MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

Desarrollo y Aplicación de un Modelo para evaluar el nivel de madurez de Gestión de Seguridad de la Información en Instituciones de Salud Pública en la Ciudad de Cuenca.

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

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:
Miriam Gabriela Capelo Vázquez

Bajo la dirección de:
Marco Sotomayor, Msc.

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador

Noviembre de 2018

Desarrollo y aplicación de un modelo para evaluar el nivel de madurez de Gestión de Seguridad de la información en Instituciones de Salud Pública en Cuenca.

Development and application of a model for evaluation of maturity level on Information Security Management at Healthcare institutions in Cuenca.

Miriam Gabriela Capelo Vázquez[1]
Marco Vinicio Sotomayor Sánchez[2]

Resumen

Hoy en día, muchas instituciones en el área de la salud aprovechan las Tecnologías de la Información para la mejora de servicios, reducción de costos y toma de decisiones. Los Sistemas de Información utilizados actualmente se vuelven una herramienta vital para el diagnóstico y tratamiento oportunos a los pacientes. Por tanto, se hace necesario implementar políticas y estándares que aseguren la confiabilidad, disponibilidad e integridad de la información de registros médicos y exámenes complementarios; y por supuesto, estas estrategias implementadas necesitan ser monitorizadas y controladas de forma periódica. Luego de la revisión de literatura, no se evidencian trabajos realizados en el Ecuador con respecto a la medición de la madurez de la Seguridad de la Información en el área de salud; por tanto el presente trabajo de investigación tiene como objetivo proponer un modelo para evaluar la madurez de seguridad de la información en instituciones de salud pública; para lo cual se evaluaron los estándares más utilizados y las normativas a cumplir en el sector salud; para con esto generar un Modelo de Madurez siguiendo la metodología propuesta por Becker, Knackstedt y Pöppelbub, el cual será validado por expertos de diferentes áreas y posterior a la corrección de las observaciones recibidas, se calculará en nivel de confianza de la validación realizada utilizando el método del coeficiente de alfa de Cronbach; una vez verificado un nivel aceptable de confiabilidad, se aplica el modelo propuesto en una Institución Hospitalaria Pública de Especialidades (Tercer Nivel de Complejidad dentro del Sistema Nacional de Salud), para finalmente proponer las recomendaciones con base a los resultados analizados.

Palabras clave:	Seguridad, información, modelo, madurez, salud.

Abstract

Nowadays, many institutions have taken advantage of information technologies to improve services, reduce costs and make decisions; in healthcare. The Information Systems currently used become a vital tool for the timely diagnosis and treatment of patients. Therefore, it is necessary to implement policies and standards that ensure the reliability, availability and integrity of medical record information and complementary examinations; and of course, these implemented strategies need to be monitored and controlled on a regular basis. After the literature review, there are no works in Ecuador regarding the measurement of the maturity of Information Security in the health area; therefore, the present research work aims to propose a model to evaluate the maturity of information security in public health institutions; for that matter, it was an evaluation of the regulations to be met in the health sector was carried out; in order to generate a Maturity Model developed by following the methodology proposed by Becker, Knackstedt and Pöppelbuß, which will be validated by experts from different areas and after the correction of the observations received, the reliability of the validation carried out using the Cronbach's alpha coefficient method; Once an acceptable level of reliability has been verified, the proposed model is applied in a Public Hospital Institution of Third Level of complexity, to finally propose the recommendations based on the results analyzed.

Key words	Security, information, model, maturity, healthcare.

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

INTRODUCCIÓN

En la actualidad, las Tecnologías de la Información se han convertido en una potente herramienta para la toma de decisiones en todas las organizaciones, y más aún, en el sector de los servicios de Salud, en donde los Sistemas de Información bien utilizados toman un rol importante en el registro de información. Así lo mencionan Narayana Samy, Ahmad & Ismail (2010), en referencia a que la importancia de las Tecnologías de la Información y Comunicación (TIC) en el área de salud está creciendo conforme muchas organizaciones buscan incrementar las maneras de mejorar la seguridad del paciente y reducir costos de los servicios; también indican que el uso de buenas prácticas o estándares como ISO/IEC 27000 y las normativas Health Insurance Portability and Accountability Act (HIPAA) en el sector de salud, son esenciales para proteger los activos de información.

Luego, en lo que se refiere a la implementación de sistemas de registro médico electrónico según indica la Organización Panamericana de la Salud OPS (2016b) actualmente en América Latina no se cuenta con datos que den cuenta del nivel de implantación de los mismos. Sin embargo, se tienen muy claros los beneficios del uso de las Tecnologías de la Información para los registros médicos, entre ellos se puede resaltar el beneficio de mejorar la confidencialidad de la información a través de una correcta administración de accesos a la información electrónica de cada paciente, además de la capacidad de lograr una interoperabilidad con otros sistemas de apoyo diagnóstico como imagenología y laboratorio clínico y patológico (Organización Panamericana de la Salud, 2016).

Por otro lado, Williams, Austin, y Mha (2008) detallan que uno de los principales beneficios de contar con un Sistema Médico electrónico es la disponibilidad de la información médica más valiosa en el momento adecuado, además de que esta información puede ser utilizada por investigadores para mejorar la prevención y tratamiento de cada patología.

Por otra parte, Williams, Austin y Mha (2008) y Holroyd-Leduc, Lorenzetti, Straus, Sykes, y Quan (2011) recopilan la preocupación existente en cuanto a la confidencialidad y privacidad de la información al utilizar Sistemas Informáticos Médicos.

También Mzokov (2017) afirma que conjuntamente con el crecimiento en el uso de los Sistemas Médicos y Registros médicos electrónicos, se nota un incremento considerable de amenazas de seguridad que sobre todo arriesgan que la información de pacientes caiga en manos equivocadas; por ejemplo, un estudio del Instituto Ponemon (2016) cita en los resultados de las encuestas realizadas que el 90% de instituciones de salud han tenido una fuga de información en los dos últimos años: el 45% han tenido más de 5 fugas en el mismo periodo de tiempo, y deduce que el costo aproximado de una fuga de información asciende a 6.2 billones de dólares.

Por otra parte, tan sólo en los primeros meses del año 2016 se dieron ataques de ransomware, un tipo de virus que restringe acceso al sistema y sus archivos para luego exigir el pago de un rescate para recuperar la información; y otros tipos de intrusiones a más de 12 centros hospitalarios en los Estados Unidos (Grifantini, 2016). De igual forma en abril del 2017, se conoció que uno de los más afectados durante el ataque masivo de ransomware fue el Sistema de Salud Británico afectando al menos a 10 hospitales en el Reino Unido con graves consecuencias a los servicios de salud, pues tuvieron que derivar gran cantidad de pacientes incluso en los servicios de Urgencias (Guimón, 2017).

Finalmente, está el factor del error humano, como lo explican Portantier (2012) y Tarazona (2015), que puede convertirse en una amenaza para un sistema informático que es alimentado

casi en su totalidad a través de un Sistema Médico electrónico.

Por ello, muchos países están implementando nuevas leyes para salvaguardar la privacidad y seguridad en el sector de salud, tal es el caso de la HIPAA de los Estados Unidos (Office of Civil Rights Department of Health and Human Services, 2003), o la norma mexicana NOM-024-SSA3-2010(Secretaría de Salud, 2010), ambas normativas buscan que los sistemas médicos informáticos cumplan con los requerimientos básicos que aseguren la confidencialidad, seguridad y privacidad de la información.

También en nuestro país se formó una Comisión para la Seguridad informática y de las TIC en el año 2011, la misma que determinó la necesidad de aplicar normas y procedimientos para seguridad de la información, e incorporar a la cultura y procesos institucionales del sector público la gestión permanente de la misma, definiendo finalmente el uso obligatorio de las recomendaciones de la Norma INEC ISO 27001 (Secretaría Nacional de la Administración Pública, 2013) y la Norma 410 de Control Interno de la Contraloría General del Estado.

Por todo lo expuesto anteriormente, y considerando los trabajos encontrados en la revisión de literatura realizada, donde se han hallado estudios llevados a cabo en países asiáticos y de medio Oriente realizados por Hajrahimi, Dehaghani, y Sheikhtaheri(2013), Liu, Hwang, & Chang (2011), y Zarei y Sadoughi (2016) , que han logrado obtener como resultado un diagnóstico del estado de madurez de las Instituciones de Salud, en otros casos se han apoyado en los Ministerios Públicos para expandir el campo de aplicación; sin embargo, en Latinoamérica son pocos los trabajos realizados en el campo de la salud; existe por ejemplo la encuesta realizada por la Organización Panamericana de la Salud (2016a) sobre el uso de registros médicos electrónicos no generó resultados muy confiables debido a los pocos datos recopilados por falta de registros formales en los hospitales latinos; es decir, no se cuenta con herramientas de monitoreo o diagnóstico del estado de la seguridad de la información en las instituciones de salud de América Latina.

Luego, en el Ecuador se han encontrado trabajos de implementación de Normativas de Seguridad o de Sistemas de Gestión de Seguridad de la Información, más no se han hallado investigaciones sobre la medición del Nivel de Seguridad de la Información generada en Instituciones de Salud.

Por esta razón, esta investigación se propone desarrollar y aplicar un modelo que sirva para evaluar el nivel de madurez de seguridad de la información en instituciones de salud pública; esto considerando como base que en este país el estándar de uso obligatorio para las instituciones públicas es el ISO 27000, y por otra parte en el sector salud una de las normativas más relevantes es la Health Insurance Portability and Accountability Act, y el modelo de madurez obtenido para el cumplimiento de éste: HITRUST; por lo que el modelo propuesto estará basado en estos referentes. Con estos resultados se establecerán recomendaciones en cuanto a las buenas prácticas y mejoras a implementarse para proteger los activos de información especialmente los registros médicos electrónicos.

De manera más específica, este trabajo busca analizar las normativas vigentes en el Ecuador para las Instituciones Públicas, resaltar los aspectos más importantes en cada una de ellas que deben evaluarse en una institución de Salud y seleccionar las buenas prácticas que pueden implementarse. Observar los diferentes modelos de madurez internacionales más utilizados y adaptar los aspectos más importantes en uno solo que sea el más adecuado para las instituciones del sector salud, y aplicarlo en una unidad operativa de servicios de salud pública.

Finalmente, con este análisis se elabora las recomendaciones con base a los resultados obtenidos, y siguiendo la Norma ISO 27000 e HIPAA, que sirvan como guía a las instituciones de salud pública para la mejora en la gestión de la seguridad de la información.

MARCO TEÓRICO.

De acuerdo a la información recopilada durante esta investigación, se han encontrado datos que hacen referencia al tema específico de Seguridad de la Información en Instituciones de Servicios de Salud; sin embargo, en nuestra región no se ha dado mayor importancia a este tema (Organización Panamericana de la Salud, 2016), por lo que es necesario profundizar la investigación en el medio local; y para hacer esto, es necesario conocer en primer lugar el estado actual de las Instituciones de Servicios de Salud ecuatorianas para luego sugerir las recomendaciones necesarias para mejorar y monitorear el nivel de madurez encontrado con el Modelo desarrollado.

Registro Médico Electrónico.

Según la OPS (2016b) el registro médico es el documento que contiene lo acontecido con los pacientes durante la visita médica, incluyendo motivo de consulta, la enfermedad actual, detalles del entorno social, antecedentes familiares y personales, etc. Ahora bien, un Registro Médico Electrónico como lo define la Organización Mundial de la Salud (OMS) (2006) hace referencia a un sistema automatizado que contiene documentos e imágenes generados dentro de una institución sanitaria.

Seguridad de la Información.

