DEPARTAMENTO DE POSGRADOS

MAESTRÍA EN AUDITORÍA INTEGRAL Y GESTIÓN DE RIESGOS FINANCIEROS

Aplicación de la metodología ECU@Risk para la Gestión de Riesgos de la Información en el sector Hospitalario.

Tesis previa a la obtención del Título de

Magíster en Auditoría Integral y Gestión de Riesgos

Financieros

Autor: Ing. Nelly Rosario Ávila Ávila

Director: Mgst. Esteban Crespo Martínez

Cuenca, Ecuador 2018

Dedicatoria

“No hay distancia que no se pueda recorrer, ni meta que no se pueda alcanzar”

Las luces y los nuevos desafíos de este trabajo de investigación, que impulsan hacer de la gestión, la calidad y la información procesos de servicio a la comunidad hospitalaria; dedico a mi hijo Saúl Francisco, porque ha sido la primordial inspiración y motivación, para no detenerse en el camino, procurando siempre darle con sencillez el ejemplo de esfuerzo, dedicación y superación, como herramientas imprescindibles para construir en él, un ser humano auténtico para la sociedad; porque en el camino no hay obstáculos que puedan detener nuestro sueños.

Agradecimientos

Con la alegría del deber cumplido, doy gracias a Dios por las posibilidades que me brinda cada día para crecer como ser humano y servir mejor a la sociedad. Gracias a mi familia, por ser la impulsora en la primicia de este reto; un especial agradecimiento a mi director de tesis Ing. Esteban Crespo M., por el apoyo constante y el valioso aporte para continuar el camino emprendido y llegar a la meta.

Gracias a los señores catedráticos y compañeros que contribuyeron significativamente con fundamentos y valores humanos para el feliz término de este trabajo realizado con sacrificio y perseverancia.

Resumen

La información es uno de los activos más valiosos dentro de las organizaciones, y más aún en la actualidad, debido al avance de las ciencias computacionales. Esto conlleva a que información crítica esté al alcance de personas que no cuenten con la debida autorización. Este trabajo tiene como finalidad evaluar la metodología ECU@risk en una de las entidades del sector hospitalario. Esta metodología está basada en los principios de administración del riesgo y es una guía de aplicación de un Sistema de Gestión de Seguridad de la Información (SGSI), que permite identificar activos, amenazas determinar el nivel de riesgo al que se expone la información existente de la entidad, para posteriormente dar paso a posibles salvaguardas que puedan implementarse para evitar la materialización del riesgo.

Palabras clave: seguridad, información, ECU@risk, SGSI, riesgo.

ABSTRACT

Information is currently one of the most valuable assets within organizations due to advances in computer science. This had led to critical information available to people without proper authorization. The purpose of this work was to evaluate the ECU@risk methodology in one of the entities of the health sector. This methodology was based on the principles of risk management and constituted a guide for the application of an information security management system (ISMS). This made it possible to identify assets, threats and to determine the risk level that the information of the entity could be exposed to. Subsequently, safeguards that could be implemented to avoid the materialisation of risks.

Keywords: Security, information, ECU@risk, ISMS, risk.

UNIVERSIDAD DEL AZUAY
Dpto. Idiomas

Translated by

Ing. Paul Arpi

Contenido

Índice de Ilustraciones

Índice de Tablas

Introducción

Siendo la información y comunicación un componente del sistema de control interno, ésta debe cumplir con los principios de: *confidencialidad* (sea utilizada por los procesos autorizados), *integridad* (no sea modificada) y *disponibilidad* (cuando el proceso lo requiera).

Tomando en cuenta que la información es un recurso de mucha importancia como el resto de los activos, el uso y la protección de la misma requiere un gran esfuerzo para las organizaciones, ya que de ésta depende el buen funcionamiento en todos los procesos y la continuidad del negocio.

Este trabajo tiene como finalidad evaluar la metodología ECU@risk en una de las entidades del sector hospitalario. Esta metodología está basada en los principios de administración del riesgo y es una guía de aplicación de un Sistema de Gestión de Seguridad de la Información (SGSI).

El contar con un sistema de gestión de seguridad de la información, hace que la entidad cuente con salvaguardas para prevenir o minimizar los riesgos, de esta manera la entidad podrá lograr sus objetivos y dejar una buena imagen a los usuarios.

Para el desarrollo de este trabajo se partirá de un análisis situacional de la gestión de la información en una organización del sector hospitalario, lo que permitirá determinar ventajas y falencias en el manejo y cuidado de ésta.

Se analizará el proceso de gestión de riesgo de la información, para determinar el nivel de riesgo existente, y con la propuesta de la metodología ECU@Risk para la Gestión de Riesgos de la Información, abordar los mismos en torno a la seguridad de la información, lo que permitirá sugerir medidas para identificar, controlar y mitigarlos.

1 Estado del arte

Se vive en un mundo globalizado, y el avance de la tecnología, el internet y las redes sociales hacen que la información ya no la dispongamos solamente a través de un papel impreso o escrito, o mediante una conversación, sino que la podemos almacenar, procesar, o transmitir a través de un formato electrónico, presentar mediante imágenes o mensajes digitales. Es así que existe un número cada vez mayor de personas que tienen acceso a la información que podría ser crítica, ya que el manejo de la misma se vuelve más complejo porque está aún más expuesta al enfrentar las diferentes amenazas. Por lo tanto, la información sin importar la forma o el estado como se presente, requiere que se cumpla con una serie de medidas de protección que sean adecuadas según su importancia y criticidad para lograr la seguridad de la información.

Siendo la información y comunicación un recurso invaluable y uno de los componentes de control interno, muchas de las organizaciones no lo consideran como tal, es así que en sus empresas no le dan la debida importancia y su debido tratamiento, teniendo como resultado información mal dirigida en los procesos o simplemente sin saber a quién dirigir dicha información.

Como es de conocimiento en todos los procesos de las organizaciones siempre está presente el riesgo, *que es la probabilidad de que se produzca un evento cuyas consecuencias son negativas y que está conformado por dos factores, la amenaza y la vulnerabilidad* (CIIFEN, s.f.). Este riesgo supone la fuga de información sensible, ya sea por personas de la misma organización o por terceras personas que pueden acceder como un mecanismo de ataque con fines fraudulentos.

Por lo tanto, los líderes de las organizaciones son los responsables de la correcta gestión que realicen para una adecuada administración de los riesgos, la misma que facilitará el logro de los objetivos planteados y la continuidad del negocio.

1.1 COSO III (Committee of Sponsoring Organizations of the Treadway Commission)

COSO se dedica a desarrollar marcos y orientaciones generales sobre el control interno, la gestión del riesgo empresarial y la prevención del fraude, diseñados para mejorar el desempeño organizacional y la supervisión, y reducir el riesgo de fraude en las organizaciones. (González Martínez , s.f.)

Este Marco Integrado de Control Interno fue creado para las organizaciones de los Estados Unidos, pero ha sido aceptado a nivel mundial porque facilita a las empresas los procesos de evaluación y mejoramiento continuo de sus sistemas de control interno. Así mismo a través de sus políticas y reglas ayudan a las organizaciones a mejorar las actividades de control para alcanzar los objetivos planteados.

1.1.1 Objetivos

1. Aclarar los requerimientos del control interno;

2. Actualizar el contexto de la aplicación del control interno a muchos cambios en las empresas y ambientes operativos; y

3. Ampliar su aplicación al expandir los objetivos operativos y de emisión de informes. (González Martínez , s.f.)

COSO III está formado por 5 componentes y 17 principios que son:

1.1.2 Componentes

- Entorno de control
- Evaluación de riesgos
- Actividades de control
- Sistemas de información
- Supervisión del sistema de control (Monitoreo) (Crespo Martínez P. , 2016)

1.1.3 Principios

1: La organización demuestra compromiso con la integridad y los valores éticos

2: El consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno

3: Establece estructura, autoridad y responsabilidad

4: Demuestra compromiso para la competencia

5: Hace cumplir con la responsabilidad

6: Especifica objetivos relevantes

7: Identifica y analiza los riesgos

8: Evalúa el riesgo de fraude

9: Identifica y analiza cambios importantes

10: Selecciona y desarrolla actividades de control

11: Selecciona y desarrolla controles generales sobre tecnología

12: Se implementa a través de políticas y procedimientos

13: Usa información relevante

14: Comunicación interna

15: Comunicación externa

16: Conduce evaluaciones continuas y/o independientes

17: Evalúa y comunica deficiencias (Crespo Martínez P. , 2016)

Estos componentes y principios deben ser aplicados en el sistema de control interno y deben funcionar de manera integrada.

1.2 LA FAMILIA ISO 27000

Para que los administradores de las organizaciones puedan lograr los principales objetivos, la Organización Internacional de Normalización (ISO) nos da a conocer en la familia de las ISO 27000 estándares como guías que servirán para el análisis, implementación, control y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI)

1.2.1 ISO 27001 – Gestión de la seguridad de información de los sistemas - Requisitos

En el año 2005, la Organización Internacional de Normalización publica la ISO 27001:2005, su eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa, basándose en la gestión de riesgos, es decir investigar en donde están los riesgos para luego tratarlos sistemáticamente. (ISO 27001, s.f.)

El objetivo de la ISO 27001 es proporcionar una metodología universal para la implementación, administración y mantenimiento de la seguridad de la información dentro de una organización, a su vez proporciona un modelo para establecer, implantar, operar, monitorear y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la implementación de controles de seguridad según las necesidades individuales de cada organización, por lo tanto esta norma describe cómo gestionar la seguridad de la información en una empresa. (ISO 27001, s.f.)

Esta Organización publica en el año 2013 su más reciente revisión de la norma ISO 27001, ahora su nombre completo es Norma ISO/IEC 27001:2013 Information security management systems – Requirements; sin embargo, la norma no ha cambiado su filosofía principal que es evaluar y tratar los riesgos manteniendo sus fases del ciclo que son: Planificación, Implementación, Revisión y Mantenimiento (PDCA, por sus siglas en inglés). (ISO 27001, s.f.)

Este estándar internacional es desarrollado como una guía para el análisis, implementación, control y mantenimiento de un Sistema de Gestión de Seguridad de la información (SGSI). Su enfoque está orientado a los procesos de negocios, por lo tanto, se adapta a los diferentes giros del negocio y a los activos de la información que éstos puedan tener, permitiendo a las organizaciones la evaluación del riesgo que le ayuda a identificar los eventos que pueden ocurrir y mediante la aplicación de controles planifica la manera más adecuada para tratar mitigar o eliminar los riesgos.

Como lo menciona (Collazos Balaguer, s.f.) en su artículo llamado “La nueva versión ISO 27001:2013”, obtenido de “Un cambio en la integración de los sistemas de gestión”, *la información es un recurso que, como el resto de los activos, tiene valor para una organización y por consiguiente debe ser debidamente protegida.*

La seguridad de la información protege a ésta de una amplia gama de amenazas, realizando una evaluación de los riesgos a través de una investigación de cuáles podrían ser los problemas potenciales que podrían afectar la información, a fin de garantizar la continuidad del negocio, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

Por lo tanto, el Sistema de Gestión de Seguridad de la Información debe cumplir con los 3 principios fundamentales que son:

1. **Confidencialidad:** la información no debe ser revelada ni estar a la disposición de personas, entidades o procesos que no cuenten con la debida autorización, debe ser utilizada por los procesos autorizados. (ISO 27001, s.f.)

2. **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso no debe ser modificada, y, (ISO 27001, s.f.)

3. **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran, es decir cuando el proceso lo requiera. (ISO 27001, s.f.)

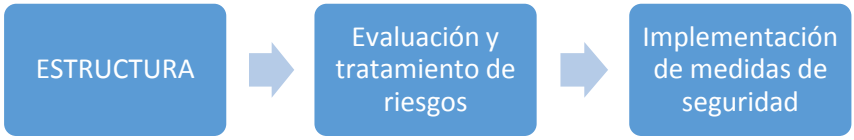

Ilustración 1.Estructura de ISO 27001. Fuente: (ISO 27001, s.f.) Elaborado por el autor.

Un Sistema de Seguridad de la Información forma parte de la gestión global el riesgo, es decir no hace referencia solamente a la seguridad de Tecnologías de la Información - TI (hardware-software), ya que los sistemas informáticos no pueden brindar seguridad de la información por si solos, sino que éstos requieren de la seguridad que los diferentes procesos puedan brindar a la organización, como pueden ser: el proceso de planificación, proceso de la unidad administrativa de talento humano, proceso jurídico, la protección física de los activos, etc.; es decir, se requiere de todos los procesos para asegurar la información.

Hay que tomar en cuenta que existe una gran diferencia entre el concepto de: Ciberseguridad y Seguridad de la Información.

La seguridad de la información se refiere a la información más allá de su formato, incluye:

Documentos, Propiedad digital e intelectual, Comunicación verbal o visual

La Ciberseguridad se refiere a la protección de los activos de la información, incluye:

Redes, Hardware, Software, y la información procesada, almacenada o transportada a través de los sistemas de información que se encuentran interconectados.

1.2.1.1 Beneficios de la implementación de ISO 27001

La norma ISO 27001 puede ser implementada en cualquier tipo de organización, ya sea ésta del sector público o privado, con o sin fines de lucro, es decir puede ser una empresa del grupo de las MPYMES, o una empresa grande.

Mediante la implementación de un SGSI, las organizaciones no solamente obtendrán controles mediante políticas y procedimientos, sino que ISO 27001 detalla también los elementos que serán la base para la determinación de las reglas de la organización necesarias para prevenir infracciones de la seguridad de la información.

Los principales beneficios de la implementación de ISO 27001, son:

1. **Cumplimiento**: Esta norma le ayuda a cumplir con los requerimientos legales según las leyes y reglamentos de cada país, e incluso hay normas de protección de datos, privacidad y control de TI que deben cumplir las empresas, más aún si son empresas del

sector Financiero, Salud o Gubernamental; esta norma les proporciona la metodología correcta para cumplir con los requisitos de manera eficiente.

2. **Obtener ventaja comercial**: Una empresa con certificación ISO 27001 tendrá un valor agregado frente a los competidores, ya que sus clientes tendrán mayor confianza porque su información que puede ser sensible está más segura.

3. **Menores costos**: Con la implementación de ISO 27001 la información de la empresa estará más segura, ya que las políticas y procedimientos implementados ayudarán a minimizar e incluso evitar el riesgo de cualquier tipo y esto será menos costoso que el enfrentar el riesgo cuando se presente.

4. **Una mejor organización**: La implementación de ISO 27001 ayuda a la organización a tener bien definidos los procedimientos porque sus empleados sabrán lo que tienen que hacer y cómo deben hacerlo, evitando así tiempos no productivos por parte del personal de la organización. (ISO 27001, s.f.)

Tabla 1. Contenido de ISO 27001.

No.	Capítulos	Descripción	Objetivos de Control	Documentos y Registros Necesarios	Documentos no Obligatorios de Uso Frecuente
0	Introducción	Objetivo y compatibilidad con otras normas de gestión			
1	Alcance	La norma puede ser aplicada a todo tipo de empresa			
2	Referencias normativas	Referencia a la norma ISO/IEC 27000 como estándar			
3	Términos y definiciones	Referencia a la norma ISO/IEC 27000 como estándar			
4	Contexto de la organización	Define los requerimientos, las partes interesadas, sus requisitos y el alcance del SGSI.	4.1 Comprensión de la organización y su contexto. 4.2 Comprensión de las necesidades y expectativas de las partes interesadas 4.3 Determinación del alcance del sistema de gestión de continuidad de negocios. 4.4 Sistema de Gestión de Continuidad de Negocios.	4.3 Alcance del SGSI	
5	Liderazgo	Definir responsabilidades de la dirección, el Establecer roles y responsabilidades, Normar la política de alto nivel sobre seguridad de la información.	5.1 Liderazgo y compromiso. 5.2 Compromiso gerencial. 5.3 Política. 5.4 Roles, responsabilidades y autoridades de la organización.	5.3 Políticas de seguridad de la información.	
6	Planificación	Define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.	6.1 Acciones para atender los riesgos y las oportunidades. 6.2 Objetivos de continuidad de negocios y planes para lograrlos.	6.1 Metodología de evaluación y tratamiento de riesgos. Declaración de aplicabilidad. Plan de tratamiento del riesgo. 6.2 Objetivos de seguridad de la información.	
7	Soporte	Define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.	7.1 Recursos 7.2 Competencia 7.3 Concientización 7.4 Comunicación 7.5 Información a documentar	7.2 Registros de capacitación, habilidades, experiencia y calificaciones.	7.5 Procedimiento para control de documentos. Controles para gestión de riesgos.
8	Operación	Define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.	8.1 Planificación y control operacional. 8.2 Análisis de impactos de negocios y valuación de riesgos. 8.3 Estrategia de continuidad de negocios. 8.5 Ejercicios y pruebas.	8.2, 8.3 Informe sobre evaluación y tratamiento de riesgos.	

No.	Capítulos	Descripción	Objetivos de Control	Documentos y Registros Necesarios	Documentos no Obligatorios de Uso Frecuente
9	Evaluación del desempeño	Define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.	9.1 Monitoreo, medición, análisis y evaluación. 9.2 Auditoría interna. 9.3 Revisión gerencial.	9.1 Resultados de supervisión y medición. 9.2 Programa de auditoría interna 9.2 Resultados de las auditorías internas. 9.3 Resultados de la revisión por parte de la dirección.	9.2 Procedimientos para Auditoría Interna.
10	Mejoramiento	Define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.	10.1 No conformidades y acciones correctivas. 10.2 Mejoramiento continuo	10.1 Resultados de acciones correctivas.	10.1 Procedimiento para medidas correctivas. (ISO 27001, s.f.)
	Anexo 10	Proporciona un catálogo de 114 controles distribuidos en 14 secciones (secciones A.5 a A.18)		Definición de funciones y responsabilidades de seguridad. Inventario de activos. Uso aceptable de los activos. Política de control de acceso. Procedimientos operativos para gestión de TI. Principios de ingeniería para sistema seguro. Política de seguridad para proveedores. Procedimiento para gestión de incidentes. Procedimientos de la continuidad del negocio. Requisitos legales, normativos y contractuales. Registros sobre actividades de los usuarios, excepciones y eventos de seguridad.	Política Trae tu propio dispositivo (BY OD). Política sobre dispositivos móviles y tele-trabajo. Política de clasificación de la información. Política de claves. Política de eliminación y destrucción. Procedimiento para trabajo en áreas seguras. Política de pantalla y escritorio limpio. Política de gestión de cambio. Política de creación de copias de seguridad. Política de transferencia de la información. Análisis del impacto en el negocio. Plan de prueba y verificación. Plan de mantenimiento y revisión.

Fuente: (ISO 27001, s.f.) *Elaborado por el autor.*

Es importante señalar que, el Anexo A está compuesto por un catálogo de 114 controles de seguridad de la información enumerados en 14 secciones. Este anexo es de mucha importancia para las empresas, ya que les ayuda a determinar qué controles pueden ser aplicables para luego implementar de acuerdo a la necesidad y giro del negocio de las mismas, pues no todos los controles son obligatorios de implementar ni serán necesarios en todas las empresas.

1.2.2 ISO/IEC 27002 – Tecnología de la información – Técnicas de seguridad -

Esta norma, aunque no es certificable, proporciona directrices para la implementación de los controles indicados en ISO 27001, mientras que ISO 27001 especifica 114 controles que pueden ser utilizados para disminuir los riesgos de seguridad, la norma ISO 27002 es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, ésta puede ser de gran utilidad ya que proporciona más información sobre cómo implementar esos controles. (Crespo Rin, 2013) (ISO 27001, s.f.) (ISO 27000)

1.2.3 ISO 27799:2008 Informática sanitaria

La norma 27799 especifica un conjunto detallado de controles y proporciona directrices de buenas prácticas en seguridad de la información sanitaria. Esta norma junto con la norma 27799, definen “qué” se requiere en términos de seguridad de la información sanitaria, pero no dan a conocer el “cómo” se hace para obtener la seguridad de la información. (NTE-INEN-ISO-27799, 2014)

1.2.4 ISO/IEC 27004 – Medición para la seguridad de la información

Esta norma proporciona técnicas para la medición de la seguridad de la información; tiene relación con ISO 27001 ya que explica cómo determinar la eficacia de un SGSI y de los controles relacionados comprobando de esta manera si el SGSI ha alcanzado los objetivos planteados. (ISO 27001, s.f.)

1.2.5 ISO/IEC 27005:2011 - Gestión de riesgos de la Seguridad la Información

Esta norma es aplicable a todo tipo de organización que tienen como finalidad gestionar los riesgos, pues proporciona las directrices necesarias para la aplicación satisfactoria de gestión de riesgos de seguridad de la información. Se complementa con ISO 27001 porque proporciona más información sobre cómo evaluar y tratar los riesgos, considerada la etapa de mayor desempeño en su implementación.

1.3 Otras normas relacionadas con seguridad de la información

1.3.1 ISO 31000:2009 GESTIÓN DEL RIESGO - Principios y directrices -

La norma **ISO 31000:2009** (noviembre 2009). Su objetivo es el establecer una serie de principios para una eficaz gestión de riesgos. Impulsa al desarrollo, la implementación y la mejora continua que una empresa debe desarrollar, vinculando la gestión de riesgos en el gobierno corporativo organizacional.

Una de las etapas que forman parte de la gestión de riesgos según esta norma, es la etapa de evaluación o apreciación del riesgo, la misma que permite identificar la afectación de los objetivos al materializarse un riesgo.

La apreciación del riesgo trata de dar respuesta a las siguientes preguntas claves:

- ¿Qué puede suceder y porque (para la identificación del riesgo)?
- ¿Cuáles son las consecuencias?
- ¿Cuál es la probabilidad de su ocurrencia futura?
- ¿Existen factores que mitiguen las consecuencias del riesgo o que reduzcan la probabilidad del riesgo? (González, 2016)

Esta apreciación del riesgo tiene como finalidad, proporcionar evidencias basadas en información y análisis, para tomar las decisiones adecuadas sobre cómo tratar los riesgos. Por lo tanto, esta norma ayuda a las empresas cualquiera sea su tamaño a realizar una efectiva gestión de riesgos. (López Jaramillo & Vásquez Mejía, 2016)

1.3.2 ISO 9001:2015 Gestión del Riesgo - Estructura de Alto Nivel-

Esta norma está diseñada para orientar a las empresas a basarse en un enfoque de prevención en lo que se refiere a la gestión del riesgo, las mismas que deben reconocer los riesgos dentro de la organización y tomar las medidas necesarias y correctivas para evitar que se materialicen dichos riesgos.

Esta norma incorpora el enfoque basado en riesgos para que cuando las empresas incorporen los sistemas de gestión que proporciona la norma ISO: 2008, deberán incluir los métodos o procedimientos para evaluar, administrar, tratar, eliminar y/o minimizar los riesgos así como dicta esta norma.

1.3.3 ISO 22301 Societal Security - Seguridad de la Sociedad -

Define los requerimientos y proporciona el mejor marco de referencia para gestionar la continuidad del negocio en una organización, se relaciona con ISO 27001 porque existe un punto de esta norma que requiere la implementación de la continuidad del negocio.

La gestión de continuidad del negocio disminuirá la probabilidad de que se produzca un suceso negativo, pero en caso de producirse, la organización está preparada para responder y reducir el daño que pueda ocasionar.

1.4 La gestión del riesgo

La gestión del riesgo es un conjunto de técnicas y herramientas de apoyo y ayuda para tomar las decisiones apropiadas, de una forma lógica, teniendo en cuenta la incertidumbre, la posibilidad de futuros sucesos y los efectos sobre los objetivos acordados; y tiene como

objeto la prevención de los mismos en lugar de la corrección y la mitigación de daños una vez que éstos se han producido, por lo que resulta claramente ventajoso para las organizaciones que adopten y pongan en uso herramientas y mecanismos de gestión de riesgos. (Gonzalez, 2015)

Por lo tanto, la gestión de riesgos permitirá el logro de un entorno controlado, minimizando los riesgos hasta niveles aceptables, a través de las medidas de seguridad o salvaguardas que el analista de riesgos decida implementar. Las actividades de la gestión de riesgos se resumen en:

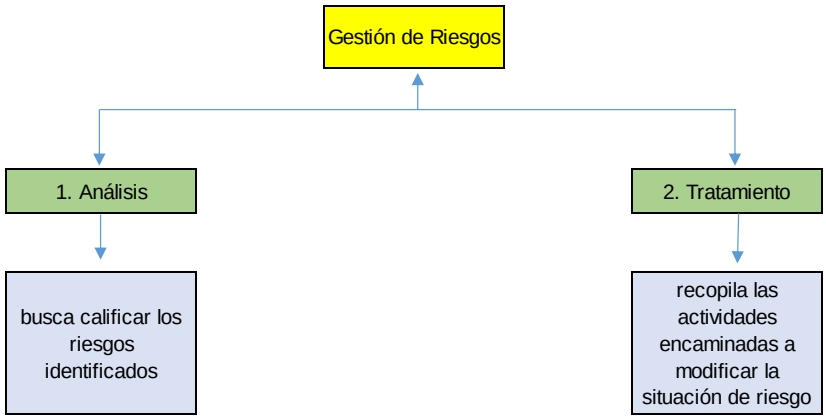

Ilustración 2. Actividades de la gestión de riesgos. Fuente: (ISO 27001, s.f.) Elaborado por el autor

1.5 El análisis y tratamiento de los riesgos

El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas (Crespo Rin, 2013). Forma parte de las actividades de planificación, en donde se toman las decisiones de tratamiento de los riesgos.

El análisis de riesgos es el proceso constante que estima la cantidad de riesgos al que está expuesta la empresa, y a su vez determina impactos y probabilidad, sabiendo lo que puede suceder al materializarse el riesgo, así como también las medidas de seguridad o salvaguardas que se puedan determinar para evitar, reducir o trasladar el riesgo. Estas medidas de seguridad son responsabilidad de todo el personal a cargo de los sistemas de información.

