FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de investigación de fin de carrera

TITULADO:

DISEÑO DE UNA POLITICA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE IMAGENOLOGÍA DEL HOSPITAL GENERAL DOCENTE DE CALDERÓN UTILIZANDO LOS ESTANDARES ISO 27001 E ISO 27799.

DIRECTOR DEL PROYECYO:

Ing. Walter Edison Estrella Mogollón, MBA

REALIZADO POR:

Ing. Cristian Eduardo Puga Jácome

como requisito para la obtención del título de:

MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD INFORMATICA

DECLARACIÓN JURAMENTADA

Yo, CRISTIAN EDUARDO PUGA JACOME, con cédula de identidad # 1002698601, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Cristian Eduardo Puga Jácome
C.C.: 1002698601

DECLARATORIA

El presente trabajo de investigación titulado:

"**DISEÑO DE UNA POLITICA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE IMAGENOLOGÍA DEL HOSPITAL GENERAL DOCENTE DE CALDERÓN UTILIZANDO LOS ESTANDARES ISO 27001 E ISO 27799**."

Realizado por:
CRISTIAN EDUARDO PUGA JACOME

como Requisito para la Obtención del Título de:
MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN

Ha sido dirigido por el profesor
Ing. Walter Edison Estrella Mogollón, MBA
quien considera que constituye un trabajo original de su autor

Ing. Walter Edison Estrella Mogollón, MBA
DIRECTOR

LOS PROFESORES INFORMANTES:

los profesores informantes:

ING. VERÓNICA RODRÍGUEZ, MBA

MSC. CHRISTIAN DAVID PAZMIÑO FLORES

Después de revisar el trabajo presentado,
lo han calificado como apto para su defensa oral ante
el tribunal examinador

Ing. Verónica Rodríguez, MBA	Msc. Christian David Pazmiño Flores

Quito, 21 de Marzo de 2019

DEDICATORIA

Dedico el presente trabajo de Investigación como todos los logros de mi vida a mi madre Lupe Jácome, quien, con su ejemplo de fortaleza, perseverancia y humildad, me ha demostrado que con trabajo y esfuerzo se obtienen las cosas.

A mi esposa Valeria Chamba e hija Nayeli Puga que son parte fundamental de mi crecimiento profesional y el más importante como ser humano, me han apoyado y acompañado en la realización de mis ideales de crecimiento familiar, donde se han superado grandes sacrificios como el tiempo de compartir, que no lo podré recuperar.

A demás familiares, que a través de sus palabras y acciones han generado en mi la energía suficiente para cumplir con un objetivo más en mi formación académica y personal.

AGRADECIMIENTO

El desarrollo del Tema de Investigación quiero agradecer a Dios quien me protege día a día, me da la capacidad intelectual y paciencia para enfrentar sus pruebas y hacer de mi un hombre de bien.

A mi Madre, esposa e hija y demás familiares que con sus palabras y acciones generaron en mi la confianza y energía para cumplir con el objetivo planteado.

Al director de Tesis Ing. Edison Estrella, MBA y profesor quien supo guiarme con sus conocimientos, experiencia, tiempo en el desarrollo y finalización del tema de investigación,

Al personal del área de imagenología del Hospital General Docente de Calderón, que con su predisposición ayudaron a que esta investigación se desarrolle y culmine.

RESUMEN

El Hospital General Docente de Calderón, al ser un centro de salud de segundo nivel de atención , cuenta con varios servicios de salud como el de imagenología, área que produce gran cantidad de información con los exámenes solicitados por los especialistas médicos, coexistiendo con la tecnología, misma que la transfiere y almacena en medios digitales, en Ecuador este tipo de información se la considera reservada, para ello se ha establecido en la ley nacional del COIP (Código Orgánico Integral Penal) en su Artículo 179, que: "*La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año*", la información generada dentro del hospital al ser de carácter médico es aún más crítica su revelación sin autorización alguna.

Para el cumplimiento de esta y otras leyes nacionales e internacionales se propone el Diseños de una Política de Gestión de Seguridad de la Información, apoyándonos en las normas o estándares ISO 27001 e ISO 27799, mismas que serán las directrices para la elaboración del plan y demás consideraciones como los controles para el área sanitaria (salud) respectivamente, generando un documento guía de buenas prácticas de la seguridad de la información, que deberá ser aprobado por la gerencia del hospital, transformándose en una herramienta de control para las actividades relacionada con información dentro del área de imagenología.

El plan se lo desarrolló dentro del área de imagenología, donde se analizarán las amenazas identificadas en la norma ISO 27799 para el área sanitaria, mismas que se transformarán en riesgos y a las que se deberán establecerse controles para mitigar su impacto o controlarlo.