Areitio y Bertolín (2008) definen la Seguridad de la información como un proceso que está compuesto de aspectos tecnológicos, organizacionales, de recursos humanos, económicos, de negocio, legales, de cumplimiento, etc. y es un factor crítico en las Instituciones públicas y privadas de salud, entre otras. Por otro lado, Matalobos (2011) define a la Seguridad de la Información como la aptitud para administrar acciones ilegales, malintencionadas o accidentales que puedan dañar los activos de información. Luego Carmona, Nieto, Angelo, y Polo (2009) aseguran que la seguridad de la información debe ser integral, empezando desde las personas involucradas, los procesos y los sistemas.
Así también lo aseguran Whitman & Mattord (2011), al decir que la seguridad de la información es la protección de la información y de sus elementos críticos, incluyendo los sistemas y hardware que usa, almacena y transmite la información; es decir, seguridad computacional, de datos y de red.

En cuanto a la seguridad de la información en el Sector de Salud, el Departamento de Servicios de Salud de los Estados Unidos (HHS) indica que la Seguridad de la Información es la protección tanto de la información como de los sistemas de información de accesos no autorizados, usos, divulgación, disrupción, modificación y destrucción; y se logra al asegurar la confidencialidad, integridad y disponibilidad de la misma (Human & Health Services, 2015).

Sin embargo, es importante considerar las palabras de Mitnik, Simon, y Wozniak (2003) y Boss, Kirsch, Angermeier, Shingler, y Boss (2009) cuando afirman que el punto más vulnerable de una organización son las personas. De ahí pues, la importancia de implementar estrategias para concientizar a todo el personal sobre la importancia de la seguridad de la información sobre todo en el área médica.

La Figura 1 muestra los elementos que involucran la Seguridad de la Información:

Figura 1 Elementos de la Seguridad de la Información. Adaptada Copyright (2018) *por Kostadinov*

Estos tres elementos involucran a su vez, los sistemas, los procesos y las personas, que deben ser protegidos a través de Buenas Prácticas de Seguridad de la información.

Finalmente, en la Norma ISO 27001 aclara que la seguridad de la información velará por estas características de la información, sea cual fuere el formato que ésta tenga: electrónico, papel, audio, video, etc.

Modelo de Madurez.

Rosmiati, Riadi y Prayudi (2016) definen un Modelo de Madurez como una herramienta que permite medir el rendimiento de un sistema de información. También Pérez Mergaerjo, Pérez Vergara y Rodríguez Ruíz (2014) coinciden en que esta herramienta puede valorar el estado en el que se encuentra una organización y a la vez permite que pueda recorrer los diferentes niveles para alcanzar el estado óptimo de mejora continua para cumplir sus objetivos de negocio.

Así pues, si bien el concepto de un modelo de madurez de seguridad y la teoría detrás se originó en el área de desarrollo de software, actualmente ha tomado nombres y formas muy diversas; sin que haya habido cambios en los aspectos básicos (Boswell & Bhargava, 2014)

También Fernández-medina (2006) muestra que un Modelo de Madurez permite establecer un sistema de valoración estándar que determine acertadamente el estado de una institución en materia de seguridad de la información; generando una escala progresiva que permita incrementar las medidas de seguridad de la información ya implementadas hasta obtener un estado aceptable.

Fuga de información.

El Instituto Nacional de Cibeseguridad define el término como la divulgación de información sensible o confidencial ya sea de manera involuntaria o deliberada (Instituto Nacional de Ciberseguridad, 2017).

ESTUDIOS RELACIONADOS

Durante la investigación realizada para recopilar información sobre trabajos similares a la investigación propuesta, se revisaron varias bases de datos, entre ellas Scopus, PubMed, Scielo y ResearchGate donde se pudieron rescatar trabajos importantes como el realizado por Park et al (2010) que consiste en un análisis de los Sistemas de Gestión de Seguridad de la Información (SGSI) en 5 hospitales de más de 500 camas. En este trabajo, los autores elaboran listas de verificación con base a estándares internacionales y los distribuyen al personal de TI de los hospitales investigados, para luego, realizar entrevistas para ampliar la información recopilada en las listas y obtener las conclusiones de que los SGSI implementados en las instituciones evaluadas son insuficientes para cumplir con los requerimientos mínimos de seguridad, y el tiempo de implementación de SGSI adecuados es bastante amplio.

Así también, otro trabajo interesante que puede relacionarse con este documento es el de Zarei & Sadoughi (2016), quienes realizan un estudio en 551 hospitales de Irán en el cual los autores buscan determinar el conjunto de mejores prácticas para gestionar los riesgos de seguridad de la información; este estudio lo realizan a través de una encuesta en primer lugar y luego con observación directa en 5 hospitales seleccionados de los 551 encuestados;

finalmente toman criterios de expertos para validar los resultados encontrados.

Por otra parte, y hablando en el contexto del sector de salud se ha considerado también relevante el artículo de Kwon & Johnson (2013) en el cual los autores tratan de concientizar a los lectores en cuanto a la criticidad de la información médica y las mejores prácticas que pueden coadyuvar a incrementar el nivel de cumplimiento con las normativas vigentes. En este artículo los autores luego de realizar una encuesta a 255 instituciones de servicios de salud, echan mano del Clúster de Ward con varianza mínima para procesar las respuestas recopiladas y determinar la existencia o no de las prácticas de seguridad evaluadas; finalmente identifican factores de relación entre clústeres de estas prácticas para evaluar el nivel de cumplimiento.

Luego, se debe también tomar en cuenta el trabajo de Hajrahimi, Dehaghani, y Sheikhtaheri (2013), en esta investigación se realiza la evaluación de la seguridad de la información en tres hospitales seleccionados por los autores. La metodología utilizada se basa en el Modelo difuso TOPSIS (Technique for Order Performance by Similaritiy to Idea Solution), el cual es una técnica que ordena las preferencias de acuerdo a la similitud a la solución ideal; de esta forma, en el artículo se documenta la realización de una encuesta y posterior aplicación del Modelo TOPSIS para determinar los puntos fuertes encontrados en cada uno de los hospitales estudiados, para finalmente validar a través de la opinión de expertos el resultado de la aplicación del Modelo.

Cabe mencionar además la investigación realizada Liu, Hwang, & Chang (2011) quienes analizan el estado de la madurez de los registros médicos electrónicos en Taiwan, para realizar este trabajo los autores contaron con la ayuda del Ministerio de Salud, y aplicaron entrevistas en 538 hospitales, con un nivel de respuesta del 94.4%. Para la elaboración del cuestionario, tomaron como base la Política Nacional de Aseguramiento de la Salud (NHI) y generaron un análisis comparativo del estado de los hospitales de Taiwan con respecto a los de otros países; al final del estudio se concluye que el nivel de madurez de los registros médicos electrónicos Taiwaneses son bastante altos en comparación con los similares.

Por otro lado, al realizar la búsqueda bibliográfica a nivel nacional sobre trabajos similares se logró menos resultados; únicamente se encontraron tres artículos compatibles con el tema de investigación, de los cuales, uno solo, destaca por tratarse del sector salud en el país; es el trabajo de Caiza-Acero y Bolaños-Burgos (2014), que consiste en un caso de estudio en la Sociedad de Lucha contra el Cáncer (SOLCA) sobre la implementación de normas de seguridad de la información; en este trabajo los autores se enfocan principalmente en la seguridad de la infraestructura física tecnológica, realiza una selección de las normativas de seguridad que se pueden adaptar mejor a las características de la Institución y se realiza un análisis comparativo entre ellas, para terminar escogiendo la ISO 27002 por adaptarse mejor a la realidad del Hospital; finalmente el análisis concluye con la evaluación del nivel de cumplimiento de la Institución con respecto a la normativa escogida y genera las recomendaciones necesarias para en un futuro seguir evaluando las otras áreas que contempla la normativa.

Así pues, luego de haber revisado los trabajos anteriores, se debe indicar que a nivel internacional existe variedad de investigaciones para realizar la medición y diagnóstico de la Seguridad de la Información y las buenas prácticas utilizadas en el sector hospitalario; no así en los países latinoamericanos y en el Ecuador, los trabajos investigativos encontrados con enfoque a la Seguridad de la Información en el sector salud son pocos, se concentran más en la implementación de buenas prácticas, y no se centran en la medición del nivel de seguridad de la información; por lo que existe aún un vacío investigativo en cuanto a este tema que es necesario abordar para poder enfrentar los retos de seguridad actuales como virus, fugas o robos

de información que empiezan a generarse actualmente en las instituciones de salud.

Importancia de la Seguridad de la Información en organizaciones del sector salud.

En el sector de los servicios Salud, la confianza se vuelve un factor crítico, debido a que los pacientes confían su información personal estas instituciones y existen requerimientos específicos de confidencialidad, privacidad y seguridad. Existe un mayor énfasis en la integridad de la información que depende por completo del correcto llenado de los registros médicos electrónicos, y en general de un uso correcto de los recursos informáticos (Ahima, 2014).

Además, según lo mencionan Fernández-Alemán, Carrión Señor, Oliver Lozoya, y Ambrosio (2013) los avances de TI y su aplicación en el campo médico han generado nuevas amenazas de seguridad y privacidad para los datos médicos, y, considerando que la información médica de pacientes es vital tanto para su tratamiento integral como para los aspectos legales, se debe asegurar que la información sea auditable durante todo el ciclo de vida.

Así pues, cuando se genera una fuga de información, como lo explica la Guía para la Privacidad y Seguridad de la Información Médica Electrónica elaborada por el Departamento de Servicios de Salud de EEUU y la Oficina del Coordinador Nacional para TI de Salud ONC (2015) las consecuencias para las instituciones pueden ser bastante serias, con daños que van desde los económicos o daños a los pacientes. Las prácticas mal llevadas de seguridad y privacidad incrementan la vulnerabilidad de la información médica, además de incrementar el riesgo de ataques cibernéticos exitosos.

Así pues, un reporte realizado por Safenet (2010) que genera un compendio de varios reportes y estadísticas realizadas, muestra que el robo de identidad médica se encuentra en incremento constante, y sus consecuencias son diversas y graves, tanto para los pacientes como para los prestadores de servicios, por lo tanto, se concluye la necesidad de proteger estos registros electrónicos de empleados maliciosos y una variedad de amenazas externas.

Además de las razones anteriores, cabe mencionar el alto costo que implica una falla en la seguridad de la información médica, por ejemplo, el caso de las instituciones que forman parte del St. Joseph Heatlh System de los Estados Unidos, en donde una falla en la configuración de seguridad dejó expuestos en internet 31000 registros médicos durante casi un año, con un costo que rondaba aproximadamente 28 millones de dólares(ESSet, s/f).

Luego, Laura Shin (2015) muestra en una publicación de Forbes la amenaza del robo de identidad médica, donde los datos expuestos pueden ocasionar el robo de datos como número de seguro social, lo cual permitiría utilizar el seguro médico de la víctima para tratamientos médicos, recibir medicación, etc.

Finalmente, el Centro de Recursos de Robo de identidad de los Estados Unidos registra hasta el 21 de septiembre de este año, un total de 273 fugas de datos médicos exponiendo un total de 4.352.681 registros médicos sólo en ese país(Identity Theft Resource Center, 2017).

Por esta razón, las instituciones prestadoras de servicios de salud tienen la obligación de definir los usos de la información y las políticas y prácticas para gobernar el uso de esa información. Según la investigación realizada por el Identity Theft Resource Center (2013) existen desafíos que hoy se presentan para las Instituciones del Sector de Salud, como por ejemplo el creciente número de sistemas electrónicos o aplicaciones que se utilizan dentro y entre instituciones, incremento del volumen y variedad de datos e información, proliferación de dispositivos médicos que crean datos para los que es esencial la integración con los sistemas informáticos y finalmente, la confiabilidad de la información que se comparte o se intercambia.

ISO 27000, 27002

La familia de normativas ISO 27000 aparece por primera vez en 1995 creada por el British Standards Institution – BSI, entonces conocida como la norma BS 7799 con el objetivo de brindar un conjunto de buenas prácticas para la gestión de seguridad de la información (ISO - International Organization for Standardization, 2011).