El análisis y el tratamiento de los riesgos son las tareas de la gestión de riesgos que deben mantenerse en actividad continua de la gestión de la seguridad. El análisis de los riesgos permite determinar el estado de los activos, su valor, su capacidad, y si éste se encuentra protegido; de esta manera se puede elaborar un plan de seguridad a través de la implantación de medidas, controles o salvaguardas, que, alineado con los objetivos de la organización pueden determinar el nivel de riesgo que la organización puede aceptar.

El plan de seguridad diseñado por los responsables de la seguridad de los activos, lo debe conocer todo el personal de la organización que trabaja con el sistema de información, ya que es el personal el responsable de las operaciones y actividades que manejan en el día a día de la organización con el fin de determinar el cumplimiento de los objetivos planteados.

El análisis de riesgos considera los siguientes elementos:

1. Activos, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización.

2. Amenazas, que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización.

3. Salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen daños considerables.

Con estos elementos se puede estimar:

1. el impacto: lo que podría pasar

2. el riesgo: lo que probablemente pase (Magerit 1, 1997)

1.5.1 Método de análisis de riesgos

El análisis de riesgos es una aproximación metódica, y debe seguirse los siguientes pasos para determinar el riesgo.

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de que perjuicio supondría su degradación, tomando en cuenta que en un sistema de información hay dos cosas esenciales para determinar la valoración de los activos: la información que maneja y los servicios que presta.

2. Determinar a qué amenazas están expuestos aquellos activos, definiéndole a las amenazas como aquellas cosas que les puede pasar a los activos causando un perjuicio para la organización.

3. Determinar qué salvaguardas hay dispuestas y cuan eficaces son frente al riesgo, siendo las salvaguardas medidas de protección que puedan tomar los responsables de la seguridad.

4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza, es decir lo que podría pasar.

5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza, es decir lo que probablemente pase. (Magerit 2, 2006)

1.6 Metodologías de la gestión de riesgos

Un método es un procedimiento o proceso sistemático y ordenado que se utiliza para alcanzar algún objetivo preciso a través de un conjunto de estrategias y herramientas.

Una metodología consiste en un conjunto de métodos, técnicas y herramientas. No contiene métodos específicos; sin embargo, lo especifica por procesos que conforman el marco de gestión de riesgo.

La metodología cualitativa es la más utilizada para el análisis de riesgos y cumple con los requisitos de ISO 27001. El nivel de riesgo se basa en niveles de probabilidad e impacto. (Molina Miranda , 2015)

1.6.1 COBIT (Control Objectives for Information and related Technology)

Es un conjunto de propósitos definidos y controles de TI, que tiene como principio la implementación de un marco para el gobierno y gestión de TI.

Su última versión está enfocada a la seguridad de la información (COBIT 5 for Information Security). Es una nueva versión del ya conocido estándar para el cumplimiento de objetivos de control. Esta versión, profundamente revisada y mejorada, provee un marco de referencia integral que contribuye en la organización al logro de los objetivos y entrega de valor a través de un efectivo gobierno y gestión de la TI empresarial. (Crespo Martínez P. , 2016)

El propósito de su creación fue el ayudar a las organizaciones a obtener el valor óptimo de TI, orientados a la realización de beneficios, la utilización de los recursos y los niveles de riesgos asumidos; y puede ser aplicada en las organizaciones sean éstas públicas o privadas, pequeñas o grandes.

Con la intención de proteger los datos, otros activos y en general el negocio, COBIT 5 tiene como base el entorno de trabajo de mejores prácticas, las mismas que son medidas de seguridad para la protección de la información en todos los niveles de las organizaciones. Así mismo plantea la idea de que la seguridad de la información es una disciplina transversal, por lo que considera aspectos de protección de datos en cada actividad y proceso desempeñado, brindando una guía básica para definir, operar y monitorear un sistema para gestión de la seguridad.

COBIT 5 determina cinco principios fundamentales para la gestión de tecnologías de la información de las empresas, los mismos que se deben cumplir para que la organización obtenga el uso de las tecnologías de la información de manera eficiente y eficaz. Los principios son:

Ilustración 3. Principios de COBIT 5. Fuente: (Velásquez Pérez, Puentes Velásquez, & Pérez Pérez, 2015)

COBIT está formado por 7 habilitadores de gestión, que se preocupa en tomar los controles técnicos y acoplarlos a los requerimientos del negocio (Crespo Martínez P. , 2016)

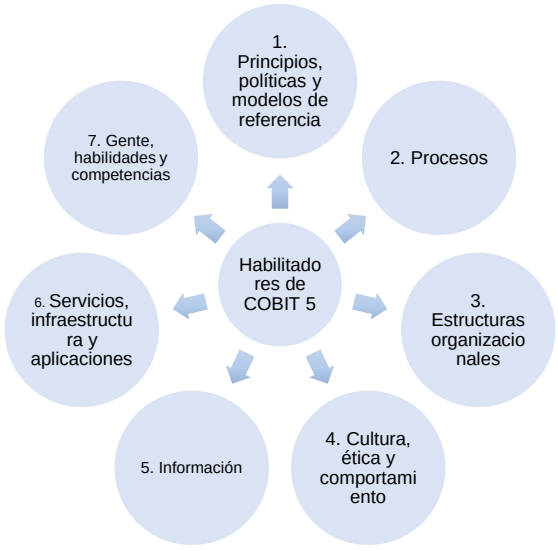

Ilustración 4. Habilitadores de COBIT 5. Fuente: (Crespo Martínez P. , 2016)

1.6.2 MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Creada por el Consejo Superior de Administración Electrónica, en el año 1997 llamada Magerit 1, la misma que ofrece una aplicación para el análisis y gestión de riesgos de un Sistema de Información, cuyo objetivo es disminuir los riesgos mediante el uso y la implantación de las tecnologías de la información, enfocada a las Administraciones Públicas.

En el año 2006, publica la segunda versión Magerit 2, lo plantea como una revisión constructiva que le permite mejorar la primera versión y como consecuencia de la creciente utilización de las tecnologías de la información. (Magerit 2, 2006)

Su más reciente actualización es la publicada en el año 2012, en su versión Magerit 3, la misma que tiene un mayor acercamiento a la normativa ISO, la misma que busca integrar las actividades de análisis de riesgos en el marco organizacional de gestión de riesgos.

La metodología Magerit V3, está compuesta por 3 libros como son:

Libro I: Método.- Explica detalladamente cuales son las tareas para realizar el Análisis y la Gestión de Riesgos.

Libro II: Catálogo de Elementos.- Se encuentra explicados detalladamente los tipos de amenazas y salvaguardas.

Libro III: Guía de Técnicas.- Explica cómo se calcula los riesgos.

Partiendo del concepto de riesgo, que según la metodología Magerit dice: *Riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos, causando daños o perjuicios a la organización.* (Magerit 3, 2012) (Crespo Rin, 2013)

El riesgo indica lo que puede suceder a los activos si no se protegen adecuadamente, por lo tanto los responsables de la seguridad de los sistemas de información deben conocer los problemas que puede ocasionar la falta de seguridad de los mismos, ya sea porque un sistema puede colapsar, por daños malintencionados o por un desastre natural que podría ocurrir; éstos deben estar protegidos, porque cualquier evento que se pueda dar, su resultado se verá expresado en valores económicos y/o afectar la imagen de la organización.

Objetivos de Magerit

1. Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de eliminarlos a tiempo.

2. Ofrecer un método sistemático para analizar tales riesgos.

3. Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

4. Preparar a la organización para los procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso. (Magerit 2, 2006) (Molina Miranda , 2015)

Proceso de Magerit

El proceso de Magerit consta de 4 etapas:

1. Planificación.- Definición de objetivos y planificación de los medios naturales y humanos para la realización y lanzamiento del proyecto.

2. Análisis de Riesgos.- Identificación y valoración de los diferentes elementos de riesgo.

3. Gestión de Riesgos.- Identificación de las posibles funciones de servicios y salvaguarda reductores del riesgo calculado.

4. Selección de Salvaguardas .- Es esta etapa es necesario seguir los siguientes pasos:

    1. Seleccionar los mecanismos de salvaguarda a implantar.

    2. Elaborar una guía del plan de implantación.

    3. Establecer los procedimientos de seguimiento para la implantación.

    4. Recopilar la información necesaria para obtener los productos finales del proyecto.

    5. Realizar la presentación de los resultados. (Magerit 1, 1997)

Por lo tanto esta metodología es una herramienta para que las organizaciones puedan implementar en la búsqueda de la gestión del riesgo, la misma que tiene que entender que la seguridad es un proceso que nunca termina, tomando en cuenta que la seguridad de la información no es competencia única de Tecnologías de la Información, ésta debe fluir desde la alta gerencia hacia todos los procesos de la organización.

1.6.3 CRAMM-CCTA: Risk Analysis and Management Methodology

CRAMM es una metodología de análisis y la gestión de riesgos desarrollado por el Centro de Informática y la Agencia Nacional de Telecomunicaciones del Reino Unido. Data desde 1987 y su versión vigente es la 5.2. Tienen una alta preferencia en el sector público, pero que también es utilizada por el sector privado en organizaciones de gran tamaño.

Metodología que aplica los conceptos de manera formal, estructurada y disciplinada; y que está orientada a proteger la confidencialidad, integridad y disponibilidad de un sistema de información y de sus activos, y utiliza evaluaciones cuantitativas y cualitativas, por esta razón se le denomina como una metodología de carácter mixto. (Crespo Rin, 2013)

Esta metodología incluye una amplia gama de herramientas de evaluación del riesgo, por lo que es aplicable a todo tipo de sistemas y redes de información, mediante las tres etapas del ciclo de vida del sistema de información; las mismas que son:

Etapa 1: Identificación y valoración de activos

Esta etapa le permite al analista identificar, clasificar y valorar los activos de TI, en:

1. activos físicos (hardware y las instalaciones)
2. software y aplicaciones (paquetes de aplicaciones)
3. datos (información contenida en los sistemas)

Los activos físicos se valoran se valoran en términos de coste de reemplazo y los activos de software y datos se valoran en términos del impacto que se produciría si la información no estuviera disponible, fuera destruida, divulgada o modificada. (Crespo Rin, 2013)

Etapa 2: Evaluación de amenazas y vulnerabilidad

En esta etapa identifica las áreas de debilidad o de mayor exposición al riesgo y la probabilidad de ocurrencia que se produzca un problema.

Etapa 3: Selección y recomendación de contramedidas

Con el resultado del análisis de riesgos, esta metodología cuenta con una serie de contramedidas para la gestión de los riesgos identificados, para de esta manera disminuir el riesgo de que los sistemas de información se vean afectados; y será el analista de riesgos el que decida las contramedidas a implementar.

1.6.4 OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Evaluación de Amenazas Operacionalmente Críticas, Activos y Vulnerabilidades

Metodología de análisis de riesgos que está orientada a los activos, desarrollado por el CERT (Coordination Center, del Software Engineering Institute de la Universidad Carnegie Mellon de Pensilvania, Estados Unidos), orientada a agilitar y optimar el proceso de evaluación de riesgos de seguridad de la información con el propósito de vincular los objetivos y metas de la misma. (Crespo Rin, 2013)

En este metodología los activos se dividen en dos grupos: Sistemas (hardware, software y los datos) y las personas, los mismos que están ordenados según la importancia que tienen para el logro de los objetivos, esto es: según las posibles amenazas y según las vulnerabilidades a las que están expuestos los activos; y según el impacto que causaría un problema en cada activo al materializarse un riesgo.

OCTAVE tiene dos objetivos específicos que son:

1. Desmitificar la falsa creencia de que la seguridad informática es un asunto meramente técnico.

2. Presentar los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos. (Crespo Rin, 2013)

Estos objetivos van direccionados a dos aspectos diferentes: riesgos operativos y prácticas de seguridad, es decir esta metodología se enfoca en el desarrollo de una perspectiva de seguridad, con el objetivo de que la organización tome decisiones para todos los niveles y así asegurar que las soluciones se implementen con facilidad. Esto permite a que la organización tome las debidas medidas para proteger los activos de información, y así evitar que los riesgos de confidencialidad, integridad y disponibilidad a los que están, se materialicen.

1.6.5 La Metodología Ecu@Risk

La metodología Ecu@Risk está basada en los principios de la administración de riesgos, provista por los estándares ISO 31000:2009, y en las mejores prácticas de seguridad de la información: ISO 27001, ISO 27002 e ISO 27005, además del estudio de las principales metodologías internacionales usadas para la gestión del riesgo y seguridad de la información. (Crespo Martínez P. , 2016)

Esta metodología provee de manera detallada los principios y procesos que son necesarios para identificar y valorar los activos y las amenazas, calcular los riesgos, identificar las contramedidas y el establecer políticas de seguridad.

Tabla 2. Principios de Ecu@Risk.

Principios	¿Qué pretende garantizar?
Crear y proteger el valor	La metodología desarrollada desde el punto de vista universitario puede perseguir objetivos estratégicos demostrables mediante la investigación, el aprendizaje y la enseñanza, su cooperación con la industria, y la participación de la comunidad.
Es una parte integral de los procesos organizacionales	El riesgo siempre está presente en todos los procesos. Es así que la metodología de gestión de riesgo debe considerar adaptarse a la gobernabilidad, las estrategias empresariales y operacionales, la planeación y la gestión, las políticas, los valores y la cultura.
Es parte de la toma de decisiones	El personal de la organización, debe conocer que la empresa u organización es liderada generalmente por su Gerente General o por un Director General, ejecutivos que son los responsables de tomar decisiones en base a correctos elementos de juicio, además de priorizar las acciones, y reconocer que cualquier alternativa tomada tiene sus con-secuencias.

Principios	¿Qué pretende garantizar?
Es sistemática, estructurada y temporal	El riesgo se debe tratar de forma ordenada, estructurada, y saber que tiene fecha de caducidad. Una metodología debe ser consistente, clara y que permita alcanzar resultados comparables y confiables.
Está basada en la mejor información disponible	En base al juicio y discernimiento, quienes toman las decisiones deben considerar la información disponible, la experiencia, los pronósticos y la retroalimentación de la parte interesada.
Debe ser adaptada en el contexto interno y externo	Los responsables considerarán los mandatos legales y operacionales, los requisitos y expectativas de las entidades reguladoras tanto internas como externas, auditores, proveedores de fondos, de gobierno, autoridades y organismos; y dar cuenta de los planes estratégicos institucionales y su perfil de riesgo.
Considera factores humanos y culturales	Una metodología debe considerar las capacidades, percepciones e intenciones del usuario interno y externo, que pueden facilitar o entorpecer el alcance de los objetivos empresariales.
Es transparente e inclusiva	La gestión de riesgo debe ser transparente para la parte interesada, las entidades de control y los tomadores de decisiones.
Es dinámica, iterativa y sensible al cambio	Debe responder constantemente a los cambios. Para ello, debe ser evaluada permanentemente.
Facilita la implementación continua de la organización	Es inminente que una metodología para la gestión de riesgo debe trabajar a la par con las estrategias empresariales, a manera de apoyar a la empresa a alcanzar los objetivos que podrían verse impedidos debido a los riesgos y amenazas de entorno que se presentan. Por ello, es mandatorio el comunicar constantemente los eventos relacionados con la gestión de riesgos.

Fuente: (Crespo Martínez P. , 2016)

Procesos de gestión de Ecu@Risk

Esta metodología se compone de 7 procesos de gestión, 1 proceso de monitoreo y control, y 1 proceso comunicacional; este proceso de gestión será de mucha importancia para las organizaciones en su afán de asegurar la información.

Proceso 1: Determinación del contexto

Consta en determinar lo siguiente:

- Tipo de organización
- Tamaño de la organización
- Alcance de la investigación
- Objetivos
- Partes interesadas y/o involucradas
- Factores internos o externos
- Identificar el contexto interno de la empresa (Crespo Martínez P. , 2016)

Proceso 2: Identificar los activos de información

Se refiere a cualquier elemento que contenga información. Según esta metodología los grupos de activos de información a considerar, son:

- (ED) Edificaciones
- (HW) Hardware
- (SW) Software
- (IE) Informática electrónica
- (IP) Información en papel
- (Extraíble) Medios de almacenamiento extraíble
- (IC) Infraestructura de comunicaciones
- (RRHH) Recursos humanos (Crespo Martínez P. , 2016)

Ecu@Risk señala que es importante que la organización registre a cada activo de información de acuerdo a cada una de sus categorías y deberán ser valorados conforme a las dimensiones de valoración, las mismas que se detallan a continuación:

Disponibilidad: Propiedad o característica de los activos que consiste en el libre acceso y cuando lo requieran las entidades o procesos debidamente autorizados.

Integridad: Propiedad o característica consistente en que el activo de información no ha sido modificado por personas sin autorización.

Confidencialidad: Propiedad o característica consistente en que la información debe estar a disposición y se revelada solamente por las personas y procesos autorizados.

Luego de determinar las dimensiones de valoración de los activos de información, esta metodología valora a los activos de información de acuerdo a los criterios de valoración, pudiendo ser una valoración cuantitativa como cualitativa, y considera los siguientes puntos:

- Usar una escala común para todas las dimensiones, permitiendo comparar riesgos,
- Usar una escala logarítmica, centrada en diferencias relativas de valor, y no en diferencias absolutas, y;

- Utilizar un criterio homogéneo que permita comparar análisis realizados por separado. (Crespo Martínez P. , 2016)

Tabla 3. Criterios de valoración de los activos de información.

VALOR	CRITERIO	
10	Extremo	daño extremadamente grave
9	Muy alto	daño muy grave
6-8	Alto	daño grave
3-5	Medio	daño importante
1-2	Bajo	daño menor
0	Despreciable	irrelevante a efectos prácticos

Fuente: (Crespo Martínez P. , 2016)

Proceso 3: Identificación de los riesgos

Para la identificación de los riesgos, Ecu@Risk plantea las siguientes preguntas:

- ¿Qué puede pasar?
- ¿Cómo puede pasar?
- ¿Dónde puede suceder?
- ¿Cuál podría ser el impacto?

La metodología señala que es importante proporcionar datos cualitativos o cuantitativos, los mismos que pueden basarse en datos o hechos históricos, la experiencia del personal y la opinión de los expertos. Esto ayudará a determinar y calificar el riesgo.

Es importante también para la organización la identificación de amenazas, las mismas que pueden afectar la imagen de la organización y la continuidad del negocio. (Crespo Martínez P. , 2016)

Proceso 4: Análisis de los riesgos

Luego de la identificación del riesgo, se deberá considerar las fortalezas y debilidades de los sistemas y procesos encargados de controlar el riesgo.

Se deberá determinar la eficacia de los controles ya implementados y verificar que éstos puedan mitigar el impacto del riesgo, luego se deberá realizar una evaluación probabilística de la ocurrencia del riesgo y sus consecuencias si se materializa para determinar si el riesgo es aceptable o necesita otras medidas de control, esta evaluación de realiza a través de la siguiente matriz.

Tabla 4. Matriz de riesgos

Matriz de Riesgos						
		Consecuencias				
		1. Leve	**2. Menor**	**3. Moderado**	**4. Alto**	**5. Extremo**
Probabilidad	**E = Casi certero (frecuente)**	M	M	A	E	E
	A = Probable	B	M	A	A	E
	M = Posible	B	M	M	A	A
	B = No muy común	B	B	M	M	A
	L = Raro	L	L	B	B	M

Fuente: (Crespo Martínez P. , 2016)

Proceso 5: Evaluación de los riesgos

Este proceso consiste en decidir cuáles de los riesgos son aceptables o inaceptables, esta decisión hace referencia a la disposición de la organización a tolerar el riesgo, o asumir el riesgo luego de ser tratado. La metodología detalla las siguientes decisiones sobre acciones futuras que se podrían tomar.

- No emprender o continuar con el evento, actividad, proyecto o iniciativa
- Tratar activamente el riesgo
- Priorizar las acciones necesarias, si el riesgo es complejo y se requiere un tratamiento
- Aceptar el riesgo (Crespo Martínez P. , 2016)

Para que un riesgo sea aceptable o tolerable, deberá estar dentro de las siguientes circunstancias:

- No se dispone de tratamiento
- Los costos del tratamiento son prohibitivos (particularmente relevante con referencia a riesgos de bajo impacto)
- El nivel de riesgo es bajo y no justifica el uso de los recursos para tratarla
- Las oportunidades involucradas superan significativamente las amenazas (Crespo Martínez P. , 2016)

Con este proceso de evaluación de riesgos se identifican consecuencias potenciales que pueden ser analizadas en el proceso de tratamiento de riesgos. Por lo tanto, la identificación, el análisis y la evaluación del riesgo forman la fase de evaluación de riesgos en el proceso de gestión de riesgos, estos pasos son fundamentales y se adaptan bien en un proceso estructurado y sistemático.

Proceso 6: Tratamiento de los riesgos

Los niveles de aceptación de riesgo, luego del análisis de los resultados de la matriz de

riesgo de esta metodología, son:

Tabla 5. Nivel de riesgo-Acción de gestión requerida

Niveles de riesgo	Acción de gestión requerida
Riesgo Extremo (E)	Requiere respuesta y atención inmediata
Riesgo Alto (A)	Debe otorgárselo la atención apropiada
Riesgo Medio (M)	Evaluar el riesgo y determinar si los controles implementados son suficientes y si están siendo efectivos
Riesgo Bajo (B)	Administrar mediante procedimientos rutinarios, informar a los gestores locales, supervisar y revisar localmente como sea necesario
Riesgo Leve (L)	Monitoreo constante a las actividades diarias. Registrar eventos en bitácora

Fuente: (Crespo Martínez P. , 2016)

El proceso para el tratamiento de riesgo consta de los siguientes pasos:

Paso 1: En este paso se debe decidir si es necesario un tratamiento específico para el riesgo, o puede ser tratado con el proceso normal de gestión de riesgo mediante los controles implementados.

Paso 2: Se determina cual es el objetivo del riesgo, pudiendo tomar la decisión de evitar, reducir, transferir o aceptar el nivel de riesgo existente.

Paso 3: Luego de conocer el objetivo del tratamiento, se debe identificar y diseñar una opción preferente de tratamiento. Es importante determinar la naturaleza del evento de riesgo y de qué manera se produce, lo cual ayudará a tomar las mejores y más oportunas decisiones de tratamiento de riesgo.

Cualquiera de las decisiones tomadas en el tratamiento de riesgo deben ser debidamente documentadas porque servirán de referencia para evidencias de riesgo futuras.

Paso 4: Este paso evalúa las diferentes opciones de tratamiento y la posibilidad de tolerar el riesgo.

Paso 5: Documentar el plan de tratamiento de riesgo, a través de la identificación de: roles, responsabilidades y cronograma de implementación, el presupuesto, indicadores de desempeño y revisión de procesos apropiados.

Paso 6: Aplicar los tratamientos acordados. Las personas que hayan identificado los riesgos serán las responsables de aplicar el tratamiento de riesgos; de no ser el caso, será el responsable principal del riesgo el encargado de hacerlo.

Paso 7: Luego del tratamiento del riesgo, de determina el nivel de riesgo residual, a través del análisis de la probabilidad y consecuencia de que el riesgo se materialice luego de haber implementado el control.

Proceso 7: Identificación de contramedidas

La importancia de implementar las contramedidas es que éstas permiten mitigar las amenazas y su materialización del riesgo, tomando en cuenta que las contramedidas ligadas a la tecnología necesitan constante actualización, ya que el avance de la tecnología hace que puedan variar. Puede darse cuando:

1. Aparecen tecnologías nuevas
2. Van desapareciendo tecnologías antiguas
3. Cambian los [tipos de] activos a considerar
4. Evolucionan las posibilidades de los atacantes o
5. Evoluciona el catálogo de contramedidas disponibles. (Crespo Martínez P. , 2016)

La selección de las contramedidas que protegerán a los activos de información se seleccionará de acuerdo al análisis de los controles ya implementados en la organización, y luego de realizar el estudio de los posibles elementos de control que podrán ser implementados.

Proceso de monitoreo y control / revisión

Siendo el monitoreo y control parte del proceso de la planificación de la gestión de riesgos, éste es de mucha importancia ya que busca garantizar que los procesos que se encuentran implementados en la organización, sirvan para revisar, evaluar, e informar sobre los riesgos en cada una de las áreas de la organización. Por lo tanto es de vital importancia que los controles implementados sean los adecuados y que éstos permitan identificar los riesgos.

Proceso comunicacional / comunicar y consultar

Este proceso consiste en comunicar de manera efectiva y oportuna a los responsables de la implementación de la gestión de riesgos, sobre las decisiones y razones por las que se seleccionan dichos controles. Esta comunicación puede darse a través de reuniones, reportes, comunicación en línea, etc., cualquiera de los métodos de comunicación tendrán como objetivo asegurar que los riesgos sean identificados oportunamente y éstos sean tratados de manera adecuada y efectiva.

En resumen, la gestión de riesgos está conformada por cuatro grandes etapas: Planificar, Ejecutar, Verificar y Actuar. Por lo tanto, ésta debe integrar todos los procesos que le permitan administrar el riesgo en todos sus niveles de gestión.

De las metodologías analizadas se puede decir que proveen herramientas adicionales para apoyar el trabajo del análisis y la gestión de riesgos, que sirven para proteger e incrementar el valor de un activo de información, tomando en cuenta que la seguridad de la información debe ser un proceso integrado, mediante el uso de controles técnicos, administrativos, físicos y políticas de seguridad de la información; y que éstos puedan garantizar que se cumplan los parámetros de disponibilidad, integridad y confidencialidad de la información.

1.7 Las TIC en el sector salud

Las tecnologías de la información han revolucionado nuestro tiempo, se han ido cada vez más posicionando en todos los ámbitos sin quedarse fuera el sector de la salud, es así que la implementación de las TIC ha dejado de ser algo deseable y se ha convertido en una necesidad. Su evolución ha ido generando cambios en las relaciones empresas, usuarios o consumidores; en la actualidad con la tecnología móvil se facilita el acceso a la información y comunicación desde cualquier lugar a través de aplicaciones, mensajería, chat, sitios web, etc.

