MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

# Estudio de la seguridad de la información de los pacientes en los hospitales Públicos tipo II de Ecuador

**Propuesta de artículo presentado como requisito para la obtención del título:**

## Magíster en Auditoría de Tecnologías de la Información

**Por la estudiante:**
**Mauricio Alexander QUIMIZ MOREIRA**

**Bajo la dirección de:**
**Rayner Stalyn DURANGO ESPINOZA.**

**Universidad Espíritu Santo**
**Maestría en Auditoría de Tecnología de la Información**
**Samborondón - Ecuador**
**Febrero del 2019**

# *Estudio de la seguridad de la información de los pacientes en los hospitales Públicos nivel II del Ecuador.*

Study of the safety of patient information in Public hospitals level II of Ecuador.

**Mauricio Alexander QUIMIZ MOREIRA**[1]
**Rayner Stalyn DURANGO ESPINOZA** [2]

Resumen

La información es un activo muy importante para la mayoría de las organizaciones o empresas, en el sector sanitario la información que se maneja es de alta sensibilidad al contener información detallada de los pacientes sobre su estatus socioeconómico, análisis, diagnósticos y tratamientos médicos que son llevados por estos centros de salud. Es indispensable que estas instituciones consideren la seguridad de la información como eje primordial para un buen manejo y gestión de la información, esto debido a que actualmente la filtración, alteración o robo de datos es un problema latente que puede afectar a los sistemas de información que se manejan en estos entornos. La ciberseguridad en los hospitales públicos debe estar acorde a políticas claras de aseguramiento de la información para defenderse de cualquier tipo de amenazas que cada vez son más avanzadas. En el presente trabajo se estudia la situación actual de la seguridad de la información de los pacientes en los hospitales públicos tipo II de Ecuador, estableciendo una metodología de análisis de la Ley HIPAA, Reglamento 2016/679 e ISO 27799, estableciendo grupos de evaluación en cada una de las entidades de salud escogidas en las que rigen normas y acuerdos ministeriales emitidos por el Ministerio de Salud Pública del Ecuador que son generales en el ámbito de la seguridad de la información. Finalmente se definen directrices para la seguridad de la información del paciente como un componente esencial para el adecuado tratamiento de la información de los pacientes. El resultado de este estudio demuestra claramente las falencias en el aseguramiento de la información de los pacientes a pesar de los esfuerzos que se hacen, por lo que se hace un proceso de mejora continua.

| Palabras clave: | Privacidad, Integridad, Información de pacientes, Ciberseguridad, Seguridad integral. |
|---|---|

Abstract

Information is a very important asset for most organizations or companies. In the health sector, the information handled is highly sensitive because it contains detailed information on patients about their socioeconomic status, analyzes, diagnoses and medical treatments that are taken for these health centers. It is essential that these institutions consider the security of information as the primary axis for good management and information management, this is because currently filtering, alteration or theft of data is a latent problem that may affect the information systems that they are managed in these environments. Cybersecurity in public hospitals must be in accordance with clear information assurance policies to defend against any type of threats that are increasingly more advanced. This paper studies the current situation of patient information security in type II public hospitals in Ecuador, establishing a methodology for analyzing HIPAA, Regulation 2016/679 and ISO 27799, and establishing evaluation groups in each of the health entities chosen, which are governed by standards and ministerial agreements issued by the Ministry of Public Health of Ecuador, which are general in the area of information security. Finally, guidelines for the security of patient information are defined as an essential component for the adequate treatment of patient information. The result of this study clearly demonstrates the shortcomings in the assurance of patient information despite the efforts made, thus making a process of continuous improvement.

| Keywords | Privacy, Integrity, Patient information, Cybersecurity, Comprehensive security. |
|---|---|

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail mquimiz@uees.edu.ec.

[2] Magíster en Sistemas de Información Gerencial. Docente de Postgrado Universidad Espíritu Santo- Ecuador.

## INTRODUCCIÓN

Toda empresa u organización independientes de su naturaleza y actividad requieren de medidas y controles de seguridad para resguardar la información de acciones malintencionadas que comprometan a la misma y cause graves daños en el prestigio institucional o pérdidas económicas considerables (Julio & Flores ,2017).

Desde este punto inicial se abordan dos conceptos importantes que son descritos por (Bracho et al., 2017) donde habla de la seguridad de la información y seguridad informática, términos que se encuentran estrechamente ligados ya que el primero asegura a la información en todo su conjunto, y el segundo considera exclusivamente controles técnicos para asegurar la información digital. Todo esto basado en los principios básicos o denominado triángulo de la seguridad que abarca tres elementos: disponibilidad, confidencialidad e integridad de la información, cada uno aporta para que la seguridad de la información sea integral(Casas, 2015).

Estos conceptos son de gran importancia, al ser la información un activo muy valioso y sensible para las organizaciones o empresas(Cuzme, León, Suárez, & Dominguez, 2019),pero aquí nace una pregunta: ¿Qué tan valiosa es la información para una organización orientada a la salud?, pueden existir muchas respuestas, pero todas coincidieron en la relevancia que es asegurar la información sensible que manejan estas entidades, como es el caso de los datos de los pacientes(Klonoff, 2015).

Existen algunas leyes, normas, reglamentos y acuerdos ecuatorianos orientados al manejo y seguridad de la información para las organizaciones públicas o privadas que manejen recursos públicos, como lo indica (Bracho , 2017), entre las que citamos:

- ✓ Constitución de la República del Ecuador (2008)
- ✓ Plan Nacional del Buen Vivir 2017-2022
- ✓ Ley del Sistema Nacional de Registro de Datos Públicos.
- ✓ Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- ✓ Ley Orgánica de Transparencia y Acceso a la Información Pública.
- ✓ Ley Orgánica de Telecomunicaciones.
- ✓ Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional.
- ✓ Código Orgánico Integral Penal (COIP).
- ✓ Normas de Control Interno de la Contraloría General del Estado
- ✓ Acuerdos Internacionales.

Las orientadas al ámbito de la salud se citan:

- Ley Orgánica de Salud Pública
- Ley Orgánica del Sistema Nacional de Salud.
- Acuerdos Ministeriales orientados al aseguramiento de la información de salud pública.

Si bien las organizaciones públicas de salud del Ecuador pueden hacer uso de estas leyes, normas, reglamentos y acuerdos para mejorar la seguridad de la información, no existe un documento específico que establezca lineamientos para un adecuado manejo y privacidad de la información médica de los pacientes en el Ecuador (Ayala, 2017). Algunos países han instaurado leyes y normativas para la protección de la información clínica; como es el caso de la Ley de Portabilidad y Responsabilidad de Seguros de Salud (Health Insurance Portability and Accountability Act, HIPAA por sus siglas en inglés) que existe en los Estados Unidos(Senate and House of Representatives of the United States of America in Congress assembled, 1996), o como existe dentro de la Unión Europea el Reglamento 2016/679 (Jalali & Kaiser, 2018; Pillo & Enríquez, 2017), que sirven como referencia para el aseguramiento de la información de los pacientes en esas regiones.