Luego, en el año de 1999 aparece la segunda parte de la norma, BS 7799-2 en la cual se determinan los requisitos a cumplir en un Sistema de Gestión de Seguridad de la Información; estas dos partes, son las que en el año 2000 adoptó la ISO formando la ISO 17799. Finalmente en el 2002 las normativas adoptaron la filosofía de Sistemas de Gestión(ISO - International Organization for Standardization, 2011).

Un Sistema de Gestión de Seguridad de la información se define según Fernández-medina (2006) y Boswell & Bhargava (2014) como un Sistema de Gestión que tiene como propósito implantar controles adecuados para asegurar que se está gestionando la seguridad de la información de manera apropiada, controlando de manera constante si los procedimientos, políticas, estrategias, y demás mecanismos que se han implementado están consiguiendo los objetivos planteados.

Además, según lo determinado en la Norma ISO 27000, un Sistema de Gestión de Seguridad de la información es un proceso que debe llevarse de forma sistemática, documentada y debe ser conocido por toda la organización (Grupa, 2015).

Así también lo asegura Pérez de la Universidad de Valencia (s/f) cuando determina que un SGSI ayuda a una organización a implementar procedimientos, políticas y controles alineados a sus objetivos para lograr reducir los riesgos a los que está expuesta su información, sean éstos físicos o de fugas, daño o falta de disponibilidad de la misma; gestionando estos riesgos de forma documentada y conocida por todos los que conforman la organización.

ISO 27001: Estructura.

En esta parte, hay que tener claro que la ISO 27001 no obliga a controles de información específicos debido a la enorme variedad de validaciones que pueden ser necesarias en cada organización; las verificaciones sugeridas en la ISO 27002 pueden escogerse según las necesidades y características propias de la institución(IsecT Ltd., s/f).

Así, la estructura de la norma ISO 27001 (ISO - International Organization for Standardization, 2011), es la siguiente:

1. Introducción
2. Alcance
3. Referencias normativas
4. Términos y Definiciones
5. Contexto de la Organización
    a. Comprensión de la organización y su contexto
    b. Comprensión de las necesidades y expectativas de las partes interesadas.
    c. Determinar el alcance del sistema de gestión de seguridad de la información.
    d. Sistema de Gestión de Seguridad de la Información.
6. Liderazgo
    a. Liderazgo y compromiso
    b. Política
    c. Roles organizacionales, responsabilidades y autoridades.
7. Planificación
    a. Acciones para abordar los riesgos y oportunidades
    b. Objetivos y la planificación para alcanzarlos seguridad de la información.
8. Soporte
    a. Recursos
    b. Competencia
    c. Conciencia
    d. Comunicación
    e. Información documentada
9. Operación

   a. Planificación y control operacional
   b. Evaluación de riesgos de seguridad de la información
   c. Tratamiento del riesgo de seguridad de la información
10. Evaluación del rendimiento
   a. Monitoreo, medición, análisis y evaluación.
   b. Auditoría Interna
   c. Revisión de Gestión
11. Mejora Continua.
   a. No conformidades y acciones correctivas
   b. Mejora Continua.

El ciclo de vida de la implementación de la norma ISO 27001 está basado en Planear – Hacer – Verificar – Actuar de Demming, y adaptado a la estructura de la normativa (ISO -International Organization for Standardization, 2011).

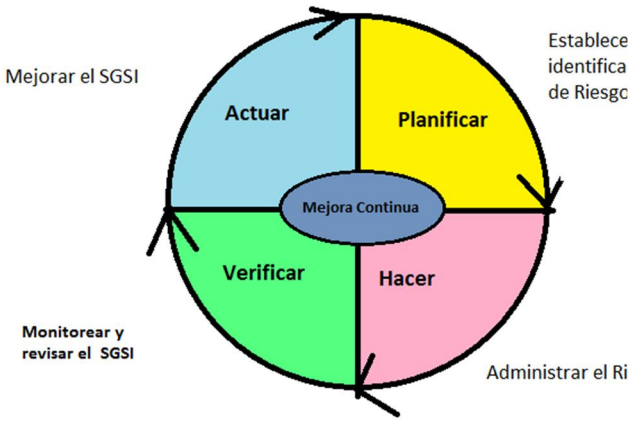

Figura 2 Implementación de un SGSI con ISO 27001, Copyright (2017), por Ellite Certification Ltd.

Como se ha mencionado anteriormente, la ISO 27001 no dicta en sí los controles que se deben implementar en el SGSI, sin embargo, en esto se puede utilizar la norma ISO 27002.

En el sector público ecuatoriano, es de uso obligatorio la norma INEN ISO 27001, misma que es la traducción exacta de la ISO 27001, realizada por el Servicio Ecuatoriano de Normalización (INEN), con base en la ISO 27001:2013 incluyendo las correcciones Corrigendum 1: 2014 y Corrigendum 2: 2015(Servicio Ecuatoriano de Normalización, 2016).

ISO 27002

Esta normativa es un complemento a la ISO 27001, su segunda edición que se encuentra actualmente vigente fue publicada en el año 2013 y su objetivo es brindar una guía para los estándares de seguridad de la información y la gestión de prácticas de seguridad de la información incluyendo la selección, implementación y administración de los controles tomando en cuenta el ambiente de riesgo de la organización(International Standarization Organization, 2016).

Así pues, esta norma está conformada por 14 Dominios, 35 objetivos de control y 114 controles para las diferentes áreas de una organización. A continuación, se listan éstos.

1. Políticas de seguridad
   a. Directrices de la Dirección de Seguridad de la información
2. Aspectos organizativos de la seguridad de la información
   a. Organización interna
   b. Dispositivos para movilidad y teletrabajo
3. Seguridad ligada a los recursos humanos
   a. Antes de la Contratación
   b. Durante la contratación
   c. Cese o cambio de puesto de trabajo.
4. Gestión de activos
   a. Responsabilidad sobre los activos
   b. Clasificación de la información
   c. Manejo de los soportes de almacenamiento.
5. Control de Accesos
   a. Requisitos de negocio para el control de accesos
   b. Gestión de acceso a usuario

   c. Responsabilidades del usuario
   d. Control de acceso a sistemas y aplicaciones.
6. Cifrado
   a. Controles de criptográficos
7. Seguridad física y ambiental
   a. Áreas seguras
   b. Seguridad de los equipos
8. Seguridad en la operativa
   a. Responsabilidades y procedimientos de operación.
   b. Protección contra código malicioso
   c. Copias de Seguridad
   d. Registro de actividad y supervisión
   e. Control del software en explotación
   f. Gestión de la vulnerabilidad técnica
   g. Consideraciones de las auditorías de los sistemas de información
9. Seguridad en las Telecomunicaciones
   a. Gestión en la seguridad de redes.
   b. Intercambio de información con partes externas
10. Adquisición, desarrollo y mantenimiento de los sistemas de información.
   a. Requisitos de seguridad de los sistemas de información.
   b. Seguridad en los procesos de desarrollo y soporte
   c. Datos de prueba
11. Relaciones con los suministradores
   a. Seguridad de la información en las relaciones con suministradores.
   b. Gestión de la prestación del servicio por los suministradores.
12. Gestión de incidentes en la seguridad de la información.
   a. Gestión de incidentes de seguridad de la información y mejoras
13. Aspectos de seguridad de la información en la Gestión de Continuidad del Negocio
   a. Continuidad de la seguridad de la información
   b. Redundancias.
14. Cumplimiento
   a. Cumplimiento de los requisitos legales y contractuales
   b. Revisiones de la seguridad de la información.

Esta normativa, tiene un enfoque para abarcar a todo tipo de empresas, sea cual fuere su tamaño, propósito o razón de ser.

Health Insurance Portability and Accountability Act – HIPAA.

La Ley HIPAA se elaboró en los Estados Unidos en el año de 1996, actualmente se encuentra en vigencia y se ha convertido en un ejemplo para otros países para implementar este tipo de leyes que salvaguarden la integridad, confiabilidad y disponibilidad de la información médica; incluye disposiciones para la necesidad de adoptar estándares nacionales o internacionales en los sistemas médicos y con esto, asegurar que las transacciones y conjunto de códigos electrónicos y de atención médica, identificadores únicos de salud y seguridad sean altamente confiables, disponibles e íntegros.

Esto obedece a que en el Gobierno Estadounidense se genera la advertencia de que los avances en materia de tecnologías de la información podrían deteriorar entre otros aspectos la privacidad de la información de salud.

Así pues, se publicó en primer lugar una Regla de Privacidad final, en diciembre de 2000, la misma que establece recomendaciones y estándares nacionales para la protección de la información médica identificable de forma individual; estos estándares estaban dirigidos a entidades que ofertan planes de salud, casas de atención médica, y prestadores que conducen transacciones por servicios médicos de forma electrónica (Office for Civil Rights, 2017).

Luego, en febrero de 2003 se publicó una Regla de Seguridad, la cual provee estándares para

proteger la confidencialidad, integridad y disponibilidad de información médica electrónicamente protegida (Office for Civil Rights, 2017), esto se genera para dar respuesta al incremento de registros electrónicos implementados y a la diversidad de los mismos; lo cual generó a su vez que los riesgos potenciales de seguridad de la información también se incrementen .

Adicionalmente, se considera que uno de los mayores objetivos de la Regulación de Seguridad es proteger la privacidad de la información médica de un individuo al mismo tiempo que permite que las organizaciones que aplican esta regulación puedan implementar nuevas tecnologías para mejorar la calidad y eficiencia del cuidado al paciente. Por otro lado, al considerar el mercado de los prestadores de salud es muy diverso, la regla de seguridad está diseñada para ser flexible y escalable de tal forma que cualquier entidad pueda implementar políticas, procedimientos, y tecnologías que son apropiadas para nivel de complejidad de cada organización; desde un centro de primer nivel hasta un hospital de especialidades complejas, aseguradoras, etc. (Office for Civil Rights, 2013)

De esta forma, para el alcance de este trabajo, se profundizará en la Regla de Seguridad HIPAA; ya que ésta se define para el concepto de Información electrónica protegida, es decir, esta regulación no aplica información escrita o transmitida de forma verbal (Office for Civil Rights, 2013)

La regulación de seguridad HIPAA requiere que las organizaciones que implementan la misma mantengan medidas físicas, técnicas, administrativas y apropiadas para proteger la información médica electrónica protegida; específicamente se debe cumplir con lo siguiente:

1. Asegurar la confidencialidad, integridad y disponibilidad de toda la información médica electrónica protegida que crean, reciben, mantienen o transmiten.
2. Identificar y proteger de las amenazas que puedan ser anticipadas a la seguridad o integridad de la información.
3. Proteger a la información de las divulgaciones o usos razonablemente previstos, no permitidos, y
4. Asegurar el cumplimiento de su equipo de trabajo (Office for Civil Rights, 2013).

Sin embargo, la normativa de seguridad HIPAA no establece que estándar o estándares utilizar, de esta forma las organizaciones se encuentran libres de utilizar uno o varios de ellos.

Por otro lado, es importante mencionar que dentro de la regla de Seguridad se define confidencialidad como el hecho de que la Información Médica Electrónica Protegida (IMEP) no esté disponible o sea divulgada a personas no autorizadas. Los requerimientos para la confidencialidad de la información que se presentan en la regulación de seguridad soportan las prohibiciones detalladas en la Regla de Privacidad en contra de usos inapropiados y divulgación de la IMEP. La regulación de seguridad también promueve dos objetivos adicionales de mantener la integridad y disponibilidad de la IMEP. Bajo la regla de seguridad, Integridad significa que la IMEP se encuentra accesible y utilizable bajo demanda por una persona autorizada (Office for Civil Rights, 2017).

Normativa en el Ecuador.