En el informe realizado por Telefónica S.A. en su libro *"Las TIC y el sector salud en Latinoamérica"*, señala los retos de la implementación de las TIC en el sector salud en algunos países de Latinoamérica como son: Argentina, Brasil, Chile, Colombia, Ecuador, México, Perú, Uruguay y Venezuela; destacando los siguientes procesos: (Editorial Ariel & Fundación Telefónica, 2008)

Gestión de pacientes.- Información enfocada al paciente.

Historia clínica electrónica.- Es uno de los procesos principales en la aplicación de las TIC. Es una herramienta que brinda mayor información a los profesionales de la salud ya que recopila toda la información referente a los pacientes, la misma que se encuentra de manera legible y disponible, teniendo que el propietario de esta información asegurar la confiabilidad y veracidad.

Sistemas de información Hospitalaria.- Se refiere al flujo de información administrativo-asistencial en los centros de salud, como son: admisiones, centros quirúrgicos, emergencia, consulta externa, laboratorio, RX, etc.

Gestión de imágenes médicas.- La implementación de las TIC son de gran aporte en este proceso porque reduce los costos y los resultados son cargados directamente en la historia clínica del paciente, de esta manera también se logra reducir los errores.

Gestión analítica de laboratorios.- Este proceso se enfoca en la toma de muestras a los pacientes, el tratamiento de los datos y el proceso de la información a través de la historia clínica.

Receta electrónica.- Las TIC han contribuido haciendo más fácil el proceso de prescripción, control y distribución de los medicamentos, tanto al médico, al paciente y al farmacéutico.

Sistemas de citas previas.- Programación de citas médicas tomando en cuenta la disponibilidad de cada especialista. (Editorial Ariel & Fundación Telefónica, 2008)

La Telemedicina.- Según el Doctor Fernando Plazzotta, del Departamento de Informática en Salud del Hospital Italiano de Buenos Aires, define a la Telemedicina como *"la atención médica cuando médico y paciente no coinciden física y/o temporalmente, utilizando tecnologías de información y comunicación",* a través de aplicaciones, correo electrónico, teléfonos inteligentes, comunicaciones inalámbricas, conferencias virtuales, etc. (Chueke, 2015).

La tele medicina traería beneficios importantes en la salud como por ejemplo: la mejora de la calidad diagnóstica y terapéutica, la fiabilidad del mapeo epidemiológico, mejor práctica clínica apoyada en una segunda opinión de los profesionales de la salud, apoyo a los trabajadores de la salud de atención primaria de las zonas rurales, todas estos beneficios contribuyen en la mejora de los sistemas de salud de manera integral. (Bebea, 2013)

La Tele salud .- La Organización Mundial de la Salud (OMS), define a la tele salud como la utilización costo-eficaz y segura de tecnologías de información y comunicaciones ofrecidas a la salud y a los ámbitos relacionados con ella. (IT/USERS, 2018)

Se trata de un proceso transformador sobre la prestación de servicios en este sector. América Latina, ha implementado iniciativas en relación con la tele salud, las mismas que se consolidan en diferentes maneras, como por ejemplo programas nacionales, campañas de prevención de enfermedades, aplicaciones, etc.

Con el transcurso del tiempo se puede observar como el avance de la tecnología ha evolucionado los sistemas de información los mismos que están relacionados según las necesidades de la población y responden a una estructura organizada en la que participan personas, procesos, redes, datos y tecnologías. (Orduña Ortegón, 2014)

Por lo tanto el uso de las tecnologías de información y comunicación en el sector salud, mejoran la eficiencia y garantizan la atención a personas de zonas aisladas de la población, de esta manera también se logra evitar la conglomeración de pacientes en las salas de espera de los hospitales.

La existencia de un sistema de información eficiente y debidamente implementado es una herramienta clave para la toma de decisiones, pues permite un amplio conocimiento por parte de los usuarios ya que manejan el estado de salud de los pacientes. (Orduña Ortegón, 2014)

Según Andrés Fernández Celuer, oficial de Asuntos Sociales en la Comisión de Economía para América Latina y el Caribe, Brasil y México son los países latinoamericanos más adelantados en el desarrollo de tecnologías y programas de salud digital. Colombia, Chile y Uruguay están haciendo esfuerzos para ponerse al día, mientras que otros como Paraguay y Bolivia y algunos centroamericanos están más rezagados en la implementación de un sistema de salud apoyado en la tecnología. (elCOLOMBIANO, 2016)

Es importante señalar que ehCOS (Plataforma y soluciones de eSalud para el mundo), señala las posibles tendencias para el año 2018, en el campo de tecnologías de salud aplicadas al sector salud de Latinoamérica. (ehCOS-, 2018)

En el artículo hace referencia a los cambios políticos que tendrán algunos de los países de Latinoamérica, los mismos que muchas de las veces ofrecen impulsar la modernización del sector de la salud, siendo un gran aporte para la comunidad.

En cuanto a la transformación digital hospitalaria indica que la principal limitación a la implementación de las TIC no es el hardware ni el software sino más bien ésta se encuentra en el brainware que hace referencia a la actitud y capacidad de los líderes y responsables sectoriales quienes deberán hacer un refresh a las viejas prácticas establecidas.

La principal barrera para implementar la interoperabilidad de la Historia Clínica Electrónica en redes de salud en el sector hospitalario público de Latinoamérica, corresponde a la inestabilidad económica, falta de personal especializado, proyectos fracasados y el escaso compromiso de los gobiernos de turno, crean serias dificultades en el proceso de modernización; esto se verá reflejado también en el lento crecimiento pero firme de la Historia Clínica Electrónica en la nube, lo cual es muy diferente para los hospitales privados medianos y pequeños, ya que cuentan con recursos financieros.

Es importante señalar que Uruguay y México, cuentan con un proyecto llamado SINBA el mismo que tiene algunos beneficios en el acceso a la información y puede servir de referente para otros países. Tomando en cuenta que la interoperabilidad de la historia clínica permitiría compartir datos de salud relevantes entre hospitales, universidades, etc., los mismos que serán de mucha importancia para la toma de decisiones de este sector.

Latinoamérica tendrá un impacto considerable en cuanto a inversiones en el sector salud por parte de empresas de EEUU y de Europa. Estas empresas cuentan con un considerable uso de tecnologías de información hospitalarias, lo que proporcionará un incremento en la demanda de soluciones TIC en el sector salud de Latinoamérica. (ehCOS-, 2018)

Mientras que los países latinoamericanos se esfuerzan por ponerse al día en tecnologías de la información, la Federación Española de Empresas de Tecnología Sanitaria (FENIN), la Asociación de Empresas de Electrónica, Tecnologías de la Información y Contenidos Digitales (AMETIC) y la Sociedad Española de Informática de la Salud (SEIS) renuevan su

acuerdo de colaboración para realizar acciones, continuadas en el tiempo, de apoyo a los distintos actores del sistema sanitario, en la implementación de la Salud Digital, dando a conocer las innovaciones tecnológicas, organizativas y de gestión que la industria promueven en este ámbito y los profesionales y pacientes demandan. (Ametic, 2018)

Este acuerdo establecido en el 2015, con el compromiso de colaborar en la búsqueda y el desarrollo de soluciones tecnológicas que mejoren la atención sanitaria y el proceso asistencial, aporta su respectivo conocimiento para impulsar la transformación digital en el sistema sanitario español, modernizarlo y avanzar en su eficiencia y calidad.

En la práctica, el texto propone trasladar el conocimiento y la experiencia de la industria al sistema sanitario nacional dando a conocer innovaciones tecnológicas, organizativas y de gestión, las mismas que establecen seis líneas de trabajo: (Ametic, 2018)

- Sensibilizar sobre el cambio de paradigma del sistema sanitario hacia un modelo centrado en el paciente.

- Definir estrategias que impulsen la adopción de la salud digital.

- Promover modelos de gobernanza que garanticen la calidad y la eficiencia de los recursos destinados a la asistencia sanitaria.

- Analizar los nuevos marcos jurídicos y contractuales que faciliten la adopción de la salud digital y protejan los derechos de los pacientes.

- Impulsar el uso de las TIC como herramientas para empoderar y facilitad la participación activa del paciente en el cuidado de su salud.

- Identificar y difundir las mejores prácticas y experiencias nacionales e internacionales. (Ametic, 2018)

La finalidad de las empresas españolas es servir como referente en la implementación de nuevos modelos de crecimiento en la inversión de tecnologías de la información, como lo es salud digital, tanto para las entidades públicas como privadas. (Ametic, 2018)

1.8 La Ley de Protección de Datos

En América Latina, las leyes de protección de los datos personales nacen por el incremento del uso de las tecnologías de la información y por ende el aumento de las vulnerabilidades asociadas. Esta Ley busca proteger la información con el fin de conservar la honorabilidad de la persona aun cuando ésta hubiese fallecido, cuyo modelo se basa en los derechos humanos de los individuos. (Rojas González , Sánchez Pérez, Toscano Medina , Prudente Tíxtico, & Aguilar Torres, 2012)

Latinoamérica ha ido implementado esta Ley, siendo Brasil el pionero en la implementación de la misma, Brasil (1997), Chile (1999), Paraguay (2000), Argentina (2000), Panamá (2002), Uruguay (2008), México (2010), Perú (2011). (Rojas González , Sánchez Pérez, Toscano Medina , Prudente Tíxtico, & Aguilar Torres, 2012).

Cada país determinará las políticas y programas de seguridad de los datos personales que garanticen el debido tratamiento de los mismos y el cumplimiento de los principios y obligaciones que dicta esta Ley.

Según Lorena Naranjo, titular de la Dirección de Registro de Datos Públicos, en su artículo de diario el Universo, dice: "*El numeral 19 del art. 66 de la Constitución vigente desde el 2008 estipula el derecho a la protección de los datos de carácter personal, pero aún no está regulado, igual que en otros dos países de la región: Venezuela y Bolivia".* (Naranjo, 2018)

El Ecuador cuenta con la Ley de Registro de Datos Públicos y con un Proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad de los Datos Personales, presentada por la Función Legislativa en el año 2016. Según la Directora de la DINARDAP (Dirección Nacional de Registro de Datos Públicos), esta normativa carece de especificación técnica, porque habla de dos derechos diferentes como son: el derecho a la intimidad (personas) y el derecho a la protección de los datos personales (identificación de las personas). (Naranjo, DINARDAP, 2018)

Por lo tanto la DINARDAP está trabajando en la redacción del proyecto de Ley de Protección de Datos Personales, que cumpla las especificaciones técnicas y jurídicas de acuerdo a la realidad de nuestro país, con el fin de resguardar la información protegiendo los derechos, así como también regular el intercambio de los datos. Esta Ley regulará también como deben regir los principios, los derechos, el tratamiento que deben cumplir las personas que manejan los datos y las sanciones que se aplicarán al incumplimiento de la normativa. (Naranjo, DINARDAP, 2018)

Mientras que en Latinoamérica algunos países no cuentan con la Ley de Protección de Datos Personales, los Estados de la Unión Europea comenzarán a aplicar a partir del 25 de mayo de 2018 el nuevo Reglamento General de Protección de Datos, cuyo objetivo es conseguir una mejor protección de los datos personales de los europeos, reforzar la seguridad jurídica y aumentar la garantía de los derechos de los ciudadanos. (CLINIC-CLOUD, 2018).

Es importante señalar que este nuevo reglamento establece el "Derecho de portabilidad", que significa que el ciudadano podrá recibir sus datos personales almacenados en un formato adecuado y a su vez poder entregarle a otra persona.

Las entidades de salud deberán efectivamente proteger los datos para evitar ser sancionados y tiene la obligación de designar a un "Data Protection Officer" (DPO), experto en la protección de datos, que será el responsable de la protección de los mismos. Cabe

indicar que en este nuevo reglamento también establece que la sanción máxima será de 20.000.000€ o un 4% de la facturación global. (CLINIC-CLOUD, 2018)

1.9 La seguridad de la información en el sector salud

"La información comunicada es el recurso por medio del cual el saber individual se socializa y se vuelve trascendente. La capacidad de la información comprende más que su solo acceso; ésta también comprende la conciencia de su existencia y las habilidades para explotarla una vez adquirida. La sociedad de la información no será socialmente inclusiva en ningún sentido si no se apunta al desarrollo de esta capacidad". (Llanusa Ruiz, Rojo Pérez, Carabolloso Hernández , Capote Mir, & Pérez Piñero, 2005)

La información dentro de la organización, es de vital importancia debido a que aumenta el conocimiento en los colaboradores que forman parte de la organización, guiándoles a tomar las decisiones correctas para que puedan desarrollar los procesos con eficiencia y calidad.

Como lo menciona (Escobar, Escobar, & Monge, 2014) en su artículo Tecnologías de información en el sector hospitalario, *"Los hospitales, con independencia de su finalidad lucrativa o no, de su dependencia o independencia financiera o su forma jurídica, son empresas de servicios que deben ser gestionadas eficaz y eficientemente, como cualquier otra."*

Es así, que las organizaciones de salud se han ido adaptando ante la necesidad del cambio con la llegada de las nuevas tecnologías, como son los sistemas de información y comunicación TIC. La implementación de tecnologías de la información que son activos importantes para la organización, propone dar respuesta a la necesidad de gestionar distintos niveles de información sobre salud, mejorando la gestión de los servicios de salud y la calidad de asistencia a los pacientes, así tenemos procesos como por ejemplo registros personales del paciente en una historia clínica virtual, resultados de intervenciones quirúrgicas, resultados de exámenes de laboratorio, etc., los cuales constituyen una herramienta útil para mejorar la eficacia y eficiencia en la prestación de servicios de salud.

El sector salud al igual que otros sectores, se ha visto beneficiado con la implementación de las tecnologías de información, lo cual conlleva a la exigencia de la seguridad y confidencialidad de la información (datos), por lo tanto la clave fundamental está en el acceso a la información por parte de los colaboradores (usuarios de contraseñas), quienes son los responsables de la seguridad, confidencialidad y disponibilidad de la información, los mismos que deben tener la formación ética y profesional, orientados al logro de este objetivo.

Si bien es cierto las tecnologías de la información han logrado un avance en la eficiencia de los procesos de gestión, también representan un nuevo peligro por el fácil acceso a los datos personales y el manejo de información extraordinariamente delicada, por lo que la necesidad de la protección de los datos se ha convertido en una prioridad. Los hospitales

deben tomar serias medidas y las adecuadas estrategias para proteger su entorno de un ciberataque, puesto que existen motivos suficientes para atacar a un hospital como es el robo de la identidad médica y la información de los pacientes con fines fraudulentos, tal es el caso del ciberataque realizado en Londres a mediados del 2017, el mismo que a través de un virus informático afectó alrededor de 16 hospitales, este virus impedía el acceso a los ordenadores de los profesionales de las entidades y a su vez les exigía un rescate por la suma de 300€, esto ha generado la cancelación de varias citas de los pacientes y ha costado cientos de millones de dólares. (PÚBLICO, 2017)

Con lo anteriormente expuesto es de suma importancia gestionar de forma apropiada la seguridad de la información, ya que un ciberataque trae consecuencias económicas y de imagen para las entidades, generando un sin número de riesgos tanto para quienes prestan el servicio de salud como para los pacientes, cuyo objetivo es controlar y proteger la información a través del uso de tecnologías y herramientas, que permitan controlar accesos a personas no autorizadas, así como también el bloqueo de virus y el registro de los accesos a la información protegida, de esta manera garantizar el acceso, la confidencialidad y privacidad de los datos. (ehCOS-, 2017)

La consultora ISOTools Excellence en su blog publicado SGSI, sobre la Seguridad de la Información, dice: *"Cada vez son más los hospitales que se encuentran interesados en proteger información de los pacientes, pero no ven que pueden utilizar la norma ISO 27001 por no ser lo suficientemente específica",* ya que esta norma no está desarrollada específicamente para un entorno de salud. (ISOTolls Excellence, 2016)

Para muchas organizaciones el implementar un SGSI todavía está en proyectos futuros, varios pretenden en algún momento contar con modelos de gestión de seguridad de la información basados en la Norma Internacional ISO 27001, pues su ventaja se resume en ser certificable. Alcanzar una norma requiere de un punto de partida, es decir la forma de organizar los controles necesarios basados en las mejores prácticas de la industria con la finalidad de reducir el impacto producido por la materialización del riesgo de la información, pudiendo resultar desastroso no solo para la imagen del hospital sino para la salud y privacidad del paciente.

2 Situación actual del riesgo de la información en el sector hospitalario

2.1 Marco Legal y Normativo del Ecuador, del sector Salud.

La Organización Mundial de la Salud (OMS), define a la salud *"como un estado de completo bienestar físico, mental y social, y no sólo la ausencia de enfermedades".* (Organización Mundial de la Salud, s.f.)

En el Ecuador, la salud es un derecho que garantiza el Estado, (Constitución del Ecuador, 2008). La base legal que respalda este derecho se encuentra en el Art. 32 de la Constitución de la República del Ecuador del año 2008. (Anexo 1)

La Ley Orgánica del Sistema Nacional de Salud (LOSNS), tiene como finalidad regular las acciones que permitan efectivizar el derecho universal de la salud así como lo dispone la Constitución de la República del Ecuador. Esta Ley señala también los principios, componentes y actividades que estarán sujetas por todos los integrantes del Sistema Nacional de Salud, a través del Ministerio de Salud Pública que es la autoridad sanitaria responsable de la aplicación, control y vigilancia del cumplimiento de esta Ley. (Ley Orgánica del Sistema Nacional de Salud, 2002)

Los servicios de salud serán seguros, de calidad y calidez, y garantizarán el consentimiento informado, el acceso a la información y la confidencialidad de la información de los pacientes, generada a través del uso de los servicios de salud. (Acuerdo Ministerial 5216, 2015)

La Ley de Derechos y Amparo al Paciente, también garantiza el derecho a la confidencialidad de la información en el procedimiento médico aplicado; así como también el derecho a la información sobre su estado de salud. (Art. 4 y 5) (Ley de Derechos y Amparo al Paciente. modificado, 2006)

El Ministerio de Salud Pública, expide el Reglamento para el manejo de información confidencial en el Sistema Nacional de Salud, con el objetivo de establecer las condiciones operativas de la aplicación de los principios de manejo y gestión de la información confidencial de los pacientes y sus disposiciones serán de cumplimiento obligatorio dentro del Sistema Nacional de Salud. (Acuerdo Ministerial 5216, 2015)

Las instituciones del Sistema Nacional de Salud, deben cumplir con los principios que dicta este reglamento, como son:

- Confidencialidad
- Integridad de la información
- Disponibilidad de la información
- Seguridad en el manejo de la información
- Secreto médico

Por lo tanto los profesionales de la salud deben cumplir con toda la normativa tal como lo dispone este reglamento.

La Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), tiene por objeto garantizar y normar el ejercicio del derecho fundamental de las personas a la información, dando cumplimiento a las garantías que establece la Constitución de la

República. (Ley orgánica de transparencia y acceso a la información pública, 2004)

Por lo tanto la LOTAIP es la encargada de hacer efectivo el principio de publicidad de la información de las entidades del Estado y de las entidades financiadas con recursos públicos.

De acuerdo a esta Ley las instituciones de salud que reciben o administran fondos públicos, están sometidas al principio de publicidad, por lo que toda información que poseen, es pública, y pertenece a los ciudadanos y ciudadanas, siendo gratuito el acceso a dicha información. Así lo dispone el Art. 5 de esta Ley.

Todo este amplio marco legal y normativo que posee el Estado Ecuatoriano, tiene como objetivo mejorar el nivel de salud y vida de la población ecuatoriana, hacer efectivo y garantizar el ejercicio del derecho a la salud, que a través de la red pública integral de salud, los servicios estatales serán universales y gratuitos en todos los niveles de atención. (Constitución del Ecuador, 2008)

2.2 La seguridad de la información en la Administración Pública del Ecuador

Por los avances de la tecnología, los gobiernos han otorgado mayor atención a la protección de sus activos de información, es así que la Secretaría Nacional de la Administración Pública, considerando que las TIC son herramientas imprescindibles para el desempeño institucional e interinstitucional y, por la necesidad de gestionar de manera eficiente y eficaz la seguridad de la información en las entidades públicas, crea la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, mediante Acuerdos Ministeriales 804 y 837. (EGSI - Acuerdo Ministerial 166, modificado, 2016)

Esta comisión mediante un análisis de la situación respecto de la gestión de la Seguridad de la Información en las Instituciones de la Administración Pública Central, determina la necesidad de aplicar normas y procedimientos para la seguridad de la información, e implementa el Esquema Gubernamental de Seguridad de la Información, el mismo que está basado en la norma técnica ecuatoriana INEN ISO/IEC 27002 para Gestión de la Seguridad de la Información y está dirigido a las Instituciones de la Administración Pública Central, Dependiente e Institucional. (EGSI - Acuerdo Ministerial 166, modificado, 2016)

De esta manera se inicia un proceso de mejora continua en las instituciones del sector público de acuerdo al ámbito de gestión, estructura orgánica y el nivel de madurez de la gestión de seguridad de la información en cada institución, las mismas que serán controladas a través de la Gestión por Resultados (GPR). (EGSI - Acuerdo Ministerial 166, modificado, 2016)

Además las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/ICE 27005

“Gestión del Riesgo en la Seguridad de la Información”. (EGSI - Acuerdo Ministerial 166, modificado, 2016)

Las entidades públicas implementarán el EGSI para definir los procesos, procedimientos y tecnologías, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información y para minimizar o anular los riesgos de la información.

2.3 Determinación del riesgo del sector hospitalario a nivel local

Para determinar el nivel de riesgo de la información, se realizó una entrevista al responsable de tecnologías de información y comunicación de diez entidades del sector salud, con el afán de obtener información acerca del manejo del software, hardware, redes y determinar el nivel de seguridad de la información. Se demuestran en la siguiente tabla.

Tabla 6. Cuestionario de preguntas para la determinación del riesgo en el sector hospitalario

Nro.	Asunto	Entidad 1		Entidad 2		Entidad 3		Entidad 4		Entidad 5		Entidad 6		Entidad 7		Entidad 8		Entidad 9		Entidad 10	
		Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No
1	¿La entidad ha implementado controles para asegurar que el acceso y la administración de la información se realicen solamente por el personal facultado?		0	1			0	1		1		1		1			0	1		1	
2	¿Las actividades de control implementadas contribuyen a que la información que utiliza y genera sea de calidad, pertinente, veraz, oportuna, accesible, transparente, objetiva e independiente?		0	1			0	1		1			0	1			0	1		1	
3	¿Evalúa periódicamente la efectividad de las actividades de control implementadas?		0		0	1		1		1			0		0		0		0		0
4	¿Los sistemas de información implementados aseguran la calidad, pertinencia, veracidad, oportunidad, accesibilidad, transparencia, objetividad e independencia de la información?	1		1			0		0	1			0		0		0	1		1	
5	¿Tiene formalmente establecidas líneas de comunicación e información con su personal para difundir los programas, metas y objetivos de la organización?	1		1			0	1		1		1			0		0	1		1	
6	¿Los sistemas de información implementados facilitan la toma de decisiones?	1			0	1		1		1			0		0		0		0		0
7	¿Las líneas de comunicación e información establecidas permiten recibir retroalimentación del personal respecto del avance del programa de trabajo, las metas y los objetivos?	1			0	1			0	1		1			0		0		0		0

Nro.	Asunto	Entidad 1		Entidad 2		Entidad 3		Entidad 4		Entidad 5		Entidad 6		Entidad 7		Entidad 8		Entidad 9		Entidad 10	
		Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No
8	¿Existe en su organización un documento que contenga las políticas de seguridad de la información?	1		1			0	1		1		1			0		0		0	1	
	En caso de existir el documento:																				
9	¿Considera usted que este documento es suficiente y apropiadamente difundido y comunicado a todos los miembros de la organización?		0		0		0		0		0	1			0		0		0	1	
10	¿Existe algún tipo de coordinación de seguridad de la información desde donde se coordine la implementación de controles a lo largo de todos los componentes de la organización?	1			0		0		0		0	1			0		0		0	1	
11	¿Están claramente definidas los responsables, roles, y responsabilidades de la protección y aplicación de procesos de seguridad de todos los activos claves de la organización?	1		1			0		0		0	1			0		0	1		1	
12	¿Se mantiene un inventario de todos los activos sensibles de cada sistema de información de la organización?	1			0		0		0		0		0		0		0		0	1	
13	¿Están definidos los procedimientos para el etiquetado y manejo de activos de información de acuerdo con el esquema de clasificación concebido por la organización?	1			0		0		0		0		0		0		0	1			0

Nro.	Asunto	Entidad 1		Entidad 2		Entidad 3		Entidad 4		Entidad 5		Entidad 6		Entidad 7		Entidad 8		Entidad 9		Entidad 10	
		Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No	Si	No
14	¿Se firman acuerdos de confidencialidad entre la organización y cada empleado como parte de los términos y condiciones de su trabajo?	1		1			0	1		1		1			0		0		0	1	
15	¿Las áreas con sistemas basados en tecnologías de la información están protegidas físicamente a través de un perímetro de seguridad?		0	1			0		0	1		1			0	1			0		0
16	¿Tienen los sistemas de información definidos y documentados todos los requerimientos legales relevantes y las normas para asegurar su cumplimiento?	1			0		0		0		0	1			0	1			0		0
17	¿Tiene implementado un sistema de gestión de la seguridad de la información?		0		0		0		0		0		0		0		0		0		0
	TOTALES	11		8		3		7		10		10		2		2		6		10	
	PONDERACIÓN TOTAL = 17																				

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

2.4 Diagnóstico de la gestión de riesgos en el sector hospitalario

Para la determinar el nivel de riesgo de la información en el sector hospitalario, es necesario primero determinar el nivel de confianza, a través de la siguiente fórmula:

$$\textbf{NIVEL DE CONFIANZA} = \frac{\text{CALIFICACIÓN TOTAL}}{\text{PONDERACIÓN TOTAL}} \text{ X } 100$$

TABLA DEL NIVEL DE CONFIANZA	
RANGO	**NIVEL DE CONFIANZA**
76% AL 95%	ALTO
51% AL 75%	MODERADO
15% AL 50%	BAJO

Tabla 7. Cálculo del nivel de confianza

ENTIDADES	CALIFICACIÓN TOTAL	PONDERACIÓN TOTAL	NIVEL DE CONFIANZA
Entidad 1	11	17	64.71%
Entidad 2	8	17	47.06%
Entidad 3	3	17	17.65%
Entidad 4	7	17	41.18%
Entidad 5	10	17	58.82%
Entidad 6	10	17	58.82%
Entidad 7	2	17	11.76%
Entidad 8	2	17	11.76%
Entidad 9	6	17	35.29%
Entidad 10	10	17	58.82%
TOTAL			405.88%
NIVEL DE CONFIANZA PROMEDIO DE LAS ENTIDADES DEL SECTOR HOSPITALARIO			**40.59%**

Fuente: (Crespo Martínez P. E., 2017)

En donde:

NIVEL DE RIESGO = 100% - % NIVEL DE CONFIANZA

TABLA DEL NIVEL DE RIESGO	
RANGO	**NIVEL DE RIESGO**
76% AL 95%	ALTO
51% AL 75%	MODERADO
15% AL 50%	BAJO

Tabla 8. Cálculo del nivel de riesgo

ENTIDADES	NIVEL DE CONFIANZA	NIVEL DE RIESGO
Entidad 1	64.71%	35.29%
Entidad 2	47.06%	52.94%
Entidad 3	17.65%	82.35%
Entidad 4	41.18%	58.82%
Entidad 5	58.82%	41.18%
Entidad 6	58.82%	41.18%
Entidad 7	11.76%	88.24%
Entidad 8	11.76%	88.24%
Entidad 9	35.29%	64.71%
Entidad 10	58.82%	41.18%
TOTAL		594.12%
NIVEL DE RIESGO PROMEDIO DE LAS ENTIDADES DEL SECTOR HOSPITALARIO		59.41%

Fuente: (Crespo Martínez P. E., 2017)

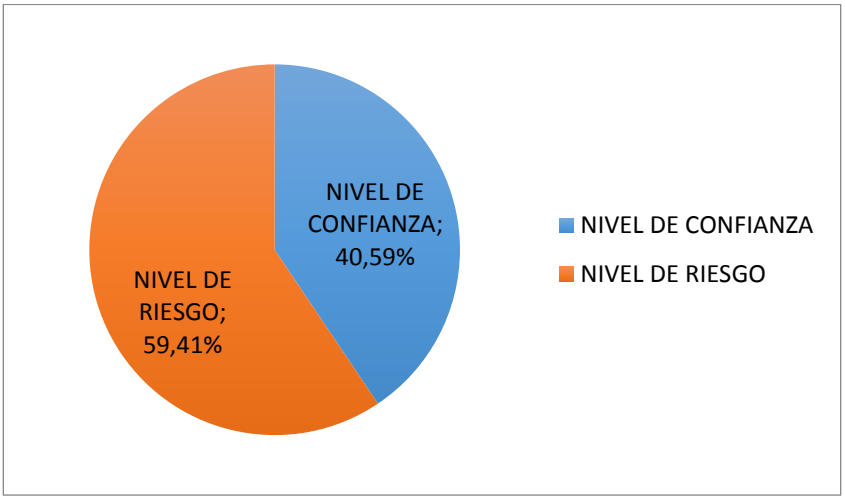

Ilustración 5. Evaluación del riesgo del sector hospitalario. Elaborado por el autor

2.5 Evaluación de riesgo de la información en el sector hospitalario

Luego de realizado el diagnóstico del nivel de riesgo en el sector hospitalario, se puede observar que el nivel de riesgo es moderado, ya que alcanza el 59.41 %; para ello las entidades deberán tomar las medidas necesarias e implementar los debidos controles y salvaguardas correspondientes, para de esta manera poder ofrecer a los usuarios de las entidades de salud, la debida seguridad en los procesos de información que reposa en las entidades de este sector, información que se considera crítica y que debe contener las tres principales características como son la confidencialidad, integridad y disponibilidad.