El sector de la salud en el Ecuador se encuentra segmentado como lo describe (Buitrón, Gea, & García, 2016), estando el Ministerio de Salud Pública (MSP), Instituto Ecuatoriano de Seguridad Social (IESS), Instituto de Seguridad Social de las Fuerzas Armadas (ISSFA) e Instituto de Seguridad Social de la Policía Nacional (ISSPOL), siendo la primera de estas entidades la que abarca a la mayor cantidad de la población y los tres últimos para trabajadores, militares y policías respectivamente. También están los servicios de salud que brindan las municipalidades y prefecturas que trabajan en conjunto con las organizaciones vinculadas a los temas sanitarios en el ámbito local (Sánchez, Caballero, Santos, Fernández & Piattini,2013). Es así que las tareas relacionadas al manejo y seguridad de la información de los pacientes que se encuentra a cargo del área de Tecnologías de la Información (TI) han sido reducidas, lo que origina la existencia de un alto índice de vulnerabilidades sobre los datos de los pacientes, ocasionado por la falta de la

aplicación de normas, leyes o estándares y en mucho de los casos esto ocurre por descuido del personal médico, administrativo y de tecnología (Barragán, 2017).

No obstante, el aseguramiento de la información en el área de la salud se ha venido dando considerando leyes y normativas ecuatorianas y estándares nacionales e internacionales como el caso del Manual técnico que establece (Chuncha, 2014) para mejorar los procesos y estar listos ante posibles vulnerabilidades; así mismo, otro caso es la Adaptación de las Normas ISO 27001 e HIPPA para la reducción de riesgos en la seguridad descrita por (Barragán, 2017). Esto hablando de ciertas instrucciones que se han visto beneficiadas de ciertas iniciativas de estudiantes de pregrado y postgrados en dar soluciones a estos problemas, de esas iniciativas muchas de ellas quedan solo en buenas intenciones y no se le da el seguimiento adecuado para ser replicadas en todas las entidades de salud, y al no ser considerarlos podría causar efectos graves como divulgación, alteración o robo de la información de los pacientes, más aún cuando se está trabajando en esas dependencias con una Historia Clínica en formato electrónico (HCE) ( Sánchez, 2014), causando graves perjuicios a la institución como al paciente.

Hay que considerar también el despliegue de las infraestructuras de Internet de las cosas (IoT) (Pacheco & Hariri, 2016; Ross, Michael, & Janet, 2016), que se encuentran presente en diferentes campos, y uno de ellos es el sector de la salud por lo que se debe tener más énfasis en la seguridad de la información, debido a que existen amenazas cibernéticas modernas orientadas a dispositivos de salud conectados (Dimitrov, 2016; Klonoff, 2015) que pueden comprometer la información del paciente.

Es por este motivo que se hace indispensable el estudio de la situación actual de la seguridad de la información de los pacientes en los hospitales públicos tipo II del Ecuador, mediante el análisis de normas y estándares, considerando como alcance del estudio a las entidades de salud de las ciudades de Portoviejo y Manta. Por lo tanto, se plantea realizar un análisis y valoración de estas normas vinculadas a temas de seguridad de la información clínica de los pacientes en los hospitales Verdi Cevallos Balda, IESS de Portoviejo y Rodríguez Zambrano de Manta, estableciendo la fundamentación teórica del estudio, la metodología aplicada, los análisis de resultados, la propuesta y sus conclusiones

## MARCO TEÓRICO

Las variables que se definen en este estudio son: independiente “Seguridad de la información” y dependiente “Pacientes de hospitales públicos”. En lo relacionado a las variables definidas hay estudios que establecen marcos metodológicos para ambientes de salud basadas en el ciclo de Deming (PDCA) donde busca establecer planes factibles para corregir errores comunes (L. Sánchez, 2013). El análisis de la seguridad de la información en entornos de telemedicina que aborda un análisis sobre los procedimientos de los servicios de Telemedicina más característicos y sus requerimientos de seguridad en base a estándares internacionales regulatorios que se adapten a las necesidades básicas de seguridad(Guillen, Ramirez, & Estupinan, 2011). (Pérez, 2019) compara sobre los derechos a la protección de los datos y privacidad de la Unión Europea y Estados Unidos, concluye en su trabajo que existe una distinción de la protección de datos como derecho fundamental y su falta de unanimidad jurídica global sobre esa percepción, sobre todo, por la falta de apuesta clara por parte de Estados Unidos en esa consideración clasificatoria como parte de los derechos humanos(Tamayo, 2016).

Estas investigaciones demuestran un contexto del interés que existe por seguir mejorando los procesos de seguridad de la información a nivel general y especialmente en los entornos hospitalarios (Figueroa,2016). Por este motivo se hace indispensable revisar algunos conceptos y temáticas tratadas en este estudio.

### Seguridad de la Información

La Asociación de Auditoría y Control de Sistemas de Información (ISACA), define a la seguridad de la información dentro de la empresa como *“la información que está protegida contra su divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y su falta de acceso cuando se la necesita (disponibilidad)”* (Cuzme, Suárez, Bracho, & Pupiales, 2017; Rocha, 2015), considerando los tres elementos del triángulo de la seguridad de la información.

La Seguridad de la información hace uso de las TI, para definir e implementar los procedimientos adecuados para el tratamiento de los datos y la información que se generan en las entidades de salud (Plazzotta, Luna, &

Bernaldo, 2015; Ross, Michael, & Janet, 2016).

**Normas, Estándares y Reglamentos**

**ISO/IEC 27002**

ISO 27002 es un manual de buenas prácticas que recomienda controles de seguridad que abordan los objetivos de control, permitiendo mitigar los riesgos que se pueden presentar. La última versión del estándar liberada en el 2013, consta de 19 secciones y está organizado en base a los 14 dominios, 35 objetivos de control y 114 controles (International Organization for Standardization(ISO), 2013; Sánchez, Fernández, & Toval, 2013).

En el Ecuador se cuenta con el Esquema Gubernamental de Seguridad de la Información (EGSI) elaborado en base a la Norma Técnica Ecuatoriana INEN-ISO/IEC 27002 (Castillo, 2013), que ha sido implementada en varias entidades públicas que dependen de la Función Ejecutiva.

**ISO 27799**

El estándar 27799:2016 fue desarrollada por el Comité Técnico ISO/TC-215 responsable de las áreas de salud Informática, se basa y amplía la orientación general proporcionada por ISO/IEC 27002, abordando las necesidades especiales de gestión de la seguridad de la información del sector de la salud, ya que se definen requisitos especiales puesto que deben garantizar la confidencialidad, integridad, auditabilidad y disponibilidad de la información de salud personal, la última versión liberada de este estándar es la del 2016 (International Organization for Standardization(ISO), 2016).

Si bien ISO/IEC 27002 es un estándar internacional amplio y complejo y su asesoramiento no está diseñado para los entornos de salud médica. ISO 27799 permite la implementación de ISO / IEC 27002 dentro de los entornos de salud de forma coherente y prestando especial atención a los desafíos únicos que plantea el sector de la salud, ya que existen controles específicos para cubrir aspectos clínicos detallados de manera puntual en el estándar (International Organization for Standardization(ISO), 2016).