Dentro de la normativa existente en el Ecuador es necesario mencionar el plan elaborado en el año 2013 por la Secretaría Nacional de la Administración Pública (SNAP), denominado Esquema Gubernamental de Seguridad de la Información (EGSI), que se basa en la norma técnica INEN ISO/IEC 27001 para Gestión de la Seguridad de la Información. Este esquema puede aplicarse en Instituciones de la Administración Pública Central, Dependiente e Institucional (Secretaría Nacional de la Administración Pública, 2013).

Dentro de las directrices dadas en este documento se pueden detallar:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información
3. Gestión de los Activos
4. Seguridad de los Recursos Humanos
5. Seguridad Física y del Entorno
6. Gestión de comunicaciones y operaciones
7. Control de Acceso
8. Adquisición, desarrollo y mantenimiento de sistemas de información
9. Gestión de los incidentes de la seguridad de la información
10. Gestión de la continuidad del negocio
11. Cumplimiento

Adicional a esta norma, existen directrices dadas en la Norma de Control Interno 410-10 de la Contraloría General del Estado, donde de manera general se indican 8 medidas que deben implementarse para asegurar confidencialidad, disponibilidad e integridad de la información.(Contraloría General del Estado, 2009).

Modelos de Madurez: ¿Qué son y cuáles son sus beneficios?

El concepto de un modelo de madurez de seguridad y la teoría detrás se originó en el área de desarrollo de software. En la actualidad ha tomado nombres y formas muy diversas; sin embargo, los aspectos básicos continúan siendo los mismos (Boswell & Bhargava, 2014).

De esta forma, un Modelo de Madurez según lo expresado por Fernández-medina (2006), establecen un sistema de valoración estándar que pueda determinar acertadamente el estado de una institución en materia de seguridad de la información; generando una escala progresiva que permita incrementar las medidas de seguridad de la información ya implementadas hasta obtener un estado aceptable.

Así también Xiao-Yan, Yu-Qing & Lu (2011), afirman que un modelo de evaluación de madurez define una escala de 5 niveles posibles en los que se puede clasificar la capacidad de madurez de una organización, utiliza también métricas de madurez de procesos para medir procesos y producción del ciclo de vida de la gestión a evaluar.

Además, un Modelo de Madurez de Seguridad informática según lo indica Arbeláez (2014) permite realizar una autoevaluación del estado inicial, y definir hacia donde llegar, identificando oportunidades de mejora, generando planes y proyectos para lograr los objetivos planteados, finalmente un modelo permite medir los avances y cumplimiento de metas y realizar correcciones de ser necesario.

Por otro lado Sánchez, Villafranca & Piattini (2007) indican que el objetivo de un modelo de madurez de seguridad es establecer una valoración estandarizada que permita planificar la manera de alcanzar las metas de seguridad; dentro de los modelos de seguridad de la información más utilizados están SSE-CMM (Systems Security Engineering Capability and Maturity Model), COBIT y ISM3 (Fernández-medina, 2006).

En cuanto a los niveles que componen a cada modelo, se puede ejemplificar con las Tablas 1, 2 y 3, mismas que detallan las escalas utilizadas en algunos de los Modelos de Madurez anteriores con una descripción breve de cada nivel.

Tabla 1 Modelo de Madurez de SSE-CMM

Nivel de Madurez	Descripción
Nivel 1	Se realizan prácticas básicas de forma informal
Nivel 2	Se realizan prácticas básicas de forma planificada y monitoreada
Nivel 3	Las prácticas base se encuentran bien definidas

Nivel 4	Las prácticas de base se encuentran controladas cuantitativamente
Nivel 5	Las prácticas de base se encuentran en mejora continua.

Tabla 2 Modelo de Madurez de COBIT 5

Nivel de Madurez	Descripción
Nivel 0 – No existente	La organización no reconoce la necesidad de la seguridad de TI. Existe una completa falta de un proceso de administración de seguridad
Nivel 1 – Inicial/ Ad hoc	La organización reconoce la necesidad de la seguridad de TI. Pero considera a los riesgos de forma "ad hoc", sin seguir procesos o políticas definidas.
Nivel 2 – Repetitivo pero intuitivo	Se han asignado las responsabilidades de la seguridad de TI a un coordinador. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan considerarse: Existe algún enfoque para evaluación del riesgo, pero el proceso es aún inmaduro y en desarrollo.
Nivel 3 – Proceso Definido	Existe conciencia de seguridad y es promovida por la Gerencia. La política de gestión define cuándo y cómo realizar evaluaciones de riesgos. La Gestión de riesgos sigue un proceso definido que está documentado y disponible para todo el personal durante el entrenamiento.
Nivel 4 – Administrado y Medible	Las responsabilidades para el personal de Seguridad de TI están claramente asignadas, administradas y reforzadas. La gestión de riesgos es un procedimiento estándar y cualquier excepción al momento de seguir el procedimiento sería notado inmediatamente
Nivel 5 - Optimizado	La Seguridad de TI es una responsabilidad compartida entre la Gerencia General y la Gerencia de TI, y se integra con los objetivos corporativos de seguridad del negocio. La Gestión de Riesgos se ha desarrollado al punto donde se refuerza un proceso estructurado, a nivel de la organización, monitoreada regularmente y bien administrada.

Tabla 3 Modelo de Madurez ISM3

Nivel de Madurez	Descripción
Nivel 1 (Indefinido)	El proceso es impredecible, es reactivo y pobremente controlado.
Nivel 2 (Definido)	El proceso es reactivo y se caracteriza por su aplicación a proyectos
Nivel 3 (Gestionado)	El proceso es proactivo y se ve a nivel de la organización
Nivel 4(Controlado) Cuantitativamente)	El proceso es medido y controlado
Nivel 5 (Optimizado)	El proceso se enfoca en la mejora continua.

Ahora bien, de manera específica para las instituciones de servicios de salud está el modelo de la Health Information Trust Alliance (HITRUST), desarrollado específicamente para cumplir con las principales normas vigentes en este sector como HIPAA, HITECH, incluye requisitos de la ISO 27001 y Normas de Riesgo Mínimo Aceptable.

El modelo propuesto por HITRUST, tiene 5 niveles como se puede visualizar en la Tabla 4; y a diferencia de los modelos anteriores no toma en cuenta un Nivel inicial en el que una empresa no considere ningún aspecto referente a la Seguridad de la Información (LLC HITRUST Alliance, 2016).

Tabla 4 Modelo de Madurez HITRUST

Nivel de Madurez	Descripción
Nivel 1 (Políticas)	Existen políticas y estándares documentados para determinar si se están controlando las especificaciones de implementación del control.
Nivel 2 (Procesos)	Deben existir procedimientos documentados o procesos desarrollados desde las políticas definidas.
Nivel 3 (Implementado)	Las políticas y procedimientos previamente definidos se han implementado dentro del alcance de la gestión.
Nivel 4(Medido)	Deben existir pruebas o métricas de la implementación de los procedimientos.
Nivel 5 (Administrado)	En este nivel se debe revisar la administración de los controles

	implementados basados en las métricas definidas.

En cuanto a los modelos más utilizados dentro del área de la Seguridad de la Información se encuentran:

- NICE CMM: Desarrollado en el 2014, enfocado a la evaluación del nivel de madurez sobre los requisitos de ciberseguridad y el desarrollo de las capacidades del personal ISM3, ISO/IEC 21827 SSE CMM e ISF CMM (Department of Homeland Security, 2014).
- C2M2: Desarrollado en 2014 por el Departamento de Seguridad Nacional de Estados Unidos, se encuentra alineado al marco de referencia propuesto por NIST y se especializa en la protección de infraestructuras críticas (Miron & Muita, 2014).
- SSE CMM desarrollado por la Asociación de Ingeniería de Seguridad de los Sistemas de información, y su enfoque va hacia lograr que el proceso de ingeniería de seguridad esté bien definido y pueda medirse (Stevanović, 2011).
- ISM3 se enfoca en alinea la Seguridad con los objetivos de la organización, cubriendo evaluación de riesgos, auditorías de cumplimiento con las normas internas, etc. Está basado en procesos (Canal, 2004).
- ISF: Desarrollado por el Information Security Forum, enfocado en la aplicación de los modelos de madurez y tiene sus propias buenas prácticas (Taich, 2015).

METODOLOGÍA DE DESARROLLO.

Este trabajo de investigación es de tipo exploratoria; ya que el problema específico que se trata no se ha estudiado a profundidad en los países de América Latina y en Ecuador; y el objetivo principal es establecer un modelo de madurez que permita evaluar el nivel de seguridad de la información en instituciones del sector de la salud; considerando el grado de confidencialidad de la información médica exigido en la normativa vigente y las amenazas informáticas existentes hoy. El enfoque dado a este artículo es cualitativo, ya que según la revisión realizada no se cuenta con herramientas prácticas para evaluar el estado actual de la seguridad de la información en el sector sanitario.

Una vez que se ha definido bien el problema se realiza una revisión de literatura de trabajos similares y de la teoría de los estándares existentes con la finalidad de recabar los datos necesarios para el desarrollo del modelo propuesto. Luego, con un análisis resultante de la investigación, y tomando como base la normativa vigente en el Ecuador, se desarrolla una matriz comparativa de los modelos más adaptables para con éstos desarrollar el modelo de madurez siguiendo una metodología sugerida por Becker, Knackstedt y PöppelbuB en donde se desarrollan los constructores centrales, se definen los dominios a evaluar, el nivel de granularidad a desarrollar y finalmente se determina cada ítem que debe ser evaluado.

Además, con el Modelo propuesto desarrollado en una primera instancia, se ha utilizado la técnica de validación por criterio de expertos para generar observaciones y cambios necesarios a la propuesta original; para esta evaluación se diseña un instrumento de validación para entregar a los expertos escogidos.

Luego, con las observaciones recopiladas de los expertos, se realiza un cálculo de confiabilidad de esta validación utilizando el coeficiente del alfa de Cronbach, y con esto se verifica que el proceso de validación es el correcto.

Finalmente, luego de contar con un adecuado porcentaje de confiabilidad, el modelo se aplica en una institución hospitalaria de especialidades utilizando técnicas de observación directa, entrevista y aplicación de la herramienta de modelo de madurez con calificación en escala de Liker, y luego aplicando una encuesta a los usuarios de las distintas áreas del Hospital. Con esto se determina finalmente el

estado actual de la misma y generar las conclusiones y recomendaciones más adecuadas para la mejora del Sistema de Seguridad de la Información de la institución.

En resumen, esta investigación se ha desarrollado en tres etapas: la primera que consiste en la investigación previa de los estándares de seguridad de uso obligatorio en el Ecuador, y las normativas internacionales más utilizadas en hospitales para asegurar la información médica y el desarrollo del Modelo de Madurez siguiendo el proceso utilizado por Becker, Knackstedt & Pöppelbuß (2009). En la segunda etapa, el modelo desarrollado debe pasar por un proceso de validación, para lo cual se ha buscado el apoyo de expertos de diferentes áreas que según su criterio emiten observaciones y calificaciones para cada ítem propuesto; finalmente se calculará el nivel de confianza de la validación realizada utilizando el coeficiente Alfa de Cronbach para obtener un porcentaje aceptable de confiabilidad.

Finalmente, en tercera etapa se realiza la aplicación del Modelo de Madurez desarrollado y validado en una Institución hospitalaria de tercer nivel de complejidad; utilizando una entrevista, la observación directa y finalmente una encuesta a usuarios para determinar el cumplimiento de los ítems de cada nivel del Modelo propuesto.

Etapa 1: Desarrollo del Modelo de Madurez

Para el desarrollo del Modelo propuesto en este trabajo, se ha considerado los aspectos mencionados por Becker, Knackstedt, & Pöppelbuß (2009) quienes indican ciertos aspectos y pasos a considerar al momento de diseñar un buen Modelo de Madurez.

En primer lugar los autores indican que el Modelo propuesto supone siempre una mejora con respecto a los existentes (Becker et al., 2009) en la Tabla 5 se puede visualizar la comparación realizada entre los modelos analizados con antelación.