3 Evaluación de la metodología

Este último capítulo hace referencia a la evaluación de la metodología ECU@Risk mediante su aplicación en una organización del sector hospitalario, con el objetivo de determinar su eficiencia y funcionalidad en el ámbito de la gestión de riesgo de información.

La implementación de un SGSI es relevante para las entidades del sector hospitalario, ya que forma parte integral de todos sus procesos. Este sistema basado en la ISO 27001, parte de la identificación de procedimientos, mecanismos y herramientas que permitan salvaguardar los activos de información de las posibles amenazas que puedan presentarse, las mismas que podrán llegar a materializarse si aprovechan las vulnerabilidades existentes, lo que conllevaría al riesgo.

Será de mucha importancia la intervención de un equipo humano multidisciplinario, que deberá estar consciente de las ventajas de implementación, ya que garantizará la seguridad de los procesos y la continuidad de los negocios.

Para considerar su implementación debe contarse con el apoyo del directorio o de la gerencia general, que es parte también del equipo.

3.1 Aplicación de la metodología

ECU@Risk contempla cuatro dimensiones. Sugiere además, que el primer paso sea un análisis del contexto. Para ello, es importante conocer la misión de la unidad de negocio, pues orienta a la delimitación del contexto y a la identificación de amenazas latentes.

Proceso Unidad de Admisiones

Misión: Asegurar la accesibilidad del paciente a los recursos asistenciales del hospital. Organizar, manejar y facilitar el uso adecuado de sus instalaciones y recursos con el objeto de mejorar el proceso de gestión y funcionamiento del hospital. (Ministerio de Salud Pública-Estatuto 1537-, 2012)

Para iniciar la aplicación de la metodología es necesario que el directorio o la gerencia general, se cuestionen lo siguiente: ¿Qué tan importante representa la información para la organización?, ¿Qué podría hacer la organización si se quedaría sin información?, ¿Existe un respaldo de la información? Por lo tanto se debe realizar el siguiente cuestionario de aplicabilidad de la metodología.

Tabla 9. Cuestionario de aplicabilidad de la metodología

Nro.	Asunto	Sí	No
	Políticas de Seguridad de la Información		
1	¿Existe en su organización un documento que contenga las políticas de seguridad de la información?	1	
	En caso de existir el documento:		
2	¿Considera Usted que este documento es suficiente y apropiadamente difundido y comunicado a todos los miembros de la organización?		0
3	¿El documento de seguridad es revisado periódicamente y en caso de ocurrencia de eventos significativos?		0
	Seguridad Organizacional		
4	¿Existe un comité de gestión de seguridad que proponga o de soporte a las iniciativas de seguridad?		0
5	¿Existe algún tipo de coordinación de seguridad de la información desde donde se coordine la implementación de controles a lo largo de todos los componentes de la organización?	1	
6	¿Están claramente definidas los responsables, roles, y responsabilidades de la protección y aplicación de procesos de seguridad de todos los activos claves de la organización?	1	
7	¿Existe el soporte y la asistencia de un servicio de consultoría especializado en seguridad de la información?		0
8	¿Están establecidos contactos y acuerdos de cooperación con organizaciones para el manejo de asuntos de seguridad?		0
9	¿Se realizan auditorias de seguridad independientes a la implantación de las políticas de seguridad de la información de la organización?		0
10	¿Se establecen contratos formales de seguridad cuando recursos de tecnologías de información de su organización serán accedidos y/o manejados por terceros?		0
	Clasificación y control de activos		
11	¿Se mantiene un inventario de todos los activos sensibles de cada sistema de información de la organización?	1	
12	¿Existen esquemas o directrices para la clasificación de la información de la organización de acuerdo al grado de protección que deban recibir?		0

Nro.	Asunto	Sí	No
13	¿Están definidos los controles de protección asociados al grado de protección que deba recibir cada activo de información?		0
14	¿Están definidos los procedimientos para el etiquetado y manejo de activos de información de acuerdo con el esquema de clasificación concebido por la organización?	1	
	Seguridad y personal		
15	¿Incluyen los perfiles de trabajo o cargo responsabilidades en el área de seguridad?	1	
16	¿Se firman acuerdos de confidencialidad entre la organización y cada empleado como parte de los términos y condiciones de su trabajo?	1	
17	¿Se educa y entrena a los empleados adecuadamente en las políticas y procedimientos de seguridad de la organización?		0
18	¿Conocen los empleados los procedimientos para reportar amenazas, riesgos, sospechas u ocurrencias de: incidentes de seguridad, debilidades en sistemas o servicios e incorrecto funcionamiento de aplicaciones/software?		0
19	¿Están definidos los procesos disciplinarios para sancionar a aquellos empleados que incurran en violaciones a las políticas y procedimientos de seguridad de la información de la organización?	1	
	Seguridad física y ambiental		
20	¿Las áreas con sistemas basados en tecnologías de la información están protegidas físicamente a través de un perímetro de seguridad?	1	
21	¿Existen controles de entrada a las áreas con activos de información sensibles?	1	
22	¿Son esos controles de entrada efectivos, es decir, sólo permiten el acceso a personal autorizado?	1	
23	¿Las oficinas, cuartos y salas contentivas de activos de información con requerimientos de seguridad especiales se encuentran en áreas creadas para ese fin?	1	
24	¿Existen normas, procedimientos y mecanismos de control adicionales para trabajar en las áreas seguras? ¿Cuáles son?		0
25	¿Están las áreas de carga y despacho de la organización, aisladas de las zonas donde se localizan los activos y sistemas basados en tecnologías de la información?	1	
26	¿Está el equipamiento en tecnologías de la información adecuadamente protegido para reducir riesgos o la exposición a amenazas ambientales o de acceso no autorizado?	1	
27	¿Está el equipamiento protegido contra fallas o anomalías eléctricas?	1	

Nro.	Asunto	Sí	No
28	¿Está el cableado eléctrico y de telecomunicaciones asociado al transporte de datos o al soporte de los sistemas basados en tecnologías de información protegido contra intercepciones o daño físico?	1	
29	¿Los equipos que conforman los servicios basados en tecnologías de la información son sometidos a las labores de mantenimiento indicadas por los fabricantes, así como en el período de tiempo especificado?	1	
30	¿Se autoriza y controla el uso de equipos para procesar información que no cumplan con las directrices de seguridad de la organización? ¿Quién lo autoriza?		0
31	¿Se realiza algún tratamiento a la información almacenada en un equipo previo a su desincorporación o reúso? ¿Qué se hace? Respuesta: Se realiza el debido respaldo	1	
32	¿Implementa su organización una política de escritorios y pantallas limpias?		0
33	¿Existen controles que sólo permitan el retiro de: equipamiento, software e información perteneciente o en custodia por la organización con la autorización de la gerencia?	1	
	Gestión de la operación y las comunicaciones	1	
34	¿Están documentados los procedimientos de seguridad contemplados en la política de seguridad de la organización?	1	
35	¿Están establecidos los procedimientos y roles para el manejo de incidentes de seguridad?	1	
36	¿Los ambientes de prueba y desarrollo de sistemas basados en tecnologías de la información están separados del ambiente operativo?	1	
37	¿Existen mecanismos para monitorear el uso de los sistemas de la organización? (Como soporte para planificar crecimiento y evitar el colapso de la capacidad de procesamiento de información de la organización)	1	
38	¿Se definen criterios y planes de prueba para aceptar el uso de nuevos sistemas de información (o nuevas versiones/actualizaciones)?		0
39	¿Se educa y concientiza a los usuarios en las medidas que deben tomar para evitar ser víctimas de software malicioso?	1	
40	¿Están implantadas medidas efectivas para detectar y prevenir contra la presencia de software malicioso?	1	
41	¿Existen políticas y procedimientos para la ejecución de respaldos y su verificación?	1	
42	¿Existen registros de las actividades o trabajos que se realizan o intentan realizarse sobre los sistemas basados en TI de la organización?	1	
43	¿Están implantados mecanismos para proteger la plataforma de red de la organización y la información que pasa a través de ella?	1	

Nro.	Asunto	Sí	No
44	¿Los dispositivos o medios de almacenamiento de información removibles como cintas, discos, información impresa, etc., tienen definido normas o controles que regulen su manejo (protección) y desecho?		0
45	¿Se protege la documentación de los sistemas de información de la organización? ¿Cómo?	1	
46	¿Existen reglas y procedimientos que gobiernen y controlen el intercambio de información y programas entre organizaciones?	1	
	Control de acceso		
47	¿Posee la organización una política de control de acceso?		0
48	¿Existen diferentes niveles de acceso o privilegios para acceder a la información? ¿Cómo se asignan? Respuesta: Mediante la asignación de claves.	1	
49	¿Existen procedimientos de auditoría para revisar y corregir los derechos de acceso de los usuarios de los sistemas de la organización?		0
50	¿Los usuarios son educados sobre sus responsabilidades o rutinas en el manejo de sus mecanismos de acceso a los sistemas?	1	
51	¿Existe una política de uso de los servicios de la red?	1	
52	¿Se restringe o controla el acceso a los servidores de la red? ¿Cómo? Respuesta: Ingresa sólo el personal autorizado	1	
53	¿La red está segregada siguiendo algún criterio? ¿Cuál o cuáles?		0
54	¿Existen mecanismos de control de tráfico para evitar que flujos de datos y conexiones de otros nodos violenten la política de control de acceso?		0
55	¿Los atributos de seguridad que poseen los servicios de red que utiliza la organización son adecuados?		0
56	¿Se utilizan mecanismos y herramientas de monitoreo para detectar usos irregulares de la red?	1	
57	¿Todos los relojes de los sistemas en la red están sincronizados?	1	
58	¿Se controla el acceso a la red y sistemas de la organización desde facilidades de computación móvil y teletrabajo? ¿Cómo es controlado? Respuesta: Existen segmentos de red sólo para wifi	1	
	Desarrollo y mantenimiento de sistemas		

Nro.	Asunto	Sí	No
59	¿Son los requerimientos de seguridad incluidos en el desarrollo de nuevos sistemas o en las mejoras a los ya existentes?	1	
60	¿Poseen los sistemas mecanismos de seguridad para prevenir su mal uso?	1	
61	¿Es el proceso de desarrollo de software conducido de una manera segura y metodológica?	1	
62	¿La implementación de cambios es realizada utilizando procedimientos formales de control de cambio?		0
	Gestión de la continuidad del negocio		
63	¿Posee la organización un proceso de gestión para desarrollar y mantener planes para la continuidad del negocio ante los efectos de fallas mayores o desastres?		0
64	¿Son los planes de continuidad del negocio, constantemente revisados y corregidos para asegurar su efectividad?		0
	Cumplimiento con el marco jurídico		
65	¿Tienen los sistemas de información definidos y documentados todos los requerimientos legales relevantes y las normas para asegurar su cumplimiento?		0
66	¿Están establecidas directrices para la retención, almacenamiento, manejo y desecho de registros e información de la organización?		0
67	¿Existen directrices a todo nivel (gerencia, usuarios y proveedores de servicio) sobre las responsabilidades y procedimientos a seguir para garantizar la protección e intimidad de la información de los usuarios?		0
68	¿Existen medidas para prevenir del uso de las facilidades de procesamiento de información en propósitos diferentes a los de la entidad?		0
69	¿Están los controles criptográficos adaptados a las normas que regulan su funcionamiento dentro de Ecuador?		0
70	¿Las normas y controles adoptados para recolectar evidencia para soportar una acción legal están acordes con las leyes pertinentes?		0
71	¿Se realizan revisiones programadas a todos los entes involucrados con el negocio para asegurar que cumplen con las políticas y estándares de seguridad de la organización?		0
	PONDERACIÓN TOTAL = 71	40	31

Fuente: (Crespo Martínez P. E., 2017)

Con el desarrollo de este cuestionario se puede observar de manera general que la metodología se puede aplicar en la entidad, ya que existen procesos que no están implementados y que serán de mucha importancia para disminuir el nivel de riesgo de la entidad.

Como siguiente paso se determina las personas que conforman el comité de riesgos de la información, este comité será el pilar fundamental para el desarrollo de la implementación del SGSI ya que todos aportarán con el cumplimiento de sus roles y actividades claves en cada proceso.

Tabla 10. Matriz de identificación de roles del comité de riesgos de información

Rol	¿Quién es?	Actividades	Observaciones
Alta Dirección	En una entidad del sector hospitalario este rol lo desempeña el Gerente o Director.	Representar legalmente y extrajudicialmente a la institución; Suscribir los actos administrativos en el ámbito de su jurisdicción, con estricto apego a las disposiciones legales y reglamentarias vigentes; Programar, dirigir, controlar la gestión de los recursos asignados a su cargo y evaluar su adecuada utilización para proveer su cartera de servicios, mediante el Plan Operativo Anual y el Compromiso de Gestión en función de resultados de impacto social; Adoptar las medidas para hacer efectiva la continuidad del funcionamiento del hospital, especialmente en los casos de crisis, emergencias, urgencias u otras circunstancias similares; Coordinar la elaboración del presupuesto institucional, su trámite, ejecución, revisión y correctivos, gestionar fondos, preparar proyectos especiales y administrar la política salarial y de contratación institucional de acuerdo a la normativa vigente; (…)	Es un rol clave ya que se debe contar con la respectiva aprobación, para la eficaz implementación de un SGSI.
Propietarios de información	En el proceso de admisiones el propietario de la información es el/la responsable el responsable del proceso encargado de gestionar la información y aprobar el acceso a la misma garantizando la confidencialidad e integridad de la información.	Coordinar y supervisar mensualmente el agendamiento de las citas de cada uno de los médicos; Supervisar y aprobar mensualmente la información de la producción hospitalaria; Participar en las reuniones como responsable del proceso de admisiones; Coordinar y elaborar el informe mensual del tablero de gestión; Participar como miembro del comité de historia clínica; Desarrollar y dirigir la organización y funcionamiento del departamento, cumplir, hacer cumplir y supervisar las normas de trabajo; Elaborar los manuales por procesos; Elaborar y controlar el requerimiento de insumos y materiales;	Es de total importancia la responsabilidad para la ejecución de este rol ya que es una información crítica la misma que debe cumplir con los principios de integridad, confidencialidad y disponibilidad.
Propietario (s) de sistemas de información	En una entidad del sector hospitalario es por lo general el Responsable o Jefe del área de TI.	Mantenimiento a las líneas de red; Acciones preventivas y correctivas del software y hardware; Informes sobre las acciones preventivas y correctivas del software y hardware realizadas; Informes sobre las redes de conectividad; Plan de mejoramiento de redes; Plan de contingencias sobre respaldos de información; Mantenimiento de programas informáticos existentes; Sistemas de información en las diferentes áreas y página web actualizada de la entidad; Central telefónica digital; Servicio de internet a las diferentes áreas de la entidad hospitalaria;	Son los responsables de los cambios y actualizaciones de los sistemas.

Rol	¿Quién es?	Actividades	Observaciones
		Correo institucional; Inventario de equipos tecnológicos computacionales y comunicacionales; Actas de entrega recepción de los equipos adquiridos en coordinación con las áreas de Activos Fijos y Bodega; Informes de funcionamiento de los equipos adquiridos y otros equipos tecnológicos computacionales y comunicacionales de la institución en coordinación con Activos Fijos y Bodega; Traslado de los equipos tecnológicos computacionales y comunicacionales de la institución en coordinación con Activos Fijos y Bodega;	
Comité de riesgo de tecnología de información (CRTI)	Este comité es quien asesora al gerente o director de la entidad sobre el tema de TI. El comité lo conforman: • Gerente / Director • Representante de TI • Representante de riesgo • Asesores: Profesionales de TI • Proveedores de soluciones tecnológicas	Definir, conducir y evaluar las políticas internas para el crecimiento ordenado y progresivo de la tecnología de información y calidad de los servicios informáticos. Evaluar la planificación del riesgo tecnológico y de información y monitorear la gestión del rendimiento. Establecer su reglamentación, definir grupos de trabajo, atribuciones y responsabilidades de los miembros del comité.	Dentro del proceso de admisiones el CRTI tiene la responsabilidad de desarrollar las políticas internas para el desarrollo de los sistemas informáticos y la seguridad de la información; evaluando la planificación del riesgo tecnológico y de información.
Coordinador de seguridad designado	Es designado por el Comité de riesgo de información, para el programa de seguridad de la información.	Coordina los programas de seguridad de la información. Analiza, adopta e introduce la metodología adecuada, estructurada para apoyar en la identificación, evaluación y minimización de los riesgos a los sistemas informáticos que apoyan la misión organizacional. Actúa como consultor principal de la Alta dirección.	Es independiente al área, proceso o departamento de TI, por la segregación de funciones.
Profesionales de TI - Proveedores de soluciones tecnológicas (PST)	Está conformado por los profesionales de TI. Pueden ser: • Ingenieros en redes de datos, proveedores del sistema informático, proveedores de aplicaciones, bases de datos y administradores • Especialistas en informática • Analistas de seguridad • Consultores de TI	Son responsables de la correcta aplicación de los requisitos en sus sistemas de TI	Es muy importante contar con un equipo eficiente de profesionales de TI, que sean de gran ayuda y soporte en la administración y seguridad de la información.

Rol	¿Quién es?	Actividades	Observaciones
Auditor de TI	Profesional con conocimientos técnicos	Velar por el cumplimiento de las políticas, la normativa y el control de TI. Analizar los sistemas de la información desde una perspectiva de la seguridad y administración de los riesgos de la información que se puedan obtener a través de las diferentes aplicaciones y programas; para de esta manera velar por los intereses y objetivos de la institución.	Es un rol de mucha importancia que en una entidad si no cuenta con este profesional, será necesario la contratación de este servicio.
Comité de certificación de TI	Debe estar conformado por: • Propietarios de información • Personal de TI • Auditor de Sistemas • Coordinador de seguridad designado • Usuario final	Evaluar las actividades de paso de un sistema en desarrollo a producción, que garantice un aplicativo o programas libres de errores. Realizar las pruebas de caja blanca, caja negra, funcionalidad, seguridad, usabilidad, entre otras. Validar los cambios realizados, a manera de identificar y evaluar nuevos riesgos potenciales, para así sugerir la implementación de nuevos controles de seguridad, según la necesidad.	Su actividad principal es la evaluación y adopción de nuevos sistemas de información de acuerdo a las necesidades de la institución, los requerimientos del proceso y del avance tecnológico.

Fuente: (Crespo Martínez P. E., 2017)

3.2 Identificación del contexto

La matriz de identificación de clasificación de las sociedades ha definido la actividad comercial de esta institución bajo el modelo de sector económico público.

Tabla 11. Clasificación de las sociedades

Clasificación de las sociedades	¿Es de este tipo?	
	SI	**NO**
a. Privadas: Son personas jurídicas de derecho privado		
b. Públicas: Son personas jurídicas de derecho público	**X**	
c. Contribuyentes especiales		

Fuente: (Crespo Martínez P. E., 2017)

3.3 Delimitar el tamaño de la Entidad

La matriz de especificación de tamaño de la entidad ha permitido encajar a este hospital público dentro del segmento de grandes empresas.

Tabla 12. Clasificación de las empresas

Variables	Micro Empresa	Pequeña Empresa	Mediana Empresa	Grandes Empresas
Personal ocupado	De 1 a 9	De 10 a 49	De 50 a 199	≥ 200
Valor bruto en ventas anuales	≤ 100.000	100.001 – 1.000.000	1.000.001 – 5.000.000	> 5.000.000
Monto de activos	Hasta US$ 100.000	De US$ 100.001 hasta US$ 750.000	De 750.001 hasta US$ 3.999.999	≥ 4.000.000

Fuente: (Boletín Jurídico-Cámara de Comercio de Quito, 2017)

3.4 Ámbito de acción de la entidad

La entidad según su ámbito de acción, es nacional.

Tabla 13. Ámbito de acción de la organización

Ámbito de acción de la organización	Si	No	Debido a:
Local			
Regional			
Nacional	**X**		Es un hospital de especialidades por lo tanto ofrece los servicios a personas de todo el país.
Internacional			
Observaciones:			

Fuente: (Crespo Martínez P. E., 2017)

3.5 Establecer el contexto externo de la entidad

El análisis PESTEL ha permitido identificar aspectos de oportunidad o amenaza que aventajen o afecten a la organización en 6 dimensiones: Político, Económico, Social, Tecnológico, Ecológico y Legal. La tabla a continuación visualiza los resultados obtenidos en el análisis a este hospital público.

