad España, INCIBE. (2016). Cómo gestionar una fuga de información: una guía de aproximación para el empresario. *Instituto Nacional de Ciberseguridad España, INCIBE, 1*, 20. Recuperado el 17 de 07 de 2023, de www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_fuga_informacion_0.pdf

Internacional Organization for Standardization (ISO). (2023). *Norma ISO 27799:2016 Informática de la salud — Gestión de la seguridad de la información en salud utilizando ISO/IEC 27002*. Recuperado el 8 de 7 de 2023, de https://www.iso.org/: https://www.iso.org/standard/62777.html

Internacional Organization for Standardization. (2023). *ISO.org*. Recuperado el 25 de 07 de 2023, de ISO/IEEE 11073-10102:2014: https://www.iso.org/standard/63903.html?browse=tc

Internacional Organization for Standardization. (2023). *ISO/TC 215 Informática de la salud*. Recuperado el 16 de 07 de 2023, de ISO.org: https://www.iso.org/committee/54960.html

International Organization for Standardization. (Octubre de 2022). *ISO/IEC 27001*. Recuperado el 15 de Junio de 2023, de https://www.iso.org/standard/27001

International Organization for Standardization. (2023). *https://www.iso.org/home.html*. Recuperado el 01 de 07 de 2023, de https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27002:ed-3:v2:en

International Organization for Standardization. (2023). *ISO*. Recuperado el 19 de Junio de 2023, de ISO: https://www.iso.org/standard/iso-iec-27000-family

International Organization for Standardization. (s.f.). *Familia ISO/IEC 27000*. Obtenido de https://www.iso.org/standard/iso-iec-27000-family

International Organization for Standardization. (s.f.). *ISO/IEC 27000:2018*. Obtenido de https://www.iso.org/standard/73906.html

ISO 27000. (17 de 07 de 2023). *https://www.iso27000.es/glosario.html*. Obtenido de https://www.iso27000.es/glosario.html

Jacek Kryszyn, Waldemar T. Smolik, Damian Wanta, Mateusz Midura, & Przemysław Wróblewski. (Marzo de 2023). Comparison of OpenEHR and HL7 FHIR Standards. (P. A. Sciences, Ed.) *International Journal of Electronics and Telecommunications, 69*(1), 48. doi:https://doi.org/10.24425/ijet.2023.144330

Kim, L. (17 de Febrero de 2018). Concienciación en materia de ciberseguridad: protección de datos y de pacientes. *Nursing, 35*(1), 62-64. doi:10.1016/j.nursi.2018.02.017.

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (27 de Marzo de 2023). El estándar de gestión de seguridad de la información ISO/IEC 27001: cómo extraer valor de los datos en el sector de TI" Sostenibilidad 15, no. 7: 5828. *Sustainability, 15*(5828), 1-17. doi:10.3390/su15075828

Martínez Jara, J. N. (2022). Protección de datos personales en la historia clínica electrónica

bajo el marco legal ecuatoriano. *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas, 7*(1), 776-801. doi:doi.org/10.35381/racji.v7i1.2203

Mendes, R. R., L. de Oliveira, R. R., & B. F. da Costa, A. F. (Junio de 2013). Uma metodologia para implantação de um Sistema de Gestão de Segurança da Informação (SGSI) baseado nas normas ABNT NBR ISO/IEC 27001 e 27002. *Revista Principia*(22), 69-80. Recuperado el 22 de 05 de 2023, de https://periodicos.ifpb.edu.br/index.php/principia/article/download/158/128

Méndez Solar, J., & Eíto Brun, R. (Noviembre de 2017). NORMAS TÉCNICAS PARA HISTORIA CLÍNICA ELECTRÓNICA EN EL PROYECTO HCDSNS. *El profesional de la información, 26*(6), 1199-1210. doi:10.3145/epi.2017.nov.19

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (26 de 01 de 2022). *https://www.telecomunicaciones.gob.ec/*. Recuperado el 10 de 9 de 2023, de https://www.telecomunicaciones.gob.ec/proyecto-de-reglamento-a-la-ley-de-proteccion-de-datos-personales/

Motii, M., & Semma, A. (Mayo de 2017). Towards a new approach to pooling COBIT 5 and ITIL V3 with ISO/IEC 27002 for better use of ITG in the Moroccan parliament. *IJCSI International Journal of Computer Science Issues, 14*(3), 49-58. doi:doi.org/10.20943/01201703.4958

Nieves, A. (2017). *DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADOS EN LA NORMA ISO/IEC 27001:2013.*

Perez Vasquez, B. (28 de 06 de 2022). *Implementación de Seguridad y Privacidad de datos clínicos con el estándar HL7 FHIR.* Barcelona, España. Recuperado el 05 de 06 de 2023, de http://hdl.handle.net/2117/371386

Pérez, S. B. (30 de junio de 2022). Situaciones de riesgo moral e incentivos desalineados en ciberseguridad. *Revista Chilena de Derecho y Tecnología, 11*(1), 103-120. doi:0.5354/0719-2584.2022.60821

Purba, A. D., Purnawan, I. A., & Eka Pratama, I. A. (Diciembre de 2018). Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 dengan COBIT 5. *Merpati, 6*(3), 148-158. doi:doi.org/10.24843/JIM.2018.v06.i03.p01