Así pues, según el artículo de Haufe, Dzombeta & Brandis (2014) y continuando con la metodología propuesta de Becker, Knackstedt & Pöppelbuß (2009) una parte vital al desarrollar un modelo propio, es la validación del mismo; mencionándose varias estrategias para cumplir este objetivo, y debe tratarse de un proceso iterativo, es decir, debe irse mejorando constantemente y con la retroalimentación de las observaciones dadas en los resultados de validación.

De esta manera, para este trabajo de investigación se aplica parte de la metodología sugerida por Pöppelbuß & Röglinger (2011), en la cual dividen principios básicos de diseño en tres grandes categorías, y van detallando cada característica en ellas:

5. Básico:
    1. Información Básica
    2. Definición de constructores centrales relacionados con la madurez y maduración
    3. Definición de constructores centrales relacionados con el dominio de aplicación
    4. Recopilar información orientada a grupos destino.
6. Descriptivos:
    1. Criterios verificables intersubjetivamente para cada nivel de madurez y de granularidad
    2. Metodología de evaluación orientada a grupos meta
7. Prescriptivos:
    1. Medidas de mejora para cada nivel de madurez y nivel de granularidad
    2. Cálculos de decisión para seleccionar medidas de mejora
    3. Metodología de decisiones orientadas a grupos.

Así pues, para determinar los constructores centrales para evaluar en el Modelo de Madurez, se han tomado en cuenta que el resultado de la investigación de Park et al., (2010) indica que uno de los puntos a reforzar son la clasificación de los activos de información y los procedimientos definidos para asegurar la

confidencialidad de los registros médicos electrónicos; de igual manera en el artículo de Hajrahimi, Dehaghani & Sheikhtaheri (2013) donde a través de un método científico determinan siete indicadores que deben ser validados en el sector salud:

1. Seguridad de los Equipos
2. Diseño y Verificación de los Sistemas
3. Administración de los accesos a usuarios
4. Control de acceso a la red
5. Controles Criptográficos
6. Seguridad en el desarrollo y procesos de soporte
7. Sistema de Control de Accesos

Finalmente tomando en cuenta la investigación de Liu, Hwang & Chang (2011) resalta la importancia de la conciencia del personal y la Planificación y Control a través de procedimientos escritos para asegurar la Integridad y Disponibilidad de la información.

Con esta base, se han seleccionado los siguientes dominios principales:

1. Confidencialidad de la Información médica según el Reglamento Interno de la Historia Clínica, sin obstaculizar la investigación biomédica.
2. Disponibilidad de la información médica
3. Gestión y Mantenimiento de los activos de información con cronogramas de respaldos y mantenimiento preventivo.
4. Impulsión de cambios en la cultura organizacional con respecto a la Seguridad de la Información y responsabilidad de los registros.

En segundo lugar, dentro de los grandes dominios listados, se encuentran las recomendaciones puntuales a evaluar para cada uno de ellos en cada nivel propuesto:

1.1. Políticas y procedimientos de acuerdo con la normativa vigente
1.2 Gestión de autenticación y control de accesos a los Sistemas Médicos.
1.3 Procedimientos para entrega de información a investigadores biomédicos

2.1 Planes de Mantenimiento de Equipos computacionales y de red

2.2 Gestión de Riesgos

2.3 Procedimientos para uso de dispositivos móviles y redes inalámbricas en la institución.

2.4 Interoperabilidad entre Sistemas Médicos de distintos proveedores.

3.1 Planes de respaldos de información y de Contingencia

3.2 Clasificación de activos de información

3.3 Creación de responsabilidad en los usuarios con respecto a los activos de información, virus, ataques de ransomware y herramientas de respaldos adicionales.

4.1 Plan de Capacitaciones, inducción a los usuarios

Luego, al tratarse de un Modelo de Madurez debe contener métodos para Monitoreo y Medición de cumplimiento y estrategias de mejora de cada uno de los aspectos detallados en los niveles superiores.

De esta forma y con base a lo analizado, se elaboró una comparación con los modelos ya existentes (Tabla 5) para concluir que debido a las normativas que rigen las instituciones públicas (ISO 27001) y las metodologías más descriptivas de los modelos estudiados, el Modelo de Madurez propuesto tendrá de base los ítems especificados por los Modelos CSF de HITRUST, COBIT 5 e ISM3.

Tabla 5 Cuadro Comparativo de Modelos de Madurez - Elaboración Propia

Modelo	***Características Base***	***Niveles***	***Se especializa en***	***Metodología para evaluación***	***Observaciones***	***Específico para Instituciones de Salud***
SSE-CMM	Prácticas Políticas Actividades	Nivel 1: Inicial Nivel 2: Repetible Nivel 3: Definido Nivel 4: Gestionado Nivel 5: Optimizado	Mide la Capacidad de Ingeniería de los Sistemas de Seguridad	Descriptivo.	Presenta estrategias específicas de cada nivel.	NO
COBIT 5	Definiciones Políticas Cultura Organizacional Prácticas	Nivel 0: Inexistente Nivel 1: Ad hoc Nivel 2: Repetitivo pero intuitivo Nivel 3: Proceso Definido Nivel 4: Administrado y Medible Nivel 5: Optimizado	Busca determinar el estado actual de la Gestión de TI de una institución, y establecer un estado deseado a futuro.	Descriptivo. Cuenta con un listado de ítems que deben cumplirse para determinar el nivel	Presenta un banco de 9 atributos de proceso divididos en los 6 niveles de capacidad. La medición se realiza entonces en dos dimensiones	NO
ISM3	Metas Actividades Políticas Motivación	Indefinido Definido Gestionado Controlado Optimizado	Se enfoca alinear los objetivos del negocio con los procesos de la Gestión de TI; y determinar los indicadores específicos para optimizar recursos	Diagnóstico. Tiene tablas con 44 ítems en total que deben cumplirse para pasar de un nivel a otro	Se basa totalmente en las métricas y es un estándar que puede utilizarse con otros para implementarse	NO
HITRUST	Políticas Procedimientos Controles Indicadores	Nivel 1: Inicial Nivel 2: Procedimientos Nivel 3: Implementado Nivel 4: Medido Nivel 5: Administrado	Modelo basado en CMM, se enfoca en el cumplimiento de las recomendaciones para pasar de un nivel a otro. Se apega a la Normativa HIPAA	Descriptivo. Es un Modelo que permite que las organizaciones personalicen los ítems según sus características.	Muestra una tabla con los ítems que deben cumplirse en cada nivel, además de una tabla donde se establecen los rangos de puntuación para determinar con exactitud el nivel de madurez	SI

Por tanto, partiendo de la matriz comparativa se han analizado las características de los modelos que pueden adaptarse de mejor manera al área de aplicación, tomando los ítems coincidentes entre las opciones examinadas, principalmente aquellos aspectos que hacen referencia a dominios o recomendaciones de la Norma ISO 27000 e HIPAA. De este modo, el análisis comparativo de los modelos seleccionados muestra que la propuesta a desarrollar debe incluir el modelo de HITRUST, por ser un marco de referencia diseñado específicamente para que las instituciones del sector de Salud puedan cumplir con las Normas HIPAA, además de los modelos COBIT e ISM3 los cuales permiten desglosar a un alto nivel de granularidad las prácticas que deben cumplirse en cada uno de los niveles para ir subiendo entre ellos.

Adicionalmente, el modelo ISM3 tiene la característica de servir como framework para implementación de la norma ISO 27001; misma que como se ha mencionado anteriormente es el estándar obligatorio para todas las Instituciones Públicas ecuatorianas.

Luego, el Modelo de Madurez propuesto, consta de 5 niveles que se describen a continuación:

Nivel 1 - No definido

En este nivel no se han definido objetivos o políticas de seguridad de la información, tampoco se han documentado los procedimientos utilizados para gestionar accesos, usuarios y resolución de incidentes de seguridad; tampoco se comprenden con claridad los riesgos de cumplimiento existentes.

Los ítems definidos en este nivel son:

Se tiene una visión estratégica de los objetivos de TI

Se han buscado y conseguido recursos necesarios para la seguridad de la información médica

Se tiene una idea de los objetivos de seguridad, pero no están documentados

Se aplican los parches de seguridad conforme es necesario, sin ninguna planificación o documento

Se cuenta con respaldos administrados, pero el procedimiento para obtenerlos no está documentado.

Se cuenta con herramientas de protección contra malware

Se realiza la administración de segmentación y filtrado de tráfico en la red

Se tiene un sistema de gestión documental

Nivel 2 – Definido Ad Hoc

Se han documentado los procedimientos base y las prácticas principales para el correcto registro de datos médicos y su almacenamiento. Existe personal seleccionado encargado de monitorear la Seguridad de la Información con funciones y entrenamiento adecuados.

Se utilizan ciertos datos recopilados para investigar y evaluar la mejora.

Se tiene una conciencia sobre seguridad entre los usuarios

Se cuenta con control de cambios de los sistemas de información y de las medidas de seguridad

Se realiza el Control de accesos y gestión de usuarios en el Sistema Médico.

Se han realizado auditorías internas.

Se cuenta con Niveles de Servicio definidos.

Se han realizado capacitaciones al personal encargado de la seguridad y soporte de TI

Se ha realizado un fortalecimiento *(hardening)* de los puntos más vulnerables

Nivel 3 – Procesos Definidos.

En este nivel se ha considerado que en la Institución cuente con una estructura ética de cumplimiento con responsabilidad desde cada dependencia; además existe un responsable asignado para las tareas del monitoreo.

Así también se ha establecido un proceso de supervisión con una visión más amplia y a un mayor nivel jerárquico, contando con el apoyo Gerencial.

Además, se ha implementado medidas de control incluyendo auditorías, procedimientos escritos, análisis de riesgos, etc. Dentro de este nivel se verificará de forma puntual:

Si se han definido los objetivos de seguridad por escrito

Se han realizado capacitaciones con evaluación posterior para concientizar al personal sobre la seguridad de la información

Existe un Control de Cambios documentado de los Sistemas de Información

Se han definido operaciones de Continuidad del Negocio

Se ha definido un proceso para entrega de información para investigaciones sin violar la normativa vigente de información médica.

Nivel 4 – Monitorizado y Verificable

Al alcanzar este nivel la organización ha establecido un proceso de verificación periódico que se reporta a la Alta Gerencia; además de haber establecido un Plan de Auditoría Interna para evaluar los riesgos detectados y un protocolo bien definido para realizar investigación forense.

Se realizan pruebas documentadas de calidad y cumplimiento de la información. Para evaluar el cumplimiento de este nivel, se verificará:

Se realizan pruebas documentadas de calidad y cumplimiento de la información

Existe detección y análisis de eventos documentada

Se ha realizado análisis forense

Se cuenta con un proceso definido para seleccionar al personal de seguridad

Se realiza un registro y administración de la confiabilidad y disponibilidad de la información

Se realiza un seguimiento de los seguros contratados

Existe detección y análisis de eventos documentada

Se ha realizado análisis forense

Se cuenta con un proceso definido para seleccionar al personal de seguridad

Se realiza un registro y administración de la confiabilidad y disponibilidad de la información

Se realiza un seguimiento de los seguros contratados

Nivel 5 – Optimizado

En este nivel se ha definido un Plan Completo de Monitoreo que lo realiza el personal de seguridad responsable; se conducen investigaciones de acuerdo con el protocolo establecido y se ha capacitado al personal

encargado de conducir estas investigaciones. El Plan de Seguridad y las tareas de cumplimiento se evalúan mínimo de forma anual.