Claves: Hospital General Docente de Calderón, Política de Seguridad de la Información, ISO 2001, ISO 27799, Integridad, Confidencialidad, Integridad, Disponibilidad

ABSTRACT

The Hospital General Docente de Calderón, being a health center of second level of care, has several health services such as imaging, an area that produces a large amount of information with the examinations requested by medical specialists, coexisting with technology , which transfers and stores it in digital media, in Ecuador this type of information is considered reserved, for it has been established in the national law of the COIP (Comprehensive Organic Penal Code) in its Article 179, that: "The person who Having knowledge by reason of their status or trade, employment, profession or art, of a secret whose disclosure could cause harm to another person and reveal it, will be sanctioned with custodial sentence of six months to a year ", the information generated within of the hospital being of a medical nature, its disclosure is even more critical without any authorization.

For the fulfillment of this and other national and international laws the Design of an Information Security Management Policy is proposed, based on the standards or standards ISO 27001 and ISO 27799, who give us the guidelines for the elaboration of the plan and considerations , controls for the health area (health) respectively, generating a guide document of good information security practices, which must be approved by hospital management, becoming a control tool for activities related to information within the area of imaging.

The plan was developed within the imaging area, where the threats identified in the ISO 27799 standard will be analyzed for the health area, which will be transformed into risks and to which controls must be established to mitigate or control their impact.

Keys: Hospital General Docente de Calderón, Information Security Policy, ISO 2001, ISO 27799, Integrity, Confidentiality, Integrity, Availability

ÍNDICE

CAPÍTULO I 13

INTRODUCCIÓN 13

1.1 Problema de investigación 13
1.2 Planteamiento del problema 15
1.3 Formulación del problema 18
1.4 Objetivos 18
1.4.1 General 18
1.4.2 Específicos 19
1.5 Justificación 19
1.5.1 Metodológica 21
1.5.2 Técnica 21
1.5.3 Relevancia social 22
1.6 Estado del arte 22
1.6.1 Estudios 23
1.6.2 Ataques cibernéticos 26
1.6.3 Productividad bibliográfica 27

CAPÍTULO II 28

MARCO TEÓRICO 28

2.1 Gestión de la información 28
2.1.1 Seguridad de la información 29
2.1.2 Política de seguridad 29
2.1.3 Marco regulatorio 30
2.1.3.1 Nacional 30
2.1.3.2 Internacional 31
2.1.4 Familia ISO/IEC 27000 32
2.1.5 Selección del estándar de seguridad 35
2.1.6 Estándar ISO 27001 35
2.1.7 Estándar ISO 27799 38
2.1.8 Fusión de las normas ISO 27001 e ISO 27799 39
2.1.9 Estándar de comunicación 40

CAPÍTULO III 40

ANALISIS SITUACIONAL 40

3.1. Antecedentes 40
3.2. La institución 41
3.3. Situación Actual 44
3.3.1. Topología de la red 45
3.3.2. Área de imagenología 47
3.3.3. Descripción técnica de equipos 49
3.3.3.1. Computadores de las áreas de trabajo 49
3.3.3.2. Estación de trabajo del tomógrafo 49
3.3.3.3. Estación de trabajo del mamógrafo 50
3.3.3.4. Tomógrafo 51
3.3.3.5. Rayos x 53
3.3.3.6. Rayos X móvil 54
3.3.3.7. Ecógrafo 1 57
3.3.3.8. Ecógrafo 2 59
3.3.4 Administración de la información médica en el área de imagenología . 61
3.3.5 Gestión de cambios en *software* y *hardware* 62
3.3.6 Seguridad física 63
3.3.7 Producción 63
3.4. Criterio de evaluación del riesgo 65
3.5. Objetivos de la seguridad de la información de la salud 65
3.6. Identificación de las amenazas y riesgos en el área de imagenología 66
3.6.1. Amenazas en el área de imagenología 67
3.6.2. Evaluación del riesgo 71
3.6.3. Tratamiento del riesgo 76
3.6.4. Aceptación del riesgo 76
3.6.5. Comunicación del riesgo 77
3.6.6. Validación de la implementación de la política de gestión de la seguridad de la información 77
3.7. Diseño de la política de gestión de la seguridad de la información 78

CAPÍTULO IV 80

PROPUESTA 80
4.1. Objetivo 80
4.2. Alcance 80
4.3. Controles para la seguridad de la información 80
4.4. Política de seguridad de la información 81
4.4.1. Organización de la seguridad de la información 81
4.4.2. Seguridad de recursos humanos 82
4.4.3. Gestión de activos 83
4.4.4. Control de acceso 84
4.4.5. Criptografía 85
4.4.6. Seguridad física y ambiental 85
4.4.7. Seguridad de las operaciones 85
4.4.8. Seguridad de las comunicaciones 86
4.4.9. Adquisición, desarrollo y mantenimiento de sistemas de información . 87
4.5. INFORMÁTICA MEDICA 87
4.5.1. SOFTWARE 88
CAPITULO V 90
CONCLUSIONES 90
RECOMENDACIONES 91
BIBLIOFRAFÍA 93
ANEXOS 95