Tabla 14. Análisis PESTEL

CUADRO DE ANÁLISIS PESTEL PARA EL HOSPITAL "XYZ"					
Factor	**Fuentes de análisis (sugeridas)**	**Descripción**	**Condición**		**P**
POLÍTICO	Constitución de la República 2008	Art. 361: El Estado garantizará la rectoría del sistema a través de la Autoridad Sanitaria Nacional, será responsable de formular la política nacional de salud, y normará, regulará y controlará todas las actividades relacionadas con la salud, así como el funcionamiento de las entidades del sector.			P
	La reforma de salud y su componente político: un análisis de factibilidad http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S0213-91112002000100006	Estudio que enfoca su atención sobre la capacidad del Estado para impulsar exitosamente propuestas de reforma de salud. Las reformas del sistema de salud son, un proceso sumamente político, que moviliza a un gran número de grupos tanto en el interior del Estado como en la sociedad.	O		
	La reforma en salud del Ecuador http://iris.paho.org/xmlui/bitstream/handle/123456789/34061/v41a962017.pdf?sequence=1&ua=1	Se crea el Modelo de Atención Integral en Salud (MAIS) se constituyó en un eje orientador de la reforma del sector y en un pilar de la reorganización institucional del sistema público de salud. Es un nuevo modelo de atención ya no centrado en la enfermedad o en la prestación de servicios curativos, sino en las personas, sus familias, sus comunidades y sus necesidades de salud, con una perspectiva de promoción, prevención, recuperación y rehabilitación.	O		
ECONÓMICO	Constitución de la República 2008	Art. 366 El financiamiento público en salud será oportuno, regular y suficiente, y deberá provenir de fuentes permanentes del Presupuesto General del Estado. Los recursos públicos serán distribuidos con base en criterios de población y en las necesidades de salud. El Estado financiará a las instituciones estatales de salud y podrá apoyar financieramente a las autónomas y privadas siempre que no tengan fines de lucro, que garanticen gratuidad en las prestaciones, cumplan las políticas públicas y aseguren calidad, seguridad y respeto a los derechos. Estas instituciones estarán sujetas a control y regulación del Estado.	A		

CUADRO DE ANÁLISIS PESTEL PARA EL HOSPITAL "XYZ"					
Factor	**Fuentes de análisis (sugeridas)**	**Descripción**	**Condición**		**P**
	Ley Orgánica del Sistema Nacional de Salud	Art. 13: El financiamiento es la garantía de disponibilidad y sostenibilidad de los recursos financieros necesarios para la cobertura universal en salud de la población. El Consejo Nacional de Salud establecerá mecanismos que permitan la asignación equitativa y solidaria de los recursos financieros entre grupos sociales, provincias y cantones del país, así como su uso eficiente.	A		
SOCIO CULTURAL	Constitución de la República 2008	Art. 358.- El sistema nacional de salud tendrá por finalidad el desarrollo, protección y recuperación de las capacidades y potencialidades para una vida saludable e integral, tanto individual como colectiva, y reconocerá la diversidad social y cultural.			P
TECNOLÓGICO	Tecnología al servicio de la salud. http://www.portafolio.co/innovacion/tecnologia-al-servicio-de-la-salud-502059	Son numerosos los procedimientos a los que ha sido aplicada la tecnología médica: • Rapidez de los procesos y bienestar del ser humano.	O		
		• Precisión en el diagnóstico y en los resultados.	O		
		• Mayor acceso a los servicios y crecimiento de la telemedicina.	O		
		• La automatización de procesos y servicios ha beneficiado la vida de los pacientes y transformando los sistemas de salud en todo el mundo.	O		
ECOLÓGICO	Ministerio de Medio Ambiente - Código Orgánico Ambiental.	• Garantiza el derecho de las personas a vivir en un ambiente sano y ecológicamente equilibrado.	O		

CUADRO DE ANÁLISIS PESTEL PARA EL HOSPITAL "XYZ"					
Factor	**Fuentes de análisis (sugeridas)**	**Descripción**	**Condición**		**P**
	http://www.ambiente.gob.ec/codigo-organico-del-ambiente-coa/	• Es un deber del Estado y las personas: Informar, comunicar o denunciar ante la autoridad competente cualquier actividad contaminante que produzca o pueda producir impactos o daños ambientales.			P
		• Es responsabilidad del Estado: Garantizar la tutela efectiva del derecho a vivir en un ambiente sano y los derechos de la naturaleza, que permitan gozar a la ciudadanía del derecho a la salud, al bienestar colectivo y al buen vivir.			P
	Dirección Nacional de Ambiente y Salud http://www.salud.gob.ec/direccion-nacional-de-ambiente-y-salud/	Su misión es: Formular y coordinar la implementación de políticas, planes, programas y demás herramientas que permitan posicionar la salud ambiental para la promoción y protección de derechos de las personas, familias y comunidades, y la generación de ambientes sanos, en base a los lineamientos estratégicos establecidos.	O		
LEGAL	Constitución de la República 2008	• Art. 32.- La salud es un derecho que garantiza el Estado (…)			P
		• Art. 359.- El sistema nacional de salud comprenderá las instituciones, programas, políticas, recursos, acciones y actores en salud (…)	O		
		• Art. 360.- El sistema garantizará, a través de las instituciones que lo conforman, la promoción de la salud, prevención y atención integral, familiar y comunitaria (…)	O		
		• Art. 361.- El Estado ejercerá la rectoría del sistema a través de la autoridad sanitaria nacional (…)	O		
		• Art. 362.- La atención de salud como servicio público se prestará a través de las entidades estatales, privadas, autónomas, comunitarias y aquellas que ejerzan las medicinas ancestrales alternativas y complementarias (…)	O		

CUADRO DE ANÁLISIS PESTEL PARA EL HOSPITAL "XYZ"					
Factor	**Fuentes de análisis (sugeridas)**	**Descripción**	**Condición**		**P**
	Ley de Derechos y Amparo al Paciente	• Art. 4.- Derecho a la confidencialidad.- Cualquier procedimiento realizado por el paciente, tiene carácter de confidencia.			P
		• Art. 5.- Derecho a la información.- Todo paciente tiene derecho a estar informado sobre su diagnóstico en cualquier etapa de su atención, en términos que el paciente pueda razonablemente entender.			P
	Reglamento para el manejo de información confidencial en el Sistema Nacional de Salud	Su objetivo es establecer las condiciones operativas de la aplicación de los principios de manejo y gestión de la información confidencial de los pacientes y sus disposiciones serán de cumplimiento obligatorio dentro del Sistema Nacional de Salud. Sus principios son: • Confidencialidad • Integridad de la información • Disponibilidad de la información • Seguridad en el manejo de la información • Secreto Médico	O		
	Ley Orgánica de Transparencia y Acceso a la Información Pública	• Art. 5.- Información Pública.- Es todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas.	O		
		• Art. 6.- Información Confidencial.- Aquella información pública personal que no está sujeta al principio de publicidad.			P
Observaciones					
Simbología: P = Prioridad; O = Oportunidad; A = Amenaza					

Fuentes: (Acuerdo Ministerial 5216, 2015) (Constitución del Ecuador, 2008) (EGSI - Acuerdo Ministerial 166, modificado, 2016) (Espinosa, Acuña, De la Torre, & Tambini, 2017) (Ley Orgánica del Sistema Nacional de Salud, 2002) (Ley orgánica de transparencia y acceso a la información pública, 2004) (Ley de Derechos y Amparo al Paciente. modificado, 2006) (Ministerio de Salud Pública, s.f.) (Ministerio de Telecomunicaciones y Sociedad de la Información, s.f.) (Ministerio del Ambiente, s.f.) (Crespo Martínez P. E., 2017)

3.6 Establecer el contexto interno de la entidad

Se han identificado aspectos internos de la entidad, los mismos que se resumen en la figura a continuación.

Fecha:	02/02/2018	
Elaborado por:	Ing. Nelly Ávila	
Aprobado por:	XXXX	
Aspectos positivos	Aspectos negativos	
Fortalezas • Personal capacitado y especializado • Especialistas en emergencia las 24 horas • Talento humano multidisciplinario • Capacidad resolutiva de problemas críticos de la región • Docencia e investigación • Programas de salud pública de exclusividad • Equipamiento y tecnología acorde a nuestras necesidades • Imagen	**Debilidades** • Déficit de talento humano • Baja productividad • Resistencia al cambio • Inequidad de horarios • Inequidad salarial • Bajo trabajo en equipo • Baja adherencia a protocolos • Falta de programas de capacitación • Poco empoderamiento en la gestión de procesos • Falta de aplicación de la estructura orgánica • Falta de sistema de información en inventarios y en historias clínicas • Equipamiento obsoleto en servicios • Infraestructura inadecuada	De origen interno
Oportunidades • Alta demanda de servicios especializados • Imagen positiva como servicios especializados • Modelo piloto para determinados programas • Realización de proyectos de investigación • Políticas de salud Nacional que apoyan a la Salud Pública.	**Amenazas** • Mejor remuneración por parte de otros prestadores • Inestabilidad laboral • Déficit presupuestal para gastos de inversión • Presupuesto limitado • Retraso en la recuperación de costos de la RPIS	De origen externo

Ilustración 6. Análisis FODA. Fuente: (Crespo Martínez P. E., 2017) (M.S.P. Coordinación Zonal 6, 2014) Elaborado por el autor

3.7 Peso y valoración de cada una de las variables del FODA

Al ser el FODA una herramienta subjetiva, se ha visto la necesidad de valorar cada uno de los elementos que conforman las fortalezas, oportunidades, debilidades y amenazas, para llegar a determinar su posición estratégica y evaluar posteriormente la acción a realizar (PEEA)

Para la valoración se realizará el análisis en un intervalo del 1 al 5, en donde:

1 es poco importante y 5 muy importante

Tabla 15. Valoración de las Fortalezas

Fortalezas	Peso relativo	Valoración	Peso ponderado
Personal capacitado y especializado	15%	5	0.75
Especialistas en emergencia las 24 horas	20%	5	1
Talento humano multidisciplinario	10%	4	0.40
Capacidad resolutiva de problemas críticos de la región	10%	4	0.40
Docencia e investigación	10%	4	0.40
Programas de salud pública de exclusividad	10%	4	0.40
Equipamiento y tecnología acorde a nuestras necesidades	15%	5	0.75
Imagen	10%	5	0.50
	100%		**4,60**

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

Tabla 16. Valoración de las Debilidades

Debilidades	Peso relativo	Valoración	Peso ponderado
Déficit de talento humano	15%	4	0.60
Baja productividad	15%	2	0.60
Resistencia al cambio	5%	2	0.10
Inequidad de horarios	5%	2	0.10
Inequidad salarial	5%	3	0.15
Bajo trabajo en equipo	5%	4	0.20
Baja adherencia a protocolos	5%	3	0.15
Falta de programas de capacitación	5%	4	0.20
Poco empoderamiento en la gestión de procesos	10%	3	0.30

Debilidades	Peso relativo	Valoración	Peso ponderado
Falta de aplicación de la estructura orgánica	5%	2	0.10
Falta de sistema de información en inventarios y en historias clínicas	10%	5	0.50
Equipamiento obsoleto en servicios	5%	3	0.15
Infraestructura inadecuada	5%	3	0.15
	100%		**3.30**

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

Tabla 17. Valoración de las Oportunidades

Oportunidades	Peso relativo	Valoración	Peso ponderado
Alta demanda de servicios especializados	20%	4	0.80
Imagen positiva como servicios especializados	25%	5	1.25
Modelo piloto para determinados programas	20%	4	0.80
Realización de proyectos de investigación	20%	4	0.80
Políticas de salud Nacional que apoyan a la Salud Pública	15%	3	0.45
	100%		**4.10**

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

Tabla 18. Valoración de las Amenazas

Amenazas	Peso relativo	Valoración	Peso ponderado
Mejor remuneración por parte de otros prestadores	20%	3	0.60
Inestabilidad laboral	15%	3	0.45
Déficit presupuestal para gastos de inversión	25%	3	0.75
Presupuesto limitado	25%	2	0.50
Retraso en la recuperación de costos de la RPIS	15%	2	0.30
	100%		**2.60**

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

3.8 Posición Estratégica y Evaluación de Acciones (PEEA)

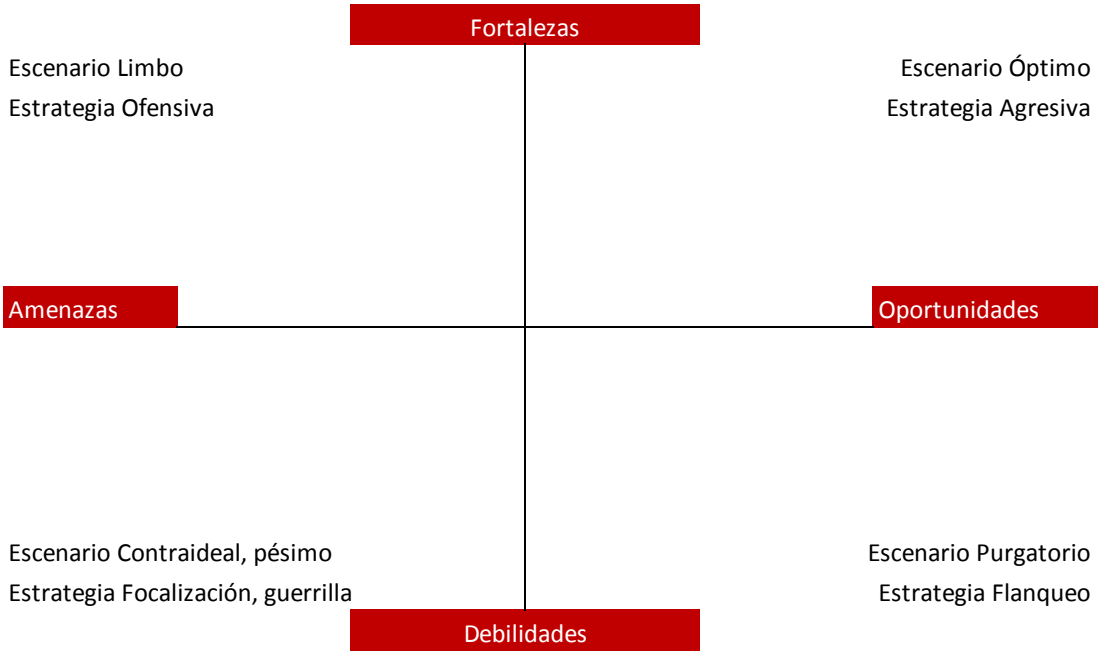

Ilustración 7. Análisis FODA de la Entidad. Fuente: (Hernández Ramírez, 2015) Elaborado por el autor

3.9 Análisis del FODA de la Entidad

El análisis del FODA de la entidad se realizó a través de la herramienta de Posición Estratégica y Evaluación de Acciones, la misma que a luego de calcular el valor de la balanza exógena y endógena, permite determinar en cuál de los cuadrantes se encuentra ubicada la entidad.

Valor de la balanza exógena (Oportunidades – Amenazas)

Atractivo = Σ Peso Ponderado Oportunidades – Σ Peso Ponderado Amenazas

Oportunidades =	4.10
Amenazas =	2.60
Atractivo =	1.50

Valor de la balanza endógena (Fortalezas – Debilidades)

Competitividad = Σ Peso Ponderado Fortalezas – Σ Peso Ponderado Debilidades

Fortalezas =	4.60
Debilidades =	3.30
Competitividad =	1.30

PEEA (X, Y)

PEEA (exógeno, endógeno)

PEEA = (Atractivo, Competitividad)

PEEA = (1.50, 1.30)

Los valores obtenidos se representan en el plano cartesiano, que nos da como resultado el siguiente gráfico.

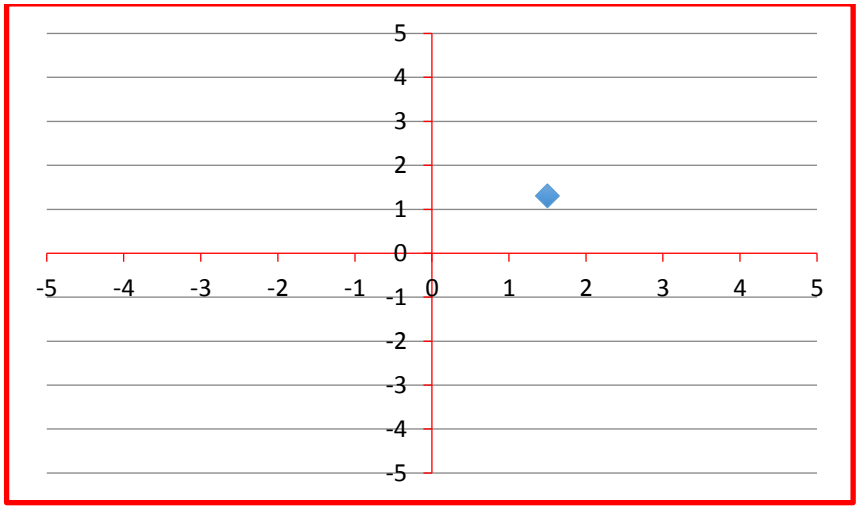

Ilustración 8. PEEA. Fuente: (Hernández Ramírez, 2015) Elaborado por el autor

En la gráfica se observa que el punto de las coordenadas se ubica en el cuadrante Fortalezas y Oportunidades, por lo que la entidad se encuentra posicionada en un escenario óptimo, deberá utilizar estrategia agresiva es decir con las fortalezas que cuenta la entidad aprovechar las oportunidades.

3.10 Identificación de roles y actividades del proceso de admisiones

Las actividades en cada proceso de la entidad se realizan de acuerdo al Estatuto Orgánico 1537 del Ministerio de Salud Pública, por lo que se puede observar que no existen actividades incompatibles en este proceso.

En el subproceso agendamiento de citas médicas de las Unidades Operativas 1 y 2, las actividades lo realizan 2 funcionarios de la entidad.

Tabla 19. Actividades del subproceso: Agendamiento de citas médicas Distrito 1 y 2

Matriz para identificación de roles y actividades incompatibles			
Fecha: 07/02/2018			
Departamento: Admisiones			
Nombre del funcionario evaluado: (RRHH)(AD)(006) ; (RRHH)(AD)(011)			
Jefe inmediato: (RRHH)(AD)(001)			
Cargo: Asistente de Admisiones			
Proceso	**Funciones**	**Roles incompatibles**	**Observaciones**
Agendamiento de citas médicas de las unidades operativas del Distrito 1 y Distrito 2	Ingresar al correo institucional;		
	Descargar los archivos adjuntos de los correos electrónicos recibidos de la matriz de agentamiento;		
	Revisar que los campos de la matriz se encuentren completamente llenos;		
	Ingresar en el sistema Medisys para la generación del turno;		
	Verificar los datos del usuario en el sistema Medisys;		
	Generar el turno según la especialidad solicitada;		
	Ingresar la información en el archivo SPSS y llenar la matriz de asignación de turnos con la respectiva información para que el usuario acuda a la cita;		
	Recibir las contra referencias de los médicos;		
	Registrar la información de las contra referencias en el archivo SPSS;		
Elaborado por: Ing. Nelly Ávila			
Revisado por: XX			
Aprobado por: XX			

Fuente: (Ministerio de Salud Pública-Estatuto 1537-, 2012) (Crespo Martínez P. E., 2017) *Elaborado por el autor*

El subproceso de agendamiento de citas subsecuentes y turnos extras lo conforman 4 funcionarios, son los encargados de agendar los turnos sistema Medisys. Estos turnos son ingresados por los médicos en las historias clínicas de los pacientes “en línea”, durante la consulta.

Tabla 20. Actividades del subproceso: Agendamiento de citas subsecuentes y turnos extras

Matriz para identificación de roles y actividades incompatibles			
Fecha: 07/02/2018			
Departamento: Admisiones			
Nombre del funcionario evaluado: (RRHH)(AD)(007) (RRHH)(AD)(012) (RRHH)(AD)(020) (RRHH)(AD)(017)			
Jefe inmediato: (RRHH)(AD)(001)			
Cargo: Asistente de Admisiones			
Proceso	**Funciones**	**Roles incompatibles**	**Observaciones**
Agendamiento de citas subsecuentes y turnos extras	Revisar el sistema Medisys y asignar turnos de acuerdo a la solicitud y disponibilidad		
Elaborado por: XX			
Revisado por: XX			
Aprobado por: XX			

Fuente: (Ministerio de Salud Pública-Estatuto 1537-, 2012) (Crespo Martínez P. E., 2017) *Elaborado por el autor*

El subproceso de agendamiento y asignación de cama lo conforma 1 funcionario, encargado de verificar la disponibilidad de las camas de los diferentes servicios del hospital para dar paso a la respectiva cirugía.

Tabla 21. Actividades del subproceso: Agendamiento y asignación de camas

Matriz para identificación de roles y actividades incompatibles			
Fecha: 07/02/2018			
Departamento: Admisiones			
Nombre del funcionario evaluado: (RRHH)(AD)(004)			
Jefe inmediato: (RRHH)(AD)(001)			
Cargo: Asistente de Admisiones			
Proceso	**Funciones**	**Roles incompatibles**	**Observaciones**
Agendamiento y asignación de camas	Receptar la solicitud de ingreso a la cirugía;		
	Verificar la disponibilidad de camas;		
	Entrega la carpeta con los documentos habilitantes, la historia clínica y la manilla para el paciente;		
	Ingresar los datos en el software de camas;		
Elaborado por: Ing. Nelly Ávila			
Revisado por: XX			
Aprobado por: XX			

Fuente: (Ministerio de Salud Pública-Estatuto 1537-, 2012) (Crespo Martínez P. E., 2017) *Elaborado por el autor*

El subproceso de ingresos y egresos hospitalarios lo conforma 1 funcionario, encargado de actualizar la matriz de los pacientes que ingresan a hospitalización, así como los que salen con el alta hospitalaria.

Tabla 22. Actividades del subproceso: ingresos y egresos hospitalarios

Matriz para identificación de roles y actividades incompatibles			
Fecha: 07/02/2018			
Departamento: Admisiones			
Nombre del funcionario evaluado: (RRHH)(AD)(003)			
Jefe inmediato: (RRHH)(AD)(001)			
Cargo: Asistente de Admisiones			
Proceso	**Funciones**	**Roles incompatibles**	**Observaciones**
Ingresos y egresos hospitalarios	Recepción de los censos diarios de los diferentes servicios de hospitalización;		
	Elaboración de las solicitudes de internación;		
	Verificación de los pacientes subsecuentes o nuevos;		
	Apertura de historias clínicas de los pacientes nuevos y manejo de historias clínicas de pacientes subsecuentes ;		
	Verificar la correcta elaboración de los censos diarios del servicio de enfermería;		
	Recopilación de historias clínicas de pacientes dados de alta y su entrega al archivo central.		
Elaborado por: Ing. Nelly Ávila			
Revisado por: XX			
Aprobado por: XX			

Fuente: (M.S.P. Coordinación Zonal 6, 2014) (Crespo Martínez P. E., 2017) *Elaborado por el autor*

El subproceso de codificación lo conforma 1 funcionario, encargado de asignar los códigos según la Clasificación Estadística Internacional de Enfermedades y Problemas relacionados con la Salud de los egresos de hospitalización y de emergencia CIE-10.

Tabla 23. Actividades del subproceso: codificación

Matriz para identificación de roles y actividades incompatibles			
Fecha: 07/02/2018			
Departamento: Admisiones			
Nombre del funcionario evaluado: (RRHH)(AD)(016)			
Jefe inmediato: (RRHH)(AD)(001)			
Cargo: Asistente de Admisiones			
Proceso	**Funciones**	**Roles incompatibles**	**Observaciones**
Codificación	Asignación de códigos según la Clasificación Estadística Internacional de Enfermedades y Problemas relacionados con la Salud de los egresos de hospitalización y de emergencia CIE-10		
	Informe estadístico de nacido vivo		
	Formularios físicos de defunciones		
Elaborado por: Ing. Nelly Ávila			
Revisado por: XX			
Aprobado por: XX			

Fuente: (M.S.P. Coordinación Zonal 6, 2014) (Crespo Martínez P. E., 2017) *Elaborado por el autor*

El subproceso de estadística lo conforma 1 funcionario encargado de elaborar las bases de datos de: codificación CIE-9-mc (investigaciones quirúrgicas), la producción de los médicos, de producción hospitalaria, morbilidad hospitalaria, etc. Este subproceso reporta los datos al INEC para los respectivos procedimientos.

Tabla 24. Actividades del subproceso: estadística

Matriz para identificación de roles y actividades incompatibles			
Fecha: 07/02/2018			
Departamento: Admisiones			
Nombre del funcionario evaluado: (RRHH)(AD)(002)			
Jefe inmediato: (RRHH)(AD)(001)			
Cargo: Asistente de Admisiones			
Proceso	**Funciones**	**Roles incompatibles**	**Observaciones**
Estadística	Codificación CIE-9-mc para tipos de investigaciones quirúrgicas;		
	Elaboración de la base de datos de morbilidad hospitalaria, intervenciones quirúrgicas y atenciones en emergencia;		
	Elaboración de la base de datos de producción hospitalaria de los servicios de apoyo, maternidad saludable, atenciones gineco-obstetricias		
	Elabora una base de datos de producción de los médicos que dan consulta del sistema Medisys		
Elaborado por: Ing. Nelly Ávila			
Revisado por: XX			
Aprobado por: XX			

Fuente: (M.S.P. Coordinación Zonal 6, 2014) (Crespo Martínez P. E., 2017) *Elaborado por el autor*

El subproceso de estadística de emergencia lo conforman 4 funcionarios, los mismos que tienen turnos de 6 horas cada uno, así este proceso no queda desabastecido.

Tabla 25. Actividades del subproceso: estadística de emergencia

Matriz para identificación de roles y actividades incompatibles			
Fecha: 07/02/2018			
Departamento: Admisiones			
Nombre del funcionario evaluado: (RRHH)(AD)(009) (RRHH)(AD)(013) (RRHH)(AD)(005) (RRHH)(AD)(015)			
Jefe inmediato: (RRHH)(AD)(001)			
Cargo: Asistente de Admisiones – Analista de Admisiones			
Proceso	**Funciones**	**Roles incompatibles**	**Observaciones**
Estadística de emergencia	Apertura y entrega de números de historias clínica;		
	Captación de pacientes asegurados: IESS, ISSFA, ISPOL, Seguro Campesino;		
	Recepción de llamadas telefónicas del ECU 911;		
	Control de las ambulancias para procesos con pacientes		
	Entrega de historias clínicas de emergencia ambulatorias y de hospitalización al archivo central.		
Elaborado por: Ing. Nelly Ávila			
Revisado por: XX			
Aprobado por: XX			

Fuente: (M.S.P. Coordinación Zonal 6, 2014) (Crespo Martínez P. E., 2017) *Elaborado por el autor*

El subproceso de recuperación de costos hospitalarios lo conforman 3 funcionarios, los mismos que son los encargados de recopilar toda la documentación concerniente de los servicios prestados a los pacientes con seguro IESS y pasar al proceso de recaudación para el respectivo planillaje.

Tabla 26. Actividades del subproceso: recuperación de costos hospitalarios

Matriz para identificación de roles y actividades incompatibles			
Fecha: 07/02/2018			
Departamento: Admisiones			
Nombre del funcionario evaluado: (RRHH)(AD)(014) (RRHH)(AD)(018) (RRHH)(AD)(019)			
Jefe inmediato: (RRHH)(AD)(001)			
Cargo: Asistente de Admisiones			
Proceso	**Funciones**	**Roles incompatibles**	**Observaciones**
Recuperación de costos hospitalarios	Recopilar la información de las historias clínicas, de los pacientes que cuentan con seguro IESS,		
	Obtener del sistema Medisys las notas de evolución (citas médicas)		
	Pasar al proceso de recaudación toda la información recopilada para que realicen el respectivo planillaje.		
Elaborado por: Ing .Nelly Ávila			
Revisado por: XX			
Aprobado por: XX			

Fuente: (M.S.P. Coordinación Zonal 6, 2014) (Crespo Martínez P. E., 2017) *Elaborado por el autor*

El subproceso de procesamiento de datos lo conforma 1 funcionario, es el encargado de realizar los reportes del dispensario del IESS y de odontología; así como también ingresar la información concerniente a los permisos y días de vacaciones de los médicos en el sistema Medisys.