En cuanto a la Gestión de Riesgos, en este nivel se ha definido un Plan que incluye la identificación, gestión y finalmente se los ha asociado con indicadores de cumplimiento. Las características de este nivel incluyen:

- Se realizan capacitaciones tanto al personal de seguridad como a usuarios finales y se monitorean los resultados
- Se realizan Auditorías Internas y se verifica el cierre de las Acciones correctivas y recomendaciones
- Se realiza una revisión periódica del cumplimiento de los objetivos de seguridad definidos
- Se realizan verificaciones periódicas de los Accesos registrados y usuarios activos
- Se realiza un análisis comparativo entre los resultados de pruebas de análisis forense en dos periodos diferentes

Etapa 2: Validación del Modelo propuesto.

Una vez redactada la propuesta de Modelo de Madurez y elaborada una herramienta de evaluación con los ítems anteriormente descritos, se realiza la validación de este, con la finalidad de asegurar la efectividad y pertinencia de la propuesta.

Para este fin, y luego de analizar los trabajos similares a esta investigación, se ha decidido utilizar la validación por criterio de expertos ya que este tipo de método se aplica frecuentemente en las investigaciones que tienen un límite para las observaciones experimentales (Utkin, s/f) como particularmente pasa en el desarrollo del presente trabajo.

Así, la validación de experto consiste en solicitar el criterio a varias personas escogidas por su trayectoria y conocimientos en los temas a validar (Escobar-Pérez y Cuervo-Martínez, 2008).

También se consideró que al utilizar la validación por criterio de expertos según Cabero y Barroso (2003) se puede profundizar en las respuestas que se obtienen, las respuestas son fundamentadas en la teoría y los resultados obtenidos son bastante detallados .

Luego, el proceso para escoger los expertos depende en su mayoría del instrumento o el tema a analizar, en el caso de las TIC tal como analizan Cabero y Llorente (2013), es vital que los expertos conozcan o hayan tenido experiencia con alguna TI o sean docentes de la especialidad.

Finalmente, el número de expertos es algo que no está estandarizado aún, algunos indican que deben ir de rango de 15 y 20, otros entre 15 y 35, 7 y 30 o entre 15 y 25, así lo resumen Cabero y Llorente (2013) en su trabajo de investigación; en cambio Delgado-Rico, Carretero-Dios, & Ruch (2012) propone que según el número de ítems a evaluar se dividan éstos entre los expertos escogidos, de manera que cada uno valide una parte; o en otro caso, se pueda escoger expertos para validar cada aspecto de los ítems propuestos.

De esta manera, para la validación de la propuesta de Modelo de Madurez, se han escogido 5 expertos de áreas multidisciplinarias según estas características: un experto Abogado encargado de Archivos y Documentación Médica con formación y conocimiento profundo de Normativa de Hospitales, dos expertos Administradores de TI de hospitales de

nivel 2 (General) y 3 (De Especialidades), un Gerente General de un Hospital de especialidades con formación de Auditoría y Gestión Pública y por último, un experto en Seguridad Informática.

Luego, para facilitar la validación del Modelo propuesto se diseñó un instrumento de validación con base al elaborado por Sosa Oliveros (2014), en el cual se fueron detallando uno a uno los ítems de cada nivel de madurez propuesto, las dimensiones a ser evaluadas, la escala de calificación, y la base de evaluación.

En las columnas del instrumento se especifican además los aspectos a evaluar de cada ítem: Redacción, Contenido, Congruencia y Pertinencia; cada uno de estos aspectos puede obtener una calificación desde Eliminar (0) a Excelente (5).

Además, para lograr un conocimiento cabal del tema a evaluar, a los expertos evaluadores se les entregó un documento con resumen y objetivos de la Investigación, una Matriz operacional comparativa de los modelos estudiados y considerados en el diseño del Modelo Propuesto, el Instrumento de Validación propiamente y el Certificado de Validación (Anexo 1).

Luego de la entrega, se coordinaron además reuniones presenciales para revisión conjunta y disolución de dudas con respecto a los objetivos de la investigación; se recopilaron los instrumentos llenos (Anexo 2) y se procedió a la tabulación de los mismos (Anexo 3) según la escala descrita anteriormente con la finalidad de poder verificar la confiabilidad de los resultados con el método de consistencia interna Alfa de Cronbach, el cual estima la fiabilidad de un instrumento a través de un conjunto de ítems generalmente valorados en una escala de Likert asumiendo que todos miden el mismo constructo y que tienen alto nivel de correlación entre ellos (Ormeño Cabrera y Orellana Molina, 2016). Adicionalmente, se puede evaluar el nivel del Alfa de Cronbach según George y Mallery (2003) de la siguiente manera:

1. > 0.9 - Excelente
2. > 0.8 - Bueno
3. > 0.7 - Aceptable
4. > 0.6 - Cuestionable
5. > 0.5 - Pobre
6. < 0.5 - Inaceptable

Luego, según la tabulación y cálculos realizados de los resultados de la validación, el Alfa de Cronbach resultante total es de **0.974** lo que equivale a **Excelente** (Tabla 7)**.**

La fórmula de cálculo del Alfa de Cronbach es:

$$\partial\ de\ Cronbach = \frac{K}{(K-1)} * \left|1 - \left(\frac{\sum V_i}{Vk}\right)\right|$$

Donde ***K*** es el número total de ítems evaluados**,** V_i es la varianza de cada ítem y ***Vk*** es la varianza total obtenida.

Por otro lado, las observaciones obtenidas sirvieron para modificar la redacción de los ítems de manera de hacerlos más objetivos para el momento de la aplicación.

El Modelo Final, validado y verificado la fiabilidad de la validación, se muestra en la Tabla 6.

Tabla 6 Herramienta de Evaluación de Madurez de Seguridad de la Información en Hospitales

MODELO DE MADUREZ DE SEGURIDAD DE LA INFORMACIÓN EN INSTITUCIONES DE SALUD PROPUESTO

Modelo híbrido basado en COBIT 5, ISM3 y HITRUST

5 Niveles

No.	**Descripción del Nivel**	**Items que deben cumplirse para pasar de un nivel a otro**
1	No definido	Se reconoce la normativa existente y se intenta seguirla sin procedimientos ni políticas escritas
		Se han buscado los recursos necesarios para salvaguardar la información médica en formato físico
		Se tiene una idea de las necesidades y debilidades en cuanto a Seguridad, pero no están documentadas
		Se han detectado vulnerabilidades a través de chequeos aleatorios o alarmas automáticas del sistema y se aplican los parches de seguridad conforme es necesario
		Se respalda la información de manera reactiva (cuando es necesario)
		Se cuenta con herramientas de protección contra malware, pero no existe un monitoreo de actualizaciones y amenazas y Centralización en la Gestión
		Se realiza la administración de segmentación y filtrado de tráfico en la red de manera empírica
		No se ha socializado a los usuarios las responsabilidades de ingreso de datos a los Sistemas médicos
2	Definido ad hoc	Se han definido políticas o estándares de uso obligatorio y se han difundido a los empleados
		La conciencia sobre seguridad entre los usuarios no se ha medido y han firmado acuerdos de confidencialidad genéricos
		Las políticas definidas determinan la estructura de seguridad de la información, responsabilidades y dejan los cimientos para medir el progreso y cumplimiento
		No se cuenta con una bitácora escrita de control de cambios de los sistemas de información y de las medidas de seguridad. Los cambios son reactivos a la necesidad de la Institución
		Se realiza el Control de accesos y gestión de usuarios sin procedimientos escritos
		Se han realizado auditorías internas, sin embargo, no se ha dado seguimiento a las recomendaciones
		Se cuenta con Herramientas de respaldo de información, pero el mismo es responsabilidad del usuario final
		Se han realizado capacitaciones al personal encargado de la seguridad y soporte de TI
		Se han realizado configuraciones básicas en los puntos más vulnerables de la red y existen restricciones administradas sin procedimiento escrito
3	Procesos Definidos	Se han definido los objetivos de seguridad por escrito
		Existe un plan de capacitaciones para concientizar al personal sobre la seguridad de la información y amenazas actuales

		El uso de dispositivos personales móviles y conexión a la red institucional está normado en un procedimiento escrito
		Se han definido procedimientos formales para implementar los controles de seguridad identificados por las políticas definidas
		Se han definido operaciones de Continuidad del Negocio
		Existen procedimientos definidos para archivo de datos físicos y Planes de Respaldo periódicos de los activos de información digitales
		Existe un procedimiento escrito para gestión de usuarios y accesos
		Se ha definido un proceso para entrega de información para investigaciones sin violar la normativa vigente de información médica
		Los procedimientos definidos se han comunicado a los individuos que necesitan seguirlos
4	Monitorizado y Verificable	Se cuenta con documentos aprobados e implementados que incluyen los requerimientos de evaluación, incluyendo el tipo y frecuencia de las pruebas
		Se realizan pruebas de evaluación al personal posterior a las capacitaciones para medir la calidad de recepción
		Existe detección y análisis de eventos o amenazas bien documentados
		Se ha realizado un fortalecimiento (hardening) apropiado a los puntos críticos de la Red institucional y de darse incidentes se ha realizado el análisis forense correspondiente
		Se cuenta con un proceso definido para seleccionar al personal de seguridad de TI
		Se realiza un registro y administración de la confiabilidad y disponibilidad de la información
		Se ha realizado una Matriz de Gestión de Riesgos y se revisa de forma periódica
		Se realizan Auditorías internas periódicas
		Se realiza un seguimiento de los seguros contratados para la infraestructura
5	Optimizado	Se realizan capacitaciones tanto al personal de seguridad como a usuarios finales y se monitorean los resultados
		Se realizan Auditorías Internas y se verifica el cierre de las Acciones correctivas y recomendaciones
		Se realiza una revisión periódica del cumplimiento de los objetivos de seguridad definidos
		Se realizan verificaciones periódicas de los Accesos registrados y usuarios activos
		Se monitorea con frecuencia la calidad e integridad de los respaldos generados
		Se realiza un análisis comparativo entre los resultados de pruebas de análisis forense en dos periodos diferentes
		Las tomas de decisiones se basan en costo, riesgo e impacto en la misión

Tabla 7 Tabulación de Datos para cálculo de alfa de Cronbach

1. Ing. Ma. Eugenia Arévalo	16	16	15	15	16	15	20	20	15	13	16	16	16	16	15	16	16	16	16	16	16	16	16	16	15	20	20	20	20	20	20	20	20	20	18	20	617
2. Dr. Oscar Chango S	20	20	16	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	716
3. Mgs. Daniel Avila L.	16	16	15	15	16	15	20	20	15	13	16	16	16	16	15	16	16	16	16	16	16	16	16	16	15	20	20	20	20	20	20	20	20	20	18	20	617
4. Dr Franklin Rojas	16	16	12	16	16	16	16	12	16	20	16	16	15	16	16	16	16	20	20	16	16	19	18	16	20	20	16	20	15	20	20	20	16	20	20	20	619
5. Ing. Mauricio Icaza S.	18	20	18	17	18	17	18	18	18	20	18	18	18	20	18	20	20	20	20	20	20	20	20	18	20	20	20	20	20	16	20	20	20	18	20	18	684
TOTAL	86	88	76	83	86	83	94	90	84	86	86	86	85	88	84	88	88	92	92	88	88	91	90	86	90	100	96	100	95	96	100	100	96	98	96	98	3253
VARIANZA	3	3	2,25	4,25	3	4,25	3	12	4,25	12,3	3	3	3,69	3	4,25	3	3	4	4	3	3	3,19	2,75	3	6,25	0	3	0	4,69	0	0	0	3	0	1	0	1730

Tabla 8 Datos para cálculo de alfa de Cronbach

K	**36**
S Vi	115,063
Vt	2178
alfa de cronbach	**97%**

Etapa 3: Aplicación del Modelo desarrollado en una Unidad Médica del Sector Público de Tercer Nivel de Complejidad.

Una vez desarrollado el Modelo de Madurez y validado por los expertos escogidos, se continúa con la aplicación del modelo propuesto en una institución hospitalaria pública.