**Ley HIPAA**

Ley HIPAA, conformada por un conjunto de regulaciones de aplicación limitada a los EEUU fue emitida por el Congreso de ese país en 1996, considerándose relativamente antigua; sin embargo, se la incluye por su relevancia en el área de la salud. Esta ley tiene la finalidad de regular y asegurar la confidencialidad e integridad sobre la información que involucre a los pacientes, evitando y previniendo las posibles fugas de los datos dentro de las casas de salud (Barragán, 2017; Sánchez,2014).

Para el estudio de la ley HIPAA, se considera la sección de Seguridad y Privacidad en el apartado C, denominada “Estándares de seguridad para la protección de la información médica electrónica protegida”, cuya finalidad se enfoca en el aseguramiento de la protección de la privacidad de los pacientes en relación con sus datos clínicos (Delgado, 2016).

La ley HIPAA incluye la protección de los pacientes y sus datos médicos, que tienen y hacen uso de los seguros médicos dentro de los Estados Unidos (Jarauta & Padro,2017). Además, se debe considerar, que los pacientes brindan la información clínica, así como también la seguridad integral de la misma(Perez,2019).

**Reglamento 2016/679-UE.**

Tiene como objeto, normas relativas a la protección de los datos y la circulación de los mismos de las personas que son atendidas por las instituciones de salud (Parlamento Europeo y del Consejo, 2016), como se describe en el Art.1.

Establece principios relativos al tratamiento de los datos de los pacientes, y sobre los consentimientos que se deben tener por parte de las personas para un buen uso de la información (Pineda,2017). Así mismo en su Art. 9 establece una categoría de datos personales, que se puede orientar a la clasificación de la información que se debe considerar para saber el tipo de información que debe estar privada de personas no autorizadas.

En sus artículos 16 y 17 dan derecho a la rectificación y suspensión de información que el interesado considere errores o irrelevante para que la institución de salud la maneje o conserve. Así también en su Art. 25 establece la protección desde el diseño y por defecto de los datos que se vayan generando. En su Art. 32 se establece medidas técnicas y organizativas para la seguridad de los datos personales conformadas por algunos literales.

Este reglamento está ligado a notificaciones y sanciones por las autoridades de control en caso de incumplimiento en el ámbito de su aplicación, como se indican en los Arts. 33, 34 y 35. Este documento solo se aplica en la Unión Europea y sus anexos, pero no limita su conocimiento para considerar sus aspectos en la seguridad de la información en el entorno de nuestro alcance como es en el Ecuador(Milane,2017).

### Otras leyes, normas y resoluciones

La Ley 41/2002 Normativa Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y Documentación Clínica, es un conjunto disposiciones que regulan la autonomía del paciente, así como los derechos y obligaciones asociadas al procesamiento y documentación de la información clínica (Medinaceli & Gil ,2015). Esta Ley es de alcance local en España y fue publicada en el año 2002 (Jefatura del Estado - Gobierno de España, 2002), su última modificación fue el 22 de septiembre de 2015.

Con la implementación de la ley 41/2002, la información clínica cuenta con una protección adecuada desde el procesamiento hasta el almacenamiento de la información en las instituciones de salud pública como privadas, y al ser de orden estatal, se debe aplicar en el territorio nacional (López, Arroyo, León & Molina,2012).

Otro de los aspectos de relevancia de esta Ley es que garantiza el derecho de la intimidad de los pacientes protegiendo la integridad y privacidad de ellos, como se establece Art. 7 (Paredes, 2017). Además, se enfoca en la protección de la información clínica de los pacientes en los documentos físicos (Jefatura del Estado - Gobierno de España, 2002).

Acuerdo Ministerial 5216-MSP tiene como objeto establecer condiciones de operación para aplicar los principios de manejo y gestión de la información confidencial de los pacientes. Los principios que se establecen en este reglamento son confidencialidad, integridad, disponibilidad y seguridad en el manejo de la información (Ministerio de Salud Pública, 2015).

En la Tabla 1 se muestra un análisis realizado con las normas, leyes y estándares considerados en este estudio, en el cual se establecen criterios basados en la norma ISO 27799, Ley de Portabilidad y Responsabilidad de Seguros de Salud (Health Insurance Portability and Accountability Act, HIPAA por sus siglas en inglés) y el reglamento 2016/679 para verificar el ámbito de importancia de cada una de ellas.

TABLA 1.
COMPARACIÓN DE LEYES Y NORMAS

| Criterios | ISO 27799 | Ley HIPAA | Reglamento 2016/679 |
|---|---|---|---|
| **Criterios generales (Principios de la seguridad de la información)** | | | |
| **Confidencialidad** | X | X | X |
| **Integridad** | X | X | X |
| **Disponibilidad** | X | | |
| **Criterios específicos** | | | |
| **Orientada a la seguridad específica de los datos del paciente** | | X | X |
| **Sugiere la implementación de controles a nivel general en el entorno de salud de acuerdo con las necesidades** | X | | |
| **Asocia sanciones a las entidades de salud por incumplimiento en el aseguramiento de la información de los pacientes** | | X | X |
| **Respalda el consentimiento del usuario para uso adecuado de la información personal del paciente** | | X | X |
| **Respalda la opción de solicitar la corrección o anulación de información que el usuario considere inadecuada** | | X | X |
| **Aplicable a nivel internacional** | X | | |
| **Considera fundamental el análisis de riesgos para la mejora de la seguridad** | X | X | X |
| **Seudonimización de la información del paciente** | | | X |
| **Clasificación de la información de salud** | X | | X |

### Historia Clínica Electrónica

La historia clínica electrónica (HCE) de los pacientes contienen información sensible del estado físico, emocional, social y demás aspectos sociodemográficos del paciente, por tanto, se debe garantizar la integridad, confidencialidad y disponibilidad en tiempo

real cuando estos se requieran (Pinto, López & Cuesta,2011). La alteración o filtración de información clínica de una persona puede ocasionar situaciones no deseables que afecten la estabilidad emocional y salud del paciente y su familia (Delgado, 2016).

En este contexto la Historia Clínica que se sigue manejando en menos porcentaje de forma física no deja de ser menos importante (Zambrano, Chafla, Moreira, & Cuzme, 2015), pero en vista que la mayor cantidad de información de los pacientes ya reposan en infraestructuras tecnológicas robustas y estos datos son transmitidos por medios de comunicación digitales, están propensos a amenazas que si no se las consideran pueden afectar a los datos de los pacientes (Cordero & Garcia,2016).

**Vulnerabilidad, Amenaza, Riesgo e Impacto**

**Vulnerabilidad**

Una vulnerabilidad es una debilidad que presenta un activo o sistema ante una amenaza latente, y que puede ser explotada en cualquier momento si no le la corrige oportunamente, causando pérdidas de información o económicas, puede estar ligada también a un mal diseño o mala configuración de los dispositivos dentro de una institución (Colobran, 2017; Onofa & Pilatuña, 2013), su valoración cualitativa por lo general está dada en alta, media o baja, aunque puede estipularse otro tipo de valoración de acuerdo a los criterios del profesional que evalúa (Rocco, & Garrido,2017).