Tabla 27. Actividades del subproceso: procesamiento de datos

Matriz para identificación de roles y actividades incompatibles			
Fecha: 07/02/2018			
Departamento: Admisiones			
Nombre del funcionario evaluado: (RRHH)(AD)(008)			
Jefe inmediato: (RRHH)(AD)(001)			
Cargo: Analista de Admisiones			
Proceso	**Funciones**	**Roles incompatibles**	**Observaciones**
Procesamiento de datos	Realizar los informes de odontología del dispensario anexo del IESS;		
	Manejo del sistema Medisys para el registro de permisos y horarios de los médicos.		
Elaborado por: Ing. Nelly Ávila			
Revisado por: XX			
Aprobado por: XX			

Fuente: (M.S.P. Coordinación Zonal 6, 2014) (Crespo Martínez P. E., 2017) *Elaborado por el autor*

El subproceso de archivo y mensajería lo conforma 1 persona encargada del archivo y custodio de las historias clínicas y demás documentos del subproceso.

Tabla 28. Actividades del subproceso: archivo y mensajería

Matriz para identificación de roles y actividades incompatibles			
Fecha: 07/02/2018			
Departamento: Admisiones			
Nombre del funcionario evaluado: (RRHH)(AD)(008)			
Jefe inmediato: (RRHH)(AD)(001)			
Cargo: Asistente de Admisiones			
Proceso	Funciones	Roles incompatibles	Observaciones
Archivo y mensajería	Apertura y eliminación de la historia clínica;		
	Archivo y conservación de las historias clínicas;		
	Depuración permanente de las historias clínicas;		
	Distribución y control de las historias clínicas entregadas a los consultorios de consulta externa, hospitalización y ambulatorios;		
	Custodio de historias clínicas y demás documentos y registros del proceso.		
Elaborado por: Ing. Nelly Ávila			
Revisado por: XX			
Aprobado por: XX			

Fuente: (M.S.P. Coordinación Zonal 6, 2014) (Crespo Martínez P. E., 2017) *Elaborado por el autor*

3.11 Identificación de habilidades del personal del proceso

Para realizar este proceso es necesario que la entidad tenga implementado un manual de competencias para la selección de personal, por lo tanto, en este caso no se puede realizar en análisis, ya que la entidad no cuenta con ese manual.

3.12 Valores Compartidos Organizacionales de la entidad

Información que se encuentra en el plan estratégico de la entidad 2014-2017.

Tabla 29. Valores compartidos organizacionales

Valores compartidos organizacionales	
Misión	Prestar servicios de salud con calidad y calidez en el ámbito de la asistencia especializada, a través de su cartera de servicios, cumpliendo con la responsabilidad de promoción, prevención, recuperación, rehabilitación de la salud integral, docencia e investigación, conforme a las políticas del Ministerio de Salud Pública y el trabajo en red, en el marco de la justicia y equidad social.
Visión	Ser reconocidos por la ciudadanía como hospitales accesibles, que prestan una atención de calidad que satisface las necesidades y expectativas de la población bajo principios fundamentales de la salud pública y bioética, utilizando la tecnología y los recursos públicos de forma eficiente y transparente.
Valores	• Respeto • Inclusión • Vocación de servicio • Compromiso • Integridad • Justicia • Lealtad
Objetivos institucionales	• Desarrollar la excelencia organizacional al 2017 • Desarrollar la excelencia operacional en los servicios especializados al 2017 • Ser un "hospital de especialidades" de 400 camas • Reorientar el trabajo en red • Fortalecer la docencia e investigación

Fuente: (M.S.P. Coordinación Zonal 6, 2014) (Crespo Martínez P. E., 2017) *Elaborado por el autor*

3.13 Identificación del estilo organizacional de la entidad

Se compone de 2 matrices las mismas que en preferencia debe ser llenada por el responsable de la unidad administrativa de talento humano y por el gerente general respectivamente. Los resultados de las entrevistas realizadas reflejan que la entidad no cuenta con un clima laboral óptimo, ya que por ejemplo existe controversia entre sus empleados y reclamos de los funcionarios a la gerencia. Será la unidad de talento humano la encargada de realizar acciones para que esta realidad vaya tomando nueva forma y con el objetivo de hacer cumplir los valores institucionales.

Matriz 1. Se califica con un intervalo de 1 a 5, en donde 1 es muy bajo y 5 muy alto.

Tabla 30. Cuestionario a la Unidad de Talento Humano

Matriz de identificación del estilo organizacional					
Cuestionamientos	1	2	3	4	5
¿La rotación del personal en la empresa es?		X			
¿La empresa tiene empleados con exceso de trabajo?			X		
¿Existe situaciones de controversia entre los empleados?			X		
¿El índice de los reclamos por parte de los usuarios es?			X		
¿El número de empleados que trabaja horas adicionales es?	X				

Fuente: (Crespo Martínez P. E., 2017) (Entrevista UATH) *Elaborado por el autor*

Matriz 2. Se considera un intervalo de 1 a 5, en donde:

1: “nunca”
2: “casi nunca”
3: “a veces”
4: “con frecuencia”
5: “siempre”

Tabla 31. Cuestionario a la Gerencia

Matriz de identificación del estilo organizacional					
Cuestionamientos	1	2	3	4	5
¿La gerencia general tiene reclamos por parte de sus funcionaros?				X	
¿Los usuarios han reclamado por mala atención del personal?		X			
¿Los usuarios han reclamado por servicios insatisfechos?		X			
¿Los usuarios han reclamado por negligencia?		X			
¿Se han producido robos internos?		X			
¿La entidad ha sido víctima de actos fraudulentos?	X				
¿La entidad ha sido víctima de sabotaje de información?	X				
¿Los valores compartidos organizacionales son transmitidos (durante el año):					X
¿Ha realizado evaluaciones a sus empleados a fin de determinar el nivel de conocimiento sobre los valores compartidos?				X	

Fuente: (Crespo Martínez P. E., 2017) (Entrevista UATH) *Elaborado por el autor*

3.14 Clasificación de los activos de información

Los activos de información podrían clasificarse en los siguientes grupos:

Tabla 32. Clasificación de los activos de información

ABREVIATURA	DESCRIPCIÓN
(ED)	Edificaciones
(HW)	Hardware
(SW)	Software
(IE)	Información electrónica
(IP)	Información en papel
(Extraíble)	Medios de almacenamiento extraíble
(IC)	Infraestructura de comunicaciones
(RRHH)	Recursos Humanos

Fuente: (Crespo Martínez P. E., 2017)

3.15 Valorar los activos de información

La valoración de los activos se realizará de acuerdo a la tabla 3. Por lo tanto los activos de información fueron valorados dentro de los parámetros que dicta esta metodología en donde 1 significa un daño menor y 5 daño extremadamente grave y se calificará de acuerdo a la importancia del mismo.

Es necesario cuestionarse las siguientes preguntas para que sea más eficiente el proceso de valoración, preguntas que hacen referencia a los 3 requisitos de la información.

Confidencialidad: ¿Qué tan importante es que solo el personal autorizado conozca esta información?

Disponibilidad: ¿Qué tan importante es que este activo esté disponible en el proceso?

Integridad: ¿Qué tan necesario es que la información que contiene este activo de información esté libre de errores?

Tabla 33. Valoración de los activos de información del proceso de admisiones

Subproceso	Actividades	Activo	Descripción	C	D	I	Valoración
Agendamiento de citas de las unidades operativas del Distrito 1 y Distrito 2	Ingresar al correo institucional; Descargar los archivos adjuntos de los correos electrónicos recibidos de la matriz de agentamiento; Revisar que los campos de la matriz se encuentren completamente llenos; Ingresar en el sistema Medisys para la generación del turno; Verificar los datos del usuario en el sistema Medisys; Generar el turno según la especialidad solicitada; Ingresar la información en el archivo SPSS y llenar la matriz de asignación de turnos con la respectiva información para que el usuario acuda a la cita; Recibir las contra referencias de los médicos; Registrar la información de las contra referencias en el archivo SPSS;	(HW)(SVR)(001)	El equipo servidor	1	4	**1**	**4**
		(SW)(STD)(OS)(001)	Sistema Server	2	4	**2**	**4**
		(SW)(STD)(DB)(001)	Base de datos Oracle	3	4	**3**	**4**
		(SW)(STD)(OS)(002)	Sistema Medisys	4	3	**4**	**4**
		(SW)(WEB)(001)	www.hvcm.gob.ec	1	4	**3**	**4**
		(SW)(EMAIL)(001)	agendamientolinea@hvcm.gob.ec	1	3	**3**	**3**
		(HW)(PC)(006)	Computador de escritorio	1	3	**3**	**3**
		(HW)(PC)(011)	Computador de escritorio	1	3	**3**	**3**
		(IE)(DATA)(001)	Matriz de agendamiento en Excel	3	4	**4**	**4**
		(IE)(DATA)(002)	Programa SPSS (hoja de cálculo Excel)	3	4	**4**	**4**
		(ED) (CPD)(001)	Centro de cómputo	4	3	**4**	**4**
		(RRHH)(AD)(001)	Responsable del proceso	2	3	**3**	**3**
		(RRHH)(AD)(006)	Usuario del módulo	3	3	**3**	**3**
		(RRHH)(AD)(011)	Usuario del módulo	3	3	**3**	**3**
Agendamiento de citas subsecuentes y turnos extras	Revisar el sistema Medisys y asignar turnos de acuerdo a la solicitud y disponibilidad	(HW)(SVR)(001)	El equipo servidor	1	4	**1**	**4**
		(SW)(STD)(OS)(001)	Sistema Server	2	4	**2**	**4**
		(SW)(STD)(DB)(001)	Base de datos Oracle	3	4	**3**	**4**
		(SW)(STD)(OS)(002)	Sistema Medisys	4	3	**4**	**4**
		(HW)(PC)(007)	Computador de escritorio	1	3	**3**	**3**
		(HW)(PC)(012)	Computador de escritorio	1	3	**3**	**3**
		(HW)(PC)(020)	Computador de escritorio	1	3	**3**	**3**
		(HW)(PC)(017)	Computador de escritorio	1	3	**3**	**3**

Subproceso	Actividades	Activo	Descripción	C	D	I	Valoración
		(ED) (CPD)(001)	Centro de cómputo	4	3	**4**	**4**
		(RRHH)(AD)(001)	Responsable del proceso	2	3	**3**	**3**
		(RRHH)(AD)(007)	Usuario del módulo	3	3	**3**	**3**
		(RRHH)(AD)(012)	Usuario del módulo	3	3	**3**	**3**
		(RRHH)(AD)(020)	Usuario del módulo	3	3	**3**	**3**
		(RRHH)(AD)(017)	Usuario del módulo	3	3	**3**	**3**
Agendamiento y asignación de camas	Receptar la solicitud de ingreso a la cirugía; Verificar la disponibilidad de camas; Entrega la carpeta con los documentos habilitantes, la historia clínica y la manilla para el paciente; Ingresar los datos en el software de camas;	(HW)(SVR)(001)	El equipo servidor	1	4	**1**	**4**
		(SW)(STD)(OS)(001)	Sistema Server	2	4	**4**	**4**
		(SW)(STD)(DBMS)(001)	Base de datos MySQL	3	4	**4**	**4**
		(SW)(STD)(SPH)(001)	SIGPH Software de camas (Sistema Integral de Gestión de	3	4	**4**	**4**
		(HW)(PC)(004)	Computador de escritorio	1	3	**3**	**3**
		(IE)(DATA)(003)	Programación de citas quirúrgicas	3	4	**4**	**4**
		(IP)(ARCHIVO)(001)	Programación de citas quirúrgicas	3	4	**4**	**4**
		(ED) (CPD)(001)	Centro de cómputo	4	3	**4**	**4**
		(RRHH)(AD)(001)	Responsable del proceso	2	3	**3**	**3**
		(RRHH)(AD)(004)	Usuario del módulo	3	3	**3**	**3**
Ingresos y egresos hospitalario	Recepción de los censos diarios de los diferentes servicios de hospitalización; Elaboración de las solicitudes de internación; Verificación de los pacientes subsecuentes o nuevos; Apertura de historias clínicas de los pacientes nuevos y manejo de historias clínicas de pacientes subsecuentes ;	(HW)(SVR)(001)	El equipo servidor	1	4	**1**	**4**
		(SW)(STD)(OS)(001)	Sistema Server	2	4	**2**	**4**
		(SW)(STD)(DBMS)(001)	Base de datos MySQL	3	4	**4**	**4**
		(SW)(STD)(SPH)(001)	SIGPH Software de camas (Sistema Integral de Gestión de	3	5	**4**	**5**
		(HW)(PC)(003)	Computador de escritorio	1	3	**3**	**3**
		(IE)(DATA)(004)	Ingresos y egresos de pacientes	3	4	**4**	**4**

Subproceso	Actividades	Activo	Descripción	C	D	I	Valoración
	Verificar la correcta elaboración de los censos diarios del servicio de enfermería; Recopilación de historias clínicas de pacientes dados de alta y su entrega al archivo central	(ED) (CPD)(001)	Centro de cómputo	4	3	**4**	**4**
		(RRHH)(AD)(001)	Responsable del proceso	2	3	**3**	**3**
		(RRHH)(AD)(003)	Usuario del módulo	3	3	**3**	**3**
Codificación	Asignación de códigos según la Clasificación Estadística Internacional de Enfermedades y Problemas relacionados con la Salud de los egresos de hospitalización y emergencia CIE-10; Informe estadístico de nacido vivo; Formularios físicos de defunciones.	(HW)(SVR)(001)	El equipo servidor	1	4	**1**	**4**
		(SW)(STD)(OS)(001)	Sistema Server	2	4	**2**	**4**
		(SW)(WEB)(003)	Registro Civil REVIT https://servicios1.registrocivil.gob.ec/rev	2	2	**4**	**4**
		(HW)(PC)(016)	Computador de escritorio	1	3	**3**	**3**
		(IE)(DATA)(005)	Matriz archivo SPSS de codificación	3	4	**4**	**4**
		(IP)(ARCHIVO)(005)	Formularios de defunciones	3	4	**4**	**4**
		(ED) (CPD)(001)	Centro de cómputo	4	3	**4**	**4**
		(RRHH)(AD)(001)	Responsable del proceso	2	3	**3**	**3**
		(RRHH)(AD)(016)	Usuario del módulo	3	3	**3**	**3**
Estadística	Codificación CIE-9-mc para tipos de investigaciones quirúrgicas; Elaboración de la base de datos de morbilidad hospitalaria, intervenciones quirúrgicas y atenciones en emergencia; Elaboración de la base de datos de producción hospitalaria de los servicios de apoyo, maternidad saludable, atenciones gineco-obstetricias Elabora una base de datos de producción de los médicos que dan consulta del sistema Medisys	(HW)(SVR)(001)	El equipo servidor	1	4	**1**	**4**
		(SW)(STD)(OS)(001)	Sistema Server	2	4	**2**	**4**
		(SW)(STD)(DB)(001)	Base de datos Oracle	3	4	**3**	**4**
		(SW)(STD)(OS)(002)	Sistema Medisys	4	3	**4**	**4**
		(HW)(PC)(002)	Computador de escritorio	1	3	**3**	**3**
		(IE)(DATA)(006)	Base de datos de investigación y docencia	3	4	**4**	**4**
		(IE)(DATA)(007)	Programa SPSS (hoja de cálculo Excel) Reporte semanal epidemiológicos	3	4	**4**	**4**
		(ED) (CPD)(001)	Centro de cómputo	4	3	**4**	**4**
		(RRHH)(AD)(001)	Responsable del proceso	2	3	**3**	**3**
		(RRHH)(AD)(002)	Usuario del módulo	3	3	**3**	**3**

Subproceso	Actividades	Activo	Descripción	C	D	I	Valoración
Estadística de emergencia	Apertura y entrega de números de historias clínica; Captación de pacientes asegurados: IESS, ISSFA, ISPOL, Seguro Campesino; Recepción de llamadas telefónicas del ECU 911; Control de las ambulancias para procesos con pacientes; Entrega de historias clínicas de emergencia ambulatorias y de hospitalización al archivo central.	(HW)(SVR)(001)	El equipo servidor	1	4	**1**	**4**
		(SW)(STD)(OS)(001)	Sistema Server	2	4	**2**	**4**
		(SW)(WEB)(002)	Ministerio de Salud Pública https://aplicaciones.msp.gob.ec/coresal	1	4	**3**	**4**
		(HW)(PC)(005)	Computador de escritorio	1	3	**3**	**3**
		(IE)(DATA)(010)	Registro Diario Automatizado de Consultas y Atenciones Ambulatorias	3	4	**4**	**3**
		(ED) (CPD)(001)	Centro de cómputo	4	3	**4**	**4**
		(RRHH)(AD)(001)	Responsable del proceso	2	3	**3**	**3**
		(RRHH)(AD)(009)	Usuario del módulo	3	3	**3**	**3**
		(RRHH)(AD)(013)	Usuario del módulo	3	3	**3**	**3**
		(RRHH)(AD)(005)	Usuario del módulo	3	3	**3**	**3**
		(RRHH)(AD)(015)	Usuario del módulo	3	3	**3**	**3**
Recuperación de costos hospitalarios	Recopilar la información de las historias clínicas, de los pacientes que cuentan con seguro IESS, Obtener del sistema Medisys las notas de evolución (citas médicas) Pasar al proceso de recaudación toda la información recopilada para que realicen el respectivo planillaje.	(HW)(SVR)(001)	El equipo servidor	1	4	**1**	**4**
		(SW)(STD)(OS)(001)	Sistema Server	2	4	**2**	**4**
		(SW)(STD)(DB)(001)	Base de datos Oracle	3	4	**3**	**4**
		(SW)(STD)(OS)(002)	Sistema Medisys	4	4	**4**	**4**
		(SW)(RED)(001)	Red LAN LABORATORIO	1	4	**3**	**4**
		(IE)(DATA)(008)	Notas de evolución de pacientes Excel	3	4	**4**	**4**
		(IP)(ARCHIVO)(002)	Notas de evolución de pacientes	3	4	**4**	**4**
		(HW)(PC)(014)	Computador de escritorio	1	3	**3**	**3**
		(HW)(PC)(018)	Computador de escritorio	1	3	**3**	**3**
		(ED) (CPD)(001)	Centro de cómputo	4	3	**4**	**4**
		(RRHH)(AD)(001)	Responsable del proceso	2	3	**3**	**3**

Subproceso	Actividades	Activo	Descripción	C	D	I	Valoración
		(RRHH)(AD)(014)	Usuario del módulo	3	3	**3**	**3**
		(RRHH)(AD)(018)	Usuario del módulo	3	3	**3**	**3**
		(RRHH)(AD)(019)	Usuario del módulo	3	3	**3**	**3**
Procesamiento de datos	Realizar los informes de odontología del dispensario anexo del IESS; Manejo del sistema Medisys para el registro de permisos y horarios de los médicos.	(HW)(SVR)(001)	El equipo servidor	1	4	**1**	**4**
		(SW)(STD)(OS)(001)	Sistema Server	2	4	**2**	**4**
		(SW)(STD)(DB)(001)	Base de datos Oracle	3	4	**3**	**4**
		(SW)(STD)(OS)(002)	Sistema Medisys	4	3	**4**	**4**
		(HW)(PC)(008)	Computador de escritorio	1	3	**3**	**3**
		(IE)(DATA)(009)	Informes de odontología y dispensario	3	4	**4**	**4**
		(IP)(ARCHIVO)(004)	Informes de odontología y dispensario	3	4	**4**	**4**
		(ED) (CPD)(001)	Centro de cómputo	4	3	**4**	**4**
		(RRHH)(AD)(001)	Responsable del proceso	2	3	**3**	**3**
		(RRHH)(AD)(008)	Usuario del módulo	3	3	**3**	**3**
Archivo y mensajería	Apertura y eliminación de la historia clínica; Archivo y conservación de las historias clínicas; Depuración permanente de las historias clínicas; Distribución y control de las historias clínicas entregadas a los consultorios de consulta externa, hospitalización y ambulatorios; Custodio de historias clínicas y demás documentos y registros del proceso.	(HW)(SVR)(001)	El equipo servidor	1	4	**1**	**4**
		(SW)(STD)(OS)(001)	Sistema Server	2	4	**2**	**4**
		(IP)(ARCHIVO)(003)	Archivo de Historias Clínicas	3	4	**4**	**4**
		(HW)(PC)(010)	Computador de escritorio	1	3	**3**	**3**
		(ED) (CPD)(001)	Centro de cómputo	4	3	**4**	**4**
		(RRHH)(AD)(001)	Responsable del proceso	2	3	**3**	**3**
		(RRHH)(AD)(010)	Usuario del módulo	3	3	**3**	**3**

Fuente: (Ministerio de Salud Pública-Estatuto 1537-, 2012) (Crespo Martínez P. E., 2017) *Elaborado por el autor*

3.16 Inventariar los activos de información

En este proceso es necesario llevar una matriz de inventarios por cada activo de información para de esta manera llevar un control más eficiente de los activos de información.

La siguiente matriz corresponde a las instalaciones en donde se encuentra ubicado el servidor.

Tabla 34. Inventario – activos de información - edificaciones

id_Activo	incremental	Descripción	Ubicación
(ED) (CPD)	(001)	Centro de Cómputo	Primer piso alto

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

Siguiendo con el inventario de los activos de información, a continuación se presenta la matriz de activos de información hardware, software, información electrónica, y recursos humanos, las mismas que contienen la siguiente información.

Tabla 35. Inventario – activos de información - hardware

id_Activo	incremental	Tipo	No. Serie	Fecha Compra	Proveedor	Garantía
(HW)(SVR)	(001)	BLD	J1146V1	26/07/2017	Compuequip DOS S.A.	Vigente
(HW)(PC)	(001)	BLD	MXJ63306LN	04/10/2006	Compuequip DOS S.A.	Vencida
(HW)(PC)	(002)	BLD	MXJ63306LZ	04/10/2006	Compuequip DOS S.A.	Vencida
(HW)(PC)	(003)	BLD	MXJ9030281	21/04/2009	TESECOMP	Vencida
(HW)(PC)	(004)	BLD	MXJ9030427	21/04/2009	TESECOMP	Vencida
(HW)(PC)	(005)	BLD	MXJ90301GN	21/04/2009	TESECOMP	Vencida
(HW)(PC)	(006)	BLD	MXJ90301GY	21/04/2009	TESECOMP	Vencida
(HW)(PC)	(007)	BLD	MXJ94706XV	28/12/2009	EQUICOMPU CÍA. LTDA	Vencida
(HW)(PC)	(008)	BLD	MXJ94706TM	28/12/2009	EQUICOMPU CÍA. LTDA	Vencida
(HW)(PC)	(010)	BLD	MXJ94706T9	28/12/2009	EQUICOMPU CÍA. LTDA	Vencida
(HW)(PC)	(011)	BLD	MXJ9470837	28/12/2009	EQUICOMPU CÍA. LTDA	Vencida
(HW)(PC)	(012)	BLD	MXL0382C4J	09/12/2010	Compuequip DOS S.A.	Vencida

id_Activo	incremental	Tipo	No. Serie	Fecha Compra	Proveedor	Garantía
(HW)(PC)	(014)	BLD	MXL1182FXZ	16/06/2011	ENTER SYSTEMS CÍA LTDA	Vencida
(HW)(PC)	(016)	BLD	MXL11908QX	16/06/2011	ENTER SYSTEMS CÍA LTDA	Vencida
(HW)(PC)	(017)	BLD	MXL2510B9G	18/03/2013	COMPUTADORAS Y FACILIDADES C A LTDA	Vencida
(HW)(PC)	(018)	BLD	MXL3101T6W	21/05/2013	COMPUFÁCIL CÍA LTDA.	Vencida
(HW)(PC)	(019)	BLD	MXL2032PBC	19/06/2012	SISCOMIN CIA LTDA	Vencida
(HW)(PC)	(020)	BLD	MJ00P01C	11/10/2014	SISCOMIN CIA LTDA	Vencida

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

Tabla 36. Inventario – activos de información - software

id_Activo	incremental	Descripción	Versión	Número de Serie	Clave activación	Fecha de compra	Actualización	Proveedor	Ubicación
(SW)(STD)(OS)	(001)	Sistema Server 2008	2003 Server R	XEON 3.4 GHZ		00/00/00		Compuequipos DOS	N / A
(SW)(STD)(DB)	(001)	Base de datos ORACLE	N / A	KQ42DOG	N / A	N / A	N / A	Coresolutions	N / A
(SW)(STD)(OS)	(002)	Sistema Medisys	N / A	N / A	N / A	N / A	N / A	N / A	N / A
(SW)(WEB)	(001)	www.hvcm.gob.ec	N / A	N / A	N / A	N / A	N / A	N / A	N / A
(SW)(EMAIL)	(001)	agendamientolinea@hvcm.gob.ec	N / A	N / A	N / A	N / A	N / A	N / A	N / A
(SW)(STD)(DBMS)	(001)	Base de datos MySQL	N / A	N / A	N / A	N / A	N / A	N / A	N / A
(SW)(STD)(SPH)	(001)	SIGPH Software de camas (Sistema Integral de Gestión de Pacientes Hospitalizados)	N / A	USE632NCL1	N / A	N / A	N / A	N / A	N / A
(SW)(WEB)	(002)	Ministerio de Salud Pública https://aplicaciones.msp.gob.ec/coresalud/app.php/publico/rpis/afiliacion/consulta	N / A	N / A	N / A	N / A	N / A	N / A	N / A
(SW)(WEB)	(003)	Registro Civil REVIT https://servicios1.registrocivil.gob.ec/revit/#_	N / A	N / A	N / A	N / A	N / A	N / A	N / A
(SW)(RED)(001)		Red LAN LABORATORIO	N / A	N / A	N / A	N / A	N / A	N / A	N / A