Para poder hacer esto, se ha seleccionado como población Hospitales Públicos que funcionan actualmente en la ciudad de Cuenca, que según datos del Instituto Nacional de Estadísticas y Censos (INEC) son:

- Un Hospital General del Ministerio de Salud
- Un Hospital Básico del Gad Municipal
- Un Hospital de Especialidades del Instituto Ecuatoriano de Seguridad Social.

Luego, considerando el tamaño de la población, se toma como muestra el Hospital de Especialidades por tratarse del más grande a nivel local, el mismo que brinda atención de especialidades a tres provincias del Ecuador, y según datos de la Coordinación General de Planificación y Estadísticas (2017) y el Anuario de Egresos Hospitalarios del INEC (2016) cuenta con 282 camas para hospitalización y tiene un promedio de 30000 atenciones mensuales en consulta externa, 1500 cirugías y 12000 atenciones en Emergencia; la selección de la institución obedece a que al ser una institución de tercer nivel cuenta con la autonomía necesaria, buena infraestructura y sistemas de información altamente desarrollados para ser evaluados (Instituto Ecuatoriano de Seguridad Social, 2015).

Para la aplicación del Modelo, se ha optado por aplicar técnicas de entrevista, observación directa, y una encuesta direccionada a los usuarios finales para conocer el estado actual de la madurez de la seguridad de la información.

En primer lugar, se aplicó la herramienta de evaluación diseñada en la Unidad de Tecnologías de la Información de la Institución (Anexo 4).

Posteriormente, para poder aplicar el modelo, se elabora un cuestionario de tipo escala, que se ha aplicado de forma aleatoria a los usuarios finales dentro del Hospital seleccionado para el estudio.

Luego, durante la entrevista con el Coordinador General de TI del Hospital se pudo verificar que desde la Entidad de control nacional (Dirección Nacional de Tecnologías de la Información) se ha emitido la Resolución C.D. 521 con las recomendaciones y políticas a cumplir por todos los usuarios de las Instituciones bajo su control (Consejo Directivo del IESS, 2016).

Adicionalmente, fuera de esta resolución no se cuenta con procedimientos institucionales propios del Hospital para documentar las acciones de respaldos de información, actualización de herramientas antivirus o antimalware, monitoreo de la red, control de activación, desactivación, perfiles de acceso a los usuarios de los sistemas, etc.

En lo que se refiere a la socialización de las políticas a usuarios finales, se han realizado pocas capacitaciones principalmente como forma de inducción a los nuevos colaboradores dentro de la institución, sin embargo, no se cuenta con procedimientos para medir la efectividad de las capacitaciones.

También se comunicó que no existe un personal designado exclusivamente para la seguridad de la información dentro de la institución, pero el personal informático está capacitado para monitorear y verificar actualizaciones de antivirus, de sistemas operativos, instalación de parches de seguridad, etc.

En cuanto a los respaldos de información y de activos como reglas de firewall, proxys, configuración de redes y demás similares, se cuentan con herramientas dedicadas al respaldo periódico de los mismos dentro de los servidores de la institución; sin existir un documento escrito del procedimiento.

A nivel gerencial, no se han definido objetivos de seguridad de la información, ni indicadores para verificar el estado y realizar las mejoras correspondientes dentro de esta área de la institución.

Además, se indicó que hasta el momento se ha realizado una Auditoría Informática interna, cumpliendo en su totalidad las recomendaciones y acciones correctivas de la misma.

En resumen, luego de la entrevista realizada y la aplicación de la herramienta de evaluación con una escala de Líker, se obtuvieron los siguientes resultados:

Tabla 9 Resultados de aplicación del Modelo

Nivel	Puntuación	%
1 -No definido	25/40	63%
2 – Ad Hoc	31/45	69%
3 – Definido	22/45	49%
4 – Monitorizado y Verificable	13/45	29%
5 – Optimizado	13/35	37%

Se puede concluir como resultado final que la Institución cumple en un 69% de lo especificado en el Nivel 2 y el 49% del Nivel 3 de Madurez, es decir, la Institución tiene un Nivel 2 (Ad Hoc), en el cual se están cumpliendo con las políticas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información; sin embargo, no se cuentan con procedimientos formales u objetivos de seguridad por escrito.

APLICACIÓN DEL CUESTIONARIO

Con la finalidad de obtener una visión desde el punto de vista del usuario final, se diseñó y realizó un cuestionario (Anexo 5) donde se evalúan aspectos básicos de la seguridad de la información; obteniendo resultados consistentes con lo recopilado en la entrevista con el Coordinador de TI.

En el cuestionario aplicado a los usuarios en cuanto al conocimiento de procedimientos para mejorar el registro de la información, el 72.7% respondió que no conoce los procedimientos institucionales y el 73.7% desconoce procedimientos para manejar la información confidencial generada; por otra parte el 66% de los usuarios notifica al Departamento de Sistemas en cuanto se genera un error en el PC; un 50% respalda la información de su computador por su cuenta y el 51.9% no tiene un antivirus actualizado instalado en el PC. Por último, 68.8% no cree que la información en la institución esté segura (Anexo 6).

Por tanto, los resultados de la aplicación del Modelo de Madurez con consistentes con los de un Nivel 2, ya que los usuarios no conocen las recomendaciones básicas de seguridad; ni cuentan con procedimientos claros para respaldos de información; y, por lo tanto, con un riesgo latente de pérdida o fuga de información, introducción de virus o programas poco seguros en la Red Institucional.

CONCLUSIONES

Al finalizar este trabajo de investigación, se puede concluir que se cumplió con el objetivo propuesto de desarrollar un Modelo de Madurez para evaluar el nivel de la Seguridad de la Información en instituciones de servicios de salud pública; el Modelo generado considera como base fundamental los estándares usados en las instituciones públicas y también la normativa internacional más conocida para hospitales; y cubre los aspectos más relevantes a evaluar en una institución del sector salud.

El criterio de los expertos consultados fue vital para el correcto desarrollo del Modelo propuesto, ya que aportaron observaciones objetivas desde sus áreas de experticia, cuyos resultados al combinarse fueron ítems concretos y completos que consideran no únicamente la parte informática, sino también la parte gerencial y legal de una institución.

Por otro lado, en cuanto al diseño de la herramienta para la validación de expertos debió ser mejorada, esto se evidencia por la necesidad de explicar personalmente el funcionamiento de

la herramienta y la forma de calificar, por lo que es algo que debe mejorarse en el futuro.

RECOMENDACIONES.

Finalmente, con respecto a la aplicación del Modelo desarrollado en la Institución Hospitalaria de tercer nivel de complejidad, se pueden emitir las siguientes recomendaciones para mejorar el Nivel de Madurez de Seguridad de la Información:

Dentro de la Institución se debe definir por escrito los objetivos de seguridad de la información y socializarlos con la Alta Gerencia, posterior a esto es importante elaborar procedimientos escritos para la obtención de respaldos, creación de usuarios y asignación de permisos en los Sistemas Institucionales, los cuales están al momento ejecutándose sin un documento de sustento. Por otra parte, se sugiere desarrollar planes de capacitación a los usuarios desde los aspectos básicos de la Seguridad de la información y su importancia.

Otra recomendación importante es continuar con las Auditorías Internas y considerar en algún momento unas pruebas de hackeo ético para verificar las configuraciones de Firewall, proxys, etc.

A futuro, también se puede elaborar una herramienta tomando en cuenta los diferentes niveles de atención y complejidad existentes en el Sistema de Salud ecuatoriano, ya que la infraestructura y volumen de información manejado en cada uno, varía considerablemente.

Referencias Bibliográficas

Ahima. (2014). AHIMA : Leading Information Governance for Healthcare. Recuperado a partir de https://www.cms.gov/ehealth/downloads/ehealthsummit_panelpress_051914.pdf

Arbeláez, R. (2014). Modelos de Madurez de Seguridad de la informacion: como debe evolucionar la seguridad en las organizaciones. En *VII Jornada Nacional de Seguridad Informática*. Recuperado a partir de http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/05-ModelosMadurezSeguridadInformatica.pdf

Areitio Bertolín, J. (2008). *Seguridad de la información : redes, informática y sistemas de información*. Paraninfo Cengage Learning.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *Business & Information Systems Engineering*, *1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151–164. https://doi.org/10.1057/ejis.2009.8

Boswell, L., & Bhargava, T. (2014). Potential Uses of Maturity Models for Capacity Development in Emerging Democracies/Conflict Nations | PAE. Recuperado el 23 de junio de 2017, a partir de https://www.pae.com/news/thought-leadership/potential-uses-maturity-models-capacity-development-emerging

Cabero, J., & Barroso, J. (2003). Bordón. *Bordón, Revista de Pedagogía*, *62*(2), 25–38. Recuperado a partir de https://docs.google.com/viewerng/viewer?url=idus.us.es/xmlui/bitstream/handle/11441/24562/file_1.pdf?sequence%3D1&isAllowed=y

Cabero, J., & Llorente, Mc. (2013). La aplicación del juicio de experto como técnica de evaluación de las tecnologías de la información y comunicación (TIC). *Eduweb. Revista de Tecnología de Información y Comunicación en Educación*, *7*(2), 11–22.

Caiza-Acero, M., & Bolaños-Burgos, F. (2014). Las implementaciones de las normas de seguridad de la información: estudio de caso la Sociedad de Lucha Contra el Cáncer del Ecuador. *Revista electrónica de Computación, Informática Biomédica y Electrónica*, *3*(3). Recuperado a partir de http://www.redalyc.org/pdf/5122/512251568001.pdf

Canal, V. A. (2004). *Ism3 1.0. nformation*

Security Management Maturity Model. Recuperado a partir de https://pdfs.semanticscholar.org/64ac/1e4585056babd78d978827bf35eae78b5ff6.pdf

Carmona, D. H., Nieto, E., Angelo, M., & Polo, R. (2009). Modelo de Madurez para la Seguridad de la Información, *8*(1).

Consejo Directivo del IESS. (2016). *Resolución C.D. 521*. Recuperado a partir de https://www.iess.gob.ec/documents/10162/33703/C.D.+521

Contraloría General del Estado. Normas De Control Interno De La Contraloria General Del Estado, Ultima § (2009). Recuperado a partir de http://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf

Delgado-Rico, E. ;, Carretero-Dios, H. ;, & Ruch, W. (2012). Content validity evidences in test development: an applied perspective. *International Journal of Clinical and Health Psychology España*, *12*(3), 449–460. https://doi.org/10.5167/uzh-64551

Department of Homeland Security. (2014). Cybersecurity Capability Maturity Model White Paper. Recuperado a partir de https://niccs.us-cert.gov/sites/default/files/Capability Maturity Model White Paper.pdf?trackDocs=Capability Maturity Model White Paper.pdf

Escobar-Pérez, J., & Cuervo-Martínez, Á. (2008). Validez De Contenido Y Juicio De Expertos: Una Aproximación a Su Utilización. *Avances en Medición*, *6*, 27–36. Recuperado a partir de http://www.humanas.unal.edu.co/psicometria/files/7113/8574/5708/Articulo3_Juicio_de_expertos_27-36.pdf

ESSet. (s/f). Datos médicos expuestos en Google y un arreglo judicial récord. Recuperado el 28 de septiembre de 2017, a partir de https://www.welivesecurity.com/la-es/2016/04/13/datos-medicos-expuestos-en-google/

Fernández-Alemán, J. L., Carrión Señor, I., Oliver Lozoya, P. A., & Ambrosio, T. (2013). Security and privacy in electronic health records: A systematic literature review. Recuperado a partir de http://ac.els-cdn.com/S1532046412001864/1-s2.0-S1532046412001864-main.pdf?_tid=9d887330-4f21-11e7-9b26-00000aab0f27&acdnat=1497239325_99a9c0593640273a98b889637753a8b2

Fernández-medina, E. (2006). Modelos de madurez para SGSI desde un enfoque práctico Modelos de madurez para SGSI desde un enfoque práctico, (February).