Una vulnerabilidad se define también como las condiciones que llegan a existir inherentes a los activos o presentes en el entorno, que facilitan de cierta manera que las amenazas puedan materializarse y que provoque que los activos lleguen a ser vulnerables (Abad, 2015;Lewis,2016).

**Amenaza**

Una amenaza es cualquier entidad o circunstancia que atente contra el buen funcionamiento del sistema informático o red (Colobran, 2017). Según MAGERIT v3 establece grupos de amenazas: de origen natural, de origen industrial, defectos de aplicaciones, accidentales y deliberadas. Estas amenazas son las encargadas de explotar las vulnerabilidades presentes en un sistema o activo (Zarei & Sadough,2016).

**Riesgo**

El riesgo se define como el grado de valor probable de que una amenaza que existe pueda llegar a materializarse sobre el o los activos que hay dentro de la institución y provocar daños (Bracho, 2017; Chuncha, 2014). De esta forma el riesgo permite visualizar cuáles serían las repercusiones sobre los activos, sino se aplican los correctivos necesarios. La valoración del riesgo se puede dar de forma cualitativa o cuantitativa, de acuerdo con el tipo de metodología aplicada o profesional encargado del análisis (Caiza & Bolaños,2014).

**Impacto**

De acuerdo a (Colobran, 2017) es la medición y valoración del daño causado que sufre una institución al materializar una amenaza. Dicha medición y valoración puede estar reflejada en pérdidas económicas o el prestigio institucional (Isidro & Enrique,2013).

**METODOLOGÍA.**

Para el desarrollo del trabajo se hace uso de material bibliográfico vigente en cada una de las leyes, normas, estándares y reglamentos, combinada con investigación de campo, para su efecto se realizaron técnicas de investigación como la observación, encuestas y análisis en las áreas de TI de las casas de salud objeto de estudio. La información obtenida se alinea a los controles de seguridad de la información del estándar ISO/IEC 27799:2013, Ley HIPAA y Reglamento 2016/679-UE.

El proceso metodológico se establece con el análisis documental, identificación de las entidades de salud a evaluar, aplicación de los instrumentos de recolección de información, análisis y propuesta.

Las entidades de salud involucradas en el presente estudio son de la ciudad de Portoviejo y Manta, la tabla 2 detalla los nombres y se le define un código de identificación que se considera en el análisis.

TABLA 2.
POBLACIÓN TOTAL

| INSTITUCIÓN | CIUDAD | CÓDIGO |
|---|---|---|
| **Hospital IESS** | Portoviejo | HIESS |
| **Hospital Verdi Cevallos Balda** | Portoviejo | HVCB |

| | | |
|---|---|---|
| **Hospital Rodríguez Zambrano** | Manta | HRZ |

Para realizar las tareas de evaluación en las casas de salud, se contemplan a los principales elementos que interactúan con la información del paciente hospitalizado y/o ambulatorio. Por tanto, se considera integrar un equipo de evaluación conformado por:

- Encargado de la Gerencia
- Director de Tecnología
- Jefe de Talento Humano
- Jefe Financiero
- Jefe de Planificación
- Representante de los médicos
- Representante de las enfermeras

Este grupo es considerado por que tienen una interacción directa en la recolección, registro, procesamiento, almacenamiento, difusión y respaldo de la información que los pacientes.

La encuesta se divide en 14 grupos con un total de 60 preguntas considerando el estándar ISO 27799, Ley HIPAA y Reglamento 2016/679-UE, los grupos se definen a continuación:

*Grupo 1: Políticas de seguridad de la información.* - En este grupo se debe considerar las directrices de la alta gerencia para la seguridad de la información que se ven plasmadas en las políticas de seguridad de la información, su vigencia y proceso de revisión y validación regular.

*Grupo 2: Organización de la seguridad de la información.* - Se deben considerar las funciones y responsabilidades en el ámbito de la seguridad de la información dentro de un ámbito interno, los costos de las medidas de seguridad que se deben implementar estableciendo un proceso gradual hasta tener una seguridad aceptable. Uso de dispositivos móviles y teletrabajo.

*Grupo 3: Seguridad ligada a los recursos humanos.* - Se consideran un adecuado proceso de selección de personal, asignación de funciones y responsabilidades, planes de capacitación continua, y adecuado proceso de separación o cambio del puesto de trabajo. Asegurar la confidencialidad de las personas que manejan los datos del paciente.

*Grupo 4: Gestión de activos.* - Se consideran inventario de activos de la organización, personal responsable de los activos, planes de buen uso del activo, la clasificación, etiquetado y manejo de la información, y manejo de medios removibles.

*Grupo 5: Control de acceso.* - Establecimiento de políticas de control de acceso a redes y servicios en la red organizacional, gestión de usuarios considerando niveles de acceso a la información o sistemas, autenticación, revisión y reajustes de privilegios.

*Grupo 6: Gestión de los datos del paciente.* - Se deben considerar la seudonimización de los datos del paciente en caso de compartir información a terceros, mantener un adecuado proceso de aceptación por parte del paciente sobre el uso de sus datos para los fines que se crea conveniente, así mismo que se permita retirar esos permisos de su uso cuando el paciente crea conveniente.

*Grupo 7: Seguridad física y del entorno.* - Considerar los perímetros de seguridad física y lugares restringidos para usuarios internos o externos, equipamiento para la protección de la infraestructura tecnológica como sistema eléctrico, sistema de baterías, cableado, planes de mantenimiento de equipos.

*Grupo 8: Seguridad de las operaciones.* - Se consideran procedimientos y operaciones como la gestión de cambios y capacidad, protección contra códigos maliciosos, copias de respaldo, registro y seguimiento de eventos, control de software en la producción, restricciones de instalación de software, y las auditorías de sistemas de información.

*Grupo 9: Seguridad de las comunicaciones.* – Se considera la gestión de la seguridad en la red como controles en la comunicación, segmentación de redes, adecuados protocolos para la transferencia de información segura, manejo adecuado de mensajería electrónica, acuerdos de confidencialidad y divulgación de la información, alta disponibilidad de las comunicaciones para el acceso a la información, métodos de cifrado que se utilizan para cifrar la información almacena o en tránsito.

*Grupo 10: Adquisición, desarrollo y mantenimiento de sistemas de información.* - Requisitos de seguridad de los sistemas de información, seguridad en los procesos de desarrollo y soporte, ambientes de prueba seguros, procesos seguros de implementación a ambientes de producción.

*Grupo 11: Relación con los proveedores o terceros.* – Considera adecuadas políticas de seguridad de la información para las relaciones con proveedores o terceros, la adquisición de servicios o entrega de información segura, se debe tener claro las condiciones de consentimiento para el uso de los datos personales.