Índice de Gráficos

Gráfico 1 Origen de la Información Médica de un Paciente 17
Gráfico 2 Número de Documentos según su Tipo 29
Gráfico 3 Factores que influyen en la necesidad de Implementación de un SGSI 36
Gráfico 4 Hospital General Docente de Calderón 41
Gráfico 5 Organigrama del Hospital General Docente de Calderón 43
Gráfico 6 Diagrama de red del HGDC 46
Gráfico 7 Topografía de red del área de imagenología 46
Gráfico 8 Diagrama de procesos imagenología 47
Gráfico 9 Mapa del proceso de examen de imagen 48
Gráfico 10 Análisis de las amenazas en el HGDC 73
Gráfico 11 Matriz de Criticidad 74

Índice de Tablas

Tabla 1 Temas de Búsqueda 27
Tabla 2 Coincidencias de información 28
Tabla 3 Familia el estándar ISO 27000 34
Tabla 4 Personal del área de imagenología del HGDC 49
Tabla 5 Número de equipos y su ubicación 49
Tabla 6 Número de equipos y su ubicación 50
Tabla 7Número de equipos y su ubicación 50
Tabla 8 *Estadísticas de Producción del Área de Imagenología* 64
Tabla 9 *Estadísticas de Pacientes* 64
Tabla 10 Tamaño de Imagen en KB 64
Tabla 11 Mapa de calor del riesgo 71
Tabla 12 Evaluación de las amenazas de ISO 27799 en HGDC 72
Tabla 13 Tabla de Riesgos con relación a procedimientos de salud 76

Índice de Anexo

Anexo 1 Lista de Tiques del área de Imagenología 95
Anexo 2 Aplicación de control 28 Protección física 98
Anexo 3 Calculo de Storage para el área de Imagenología 99

CAPÍTULO I

INTRODUCCIÓN

1.1 Problema de investigación

Desde el siglo pasado, el desempeño y desarrollo de las empresas sin importar su tamaño o línea de negocio dependen de las Tecnologías de la Información y Comunicación, como herramienta de gestión empresarial, que sistematiza y respalda cada uno de los procesos y procedimientos para el desarrollo del producto o servicio.

Las tecnologías de la Información y Comunicación involucran el uso de medios informáticos para almacenar, procesar y difundir todo tipo de información de la organización.

La administración de la Información necesita de la implementación de procesos y procedimientos establecidos en estándares de tratamiento de información digital, para garantizar la confidencialidad, disponibilidad y confiabilidad, que dependerán de las leyes y controles de cada país.

El Ecuador posee varias leyes de protección a la información como el COIP aprobado por la (Asamblea Nacional República del Ecuador, 2014), que posee de varios artículos dedicados a la seguridad de la información como el Art. 178. nos expresa

> la violación a la intimidad. – señala que la persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de

otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. (p. 30)

También presenta en el Art. 229 en su tercera sección delitos contra la seguridad de los activos de los sistemas de información y comunicación

> la persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. (p. 36)

El Artículo 230 habla sobre las acciones que involucran al personal que deseen la Interceptación ilegal de datos y será sancionada con pena privativa de libertad de tres a cinco años. (p. 36)

Para el campo de la salud existe el reglamento para el Manejo de Información Confidencial en el Sistema Nacional de Salud, con acuerdo ministerial 5216, publicado en el registro oficial suplemento 427 del 29 de enero 201, que establece en sus capítulos y artículos 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.

En una casa de salud el área de imagenología genera una considerable cantidad de imágenes digitales que están sujetas a normas, leyes y estándares nacionales como internacionales de protección y administración.

El área de imagenología del Hospital General Docente de Calderón genera información digital de acuerdo a 5 tipos de exámenes: Mamografías, Rx, Tomografías, Ecografías, el resultado de

los exámenes son imágenes que posee el estándar de comunicación DICOM (*Digital Imaging y Comunication in Medicine*), utiliza el protocolo de comunicación TCP/IP (López, Barreras, & Fernández, 2014). para la comunicación entre sistemas, el tipo de examen establecerá el tamaño en KBites de acuerdo con el número de imágenes.

Con estos antecedentes el personal como el área de imagenología debe hacer uso de una Política de Gestión de la Información, que permitirá la administración y protección de la información digital de los pacientes, así como la protección del personal ante cualquier fuga de información.

La identificación de la situación actual del área de imagenología permite presentar el desarrollo de una política de gestión de la Información, que es el primer paso para la producción de un Sistema de Gestión de Seguridad de la Información Integral para todas las áreas del Hospital.

1.2 Planteamiento del problema

Los niveles de seguridad que exigen hoy en día las tecnologías de la información son cada vez más altos y complejos, esto debido al crecimiento exponencial que ha tenido la Internet en los últimos años.

La protección de la información y bloqueo de intrusos, son unos de los objetivos a lograr para que la infraestructura informática de una organización sea segura.

La posibilidad de expandir la cobertura de servicios, de interconectar bases de datos y de acercar a los usuarios de áreas rurales a la información, ha llevado a la aparición de nuevas amenazas en los sistemas computarizados y se puede establecer una relación que, si crece la cobertura, crece la vulnerabilidad.