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

Tabla 37. Inventario - activos de información – información electrónica

id_Activo	Incremental	Tipo	Fecha de creación	Tamaño	Permisos	Ubicación	Nombre	Fecha de modificación	Creador
(IE)(DATA)	(001)	Matriz de agendamiento en Excel	02/01/2018	503 KB	N / A	(HW)(PC)(011)	Matriz de agendamiento	09/04/2018	(RRHH)(AD)(011)
(IE)(DATA)	(002)	Programa SPSS (hoja de cálculo Excel)	02/01/2018	450 KB	N / A	(HW)(PC)(006)	Archivo SPSS	09/04/2018	(RRHH)(AD)(006)
(IE)(DATA)	(003)	Programación de citas quirúrgicas	02/01/2018	230 KB	N / A	(HW)(PC)(004)	Programación de citas quirúrgicas	09/04/2018	(RRHH)(AD)(004)
(IE)(DATA)	(004)	Ingresos y egresos de pacientes	02/01/2018	611 KB	N / A	(HW)(PC)(003)	Ingresos y egresos de pacientes	09/04/2018	(RRHH)(AD)(003)
(IE)(DATA)	(005)	Matriz archivo SPSS de codificación	02/01/2018	436 KB	N / A	(HW)(PC)(016)	Matriz archivo SPSS de codificación	09/04/2018	(RRHH)(AD)(016)
(IE)(DATA)	(006)	Base de datos de investigación y docencia	02/01/2018	83 KB	N / A	(HW)(PC)(002)	Base de datos de investigación y docencia	09/04/2018	(RRHH)(AD)(02)
(IE)(DATA)	(007)	Programa SPSS (hoja de cálculo Excel) Reporte semanal epidemiológicos	02/01/2018	135 KB	N / A	(HW)(PC)(002	Reporte semanal epidemiológicos	09/04/2018	(RRHH)(AD)(02)
(IE)(DATA)	(008)	Notas de evolución de pacientes Excel	02/01/2018	168 KB	N / A	(HW)(PC)(014) (HW)(PC)(018) (HW)(PC)(019)	Notas de evolución de pacientes	09/04/2018	(RRHH)(AD)(014) (RRHH)(AD)(018) (RRHH)(AD)(019)
(IE)(DATA)	(009)	Informes de odontología y dispensario	02/01/2018	43K	N / A	(HW)(PC)(008)	Informes de odontología y dispensario	09/04/2018	(RRHH)(AD)(008)
(IE)(DATA)	(010)	Registro Diario Automatizado de Consultas y Atenciones Ambulatorias (RDACAA)	02/01/2018	32K	N / A	(HW)(PC)(009) (HW)(PC)(013) (HW)(PC)(005) (HW)(PC)(013)	(RDACAA)	09/04/2018	(RRHH)(AD)(009) (RRHH)(AD)(013) (RRHH)(AD)(005) (RRHH)(AD)(013)

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

Tabla 38. Inventario – activos de información – recursos humanos

id_Activo	incremental	Identificación	Cargo	Género	Fecha de ingreso	Fecha de salida
(RRHH)(AD)	(001)	Personal admisión 1	Responsable de admisiones	F	01/10/2014	N / A
(RRHH)(AD)	(002)	Personal admisión 2	Asistente de admisiones	M	01/09/2016	N / A
(RRHH)(AD)	(003)	Personal admisión 3	Asistente de admisiones	F	01/02/2017	N / A
(RRHH)(AD)	(004)	Personal admisión 4	Asistente de admisiones	F	01/10/2014	N / A
(RRHH)(AD)	(005)	Personal admisión 5	Analista de admisiones	F	01/11/2016	N / A
(RRHH)(AD)	(006)	Personal admisión 6	Asistente de admisiones	F	01/06/2017	N / A
(RRHH)(AD)	(007)	Personal admisión 7	Asistente de admisiones	M	01/07/2004	N / A
(RRHH)(AD)	(008)	Personal admisión 8	Analista de admisiones	F	01/07/2004	N / A
(RRHH)(AD)	(009)	Personal admisión 9	Asistente de admisiones	M	01/08/2017	N / A
(RRHH)(AD)	(010)	Personal admisión 10	Asistente de admisiones	F	01/07/2004	N / A
(RRHH)(AD)	(011)	Personal admisión 11	Asistente de admisiones	M	01/01/2016	N / A
(RRHH)(AD)	(012)	Personal admisión 12	Asistente de admisiones	F	01/11/2016	N / A
(RRHH)(AD)	(013)	Personal admisión 13	Analista de admisiones	F	05/09/2017	N / A
(RRHH)(AD)	(014)	Personal admisión 14	Asistente de admisiones	F	01/07/2004	N / A
(RRHH)(AD)	(015)	Personal admisión 15	Asistente de admisiones	M	01/07/2004	N / A
(RRHH)(AD)	(016)	Personal admisión 16	Asistente de admisiones	F	01/10/2017	N / A
(RRHH)(AD)	(017)	Personal admisión 17	Asistente de admisiones	F	01/02/2018	N / A
(RRHH)(AD)	(018)	Personal admisión 18	Asistente de admisiones	F	02/02/2018	N / A
(RRHH)(AD)	(019)	Personal admisión 19	Asistente de admisiones	F	01/02/2018	N / A
(RRHH)(AD)	(020)	Personal admisión 19	Asistente de admisiones	F	01/10/2017	N / A

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

3.17 Identificación de las amenazas

Es necesario identificar claramente cuáles podrían ser las posibles amenazas a las que está expuesta la entidad. Para una mejor determinación será necesario cuestionarse:

¿Qué puede pasar al suceder un evento no previsto? Seguido de las preguntas: ¿Cómo? ¿Dónde? ¿Por qué?, interrogantes que ayudarán en la identificación de las amenazas.

La metodología señala los siguientes grupos de amenazas.

Ilustración 9. Grupos de amenazas. Fuente: (Crespo Martínez P. E., 2017)

Será responsabilidad del comité de riesgos la eficiente identificación de las amenazas, que conlleva a tomar las mejores decisiones en la asignación de salvaguardas.

Las amenazas serán identificadas mediante la utilización de la técnica sinérgica que sugiere la guía, la misma que plantea lo siguiente.

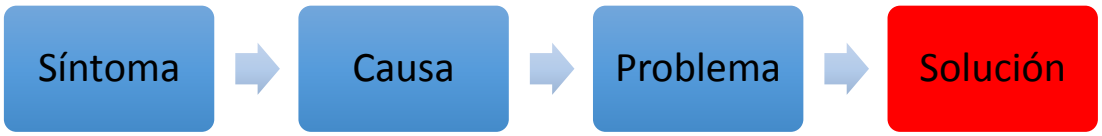

Ilustración 10. Técnica identificación de amenazas. Fuente: (Crespo Martínez P. E., 2017)

La siguiente matriz da a conocer la identificación de los síntomas, causas y problemas de la entidad, en donde también se coloca la frecuencia de ocurrencia en el último año. Es necesario llevar un registro de las amenazas las mismas que llevan un código y nombre para que sean de fácil identificación.

Tabla 39. Identificación de problemas

Síntoma	Causa	Problema	Código amenaza	Nombre	Frecuencia
Errores en el proceso de agendamiento	Un problema con el hardware del equipo	El equipo se apagó debido a un corto circuito	[PROVOCADO.3]	Cortocircuito	1
		Fallo en el sistema de ventilación del equipo	[NO_INTENCIONADO.3]	Errores de mantenimiento físico	2
		El disco duro tiene fallas	[PROVOCADO.2]	Corte energético	3
	Un problema de acceso a los sistemas	El disco duro del servidor se saturó	[NO_INTENCIONADO.3]	Errores de monitorización (log)	3
		Un virus informático dañó el sistema operativo	[EL.1]	Difusión de software dañino	2
		Fallas en la red	[NO_INTENCIONADO.NN]	Desconexiones por cambios en producción	3
		Una actualización del software	[PROVOCADO.1]	Alteración en la configuración	2
		Falla del correo electrónico	[NO_INTENCIONADO.2]	Errores del administrador	4
Reportes de codificaciones con datos incorrectos	Error en la asignación de los códigos CIE-10	Falta de criterio para la codificación	[NO_INTENCIONADO.NN]	Errores del administrador	3
		Personal con poco conocimiento en la codificación	[NO_INTENCIONADO.NN]	Sistema poco amigable	5
Reportes con datos erróneos de los diferentes servicios	Un problema con el software	Base de datos desactualizada de los diferentes servicios	[NO_INTENCIONADO.NN]	Error de consistencia en bases de datos	3
Usuario insatisfecho	Turnos mal agendados	Error en la asignación de la especialidad	[NO_INTENCIONADO.NN]	Elección incorrecta de parámetros / Complejidad del sistema	6
		Pacientes con más de una historia clínica en el sistema	[NO_INTENCIONADO.NN]	Error de consistencia en bases de datos	5
Error en la asignación de camas	Problemas en la atención al paciente	Historias clínicas con	[NO_INTENCIONADO.NN]	Error del usuario	6

Síntoma	Causa	Problema	Código amenaza	Nombre	Frecuencia
		documentación ilegible			
Reportes de hospitalización con errores	Datos erróneos de los ingresos y egresos de las hospitalizaciones	Control inadecuado de las historias clínicas	[NO_INTENCIONADO.NN]	Error del usuario	6
Historias clínicas con información errada	Errores de organización de la información física Mala conservación de las historias clínicas	Personal sin capacitación en documentación y archivo	[NO_INTENCIONADO.NN]	Error del administrador	4
Retrasos en la recuperación de costos	Falta de personal en el proceso	Planillaje atrasado de los servicios, para la recuperación de costos	[NO_INTENCIONADO.NN]	Error en rutinas del software – Error del administrador	2

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

Luego de la identificación de problemas y amenazas, es necesario llevar en una matriz el registro de las amenazas encontradas, las mismas que se les proporcionarán un código y nombre para que sean de fácil identificación y así llevar el control correspondiente. En esta matriz también se identificará los activos que podrían ser afectados y la respectiva dimensión en cuanto a la afectación ya sea a la confidencialidad, disponibilidad e integridad, así como lo demuestra la siguiente tabla.

Tabla 40. Matriz de identificación de las amenazas

Problema	Código de la amenaza	Nombre	Descripción	Tipo de Activos afectados	Dimensiones
Una configuración mal realizada por parte del administrador del sistema	[NO_INTENCIONADO.2]	Errores del administrador	Errores involuntarios de personas con responsabilidades de instalación y operación	[IE] información electrónica [IP] información en papel [SW] aplicaciones software [HW] equipos informáticos (hardware) [IC] infraestructura de comunicaciones	[D] disponibilidad [I] integridad [C] confidencialidad
Un virus informático dañó el sistema operativo	[EL.1]	Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, malware en general	[SW] software [IE] información electrónica	[D] disponibilidad [I] integridad [C] confidencialidad
Una actualización del sistema operativo	[NO_INTENCIONADO.4]	Errores de configuración	Introducción de datos de configuración errónea. Los activos dependen de su configuración y de la diligencia del administrador.	[IE] información electrónica [IP] información en papel	[I] integridad
El disco duro del servidor se saturó	[NO_INTENCIONADO.3]	Errores de monitorización (log)	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados y/o atribuidos.	[IE] información electrónica [IP] información en papel – Sobre registro de actividad / registro de errores	[I] integridad
Una actualización al sistema de ventanillas	[NO_INTENCIONADO.4]	Errores de configuración	Introducción de datos de configuración errónea. Los activos dependen de su configuración y de la diligencia del administrador.	[IE] información electrónica [IP] información en papel	[I] integridad

Problema	Código de la amenaza	Nombre	Descripción	Tipo de Activos afectados	Dimensiones
	[PROVOCADO.1]	Alteración en la configuración	Desastres debido a la actividad humana. Alteración deliberada al sistema informático Origen: Entorno (accidental) Humano (accidental o deliberado)	[IE] información electrónica	[I] integridad [D] disponibilidad
El disco duro tiene fallas	[PROVOCADO.2]	Corte energético	Corte energético Origen: Entorno (accidental) Humano (accidental o deliberado)	[HW] equipos informáticos (hardware) [EXTRAIBEL] soportes de información [RRHH] Recursos Humanos [ED] Edificaciones	[D] disponibilidad
El equipo se apagó debido a un cortocircuito	[PROVOCADO.3]	Cortocircuito	Cortocircuito Origen: Entorno (accidental) Humano (accidental o deliberado)	[HW] equipos informáticos (hardware) [EXTRAIBEL] soportes de información [RRHH] Recursos Humanos [ED] Edificaciones	[D] disponibilidad
Un módulo de memoria se ve afectado	[PROVOCADO.2]	Sobrecarga eléctrica	Corte energético Origen: Entorno (accidental) Humano (accidental o deliberado)	[HW] equipos informáticos (hardware) [EXTRAIBEL] soportes de información [RRHH] Recursos Humanos [ED] Edificaciones	[D] disponibilidad

Problema	Código de la amenaza	Nombre	Descripción	Tipo de Activos afectados	Dimensiones
Fallo en el sistema de ventilación del equipo	[NO_INTENCIONADO.3]	Errores de mantenimiento físico	Falta de mantenimiento a los equipos computacionales	[HW] equipos informáticos (hardware) [ED] Edificaciones	[D] disponibilidad
Fallas en la red	[NO_INTENCIONADO.NN]	Desconexiones por cambios en producción	Realizar cambios de producción en horarios inadecuados (Cuando los funcionarios están con la red en uso). Falta de comunicación al personal indicado para realizar este procedimiento	[RRHH] Recursos Humanos [IE] información electrónica	[D] disponibilidad [I] integridad
Falta de criterio para la codificación	[NO_INTENCIONADO.NN]	Errores del administrador	Falta de conocimiento de la codificación CIE-10	[IE] información electrónica	[I] integridad
Personal con poco conocimiento en la codificación	[NO_INTENCIONADO.NN]	Sistema poco amigable	Falta de capacitación al personal	[IE] información electrónica	[I] integridad
Base de datos desactualizada de los diferentes servicios	[NO_INTENCIONADO.NN]	Error de consistencia en bases de datos	Información que no corresponde a los datos reales	[SW] software [IE] información electrónica	[D] disponibilidad [I] integridad
Error en la asignación de la especialidad	[NO_INTENCIONADO.NN]	Elección incorrecta de parámetros / Complejidad del sistema	Introducción de datos erróneos	[IE] información electrónica	[D] disponibilidad [I] integridad

Problema	Código de la amenaza	Nombre	Descripción	Tipo de Activos afectados	Dimensiones
Pacientes con más de una historia clínica en el sistema	[NO_INTENCIONADO.NN]	Error de consistencia en bases de datos	Error en la búsqueda del paciente genera duplicidad de historias clínicas	[IE] información electrónica [IP] información en papel	[D] disponibilidad [I] integridad
Historias clínicas con documentación ilegible	[NO_INTENCIONADO.NN]	Error del usuario	Documentación generada por los médicos con letra ilegible	[IP] información en papel	[I] integridad
Control inadecuado de las historias clínicas	[NO_INTENCIONADO.NN]	Error del usuario	Rotación de personal	[IP] información en papel	[D] disponibilidad [I] integridad [C] confidencialidad
Personal sin capacitación en documentación y archivo	[NO_INTENCIONADO.NN]	Error del administrador	Rotación de personal	[IP] información en papel	[D] disponibilidad [I] integridad [C] confidencialidad
Planillaje atrasado de los servicios, para la recuperación de costos	[NO_INTENCIONADO.NN]	Error en rutinas del software – Error del administrador	Déficit de personal para este proceso	[IE] información electrónica [IP] información en papel	[D] disponibilidad [I] integridad

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

3.18 Análisis de los riesgos

En la siguiente matriz se hace un análisis de la situación actual de los riesgos y de las posibles causas que pudieron haber generado el problema, para de la misma manera establecer si existe un control actual que permita contrarrestar estas amenazas, de lo contrario se establecerán los controles en la matriz niveles de riesgo – acción de gestión requerida.

Tabla 41. Análisis de los riesgos de la entidad

Problema	Análisis	Control actual
El equipo se apagó debido a un corto circuito	La capacidad del generador eléctrico no abastece a toda la infraestructura sino solamente a las áreas críticas	Existe baterías UPS pero no tienen suficiente duración
Fallo en el sistema de ventilación del equipo	Si hay un error en el sistema de ventilación, se apaga el equipo	El equipo tiene un control de temperatura pero no existe un monitoreo
El disco duro tiene fallas	Estas fallas pueden ocasionar información inaccesible o incompleta	No existe control ya que no se puede predecir la falla de un disco
El disco duro del servidor se saturó	El crecimiento de los datos almacenados es mayor al de la capacidad o a lo previsto	Existen las alarmas de llenada del disco duro y su respectivo monitoreo y gestión
Un virus informático dañó el sistema operativo	Uso constante de dispositivos de almacenamiento extraíbles	Se cuenta con un antivirus corporativo de actualización centralizada
Fallas en la red	Instalaciones y equipos de red antiguos y defectuosas	Monitoreo de la red
Una actualización del software	Actualización liberada sin las suficientes pruebas	No existe el control
Falla del correo electrónico	Ataques de virus al servidor o falla en los equipos donde se encuentra alojado el servicio	No existe control porque el servicio es prestado por agentes externos al hospital

Problema	Análisis	Control actual
Falta de criterio para la codificación	Alta rotación del personal	No existe control
Personal con poco conocimiento en la codificación	No hay programas de capacitación	No existe control
Base de datos desactualizada de los diferentes servicios	Fallas en el equipo, muchas versiones de las mismas bases sin una correcta identificación	No existe el control
Error en la asignación de la especialidad	Por información incompleta o falsa para el Agendamiento de los turnos	Existe control de verificación con documentos físicos
Pacientes con más de una historia clínica en el sistema	Fallas de criterio de búsqueda y de identificación del paciente	Solicitud de documento de identificación al paciente
Base de datos desactualizada de la información de los pacientes	Fallas en el equipo, muchas versiones de las mismas bases sin una correcta identificación	No existe el control
Historias clínicas con documentación ilegible	Mal manejo físico de los documentos, falta de claridad en los registros	No existe el control
Planillaje atrasado de los servicios, para la recuperación de costos	Volumen de información y falta de personal para el proceso	No existe control
Control inadecuado de las historias clínicas	Falta de eficiencia en el proceso	No existe control
Personal sin capacitación en documentación y archivo	Por alta de rotación en el proceso y no hay inducción al personal	No existe control

Fuente: (Crespo Martínez P. E., 2017)

3.19 Cálculo del riesgo

El nivel de riesgo obtenido, es el resultado de multiplicar la probabilidad (frecuencia) por el impacto, se multiplica la frecuencia por cada una de las dimensiones afectadas según la matriz de la valoración de los activos. Para realizar esta matriz es muy necesario clasificar las amenazas por cada activo de información, de esta manera se puede llevar de una manera ordenada y de fácil comprensión.

En esta matriz se puede visualizar el nivel de riesgo al que está expuesta la entidad, y cómo podemos ver, existen amenazas que ocasionarían un nivel de riesgo alto, mediano y bajo, cuyos controles serán determinados en las matrices nivel de riesgo- acción de gestión requerida.

Tabla 42. Cálculo del riesgo

			Valor					Impacto			Riesgo Acumulado			Riesgo absoluto
PROCESO	ACTIVO	DESCRIPCIÓN	C	D	I	T	Frecuencia	C	D	I	C	D	I	
ADMISIONES	(HW)(SVR)(001)	El equipo servidor	1	4	1	4								
	[PROVOCADO.2]	Corte energético		D			3	0	4	0	0	12	0	12
	[NO_INTENCIONADO.3]	Errores de mantenimiento físico		D			2	0	8	0	0	8	0	8
	[PROVOCADO.3]	Cortocircuito		D			1	0	4	0	0	4	0	4
	(SW)(STD)(OS)(001)	Sistema Server	2	4	2	4								
	[EL.1]	Difusión de software dañino	C	D	I		2	2	4	2	4	8	4	8
	[PROVOCADO.1]	Alteración en la configuración		D	I		2	0	4	2	0	8	4	8
	[NO_INTENCIONADO.3]	Errores de monitorización (log)			I		3	0	0	2	0	0	6	12
	[NO_INTENCIONADO.NN]	Error de consistencia en bases de datos		D	I		3	0	4	2	0	12	6	12
	(IE)(DATA)	[IE] información electrónica	3	4	4	4								
	[NO_INTENCIONADO.NN]	Error de consistencia en bases de datos		D	I		3	0	4	4	0	12	12	12
	[NO_INTENCIONADO.NN]	Desconexiones por cambios en producción		D	I		3	0	4	4	0	12	12	12
	[NO_INTENCIONADO.2]	Errores del administrador			I		4	0	0	4	0	0	16	16
	[NO_INTENCIONADO.NN]	Errores del administrador			I		3	0	0	4	0	0	12	12
	[NO_INTENCIONADO.NN]	Sistema poco amigable			I		5	0	0	4	0	0	20	20

			Valor					Impacto			Riesgo Acumulado			Riesgo absoluto
PROCESO	ACTIVO	DESCRIPCIÓN	C	D	I	T	Frecuencia	C	D	I	C	D	I	
	[NO_INTENCIONADO.NN]	Elección incorrecta de parámetros / Complejidad del sistema		D	I		6	0	4	4	0	24	24	24
	[NO_INTENCIONADO.NN]	Error de consistencia en bases de datos		D	I		5	0	4	4	0	20	20	20
	[NO_INTENCIONADO.NN]	Error en rutinas del software – Error del administrador		D	I		2	0	4	4	0	8	8	8
	(IP)(ARCHIVO)	[RRHH] Recursos Humanos	3	3	3	3								
	[NO_INTENCIONADO.NN]	Desconexiones por cambios en producción		D	I		3	0	3	3	0	9	9	9
	(IP)(ARCHIVO)	[IP] información en papel	3	4	4	4								
	[NO_INTENCIONADO.NN]	Error de consistencia en bases de datos		D	I		5	0	4	4	0	20	20	20
	[NO_INTENCIONADO.NN]	Error del usuario			I		6	0	0	4	0	0	24	24
	[NO_INTENCIONADO.NN]	Error del usuario	C	D	I		6	3	4	4	18	24	24	24
	[NO_INTENCIONADO.NN]	Error del administrador	C	D	I		4	3	4	4	12	16	16	16
	[NO_INTENCIONADO.NN]	Error en rutinas del software – Error del administrador		D	I		2	0	4	4	0	8	8	8

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

3.20 Tratamiento de los riesgos

Luego de la identificación del riesgo, la siguiente matriz tiene por objetivo determinar el tipo de tratamiento que se puede implementar para evitar o minimizar el riesgo. Es importante también identificar que busca el control implementado para de esta manera realizar la respectiva evaluación y supervisión.

Tabla 43. Niveles de riesgos – acción de protección sugerida

Niveles de Riesgo – Acción de gestión sugerida						
Nivel de Riesgo	**Acción requerida**	**Riesgo identificado**	**Tipo de tratamiento**	**Objetivo del tratamiento del riesgo mencionado**	**Origen del riesgo (posibles causas)**	**Que busca el control**
Alto (A)	Debe otorgársela la atención apropiada	Sistema poco amigable	El tratamiento debe ser específico, como por ejemplo un programa de capacitación	Reducir los errores en la asignación de los códigos CIE-10	Falta de experiencia del personal en esa actividad por la alta rotación	Reducir los errores en la codificación de enfermedades para que los reportes generen los indicadores respectivos
		Elección incorrecta de parámetros / Complejidad del sistema	Mayor responsabilidad en el agendamiento de turnos	Reducir el agendamiento inadecuado y buscar la satisfacción del usuario	Alta demanda en el agendamiento	La optimización de los turnos asignados a los especialistas correspondientes
		Error de consistencia en bases de datos	Actualización de los datos de los usuarios	Reducir la duplicidad de las historias clínicas	Rápida asignación de los turnos hace que el personal le asigne una nueva historia clínica	Evitar tener información inadecuada y disminuir el archivo de papel
		Error de consistencia en bases de datos	Monitoreo de la base de datos	Detectar a tiempo los errores de la inconsistencia en base de datos	Falla en la escritura de los datos Falla introducida por cortes de energía eléctrica	Minimizar las inconsistencias de la base de datos

Niveles de Riesgo – Acción de gestión sugerida						
Nivel de Riesgo	**Acción requerida**	**Riesgo identificado**	**Tipo de tratamiento**	**Objetivo del tratamiento del riesgo mencionado**	**Origen del riesgo (posibles causas)**	**Que busca el control**
		Error del usuario del proceso	Control oportuno en el seguimiento de la historia clínica Concienciar a los profesionales de la salud en la clara y precisa información detallada	Llevar el registro eficiente de los ingresos y egresos de las hospitalizaciones Evitar la incorrecta codificación de las enfermedades	Retraso en las devoluciones de las historias clínicas al proceso Cantidad de turnos agendados	Llevar un adecuado y eficiente archivo de la documentación Información exacta y confiable
Medio (M)	Evaluar el riesgo y determinar si los controles implementados son suficientes y si están siendo efectivos	Corte energético	El tratamiento debe ser específico en este caso aumentar la capacidad del generador eléctrico	Dar continuidad al procesamiento de las plataformas informáticas ante los eventos de energía eléctrica	Generador con baja capacidad	Evitar la paralización de los servicios por un corte de energía eléctrica
		Errores de mantenimiento físico	El tratamiento específico es la implementación de una política de limpieza física periódica (al menos dos veces por año)	Evitar el recalentamiento de los equipos de computación por acumulación de polvo en ventiladores y circuitos electrónicos	No existe una política de mantenimiento físicos de los equipos No se reemplaza partes móviles como ventiladores dentro de un tiempo prudencial	Realizar mantenimientos preventivos a los equipos computacionales
		Difusión de software dañino	Mantener actualizado las políticas de antivirus y seguridad de instalación	Eliminar la introducción de software malicioso	La falta de políticas de instalación del software y fallas en la actualización del antivirus	Implementar el debido control para evitar este riesgo
		Alteración en la configuración	Implementación de políticas de configuración	Recudir el número de incidentes producidos	Que se encuentren habilitados las actualizaciones automáticas sin ninguna configuración	Evitar que se produzcan problemas de configuración

Niveles de Riesgo – Acción de gestión sugerida						
Nivel de Riesgo	**Acción requerida**	**Riesgo identificado**	**Tipo de tratamiento**	**Objetivo del tratamiento del riesgo mencionado**	**Origen del riesgo (posibles causas)**	**Que busca el control**
		Errores de monitorización (log)	Establecer un procedimiento periódico de revisión de los log	Detectar a tiempo los errores en el disco duro para solventar los problemas	Falta de tiempo y organización del personal	Detectar a tiempo los errores en el disco duro para solventar los problemas
		Desconexiones por cambios en producción	Revisar periódicamente los ups eléctricos para evitar cortes	Prevenir errores y cortes en la red por fallas en os quipos	Infraestructura eléctrica antigua	Minimizar el impacto de fallas en los equipos
		Errores del administrador	Confirmación de tareas	Verificar los datos ingresado	Elevada carga de trabajo del personal	Disminuir los errores del administrador
Bajo (B)	Administrar mediante procedimientos rutinarios; informar a los gestores locales; supervisar y revisar localmente como sea necesario	Cortocircuito	Implementar una política de verificación periódica del sistema eléctrico de la entidad	Prevenir la posibilidad de corto circuito provocado por el recalentamiento de equipos de computación	No existe una política de mantenimiento preventivo de la organización	Evitar el problema de disponibilidad de recursos de tecnologías causado por un cortocircuito

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

3.21 Políticas y contramedidas a los riesgos identificados

La implementación de una política de seguridad podría definirse en cuatro etapas:

1. Identificar las necesidades de la seguridad de los riesgos de información a los que se expone la entidad y sus posibles efectos,
2. Proporcionar una perspectiva general de las reglas y procedimientos a implementarse en las diferentes áreas,
3. Controlar y determinar las vulnerabilidades de los sistemas de información,
4. Determinar las acciones y contactos a realizarse en caso de la materialización del riesgo. (Benchmark, 2018)

En la siguiente tabla se recomienda las políticas y contramedidas a los riesgos identificados en la entidad, los mismos que afectarían a los activos de información de la organización, el objetivo de las contramedidas es realizar las acciones correspondientes para minimizar la materialización del riesgo.