*Grupo 12: Gestión de incidentes de seguridad de la información.* - Planificación de la gestión de los incidentes y mejoras de la seguridad de la información, responsabilidades y procedimientos, reporte de eventos, reporte de debilidades, evaluación de eventos, respuesta a incidentes, aprendizaje y recolección de evidencias. Notificación a autoridades competentes sobre los incidentes ocurridos y comunicar a los usuarios afectados sobre la filtración de la información.

*Grupo 13: Continuidad del negocio.* - Planes de contingencia que permitan dar continuidad al negocio en caso de verse afectado en algunas de sus áreas de interés, la verificación, revisión y evaluación del plan es importante.

*Grupo 14: Cumplimiento.* - Adoptar estándares de seguridad de la información acordes al entorno, y que estén alineados a las políticas, leyes y normas involucrados en el aseguramiento de la información de sanitaria de los pacientes.

## ANÁLISIS DE RESULTADOS

Para la evaluación del instrumento se establece tres parámetros, para validar los controles con los que cuenta las unidades de salud:

- ✓ NC = No cumple
- ✓ CP = Cumple parcialmente
- ✓ CS = Cumple satisfactoriamente

Los resultados que se obtuvieron de la aplicación de un banco de preguntas vinculadas a los controles presentados en el estándar analizados son instrumento para el estudio de la seguridad de la información de los pacientes en los hospitales Públicos tipo II del Ecuador, en los tres centros de salud se observan en la tabla 3, 4 y 5, y en la figura 1 el gráfico porcentual de cada unidad de salud respectivamente.

La encuesta con sus respectivas preguntas se encuentra en los anexos de la presente investigación.

TABLA 3.
DATOS TABULADOS DE RESPUESTAS HRZ

| DETALLE | NC | CP | CS | No. PREGUNTAS |
|---|---|---|---|---|
| *Grupo 1* | 0 | 1 | 1 | 2 |
| *Grupo 2* | 3 | 1 | 0 | 4 |
| *Grupo 3* | 0 | 3 | 2 | 5 |
| *Grupo 4* | 1 | 3 | 2 | 6 |
| *Grupo 5* | 0 | 3 | 3 | 6 |
| *Grupo 6* | 1 | 2 | 0 | 3 |
| *Grupo 7* | 0 | 2 | 3 | 5 |
| *Grupo 8* | 5 | 3 | 0 | 8 |
| *Grupo 9* | 0 | 4 | 1 | 5 |
| *Grupo 10* | 3 | 1 | 0 | 4 |
| *Grupo 11* | 2 | 1 | 0 | 3 |
| *Grupo 12* | 0 | 2 | 0 | 2 |
| *Grupo 13* | 2 | 1 | 0 | 3 |
| *Grupo 14* | 1 | 2 | 1 | 4 |
| **TOTAL** | 18 | 29 | 13 | 60 |
| **%** | 30% | 48% | 22% | |

TABLA 4.
DATOS TABULADOS DE RESPUESTAS HIESS

| DETALLE | NC | CP | CS | No. PREGUNTAS |
|---|---|---|---|---|
| *Grupo 1* | 0 | 1 | 1 | 2 |
| *Grupo 2* | 2 | 2 | 0 | 4 |
| *Grupo 3* | 0 | 3 | 2 | 5 |
| *Grupo 4* | 2 | 2 | 2 | 6 |
| *Grupo 5* | 1 | 3 | 2 | 6 |
| *Grupo 6* | 2 | 1 | 0 | 3 |
| *Grupo 7* | 0 | 3 | 2 | 5 |
| *Grupo 8* | 3 | 5 | 0 | 8 |
| *Grupo 9* | 0 | 3 | 2 | 5 |
| *Grupo 10* | 2 | 2 | 0 | 4 |
| *Grupo 11* | 2 | 1 | 0 | 3 |
| *Grupo 12* | 0 | 2 | 0 | 2 |
| *Grupo 13* | 2 | 1 | 0 | 3 |
| *Grupo 14* | 0 | 3 | 1 | 4 |
| **TOTAL** | 16 | 32 | 12 | 60 |
| **%** | 27% | 53% | 20% | |

TABLA 5.
DATOS TABULADOS DE RESPUESTAS HVCB

| DETALLE | NC | CP | CS | No. PREGUNTAS |
|---|---|---|---|---|
| *Grupo 1* | 0 | 1 | 1 | 2 |
| *Grupo 2* | 3 | 1 | 0 | 4 |
| *Grupo 3* | 0 | 3 | 2 | 5 |
| *Grupo 4* | 2 | 2 | 2 | 6 |
| *Grupo 5* | 1 | 3 | 2 | 6 |
| *Grupo 6* | 1 | 2 | 0 | 3 |
| *Grupo 7* | 0 | 2 | 3 | 5 |
| *Grupo 8* | 4 | 4 | 0 | 8 |
| *Grupo 9* | 0 | 4 | 1 | 5 |
| *Grupo 10* | 3 | 1 | 0 | 4 |
| *Grupo 11* | 2 | 1 | 0 | 3 |
| *Grupo 12* | 1 | 1 | 0 | 2 |
| *Grupo 13* | 2 | 1 | 0 | 3 |
| *Grupo 14* | 0 | 3 | 1 | 4 |
| **TOTAL** | 19 | 29 | 12 | 60 |
| **%** | 32% | 48% | 20% | |

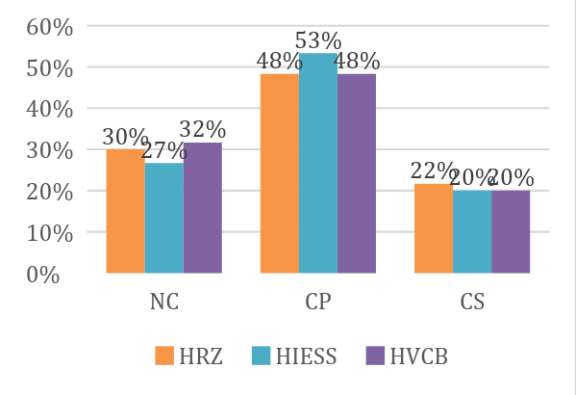


Figura 1. Cumplimiento general de controles

En la figura 1, se consideran las tres unidades de salud donde se muestra de forma general el estado de la seguridad de la información de acuerdo a los grupos presentados que contemplan en total 60 preguntas que establecen el no cumplimiento, cumplimiento parcial o cumplimiento satisfactorio de cada uno de los controles evaluados, arrojando como resultado porcentajes similares en cada una de las unidades de salud, donde se muestra del 27% a 32% de no cumplimiento (NC), del 48% a 53% cumplimiento parcial (CP), y del 20% al 22% con un cumplimiento satisfactorio. Demostrando que existen brechas de seguridad identificadas en cada grupo que deben ser tomadas en cuenta, para lograr una seguridad integral.

La seguridad de los datos del paciente es de vital importancia, pero también se deben considerar otros parámetros que contribuyen a tener una seguridad integral, se considerarán la revisión de los grupos con ningún cumplimiento.