Las políticas de gestión de seguridad de la información surgen como una herramienta organizacional necesaria para concientizar a cada integrante de una empresa sobre la importancia, la sensibilidad de la información y la necesidad de su conservación con el mínimo de riesgo y un alto nivel de seguridad que favorezca el desarrollo de la organización, garantice su óptimo funcionamiento y el buen uso de los equipos como la recuperación de la información en el menor tiempo posible en caso de incidentes o eventos catastróficos.

Es así como muchas organizaciones gubernamentales y no gubernamentales, nacionales e internacionales, implementan políticas de gestión de seguridad de la información, que rigen el uso adecuado de la tecnología, efectuando recomendaciones al cliente interno, para maximizar las ventajas y evitar su uso indebido; anticipando así problemas en el uso de los bienes y servicios informáticos de las entidades. Para su implementación existe la norma ISO 27001, misma que establece los requisitos necesarios para implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información para todas las áreas de la organización, y al desear definirla para un campo específico como el de la salud existe la norma ISO 27799 cual proporciona controles de seguridad para proteger la información personal en cuanto a los temas de salud.

El uso y aplicación de las dos normas genera un conjunto de documentos, que pueden ser sistematizados e indicaran los procedimientos y las actuaciones que se deben cumplir por parte del personal de la organización, permitiendo administrar los recursos de la red, la información, la atención de los pacientes, y la continuidad del negocio.

Un hospital se encuentra segmentado en áreas, donde la información médica del paciente es el común denominador, se la distribuye a través de redes LAN (red de área local) y fuera de esta a

través de la red WAN (internet), dejándola vulnerable a ataques como: bloqueo, eliminación, modificación etc., durante la transmisión como en los medios de almacenamiento.

Gráfico 1 *Origen de la Información Médica de un Paciente*
Fuente: *Ramos (2007)*

El área de imagenología del Hospital General Docente de Calderón a la fecha se encuentra con una brecha de capacidad de almacenamiento de la información que se genera en los procesos de Rayos-X, Mamografías, Tomografías y Ecografías, esta data se almacena en la memoria de los mismos equipos y como máximo el respaldo lo generan en computadores convencionales, sin ninguna seguridad, los equipos se encuentran conectados a la red, por lo tanto, son vulnerables a ciber ataques.

El área no posee políticas de uso, almacenamiento, respaldo y entrega de la información digital (imágenes - resultados de exámenes) a través de medios de almacenamiento ópticos, que permitan salvaguardar la integridad y confidencialidad de la información hospitalaria de los pacientes.

Las vulnerabilidades expuestas se las obtuvo de la aplicación de entrevistas: al líder del área, técnicos radiólogos y la inspección misma de la infraestructura del hospital.

El Hospital General Docente de Calderón casa de salud del norte de Quito, tienen como misión prestar servicios de salud de calidad a través de su cartera de servicios, cumpliendo con la responsabilidad de promoción, prevención, recuperación, rehabilitación de la salud integral, conforme a las políticas del Ministerio de Salud Pública dispone (HGDC, 2017 - 2020).

Por lo expuesto, se desea desarrollar la política de gestión de seguridad de la información, para el área de imagenología del Hospital General Docente de Calderón, que permita aplicar controles de protección y administración utilizando las normas internacionales ISO 27001 e ISO 27799, y garantizar la confidencialidad, integridad y disponibilidad de la información producida en la ejecución de los exámenes anteriormente expuestos.

1.3 Formulación del problema

El Área de Imagenología del Hospital General Docente de Calderón posee una alta probabilidad de que la confidencialidad, Integridad, disponibilidad de la información, y la infraestructura se vean afectadas por la falta de una correcta administración y carecer de la aplicación de políticas de gestión de seguridad de la información, lo cual minimiza la probabilidad de recuperación ante un siniestro o evento de intrusión interno o externo.

1.4 Objetivos

1.4.1 General

Diseñar una política de gestión de seguridad de la Información con el análisis de las normas ISO 27001 e ISO/ 27799, identificando los controles de mayor relevancia para el área de

imagenología del Hospital General Docente de Calderón, con la intención de proteger la información como los activos fijos informáticos de posibles riesgos internos como externos.

1.4.2 Específicos

- Analizar el estándar de comunicación de los equipos de Imagenología para la transmisión de las imágenes a los diferentes equipos de la red, con el objetivo de conocer las seguridades y vulnerabilidades que este posee al usarlo.
- Realizar un estudio de amenazas y vulnerabilidades a la infraestructura tecnológica del área de Imagenología del Hospital General Docente de Calderón, mediante la aplicación de herramientas y proceso de análisis, obteniendo un punto de referencia para la determinación de los controles a aplicar.
- Analizar los controles de las ISO/IEC 27001 e ISO/IEC 27799, mediante la lectura comprensiva de las normas, para implementarlos en el diseño de la política de Gestión de seguridad de la información para el Hospital General Docente de Calderón en el área de Imagenología.
- Aplicar las normas ISO/IEC 27001 e ISO/IEC 27799, para establecer controles que permitan proteger la información del área de imagenología del Hospital General Docente de Calderón, a través del desarrollo en la política de gestión de seguridad de la información.