Ramirez Benavides, J. (2020). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS DE SOPORTE Y DESARROLLO DE SOFTWARE EN LA EMPRESA ALFCOM S.A BASADO EN LA NORMA ISO/IEC 27001:2013.* Trabajo de grado, Bogotá. Recuperado el 5 de Junio de 2023, de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/11101/TRABAJO%20DE%20GRADO%20ESI43.pdf?sequence=1&isAllowed=y

Ramos Mamami, R. G., Cahuaya Ancco, R., & Llanqui Argollo, R. R. (2023). Política informática y la gestión de la seguridad de la información en base a la norma ISO 27001. *Revista Innovación y Software, 4*(1), 96-106. Obtenido de revistas.ulasalle.edu.pe/innosoft

Ramos Mamami, R., Cahuaya Ancco, R., & Llanqui Argollo, R. (Marzo de 2023). Política informática y la gestión de la seguridad de la información en base a la norma ISO 27001. *Revista Innovación y Software, 4*(1), 96-106.

Red Iberoamericana de Protección de Datos. (2016). *Estándares de Protección de Datos de los Estados Iberoamericanos.* Montevideo, Uruguay. Recuperado el 01 de 07 de 2023, de https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD

Rivera Barrantes, V. (2019). Realidad sobre la Privacidad de los Datos Personales en Costa Rica. *e-Ciencias de la Información, 9*(2). doi:10.15517/eci.v9i2.37503

Rodríguez Arroyo, H. A. (2020). *Importancia de controlar todas las amenazas detectadas a través de Magerit v.3 e ISO/ IEC 27002 según análisis de ataques informáticos en Latinoamérica.* Barranquilla, Colombia: UNAD. Recuperado el 18 de 05 de 2023, de repository.unad.edu.co/handle/10596/31879

Sanchez Henarejos, A., Fernández Alemán, J. L., & Toval Álvarez, A. (2013). Recomendaciones sobre seguridad y privacidad informática en el tratamiento de datos de salud. *Revista eSalud, 9*(34), 1-7. Recuperado el 20 de 07 de 2023, de https://dialnet.unirioja.es/servlet/articulo?codigo=4339745

Servicio Ecuatoriano de Normalización. (2023). *Academia.* Recuperado el 1 de Julio de 2023, de Academia: https://www.academia.edu/35400585/NTE_INEN_ISO_IEC_27000_TECNOLOG%C3%8DAS_DE_LA_MACI%C3%93N_T%C3%89CNICAS_DE_SEGURIDAD_SISTEMAS_DE_GESTI%C3%93N_DE_SEGURIDAD_DE_LA_INFORMACI%C3%93N_DESCRIPCI%C3%93N_GENERAL_Y_VOCABULARIO_ISO_IEC_27000_2016_IDT

Socarrás Benitez, D., Vega Izaguirre, L., & Afonso Artiles, Y. (Febrero de 2021). Propuesta de nuevas funcionalidades para la gestión de la Historia Clínica Electrónica en el sistema XAVIA HIS. *Revista Cubana de Informática Médica, 1*(1), 6. Obtenido de https://doaj.org/article/318d1191847b409cb463b8d1441e2dd9

Suárez-Obando, F., & Camacho Sánchez, J. (Septiembre de 2013). Estándares en informática médica: generalidades y aplicaciones. *Revista colombiana de Psiquiatría, 42*(3), 295-302. doi:10.1016/S0034-7450(13)70023-4

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2022). Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *International Journal on Informatics Visualization, 4*(4), 225-230. doi:http://dx.doi.org/10.30630/joiv.4.4.482

Sungkee, L., & Hyoungho, D. (31 de 01 de 2018). Comparison and Analysis of ISO/IEEE 11073, IHE PCD-01, and HL7 FHIR Messages for Personal Health Devices. (K. S. Informatics, Ed.) *Healthc Inform Research, 24*, 46-52. doi:10.4258/hir.2018.24.1.46

Thales group. (04 de 07 de 2023). *Thales Group*. Obtenido de https://cpl.thalesgroup.com/es/compliance/iso-277992016-compliance

Velasco Melo, A. H. (Junio de 2008). El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27 001. *Revista de Derecho*(29), 333-366. Recuperado el 08 de 07 de 2023, de https://doaj.org/article/d0b89750c953459a80efac6c2b2f5fa4

Velepucha Sánchez, M. A., Morales Carrillo, J., & Pazmiño Campuzano, M. F. (2022). Análisis y evaluación de riesgos aplicados a la seguridad de la información bajo la norma ISO. *Revista de Tecnologías de la informática y las telecomunicaciones, 6*(1), 63-78. doi:doi.org/10.33936/isrtic.v6i1.4473

Vidal Ledo, M., García Pierrot, G., & Cazes, G. (2005). Seguridad, Información y Salud. *Revista Cubana de información médica*. Recuperado el 15 de 07 de 2023, de http://www.rcim.sld.cu/revista_7/articulo_htm/segurinfsalud.htm

Viguri Cordero, J. (Octubre de 2021). Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos. *IDP: Revista de Internet, Derecho y Politica*(33), 1-12. doi:10.7238/idp.v0i33.376366