Dentro de las preguntas evaluadas en el grupo 1, a pesar de tener políticas de seguridad establecidas de forma general, no se hacen revisiones regulares del cumplimiento de estas, ni se realizan un proceso de retroalimentación para reajustar las políticas que no se ajustan a las necesidades actuales.

En las preguntas del grupo 2, la organización de la seguridad de la información presenta falencias en establecer las responsabilidades y funciones, planificar los costos de las medidas de seguridad a implementarse, estas deben estar claramente identificadas en las políticas y planificadas para su ejecución gradual.

En las preguntas del grupo 4, se detecta que, a pesar de tener un inventario de activos, no se maneja una clasificación, etiquetado y manejo de la información adecuada.

Las preguntas del grupo 6 referente a la gestión de datos del paciente, indica que no se tiene claro para establecer la seudonimización de los datos del paciente, ni se tiene establecido un proceso adecuado de la aceptación o rechazo para un adecuado tratamiento de los datos del paciente.

Las preguntas del grupo 8, hace conocer los inconvenientes en la segmentación de las redes, no se establecen métodos de cifrado para la información que se transmite por medios digitales, tampoco se establecen acuerdos de confidencialidad y divulgación de la información entre sistemas de información.

Las preguntas del grupo 10, demuestran falencias en los procesos para la adquisición, desarrollo y mantenimiento de sistemas de información, el establecimiento de pruebas seguro es indispensable antes de implementar nuevos sistemas o software en producción.

Las preguntas del grupo 11, muestran que en los acuerdos con proveedores o terceros no se establecen claramente acuerdos de confidencialidad, integridad y disponibilidad de la información. Debe estar respaldado con el consentimiento de los pacientes para un adecuado uso de sus datos.

Las preguntas del grupo 13, indica claramente que no existe un plan de continuidad del negocio en caso de tener problemas que comprometan la seguridad de la información, que contempla su confidencialidad, integridad o disponibilidad.

Los grupos que no se han considerado no dejan de ser menos importantes, y también deben ser revisados en detalle ya que algunos de las preguntas consideradas dentro de los grupos se cumplen parcialmente y otros satisfactoriamente.

**Propuesta**

La propuesta se orienta al aseguramiento de la información del paciente en las unidades de salud, por lo que se propone en la figura 2 un proceso de establecimiento de controles de acuerdo la Ley HIPAA, Reglamento 2016/679-UE, ISO 27799, Ley Orgánica de Salud Pública, Ley Orgánica del Sistema Nacional de Salud y Acuerdo Ministerial 5216-MSP. Considerando su aplicación en las tres unidades de salud evaluadas por sus semejanzas en los resultados obtenidos.


Figura 2. Proceso de establecimiento de controles de seguridad

*Concientización sobre la seguridad:* en este ámbito se pone en consideración soluciones que pueden ser consideradas para mejorar la seguridad de la información del paciente, de acuerdo con los grupos que fueron evaluados:

- ✓ Las políticas de seguridad deben engranarse con las necesidades de aseguramiento de la información y esto se debe enmarcar en:
  - Revisión y validación de las políticas de seguridad de la información.
  - Organización adecuada de las políticas que establezcan responsabilidades claras, de los responsables de que estas se cumplan.
  - Establecer niveles de privilegios adecuado para quienes manejan la información del paciente.
  - Definir las personas que deben recibir los informes de incidentes y respuestas a problemas de seguridad.
- ✓ Clasificación, etiquetado y manejo de la información de los pacientes que deben contemplar:
  - Adecuada gestión de los datos del paciente, donde se establezca la seudonimización de datos cuando estos son compartidos con proveedores o terceros cuando se requiera. Esto con el fin de tener información personal del paciente, identificada por códigos sin que se revele sus datos demográficos que comprometan su integridad.
  - Se debe establecer un procedimiento adecuado para la aceptación o negación de permisos de usos y eliminación de información del paciente por parte de la unidad de salud.
- ✓ Establecer mecanismos de cifrado 3DES, AES de la información de considerada como crítica cuando se mantenga almacenada o en tránsito, así como su integridad mediante funciones de resumen MD5 o SHA-1.
- ✓ Definir acuerdos con proveedores y terceros que establezcan con claridad compromisos de confidencialidad y divulgación de la información.
- ✓ Establecer procesos de autenticación adecuados a los sistemas de información y recursos de red, con la implementación de servidores RADIUS, con la generación de claves seguras.

*Impacto de controles de seguridad:* en este punto lo que se debe buscar es el impacto que se tendrá al implementar los controles, que pueden involucrar recursos económicos, tecnológicos y humanos. En este ámbito se debe considerar:

- ✓ Personal para la revisión de la política de seguridad de acuerdo con el ámbito de su aplicación.
- ✓ Capacitaciones al personal que realiza el tratamiento de los datos del paciente.
- ✓ Mejora en los sistemas de gestión de la información de los pacientes.
- ✓ Sistemas de respaldo de información a repositorios seguros.

*Operaciones de seguridad:* se deben considerar monitoreo continuo de accesos a sistemas de información, revisión de niveles de privilegios, accesos a áreas críticas, seguimiento del tratamiento de la información del paciente por parte del personal, proveedores o terceros que requieren información del paciente.

*Auditorías de seguridad:* este ámbito si bien se debe estar establecido como política y procedimiento, se debe mantener constante para mejorar los procesos de seguridad dentro del entorno de salud.

En la siguiente Tabla de la 6, se definen cláusulas donde se propone una norma que complementa la ISO 27799, Ley HIPAA y el Reglamento 2016/679 que de acuerdo con el estudio realizado se deben considerar en las entidades de salud para el aseguramiento de los datos del paciente.

TABLA 6.
PROPUESTA

| Cláusulas | Justificación | Soporte |
|---|---|---|
| **Alcance** | Definir un alcance de la seguridad en el entorno de salud, considerando los criterios adecuados con respecto a la información clínica de | ISO 27799 |

| | | |
|---|---|---|
| | los pacientes. | |
| **Políticas de la seguridad de la información** | Las políticas deben estar enmarcadas dentro del ámbito de la confidencialidad, integridad y disponibilidad. | ISO 27799 Ley HIPAA Reglamento 2016/679 |
| **Organización de la seguridad de la información** | Definir responsabilidades internas en relación con la seguridad de la información. | ISO 27799 |
| **Recursos Humanos** | Establecer adecuados procesos de contratación y educación del personal en lo referente a la seguridad de la información. | ISO 27799 Ley HIPAA Reglamento 2016/679 |
| **Gestión de activos** | Clasificar adecuadamente la información y establecer los responsables de los activos. | ISO 27799 Reglamento 2016/679 |
| **Control de acceso** | Gestionar y controlar los accesos de los usuarios a sistemas e información de los pacientes. | ISO 27799 Reglamento 2016/679 |
| **Cifrado de datos** | Establecer mecanismos de cifrado de datos que están almacenados o en tránsito. | ISO 27799 |
| **Seguridad del entorno** | Establecer perímetros de seguridad física y ambiental dentro del entorno de salud. | ISO 27799 Ley HIPAA Reglamento 2016/679 |
| **Operaciones de seguridad** | Monitoreo y control de vulnerabilidades de los sistemas e información. Establecer procesos de auditoría regulares. | ISO 27799 Reglamento 2016/679 |
| **Relaciones con proveedores y pacientes** | Establecer criterios de seudonimización de la información del paciente cuando se comparte información entre instituciones. Considerar el consentimiento de los pacientes para el uso de tratamiento de la información, su corrección o anulación en caso de ser necesaria. | ISO 27799 Reglamento 2016/679 |
| **Gestión de incidentes de seguridad** | Establecer procedimientos sobre los incidentes de seguridad suscitados y cómo deben ser reportados a las autoridades y dueños de la información en caso de ser comprometida. | ISO 27799 Ley HIPAA Reglamento 2016/679 |
| **Continuidad del negocio** | Diseño, planificación y ejecución de plan de contingencia en caso de interrupciones en los servicios de salud. | ISO 27799 |
| **Cumplimiento** | Alinearse a leyes, normas, estándares y reglamentos de orden local, para establecer sanciones en caso de incumplimiento de las políticas de seguridad. | ISO 27799 Ley HIPAA Reglamento 2016/679 |