1.5 Justificación

La proliferación del uso de las tecnologías de la Información está en todo campo de desarrollo laboral e industrial y el fácil acceso a la red mundial (internet), ha permitido que se desarrollen

procedimientos para interceptar la información que se transmite y recibe a través de esta, dando lugar a delitos informáticos provocados por los delincuentes digitales reconocidos como: ciberdelincuentes.

Estos personajes se benefician de vulnerabilidades existentes en equipos y medios de transmisión, logrando la captura o extracción de la información, para luego generar acciones de beneficio propio como la venta o extorción.

En contexto la información debe ser gestionada para garantizar el cumplimiento de los tres pilares de las Gestión de la Información: Confidencialidad, Integridad y Disponibilidad, así como la continuidad del negocio, para ello las empresas aplican los estándares ISO, que permiten establecer políticas de seguridad, procedimientos de seguridad para la información como para la infraestructura.

En el mundo y en el país se desarrollan empresas privadas y públicas, cada una genera gran cantidad de información y de gran importancia, no se podría establecer niveles de valor de la información entre ellas, pero si ésta se compromete la integridad de los clientes de la empresa la administración y alta gerencia debe asignar protección, tal que impida que sea divulgada o alterada, una de ellas son las casas de salud.

En el país existe el Reglamento para el manejo de información confidencial en el sistema nacional de salud, establecido por el MSP donde se dispone garantizar que la información se respalde durante un período de 5 años en un archivo activo y luego de este en un archivo pasivo durante 2 años más como mínimo, para el cumplimiento de esta disposición cada unidad hospitalaria del país deberá generar recursos para la adquisición de equipos de *storage* (almacenamiento), ya sea con equipos físicos o contratación en la nueve, acciones que se toman

en cuenta dentro del desarrollo del diseño de la política de gestión de seguridad de la información, aplicando las normas ISO 27001 e ISO 27799.

1.5.1 Metodológica

La organización internacional de normalización provee de la familia de normas ISO 27000 y específicamente la ISO 27001 que describe los pasos para la implementación de un SGSI, que es un sistema de gestión de la seguridad de la información aplicando la ISO 27002 con sus controles para empresas con información no incidente en la estabilidad de la salud de una persona, razón por la cual la organización provee de la norma ISO 27799 ajustando la ISO 27002 al sector sanitario predominando la seguridad de la información sobre los datos de salud de una persona.

Bajo este criterio y con él uso de las normas como un documento que agrupa un conjunto de buenas prácticas se justifica la implementación de una política institucional de gestión de seguridad de la información orientada a salvaguardar la información almacenada en los servidores de aplicaciones del hospital, donde se analizarán las amenazas que provee la norma ISO 27799 ajustados a la realidad de la infraestructura del hospital observadas en sitio.

1.5.2 Técnica

Una casa de salud al generar gran cantidad de información incidente en la estabilidad de un paciente, debe poseer una herramienta de gestión que garantice la confidencialidad, disponibilidad e integridad, a través de una política de gestión de la seguridad que genera un documento con controles o directrices direccionados a la infraestructura y al personal, cumpliendo con el criterio global de la seguridad de la información y leyes nacionales,

garantizando la continuidad del negocio y anticipándonos a daños de infraestructura o irrupción de un ciberataque.

1.5.3 Relevancia social

El proyecto se desarrolló dentro de una casa de salud de Nivel 3 ubicado en la parroquia de Calderón, este beneficia a toda la población que acuda a solicitar de los servicios médicos que este ofrece, con la garantía de recuperar la estabilidad de su salud y su información se encuentre protegida. La aplicación de los conocimientos desarrollados en el proyecto permitirá al personal administrativo y hospitalario mejorar la atención a los pacientes, aplicando la política desarrollada que protegerá la información generada durante los procesos médicos.

1.6 Estado del arte

A pesar de que el reglamento nacional fue expedido el 31 de diciembre del 2014, dentro del país el conocimiento y uso de los estándares de seguridad de la información sanitaria se encuentran en apogeo, a razón de la inclusión de equipamiento médico que poseen características similares a un computador como: conectividad a la red, capacidad de almacenamiento y procesamiento,

Las funcionalidades de los equipos permiten la transmisión y extracción de información digital generada con los procedimientos médicos efectuados por los profesionales de la salud en mira de la recuperación y estabilidad de la salud de la persona.

En tal sentido el estado del arte se realizó presentando casos de ciberataques a hospitales, consecuencias, presentación de proyectos e investigaciones en el país y el mundo, que tienen como objetivo la administración y seguridad de la información sanitaria con enfoque al área de imagenología.

El uso de estándares nacionales e internacionales para el desarrollo y complimiento de procesos y procedimientos para lograr el bien común, que permite establecer directrices de adaptabilidad para el trabajador o profesional que desee dar continuidad, eficiencia y calidad a los servicios ofrecidos.