Tabla 44. Políticas y contramedidas

RIESGOS IDENTIFICADOS	POLÍTICA	PROCEDIMIENTO	ACTIVIDADES
• Sistema poco amigable • Elección incorrecta de parámetros / Complejidad del sistema • Error de consistencia en bases de datos • Error del usuario del proceso	Gestión de software	Adquisición del software	• Evaluar soluciones en ambientes controlados, • Evaluar al proveedor en parámetros de: Experiencia con el producto, experiencia en el mercado, sostenibilidad financiera, • Solicitar al menos 3 propuestas previo a la toma de decisiones, • Realizar la evaluación del software considerando: 1) aspectos técnicos, 2) aspectos funcionales, 3) aspectos de seguridad, 4) aspectos legales, 5) aspectos de escalabilidad.
		Implementación	• Cronograma de implementación, • Cronograma de capacitación a los usuarios, • Parametrización del sistema adquirido,

RIESGOS IDENTIFICADOS	POLÍTICA	PROCEDIMIENTO	ACTIVIDADES
			• Puesta en marcha del sistema de respaldos, • Implementar los métodos de contingencia para solventar problemas de inconsistencias por corte de energía.
		Uso	• Evaluación del nuevo sistema.
		Baja	• Respaldar la información generada, • Respaldar los instaladores del programa y de las bases de datos para consultas futuras.
• Error de consistencia en bases de datos (Falla introducida por cortes de energía eléctrica)	Gestión de UPS	Adquisición del UPS	• Evaluar al proveedor en parámetros de: Experiencia con el producto, experiencia en el mercado, sostenibilidad financiera, • Solicitar al menos 3 propuestas previo a la toma de decisiones, • Evaluar las características de los equipos.
		Implementación	• Instalación de los equipos.
		Uso	• Mantenimiento y monitoreo de las alarmas del equipo.
		Baja	• Informe técnico del funcionamiento (área de mantenimiento).
• Corte energético (Generador con baja capacidad) • Desconexiones por cambios en producción	Gestión de infraestructura de alimentación eléctrica	Adquisición de componentes eléctricos	• Realizar un estudio de carga / requisitos de alimentación eléctrica, • Evaluar al proveedor en parámetros de: Experiencia con el producto, experiencia en el mercado, sostenibilidad financiera,

RIESGOS IDENTIFICADOS	POLÍTICA	PROCEDIMIENTO	ACTIVIDADES
• Cortocircuito			• Realizar la evaluación del las fuentes de alimentación ininterrumpida considerando: • 1) aspectos técnicos, • 2) aspectos funcionales, • 3) aspectos de seguridad, • 4) disposición ambiental, • 5) aspectos de escalabilidad.
		Implementación	• Cronograma de la implementación, • Elección de los servicios de inicio, • Pruebas de tiempos de respuestas, • Puesta en marcha del equipo.
		Uso	• Realizar el monitoreo preventivo del equipo.
		Baja	• Realizar la evaluación técnica del funcionamiento de equipos.
• Errores de mantenimiento físico de los equipos	Gestión de mantenimiento preventivo y correctivo de equipos	Plan de mantenimiento de los equipos	• Realizar la adquisición de repuestos de equipos informáticos.
		Implementación	• Desarrollar el plan de mantenimiento preventivo, • Actualizar del plan de mantenimiento.
		Reemplazo de componentes y partes	• Solicitar informe técnico, • Adquirir componentes, • Recibir el componente defectuoso, • Registrar el componente defectuoso y registrar su baja.
		Ejecución	• El mantenimiento de los equipos deberá ser realizado únicamente por empresas externas y/o personal interno debidamente capacitado, y que demuestren al

RIESGOS IDENTIFICADOS	POLÍTICA	PROCEDIMIENTO	ACTIVIDADES
			menos 1 año de experiencia en esta actividad.
		Monitoreo	• Realizar un tablero de control de las actividades relacionadas con el mantenimiento preventivo, • Registrar los mantenimientos correctivos realizados a los equipos e impresoras de la entidad.
• Difusión de software dañino	Monitoreo de funcionamiento y políticas del antivirus	Establecer frecuencias del monitoreo del antivirus	• Revisar el correcto funcionamiento del antivirus verificando la respectiva actualización (diariamente), • Realizar un muestreo del monitoreo del antivirus, • Realizar la gestión del nuevo antivirus al término de la licencia.
	Gestión de antivirus	Adquisición de antivirus	• Evaluar soluciones en ambientes controlados, • Evaluar al proveedor en parámetros de: Experiencia con el producto, experiencia en el mercado, sostenibilidad financiera, • Solicitar al menos 3 propuestas previo a la toma de decisiones, • Realizar la evaluación del software considerando: 1) aspectos técnicos, 2) aspectos funcionales, 3) aspectos de seguridad, 4) aspectos legales, 5) aspectos de escalabilidad. • Realizar pruebas comparativas del antivirus, puede ser a través de: Pruebas de protección contra malware, pruebas de rendimiento, con el afán de seleccionar un proveedor confiable.

RIESGOS IDENTIFICADOS	POLÍTICA	PROCEDIMIENTO	ACTIVIDADES
			• Definir un entorno aislado para las pruebas.
		Implementación y despliegue	• Instalar el antivirus, • Instalar la licencia, • Registrar la licencia, • Realizar las configuraciones de tipo de detección (Normal/Heurística/Avanzada).
		Operación	• Identificar los equipos alertados en la consola de administración, • Aislar el equipo infectado, • Evaluar el tipo de amenaza encontrada, • Registrar el incidente identificado en bitácora, • Ejecutar el procedimiento de desinfección.
		Monitoreo	• Registrar los incidentes identificados en la consola de administración en una bitácora.
		Baja	• Reportar la baja del antivirus a contabilidad, • Actualizar el estado del activo de información (SW) (AV) en la base de datos, a BAJA.
• Alteración en la configuración	Monitero de la configuración de los sistemas	Esblecer la frecuencia de configuraciones	• Realizar el muestreo del monitoreo de las configuraciones del sistema mensualmente.
• Errores de monitorización (log) • Errores del administrador (elevada carga	Realizar evaluaciones del nivel de desempeño del personal	Evaluar el nivel de desempeño y la carga laboral del personal	• Verificar el cumplimiento de las funciones del personal de TIC, • Medir en porcentajes el desempeño del personal por parte de la Unidad de Talento Humano, • Establecer si existe brecha de personal en el área de TIC, y de ser afirmativa realizar las gestiones

RIESGOS IDENTIFICADOS	POLÍTICA	PROCEDIMIENTO	ACTIVIDADES
de trabajo del personal)			pertinentes para contar con la respectiva aprobación y recursos para la contratación.

Fuente: (Crespo Martínez P. E., 2017) *Elaborado por el autor*

4 Conclusiones

- El sector de la salud, cuenta con un amplio marco legal y normativo que garantizan la salud de los ecuatorianos, su deber fundamental es la implementación de políticas y normas así como la regulación y control de las entidades del sector salud.

- El Art. 66 de la Constitución de la República (2008) estipula el derecho a la protección de datos de carácter personal, pero todavía no está regulado; por lo que el Ecuador cuenta con un Proyecto de Ley de Protección de Datos Personales, cuyo objetivo es resguardar la información protegiendo los derechos, así como también regular el intercambio de los datos.

- Mientras que los países latinoamericanos se esfuerzan por ponerse al día en tecnologías de la información, empresas españolas se comprometen en colaborar en la búsqueda y el desarrollo de nuevas soluciones tecnológicas de apoyo a los actores del sistema sanitario, así como la implementación de la Salud Digital.

- El sector hospitalario, al contar con sistemas de información necesita proteger la misma, por lo que es clave determinar la necesidad de implementar una política de seguridad de la información, por lo que es fundamental saber qué información tiene, en dónde se encuentra, quiénes tienen acceso y a que velocidad la obtienen y por ende el valor de dicha información, para que de esta manera puedan definir los controles correspondientes.

- La metodología ECU@Risk ha dado a conocer los principios y procedimientos para la aplicación de la gestión de riesgos en una entidad, los mismos que traerán múltiples beneficios a la misma, ya que podrá identificar, valorar y tomar medidas preventivas para evitar la materialización de las amenazas. Mediante su aplicación se inventarió los activos de información y se identificaron posibles amenazas, lo que conllevó a determinar tipos de tratamiento y posibles controles que se puedan implementar.

- Mediante la implementación de un SGSI, las organizaciones no solamente obtendrán controles mediante políticas y procedimientos, sino que las normas detallan también los elementos que serán la base

para la determinación de las reglas de la organización, las mismas que son necesarias para prevenir infracciones de la seguridad de la información.

- El nivel de riesgo del sector hospitalario, es moderado para lo cual las entidades deberán tomar las medidas necesarias e implementar los controles adecuados y salvaguardas correspondientes para de esta manera ofrecer a los usuarios de las entidades de salud, la seguridad requerida en los procesos de información que reposa en las entidades de este sector, información que se considera crítica.

- La aplicación del SGSI, permitió identificar las diferentes probabilidades de materialización del riesgo, para luego analizar el nivel de riesgo de la entidad, el mismo que está compuesto por riesgos altos, moderados y bajos en el proceso analizado, los mismos que se centran en errores del usuario del proceso, un sistema poco amigable y en errores de consistencia de las bases de datos.

5 **Recomendaciones**

- Socializar y verificar el cumplimiento del acuerdo de confidencialidad de la información, que el hospital mantiene con los funcionarios.

- Considerando la determinación de los riesgos identificados, se recomienda la aplicación de las contramedidas y políticas de seguridad detalladas, las mismas que servirán para un correcto desarrollo en la seguridad de la información.

- Tomar las medidas necesarias para proteger los activos de información de la entidad con la finalidad de evitar que se produzcan los riesgos, como es el monitoreo del antivirus y configuraciones.

- Implementar políticas de acceso a las redes institucionales (red de cableado, red inalámbrica) y verificar el uso solamente del personal autorizado.

- Implementar tablas de auditoría en el sistema Medisys y de agendamiento, con la finalidad de llevar un registro de fechas y horas de acceso a las historias clínicas y a los movimientos de turnos agendados.

- Realizar un programa de capacitación para el personal encargado de la codificación de enfermedades según la Clasificación Estadística Internacional de Enfermedades y Problemas relacionados con la Salud de los egresos de hospitalización y emergencia CIE-10; así como en el correcto manejo del archivo físico de las historias clínicas.

- Realizar un plan de contingencia en la actualización de los datos de los usuarios a fin de que se cuente solo con una historia clínica y evitar la saturación del software.

- Implementar una política de verificación periódica del sistema eléctrico de la entidad con la finalidad de evitar que se produzcan eventos de corto circuitos, así como el mantenimiento preventivo de los equipos de información Hardware.

- Se recomienda realizar la implementación de la metodología analizada, la misma que servirá para el correcto funcionamiento del área de admisiones en cuanto a la seguridad de la información, con el fin de resguardar la información de los pacientes como de los profesionales de la entidad, evitando así fugas de información que terminarán afectando la imagen de la entidad como la integridad de los pacientes.

6 Bibliografía

(s.f.).

Acuerdo Ministerial 5216. (29 de 01 de 2015). *Reglamento de información confidencial en sistema nacional de salud.* Obtenido de http://instituciones.msp.gob.ec/cz6/images/lotaip/Enero2015/Acuerdo%20Ministerial%205216.pdf

Ametic. (19 de 01 de 2018). *Acuerdo de colaboración para impulsar el uso de las TIC en el sector salud.* Obtenido de http://ametic.es/es/noticias/acuerdo-de-colaboracion-para-impulsar-el-uso-de-las-tic-en-el-sector-salud

Bebea, I. (2013). *TIC Y SALUD.* Obtenido de https://ongawa.org/publicaciones/tic-y-salud/

Benchmark, C. (04 de 2018). *Introducción a la seguridad infromática.* Obtenido de https://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica

Boletín Jurídico-Cámara de Comercio de Quito. (06 de 2017). *Clasificación de las PYMES, PEqueña y Mediana Empresa.* Obtenido de http://www.ccq.ec/wp-content/uploads/2017/06/Consulta_Societaria_Junio_2017.pdf

Chueke, D. (16 de 04 de 2015). *Panorama de la Telemedicina en América Latina.* Obtenido de http://teleiberoamerica.com/publicaciones/TelemedicinaAmericaLatinaEyeforPharma04-16-2015.pdf

CIIFEN. (s.f.). *Aproximación para el cálculo de riesgo.* Obtenido de http://www.ciifen.org/index.php?option=com_content&view=category&id=84&layout=blog&Itemid=111&lang=es

CLINIC-CLOUD. (09 de 05 de 2018). *Nueva Ley de Protección de Datos.* Obtenido de https://clinic-cloud.com/blog/nueva-ley-proteccion-datos/

COBIT 5. (s.f.). *Isaca - Pablo, Caneo Gutierrez*. Obtenido de http://www.isaca.org/chapters8/montevideo/cigras/documents/cigras2015/cigras-2015.09.09-07-cobit%205%20para%20riesgos.%20metodologia.%20una%20vision%20general-pablo%20caneo.pdf

Collazos Balaguer, M. (s.f.). *La nueva versión ISO 27001:2013*. Obtenido de Un cambio en la integración de los sistemas de gestión: file:///C:/Users/Juan%20Fernando/Downloads/PRESENTACION_MANUEL_COLLAZOS_-_1%20(2).pdf

Constitución del Ecuador. (2008). Obtenido de http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf

Cordero Torres, G. (2015). *Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para Análisis y Gestión de Riesgos de Seguridad de la Información.* Obtenido de http://dspace.uazuay.edu.ec/bitstream/datos/5051/1/11490.pdf

Crespo Martínez, P. (29 de Noviembre de 2016). *Metodología de Seguridad de la Información para la Gestión del Riesgo Informático aplicable a MPYMES*. Obtenido de http://dspace.ucuenca.edu.ec/bitstream/123456789/26105/1/Tesis.pdf

Crespo Martínez, P. E. (2017). *Guía Metodológica para la implementación de ECU@risk.* Cuenca.

Crespo Rin, M. d. (01 de 2013). *El Análisis de Riesgos dentro de una Auditría Informática: Pasos y posibles metodologías.* Obtenido de https://e-archivo.uc3m.es/bitstream/handle/10016/16802/PFC_Carmen_Crespo_Rin.pdf?sequence=1&isAllowed=y

Editorial Ariel, & Fundación Telefónica. (04 de 2008). *Las TIC y el sector salud en Latinoamérica.* Obtenido de https://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/27/

EGSI - Acuerdo Ministerial 166, modificado. (15 de 06 de 2016). *Esquema Gubernamental de Seguridad de la Información.* Obtenido de http://www.politica.gob.ec/wp-content/uploads/2017/04/EGSI.pdf

ehCOS-. (2017). *Ciberseguridad en los hospitales: prevenir como defensa a cualquier ataque.* Obtenido de https://www.ehcos.com/ciberseguridad-hospitales-prevenir-como-defensa-ataque/

ehCOS. (2017). *Seguridad, privacidad y confidencialidad de la información médica del paciente.* Obtenido de https://www.ehcos.com/seguridad-privacidad-confidencialidad-la-informacion-medica/

ehCOS-. (2018). *10 tendencias de las tecnologías de salud (I).* Obtenido de https://www.ehcos.com/tendencias-esalud-latinoamerica-i/

ehCOS-. (2018). *10 tendencias de las tecnologías de salud (II).* Obtenido de https://www.ehcos.com/predicciones-salud-latinoamerica-ii-2018/

ehCOS-. (2018). *10 tendencias de las tecnologías de salud (III).* Obtenido de https://www.ehcos.com/tendencias-tic-salud-2018-iii/

elCOLOMBIANO. (19 de 09 de 2016). *Las TIC guardan revolución para la salud.* Obtenido de http://www.elcolombiano.com/antioquia/las-tic-revolucionaran-la-atencion-de-la-salud-XE5006044

Escobar, B., Escobar, T., & Monge, P. (2014). Tecnologías de la información en el sector hospitalario. *Revista aeca105*, 31-33.

Espinosa Diego, Martínez Juan, Amador Siler . (Julio-Diciembre de 2014). *Gestión del riesgo en la seguridad de la información*. Obtenido de http://web.usbmed.edu.co/usbmed/fing/v5n2/pdf/Articulo_Gestion_Riesgo_Seguridad_Informacion

Espinosa, V., Acuña, C., De la Torre, D., & Tambini, G. (2017). La reforma en salud del Ecuador. *Revista Panamericana de Salud Pública*, 41:e96.

Esquema gubernamental de seguridad de la información. (s.f.).

González Martínez , R. (s.f.). *Qualpro Consulting S.C.* Obtenido de COSO III - Marco Integrado de Control Interno: https://www.ofstlaxcala.gob.mx/doc/material/27.pdf

Gonzalez, H. (10 de 08 de 2015). *ISO 9001:2015 Enfoque basado en riesgos.* Obtenido de https://calidadgestion.wordpress.com/2015/08/10/iso-90012015-enfoque-basado-en-riesgos/

González, H. (10 de 10 de 2016). *ISO 31000:2009 Gestión del riesgo.* Obtenido de https://calidadgestion.wordpress.com/2016/10/28/gestion-del-riesgo-iso-31000/

Hernández Ramírez, N. (02 de 2015). *Análisis FODA.* Obtenido de http://ri.uaemex.mx/bitstream/handle/20.500.11799/31387/secme-18588.pdf?sequence=1

Iraburu, M. (2006). *Revista Anales del Sistema Sanitario de Navarra.* Obtenido de http://scielo.isciii.es/scielo.php?pid=S1137-66272006000600006&script=sci_arttext&tlng=pt

ISO 27000. (s.f.). Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO 27001. (s.f.). *27001Academy*. Obtenido de https://advisera.com/27001academy/es/que-es-iso-27001/

ISOTolls Excellence. (15 de 06 de 2016). *Blog especializado en SGSI.* Obtenido de https://www.pmg-ssi.com/2016/06/norma-iso-27001-iso-27799-sector-salud/

IT/USERS. (2018). Las TIC en el Sector Salud. *IT/MEDICAL*.

Ley de Derechos y Amparo al Paciente. modificado. (22 de 12 de 2006). Obtenido de http://www.salud.gob.ec/wp-content/uploads/downloads/2014/09/Normativa-Ley-de-Derechos-y-Amparo-del-Paciente.pdf

Ley orgánica de transparencia y acceso a la información pública. (18 de 05 de 2004). Obtenido de http://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cpccs_22_ley_org_tran_acc_inf_pub.pdf

Ley Orgánica del Sistema Nacional de Salud. (17 de 09 de 2002). Obtenido de http://www.todaunavida.gob.ec/wp-content/uploads/downloads/2013/10/ley-sis-nac-salud.pdf

Llanusa Ruiz, S. B., Rojo Pérez, N., Carabolloso Hernández , M., Capote Mir, R., & Pérez Piñero, J. (05 de 04 de 2005). *Revista Cubana de la Salud Pública.* Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-34662005000300008

López Jaramillo, D. M., & Vásquez Mejía, S. A. (2016). *Comparación entre metodologías de gestión de riesgo informático.*

M.S.P. Coordinación Zonal 6. (05 de 2014). *Plan Estratégico HVCM 2014-2017.* Obtenido de http://hvcm.gob.ec/wp-content/uploads/2015/08/Planificacio%CC%81n-Estrategica-Hospital-Vicente-Corral-Moscoso-2014-2017.pdf

Magerit 1. (1997). *Consejo Superior de Administración Electrónica.* Obtenido de http://dis.um.es/~barzana/Curso03_04/MAGERIT.pdf

Magerit 2. (2006). *Consejo Superior de Administración Electrónica.* Obtenido de http://www.pilar-tools.com/doc/magerit/v2/meth-es-v11.pdf

Magerit 3. (2012). *Consejo Superior de Administración Electrónica.* Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Minchala Márquez, P. A. (2016). *Estudio Comparativo de las metodologías COBIT 5 y COSO III para la gestión de riesgo de TI.*

Ministerio de Salud Pública. (s.f.). *Direción Nacional de Ambiente y Salud*. Obtenido de http://www.salud.gob.ec/direccion-nacional-de-ambiente-y-salud/

Ministerio de Salud Pública-Estatuto 1537-. (31 de 07 de 2012). *Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Salud Pública 1537 .* Obtenido de http://instituciones.msp.gob.ec/somossalud/images/guia/documentos/estatuto_de_hosp_acuerdo.pdf

Ministerio de Telecomunicaciones y Sociedad de la Información. (s.f.). Obtenido de https://www.telecomunicaciones.gob.ec//wp-content/uploads/downloads/2012/11/LEY-DEL-SISTEMA-NACIONAL-DE-REGISTRO-DE-DATOS-PUBLICOS.pdf

Ministerio del Ambiente. (s.f.). *Código Orgánico del Ambiente*. Obtenido de http://www.ambiente.gob.ec/codigo-organico-del-ambiente-coa/

Molina Miranda , M. F. (2015). *Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral.* Obtenido de http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

Naranjo, L. (11 de 05 de 2018). *DINARDAP*. Obtenido de http://www.datospublicos.gob.ec/dinardap-cuestiono-el-proyecto-de-ley-de-proteccion-de-los-derechos-a-la-intimidad-que-analiza-la-asamblea-nacional/

Naranjo, L. (29 de 04 de 2018). *Ecuador no tiene ley para proteger datos personales.* Obtenido de https://www.eluniverso.com/noticias/2018/04/29/nota/6736146/ecuador-no-tiene-ley-proteger-datos-personales

NTE-INEN-ISO-27799. (01 de 2014). *Instituto Ecuatoriano de Normalización.* Obtenido de http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2014/EXTRACTO_2014/VGR/nte_inen_iso_27799extracto.pdf

Orduña Ortegón, Y. (12 de 2014). *Avances en la construcción de un sistema de información en sauld en Colombia.* Obtenido de https://revistas.lasalle.edu.co/index.php/sv/article/view/3297

Organización Mundial de la Salud. (s.f.). Obtenido de http://www.who.int/suggestions/faq/es/

Ormella Meyer , C. (16 de 01 de 2014). *Las Nuevas Versiones de las Normas ISO 27001 e ISO 27002.* Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

Plazzota , F., Luna, D., & González, F. (06 de 2015). *Revista Peruana de Medicina Experimental y Salud Pública.* Obtenido de http://www.scielo.org.pe/scielo.php?pid=S1726-46342015000200020&script=sci_arttext&tlng=pt

Portafolio. (05 de 12 de 2016). *Tecnología al servicio de la salud.* Obtenido de http://www.portafolio.co/innovacion/tecnologia-al-servicio-de-la-salud-502059

PÚBLICO. (12 de 05 de 2017). *El Gobierno británico confirma "un ataque informático a gran escala" contra el Sistema Nacional de Salud.* Obtenido de http://www.publico.es/internacional/ciberataque-hospitales-britanicos.html

Rojas González , I., Sánchez Pérez, G., Toscano Medina , L., Prudente Tíxtico, M. C., & Aguilar Torres, G. (06 de 2012). *Leyes de protección de datos personales en el mundo.* Obtenido de http://www.rpmesp.ins.gob.pe/index.php/rpmesp/article/view/1630

Rojas Mezarina, L., Cedamanos Medina, C. A., & Vargas Herrera, J. (13 de 05 de 2015). *Revista Peruana de Medicina Experimental y Salud Pública.* Obtenido de https://www.scielosp.org/article/rpmesp/2015.v32n2/395-396/es/

Secretaría Nacional de Comunicación. (s.f.). Obtenido de http://www.comunicacion.gob.ec/objetivos/

Serra, C. (s.f.). *ISO, 31000-2009*. Obtenido de Herramienta para evaluar la gestión de riesgos: https://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf

Velásquez Pérez, T., Puentes Velásquez, A. M., & Pérez Pérez, Y. M. (2015). Un enfoque de buenas prácticas de gobierno corporativo de TI. *Revista Tecnura*, 19, 166.

Yanza Gaibor, S. M. (2012). *Análisis e Interpretación de las Normas Internacionales de Auditoria y Aseguramiento.* Quito: Universidad Central del Ecuador.