## CONCLUSIONES

Los porcentajes obtenidos en la evaluación de los controles de seguridad demuestran que la seguridad de la información de los pacientes no se lleva adecuadamente ya que la norma ISO27799, la Ley HIPAA y reglamento 2016/679UE, no forman parte integral del proceso de aseguramiento de la información de los pacientes. Los acuerdos y normas en el ámbito local son muy generales, aunque esto también deber ser a que en el Ecuador no se maneja un Ley de Protección de Datos Personales, como es el caso del Reglamento 2016/679 de la Unión Europea.

Las unidades de salud evaluados establecen controles generales de aseguramiento de la información, pero se pudo observar que los controles específicos ayudan a una adecuada clasificación, etiquetado y tratamiento de la información de los pacientes que no se presentan de forma clara, al no tener esto tampoco se evidenció procedimientos de aceptación, rechazo del uso de la información, así como un adecuado procedimiento de eliminación de la información.

La propuesta que se presenta es un aporte para mejorar la seguridad y centrarse específicamente en los datos de los pacientes, por lo cual tengan un buen tratamiento ya sea dentro de la unidad de salud o cuando se requieran por entidades externas.

Por tanto, se recomienda continuar con la aplicación de los controles de seguridad sobre los recursos humanos, dentro del proceso de selección, reubicación del personal y en el encargo de funciones.

Es importante, mantener definidas e implementadas las políticas sobre el control de acceso, la asignación de las cuentas autorizadas para el acceso a la red, la suspensión, cambio y registro de privilegios a los usuarios.

Sobre la seguridad física es necesario mantener y fortalecer los controles, limitando las áreas sensibles para que sean accedidas exclusivamente por el personal autorizados.

En relación con la seguridad sobre los servicios de red, es recomendable aplicar tareas de segmentación dentro de la misma infraestructura de red, de forma parcial o total. Aunque existen políticas de seguridad sobre divulgación de información, que deben ser implementadas de mejor manera y dar cumplimiento a las mismas.

Finalmente, es recomendable mantener y fortalecer las funciones sobre la gestión de incidencias dentro de las instituciones médicas, y de ser posible mejorar el cumplimiento del debido proceso para el análisis, tratamiento y control de las incidencias de manera óptima.

**Referencias Bibliográficas**


Abad, C. (2015). *Plan de Contingencia de-tecnología de la información del Hospital IESS Zamora*.

Barragán, C. F. (2017). Adaptación de las Normas ISO 27001 e HIPPA para la reducción de riesgos en la seguridad en Hospitales Nivel I del IESS, 178.

Bracho, C. (2017). *Auditoría de seguridad informática dirigida al Gobierno Autónomo Descentralizado del Cantón Mira basado en el estándar Cobitv5, siguiendo la metodología OSSTMMv3*. Universidad Técnica del Norte.

Bracho, C., Cuzme, F., Pupiales, C., Suárez, L., Peluffo, D., & Moreira, C. (2017). Auditoría de seguridad informática siguiendo la metodología OSSTMMv3 : caso de estudio. *Maskana*, *8*, 307–319.

Buitrón, M. E., Gea, E., & García, M. V. (2016). Tecnologías en información y comunicación sanitaria. *Revista PUCE*, *0*(102), 273–289. Retrieved from http://www.revistapuce.edu.ec/index.php/revpuce/article/view/15/17

Casas, P. (2015). El Triángulo de la Seguridad | Seguridad en Cómputo. Retrieved May 20, 2018, from http://blogs.acatlan.unam.mx/lasc/2015/11/19/el-triangulo-de-la-seguridad/

Castillo, C. (2013). *Esquema Gubernamental de Seguridad de la Información EGSI*. Retrieved from www.lexis.com.ec

Chuncha, S.-F. (2014). *Manual técnico de procesos basado en normativa internacional para la gestión de riesgos informáticos en el departamento de sistemas del Hospital Provincial Docente Ambato*. Universidad Técnica de Amabato. Retrieved from http://repositorio.uta.edu.ec/handle/123456789/8100

Colobran, M. (2017). *Análisis y gestión de vulnerabilidades de sistemas informáicos con softwrae libre*.

Cuzme, F., León, M., Suárez, L., & Dominguez, M. (2019). Offensive Security : Ethical Hacking. In *Advances in Intelligent Systems and Computing* (Vol. 1, pp. 127–140).

Cuzme, F., Suárez, L., Bracho, C., & Pupiales, C. (2017). Diseño de políticas de seguridad de la información basado en el marco de referencia COBIT 5. In Msc. Daisy Ibaquingo, MSc. Cathy Guevara, MSc. Silvia Arciniega, MSc. Marco Pusdá, & MSc. Pedro Granda (Eds.), *Innovando Tecnología* (UTN, pp. 129–137). Ibarra. Retrieved from https://issuu.com/utnuniversity/docs/ebook_innovando_tecnologia_2017

Delgado, J. R. (2016). *Comparación entre COBIT 5 para la seguridad de la información y otras normas de similar naturaleza*. Universidad de Buenos Aires.

Dimitrov, D. V. (2016). Medical internet of things and big data in healthcare. *Healthcare Informatics Research*, *22*(3), 156–163. https://doi.org/10.4258/hir.2016.22.3.156

Guillen, E., Ramirez, L., & Estupinan, E. (2011). Análisis de seguridad para el manejo de la información médica en telemedicina. *Ciencia E Ingeniería Neogranadina*, *21*(2), 124–8170. Retrieved from http://www.scielo.org.co/scielo.php?pid=S0124-81702011000200004&script=sci_abstract&tlng=es

International Organization for Standardization(ISO). (2013). ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls. Retrieved September 8, 2018, from https://www.iso.org/standard/54533.html

International Organization for Standardization(ISO). (2016). *Health informatics - Information security management in health using ISO/IEC 27002*. *2016-07* (Vol. 27002). Retrieved from https://www.iso.org/standard/62777.html

Jalali, M., & Kaiser, J. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Ssrn*. https://doi.org/10.2139/ssrn.3100364

Jefatura del Estado - Gobierno de España. (2002). *Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica*. *Boletín Oficial del Estado (BOE)* (Vol. 274). https://doi.org/BOE-A-2002-22188

Klonoff, D. C. (2015). Cybersecurity for connected diabetes devices. *Journal of Diabetes Science and Technology*, *9*(5), 1143–1147. https://doi.org/10.1177/1932296815583334

Ministerio de Salud Pública. (2015). Reglamento de informacion confidencial en sistema nacional de salud.