La tecnología es una herramienta y un arma a la vez, ayuda al progreso de una persona como de un país, como la construye la puede destruir, se crea *software* de protección como virus para vulnerarlos, igual que profesionales con distintos intereses de seguridad y de beneficios.

1.6.1 Estudios

La investigación utilizará referencias de varios autores como Hodge et al. (1999) que establecen:

> tres áreas legales de la información de la salud que se encuentran interconectadas: privacidad de la información de salud identificable, confiabilidad y calidad de los datos de salud y responsabilidad basada en las acciones de una persona o de varias personas inducidas a cumplirlas.

Son consideraciones que relacionan al profesional de la salud y la integridad de la información luego de los procedimientos médicos, es por ello que la tecnología ayuda a velar por la integridad de los datos

Los autores Sunyaev, Kaletsch, Mauro, and Krcmar (2010) afirman: “Que las soluciones y estándares actuales de *e-health* se enfoca principalmente en la seguridad de la red y las políticas de control de acceso”. Sin embargo, no abordan la seguridad de la plataforma del cliente de forma apropiada, esto muestra que no existe seguridad en el *software* como *hardware* que utiliza el profesional de la salud.

Sánchez, Fernández, Ambrosio, Hernández, and Geaa (2013) en su artículo presentan recomendaciones que se las deben tomar en cuenta para el establecimiento de las seguridades como:

- Formación: al personal médico informar de las consecuencias y responsabilidades que poseen al manejar información médica.
- Asignación de contraseñas: son factores cruciales para mantener la eficacia de este mecanismo de protección frente accesos no autorizados al sistema de información sanitario.
- Uso de certificado digital conjunto de datos que permiten la identificación del titular del certificado ante terceros.
- Control con los dispositivos extraíbles al utilizarlos dentro de los equipos de la red, existe una alta probabilidad del ingreso de virus a toda la intranet.
- Uso de equipos informáticos una de las fuentes de información principales es el computador personal por cuanto se recomienda que si debe ausentarse del área de trabajo debe dejarlo con contraseña.
- Verificación de instalación de *software* el internet como fuente para instalar *software* no son confiables por la inclusión de puertas traseras dentro de ellos. Comunicar incidencias de seguridad todo el personal deberá comunicar al personal del área de seguridad de Información sobre cualquier incidencia de seguridad suscitada.

La empresa MV informática Nordeste (MVINF, 2015), en su artículo Entienda la importancia de la seguridad de la información en la gestión hospitalaria presenta posibles implementaciones que los hospitales deberían tener dentro de su red:

- Limitar el acceso a la base de datos de los sistemas.

- Utilizar algoritmos de criptografía
- Configurar servicios con SSL
- Adoptar la autenticación de 2 factores
- Construir una escala de permisos.

Los catedráticos Vidal, Gonzalo, and Cazes (2005) de la Universidad de Ciencias Médicas de la Habana presentan en su revista la aplicación de los principios de seguridad Confidencialidad, Integridad, Disponibilidad que conviene agruparlos en la política de seguridad de la institución y para ello se debe considerar ciertas reglas en su desarrollo:

- Toda regla debe ser holística, deberá cubrir a todos los aspectos de seguridad con relación a los sistemas.
- Debe proteger el sistema en todos los niveles de un modelo OSI, humano y físico.
- Incluir medios y formas que la interacción de los elementos del sistema y profesionales que los usarán sea la más clara y eficaz.
- Identificar el entorno donde se desarrollará le sistema.
- La política que se desarrolle debe ser adaptable a las condiciones de cada departamento de la entidad.
- Las seguridades implementadas deben ser proporcionales a los riesgos, el valor y costo de ataque al sistema.

La marca ESET (Eset, 2014), especialista en brindar seguridad a *endpoints* como toda la infraestructura de datos con implementaciones más robustas, está por lanzar un producto direccionado a las casas de salud con la idea: Despreocúpese por la seguridad de su organización y enfóquese en desarrollar iniciativas que mejoren el cuidado de los pacientes, con una solución

sencilla que ofrecerá: Antivirus, Antispyware, Control de dispositivos, Firewall Inteligente, Filtrado de contenido entre otras bondades.

1.6.2 Ataques cibernéticos

El 10 de agosto del año pasado el diario Infobae de Argentina, publica "Ataques Cibernéticos, la nueva amenaza de muerte en los Hospitales Del Mundo" donde se establece que los hospitales o casas de salud son un blanco para los hackers, la irrupción de estos llega a los sistemas de dispositivos médicos, sistemas de mantenimiento y monitoreo ataques realizados en el Reino Unido.

Las bases de datos de los hospitales es uno de los objetivos más ansiados de los hackers y son inesperadas las acciones que realizaran con ellas o sobre ellas como lo afirmó *Dmitry Bestuzhev*, director de Investigación para Latinoamérica de *Kaspersky Lab*.