George, D., & Mallery, P. (2003). *SPSS for Windows Step by Step: Answers to Selected Exercises*. *A Simple Guide and Reference*. https://doi.org/9780335262588

Grifantini, K. (2016). Healthcare, Hacked - IEEE PULSE. Recuperado el 6 de junio de 2017, a partir de http://pulse.embs.org/may-2016/healthcare-hacked/

Grupa, P. (2015). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. Recuperado el 26 de septiembre de 2017, a partir de http://www.iso27000.es/sgsi.html

Guimón, P. (2017). Un ciberataque paraliza 16 hospitales de Reino Unido y les exige dinero | Tecnología | EL PAÍS. Recuperado el 6 de junio de 2017, a partir de http://tecnologia.elpais.com/tecnologia/2017/05/12/actualidad/1494602389_458942.html

Hajrahimi, N., Dehaghani, S. M. H., & Sheikhtaheri, A. (2013). Health information security: a case study of three selected medical centers in iran. *Acta informatica medica : AIM : journal of the Society for Medical Informatics of Bosnia & Herzegovina : casopis Drustva za medicinsku informatiku BiH*, *21*(1), 42–5. https://doi.org/10.5455/AIM.2012.21.42-45

Haufe, K., Dzombeta, S., & Brandis, K. (2014). Proposal for a security management in cloud computing for health care. *TheScientificWorldJournal*, *2014*, 146970. https://doi.org/10.1155/2014/146970

Holroyd-Leduc, J. M., Lorenzetti, D., Straus, S. E., Sykes, L., & Quan, H. (2011). The impact of the electronic medical record on structure, process, and outcomes within primary care: a systematic review of the evidence: Figure 1. *Journal of the American Medical Informatics Association*, *18*(6), 732–737. https://doi.org/10.1136/amiajnl-2010-000019

Human & Health Services. (2015). *Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices*. Recuperado a partir de https://www.hhs.gov/sites/default/files/small-practice-security-guide-1.pdf

Identity Theft Resource Center. (2013). *Identity Theft Resource Center*. Recuperado a partir de http://www.idtheftcenter.org/images/breach/2017Breaches/ITRCBreachReport2017.pdf

Identity Theft Resource Center. (2017). *Identity Theft Resource Center: 2013 Data Breach Stats*. Recuperado a partir de http://www.idtheftcenter.org/images/breach/2017Breaches/ITRCBreachStatsReport2017.pdf

Instituto Ecuatoriano de Seguridad Social. (2015). Instituto Ecuatoriano de Seguridad Social Informe de Rendición de Cuentas 2014, 1–49. Recuperado a partir de https://www.iess.gob.ec/documents/10162/3780216/2015+04+01+Rendicion+de+cuentas+v3.pdf

Instituto Nacional de Ciberseguridad. (2017). ¿Estás preparado para hacer frente a una fuga de datos? | INCIBE. Recuperado el 24 de mayo de 2018, a partir de https://www.incibe.es/protege-tu-empresa/blog/estas-preparado-hacer-frente-fuga-datos

Instituto Nacional de Estadísticas y Censos, & SEecretaría Nacional de PLAnificación y DESarrollo. (2016). Ecuador - Estadísticas Hospitalarias Camas y Egresos 2010. Recuperado el 25 de octubre de 2018, a partir de http://anda.inec.gob.ec/anda/index.php/catalog/595/dataprocessing

International Standarization Organization. (2016). ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls. Recuperado el 1 de octubre de 2017, a partir de https://www.iso.org/standard/54533.html

IsecT Ltd. (s/f). ISO/IEC 27001 certification standard. Recuperado el 30 de septiembre de 2017, a partir de http://www.iso27001security.com/html/27001.html

ISO -International Organization for Standardization. (2011). Familias de las Normas ISO 27000, 19. Recuperado a partir de http://www.iso27000.es/download/doc_iso27000_all.pdf

Kostadinov, D. (2018). Key Elements of an Information Security Policy. Recuperado el 24 de mayo de 2018, a partir de https://resources.infosecinstitute.com/key-elements-information-security-policy/#gref

Kwon, J., & Johnson, M. E. (2013). Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association*, *20*(1), 44–51. https://doi.org/10.1136/amiajnl-2012-000906

Liu, C.-F., Hwang, H.-G., & Chang, H.-C. (2011). E-Healthcare Maturity in Taiwan. *Telemedicine and e-Health*, *17*(7), 569–573. https://doi.org/10.1089/tmj.2010.0228

LLC HITRUST Alliance. (2016). *Healthcare Sector Cybersecurity Framework Implementation Guide*. Recuperado a partir de https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf

Matalobos Veiga, J. M. (2011). *Análisis de riesgos de seguridad de la información.* Recuperado a partir de http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

Miron, W., & Muita, K. (2014). Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. Recuperado a partir de https://timreview.ca/sites/default/files/article_PDF/MironMuita_TIMReview_October2014.pdf

Mitnik, K., Simon, W., & Wozniak, S. (2003). *The Art of deception: Controlling the human element of security*.

Mzokov, V. (2017, enero). Data security risks in healthcare IT – Kaspersky Lab official blog. *Kaspersky Lab Daily*. Recuperado a partir de https://blog.kaspersky.com/healthcare-safeguarding-data/15166/

Narayana Samy, G., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health Informatics Journal*, *16*(3), 201–209. https://doi.org/10.1177/1460458210377468

Office for Civil Rights. (2013). Summary of the HIPAA Security Rule | HHS.gov. Recuperado el 8 de junio de 2017, a partir de https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Office for Civil Rights (OCR). (2017). HIPAA for Professionals | HHS.gov. Recuperado el 8 de junio de 2017, a partir de https://www.hhs.gov/hipaa/for-professionals/index.html

Office of Civil Rights Department of Health and

Human Services. (2003). *Summary of the HIPAA Privacy Rule*. *OCR Privacy Brief*. https://doi.org/10.1016/j.chroma.2005.11.119

Office of the National Coordinator for Health Information Technology. (2015). Guide to Privacy and Security of Electronic Health Information. Recuperado a partir de https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Organización Panamericana de la Salud. (2016). OPS OMS | Elaboración de listas de verificación. Recuperado el 23 de mayo de 2017, a partir de http://www.paho.org/hq/index.php?option=com_content&view=article&id=10935%3A2015-elaboracion-listas-verificacion&catid=7679%3Aauditoria&lang=es

Organización Panamericana de la Salud. (2016). *Registros médicos electrónicos en América Latina y el Caribe: Análisis sobre la situación actual y recomendaciones para la Región*. Recuperado a partir de http://iris.paho.org/xmlui/bitstream/handle/123456789/28209/9789275318829_spa.pdf?sequence=1&isAllowed=y

Ormeño Cabrera, B., & Orellana Molina, T. (2016). Gestión de personas: Resultados de investigación. *Revista Gestión de las personas y tecnología*, (27), 6–20.

Park, W. S., Seo, S. W., Son, S. S., Lee, M. J., Kim, S. H., Choi, E. M., … Kim, O. N. (2010). Analysis of information security management systems at 5 domestic hospitals with more than 500 beds. *Healthcare Informatics Research*, *16*(2), 89–99. https://doi.org/10.4258/hir.2010.16.2.89

Pérez, J. J. (s/f). Concepto de un SGSI - Servei d'Informàtica. Recuperado el 27 de septiembre de 2017, a partir de http://www.uv.es/perezj/sgsi/concepto.wiki

Pérez Mergaerjo, E., Pérez Vergara, I., & Rodríguez Ruíz, Y. (2014). Modelos de madurez y su idoneidad para aplicar en pequeñas y medianas empresas. *Ingeniería Industrial*, *35*(2), 146–158. Recuperado a partir de http://scielo.sld.cu/pdf/rii/v35n2/rii04214.pdf

Ponemon Institute. (2016). *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*. Recuperado a partir de https://media.scmagazine.com/documents/232/sixth_annual_benchmark_study_o_57783.pdf

Pöppelbuß, J., & Röglinger, M. (2011). What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management. *Ecis*, Paper28. Recuperado a partir de http://aisel.aisnet.org/ecis2011/28/

Portantier, F. (2012). Seguridad informática, 0–48. Recuperado a partir de https://books.google.com.co/books?hl=es&lr=&id=uVXOrk3kB6gC&oi=fnd&pg=PT3&dq=Cuales+son+los+principales+problemas+en+la+seguridad+informática&ots=-y1ZM4W1OZ&sig=foeRaC5xmJh2xy6Cn9d6eV3qZqY

Rosmiati, Riadi, I., & Prayudi, Y. (2016). A Maturity Level Framework for Measurement of Information Security Performance. *International Journal of Computer Applications*, *141*(8), 1–6. https://doi.org/10.5120/ijca2016907930

SafeNet. (2010). Data Protection for the Healthcare Industry Data Protection for the Healthcare Industry. Recuperado a partir de http://www.safenet-inc.com/uploadedFiles/About_SafeNet/Resource_Library/Resource_Items/White_Papers_-_SFDC_Protected_EDP/SafeNet Data Protection Healthcare White Paper.pdf?utm_source=AoDP-blog&utm_medium=blog&utm_content=Data-Protection-for-Healthcare&utm

Sánchez, L. E., Villafranca, D., & Piattini, M. (2007). *MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs*.

Secretaría de Salud. (2010). Miércoles 8 de septiembre de 2010. Recuperado a partir de http://www.dgis.salud.gob.mx/descargas/pdf/NOM-024-SSA3-2010_SistemasECE.pdf

Secretaría Nacional de la Administración Pública. Esquema Gubernamental de Seguridades de la Información (2013). Recuperado a partir de http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2016/02/Esquema-Gubernamental-de-Seguridades-de-la-Informacion.pdf

Servicio Ecuatoriano de Normalización. (2016). Prólogo nacional. Recuperado a partir de http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2016/05/nte_in

en_iso_iec_27002.pdf
Shin, L. (2015). Why Medical Identity Theft Is Rising And How To Protect Yourself. Recuperado el 28 de septiembre de 2017, a partir de https://www.forbes.com/sites/laurashin/2015/05/29/why-medical-identity-theft-is-rising-and-how-to-protect-yourself/#61a84b253608
Sosa Oliveros, M. E. (2014). *INSTRUMENTO_DE_VALIDACION_EXPERTOS (2)*.
Stevanović, B. (2011). Maturity Models in Information Security. *Journal of Information Technology (IJICT)*, *1*(2), 44–47. Recuperado a partir de http://www.esjournals.org
Taich, D. (2015). Grado de madurez de la organización en Seguridad de la Información. En *Segurinfo 2015*. Recuperado a partir de https://eventos.usuaria.org.ar/admin/upload/arch/actividades/Diego Taich - Grado de madurez de la organizacion en Seguridad de la Informacion.pdf
Tarazona, C. (2015). Amenazas Informáticas y seguridad de la informacion, 137–146. Recuperado a partir de https://revistas.uexternado.edu.co/index.php/derpen/article/view/965
Utkin, L. V. (s/f). A method for processing the unreliable expert judgments about parameters of probability distributions. Recuperado a partir de http://www.levvu.narod.ru/Papers/combpar2.pdf
Whitman, M., & Mattord, H. (2011). *Principles of Information Security*.
Williams, F., Austin, S., & Mha, B. (2008). The role of the electronic medical record (EMR) in care delivery development in developing countries: a systematic review. *Informatics in Primary Care*, *16*(2), 139–145. https://doi.org/10.14236/jhi.v16i2.685
World Health Organization. (2006). Electronic Health Records (Manual for developing countries). Recuperado a partir de http://www.wpro.who.int/publications/docs/EHRmanual.pdf
Xiao-Yan, G., Yu-Qing, Y., & Lu, L.-L. (2011). An Information Security Maturity Evaluation Mode. *Procedia Engineering*, *24*, 335–339. https://doi.org/10.1016/j.proeng.2011.11.2652
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*, 75–85. https://doi.org/10.2147/RMHP.S99908