Onofa, F. orlando, & Pilatuña, I. (2013). *Análisis y evaluación de riesgos y vulnerabilidades del nuevo portal web de la Escuela Politécnica Nacional, utilizando metodologías de hackeo ético*. Escuela Politécnica Nacional.

Pacheco, J., & Hariri, S. (2016). IoT Security Framework for Smart Cyber Infrastructures. In *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W)* (pp. 242–247). IEEE. https://doi.org/10.1109/FAS-W.2016.58

Parlamento Europeo y del Consejo. REGLAMENTO (UE) 2016/679 (2016). Retrieved from https://www.boe.es/doue/2016/119/L00001-00088.pdf

Pérez, J. (2019). El derecho a la protección de datos y a la privacidad: una perspectiva comparada entre la Unión Europea y Estados Unidos. Retrieved from https://idus.us.es/xmlui/handle/11441/83475

Pillo, D., & Enríquez, R. (2017). Gobierno de TI con énfasis en seguridad de la información para hospitales públicos. *Maskana*, *8*(0), 42–55. Retrieved from https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/1451/1125

Plazzotta, F., Luna, D., & Bernaldo de Quirós, F. G. (2015). Health information systems: Integrating clinical data in different scenarios and users. *Rev Peru Med Exp Salud Publica*, *32*(2), 343–351. Retrieved from http://www.scielo.org.pe/pdf/rins/v32n2/a20v32n2.pdf

Rocha, C. A. (2015). La Seguridad Informática. *Revista Ciencia Unemi*, *4*(5), 26–33. Retrieved from https://seguridadinformaticahoy.blogspot.com/2013/02/metodologias-y-herramientas-de-ethical.html

Ross, R., Michael, M., & Janet, C. O. (2016). Systems Security Engineering, (December), 1–78.

Sánchez, A., Fernández, J. L., & Toval, A. (2013). Recomendaciones sobre Seguridad y Privacidad Informática en el Tratamiento de Datos de Salud, *9*, 1–7.

Sánchez, A., Fernández, J. L., Toval, A., Hernández, I., Sánchez, A. B., & Carrillo, J. M. (2014). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. *Atencion Primaria*, *46*(4), 214–222. https://doi.org/10.1016/j.aprim.2013.10.008

Sánchez, L. (2013). HC+: Desarrollo de un marco metodológico para la mejora de calidad y la seguridad en los procesos de los Sistemas de Información en ambientes sanitarios. Retrieved from http://repositorio.educacionsuperior.gob.ec/handle/28000/2510

Tamayo, M. (2016). Proteccion de datos personales en la historia clinica: El documento de seguridad en la norma ISO/IEC 27 002, 1. Retrieved from https://dialnet.unirioja.es/servlet/tesis?codigo=110459

Zambrano, W., Chafla, G., Moreira, C., & Cuzme, F. (2015). Software Como Servicio De Citas Médicas En Línea, Un Modelo Aplicado a La Salud Software As a Service for Online Medical. *Espam.Edu.Ec*, *6*(1), 37–44. Retrieved from http://espam.edu.ec/revista/2015/V6N1/59.pdf

Lewis, J. A. (2016). Experiencias avanzadas en políticas y prácticas de ciberseguridad: Panorama general de Estonia, Israel, República de Corea y Estados Unidos. Inter-American Development Bank.

Ayala Medrano, M. A. (2017). Sistema de gestión de seguridad de información para mejorar el proceso de gestión del riesgo en un hospital nacional, 2017.

Sánchez, L. E., Caballero, I., Santos-Olmo, A., Fernandez-Medina, E., & Piattini, M. (2013). HC+: Desarrollo de un marco metodológico para la mejora de la calidad y la seguridad en los procesos de los Sistemas de Información en ambientes sanitarios.

Pinto, E. P. G., López, L. R., & Cuesta, E. P. E. (2011). Análisis de seguridad para el manejo de la información médica en telemedicina. Ciencia e Ingeniería Neogranadina, 21(2), 4.

Cordero Moreno, J. L., & García Reyes, Y. O. (2016). Análisis de riesgos y recomendaciones de seguridad de la información del Hospital ESE San Bartolomé de Capitanejo, Santander.

Julio, M. L. G., & Flórez, L. C. G. (2017). La gestión de riesgos y controles en sistemas de información. Puente, 6(1), 15-23.

Caiza-Acero, M., & Bolaños-Burgos, F. (2014). Las implementaciones de las normas de seguridad de la información: estudio de caso la Sociedad de L ucha Contra el Cáncer del Ecuador. ReCIBE. Revista electrónica de Computación, Informática Biomédica y Electrónica, (3).

Figueroa Cortez, M. F. (2016). Cultura de seguridad del paciente por las enfermeras y su relación con los eventos adversos en el Servicio de Emergencia del Hospital Santa Rosa Pueblo Libre–2016.

Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: a case study of Iran. Risk management and healthcare policy, 9, 75.

Jarauta Sánchez, J., & Prado Montes, Á. (2017). Seguridad en sistemas de comunicación.

Pineda, L. O. (2017). La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración. Foro Revista de Derecho, (27), 83-114.

Isidro, A., & Enrique, J. Análisis y evaluación de riesgos de la información en las oficinas de Comfaoriente Seccional Pamplona basado en la Norma ISO/IEC 27000: 2013.

López, A. A., Arroyo, M. C., León, M. T. M., & Molina, A. R. (2012). Conocimiento y cumplimiento de los profesionales sanitarios del derecho del paciente a la información clínica. Revista española de medicina legal, 38(1), 11-16.

Paredes, P. V. (2017). LA HISTORIA CLÍNICA: ACCESO, DISPONIBILIDAD Y SEGURIDAD. Bioderecho. es: Revista internacional de investigación en Bioderecho, (6), 6.

Milanes, V. (2017). Desafíos en el debate de la protección de datos para Latinoamérica. T&S TRANSPARENCIA & SOCIEDAD, 13.

Medinaceli Díaz, K. I., & Gil, E. (2015). La seguridad de la información, clave en la protección de datos sanitarios. Fuentes, Revista de la Biblioteca y Archivo Histórico de la Asamblea Legislativa Plurinacional, 9, 56.

Pérez Miras, J. (2019). El derecho a la protección de datos ya la privacidad: una perspectiva comparada entre la Unión Europea y Estados Unidos.

Rocco, C., & Garrido, A. (2017). Seguridad del paciente y cultura de seguridad. Revista Médica Clínica Las Condes, 28(5), 785-795.