Bestuzhev y Sebastián Brenner director de ingeniería para Latinoamérica de *Symatentec*, coinciden que una de las causas de que los hospitales son blancos de los *hackers*, debido a que no existe una planificación estratégica de seguridad en la infraestructura de tecnología (Gutiérrez y Brenner, 2017).

Los hospitales no fueron la excepción del ultimo virus del año según el diario *Amazing* en su publicación del 16 de mayo de 2017, *ransomware* cumplió con el objetivo para el que fue creado, bloqueando computadores con la información dentro. Ecuador fue uno de los 74 países víctimas del ataque y proliferación del virus. Inglaterra fue víctima de *ransomware* donde tomaron control de los equipos y generaron la extorción pidiendo dinero para proceder con la liberación de los mismos, el servicio nacional de salud Británico confirmo el ataque y presenta al virus responsable "*Wanna Decryptor*" (Estrada, 2017).

Conceptos, recomendaciones, incidentes generados confirman que la tecnología es parte del desarrollo de todas las áreas y como no podía ser la excepción la salud, es por eso por lo que se pretende dar un nombre a esta fusión como: *eSanidad*, *eSalud*, sanidad electrónica o *eHealth* en inglés y también como telemedicina que es el uso de las telecomunicaciones. El manejo de gran cantidad de información, que no son más que datos digitales que den ser protegidos de acciones negativas que afecten al paciente como a la casa de salud responsable del custodio de la información.

1.6.3 Productividad bibliográfica

Como medio principal de consulta el internet se buscó, libros, catálogos, revistas médicas, investigaciones de seguridad y ciberseguridad, en el país y fuera de él y se obtuvieron los siguientes resultados:

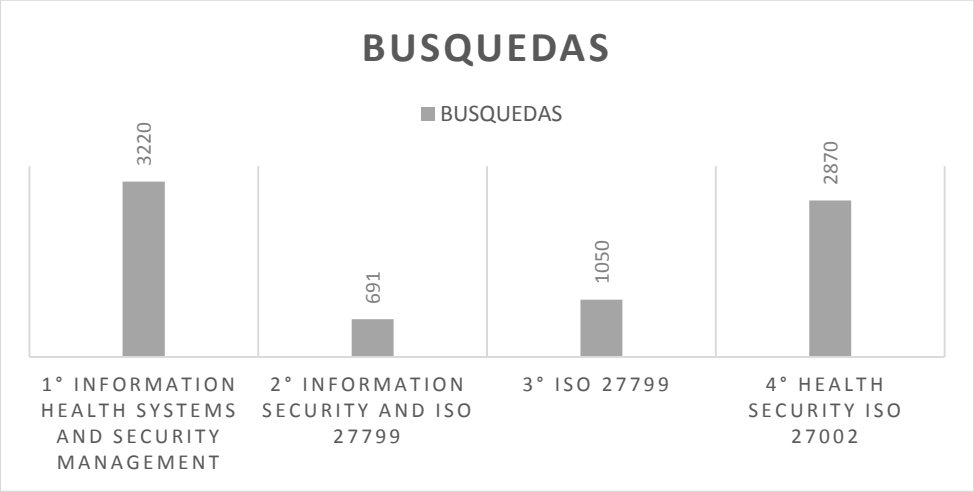


Tabla 1 *Temas de Búsqueda*
Elaborado por: *investigador*

El tema que provee el mayor número de búsquedas es ***Information health systems and security management*** con un 41%, como se comentó se encontró mucha información no definida para el área de imagenología, pero si para el área de salud en general, como para el área administrativa.

La información presentó diferencias que permite segmentarlas y hacer uso de ella como tipo de publicación (libro, artículo, etc.), y su contenido, con temas individuales, definidos para casos generales y no puntuales de autores como: B. Dawn Medlin, Joseph A. Cazier, Jung A Kim, David Blumenthal, entre otros.

Los artículos, libros e investigaciones no utilizaban en conjunto las normas en estudio, de forma individual y en conjunto las normas ISO 27001 e ISO 27002. De la selección se presenta:

Tabla 2 *Coincidencias de información*
Elaborado por: *investigador*

Al establecer consideraciones altas de coincidencias en los documentos se pudo determinar:

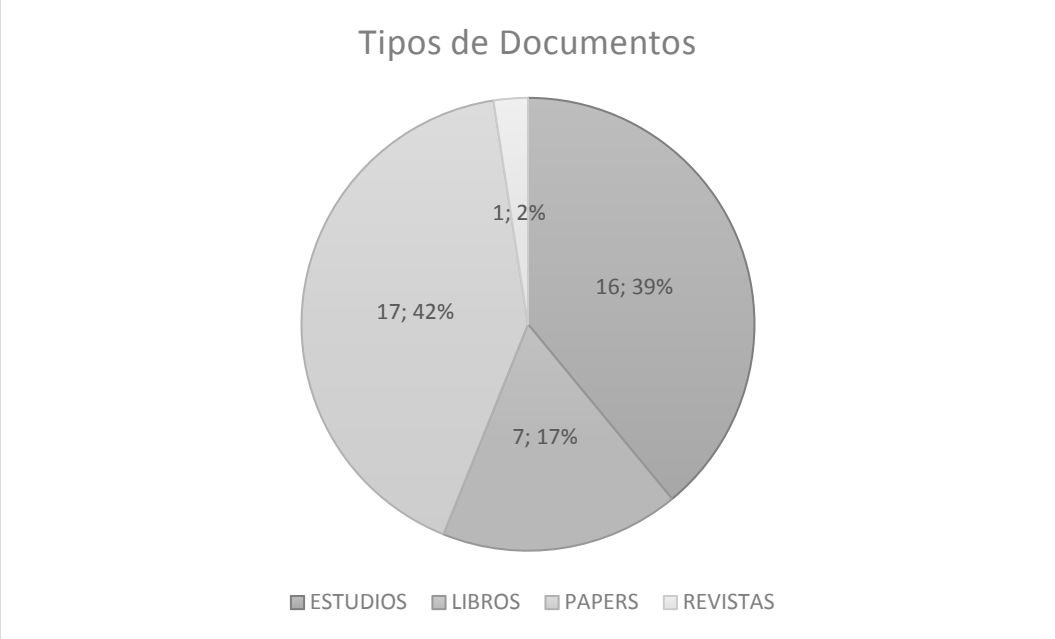


Gráfico 2 *Número de Documentos según su Tipo*
Elaborado por: *investigador*

CAPÍTULO II

MARCO TEÓRICO

La importancia y valor que la información hospitalaria llega a obtener en el transcurso del tiempo es determinante para el desarrollo mismo de un hospital, para los profesionales de la salud y el paciente, por lo tanto, es necesario establecer ciertas medidas, que permitan gestionar su seguridad, disponibilidad, credibilidad, integridad y confidencialidad.

Investigaciones establecen de la importancia de la información y la seguridad empieza con la identificación de los niveles de criticidad como los riesgos que debe soportar antes, durante y después de su origen, transporte y almacenamiento.

2.1 Gestión de la información

La información es definida como "la sucesión de datos organizados, analizados, comprendidos por un ser humano, que detallan o describen una teoría, suceso o evento" (Thompson, 2019).

Esta información ha sido plasmada, registrada y administrada sobre papel durante muchos años y en gran cantidad. Para ello se desarrollaron los medios digitales obteniendo los mismos y mejores resultados por la capacidad de almacenamiento, análisis y mantenimiento sin depender de un estado físico o material. Con la masificación de las tecnologías de la información aparecen amenazas a la integridad de la información digital, por tanto, surge un nuevo concepto: Gestión de la Información, con una cadena de procedimientos que tratan de que la información se pueda

adquirir, producir y distribuir, para poder analizarla y ocuparla en tiempos mínimos y a cualquier parte del mundo al menor coste posible.

2.1.1 Seguridad de la información

Seguridad de la Información es definida como la: "disciplina que tiene por objeto preservar la confidencialidad, integridad y disponibilidad de la información; y que puede involucrar otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la trazabilidad" (Jara y Pacheco, 2012).

Así también definen Bertolín y Areitio (2008) los conceptos de:

- **Confidencialidad**. – Toda información pertenece a una sola persona (dueño), no deberá ser divulgada o utilizada por otra persona sin consentimiento.
- **Integridad**. – Toda información deberá mantenerse igual que su origen de creación, no podrá ser alterada en ningún momento durante la transmisión o distribución.
- **Disponibilidad**. – Toda información deberá estar disponible al 100% en cualquier momento para el propietario de esta o que este autorice su uso.

2.1.2 Política de seguridad

Borghello (2017) define a la política de seguridad como: "una herramienta organizacional de protección que ocasiona una conducta de seguridad a cada uno de los miembros de una organización, sobre la importancia y sensibilidad de la información como de los servicios críticos" (p. 15). Utiliza reglas y procedimientos que mitigan los riesgos de la organización con el objetivo de establecer estándares de seguridad

2.1.3 Marco regulatorio

2.1.3.1 Nacional

El país Posee el Código Orgánico Integral Penal (COIP), en el Artículo 179, que dispone: "Revelación de secreto. - La persona que, teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año".

Como ente rector de la salud se encuentra el Ministerio de Salud Pública que ha establecido varios reglamentos como: Reglamento para el manejo de información confidencial en el sistema nacional de la salud Acuerdo No. 00005216-A, y presenta los artículos:

- Art. 2.- Confidencialidad. - Es la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implica el conjunto de acciones que garantizan la seguridad en el manejo de esa información.
- Art. 3.- Integridad de la información. - Es la cualidad o propiedad de la información que asegura que no ha sido mutilada, alterada o modificada, por tanto, mantiene sus características y valores asignados o recogidos en la fuente. Esta cualidad debe mantenerse en cualquier formato de soporte en el que se registre la información, independientemente de los procesos de migración entre ellos.
- Art. 4.- Disponibilidad de la información. - Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional.
- Art. 5.- Seguridad en el manejo de la información. - Es el conjunto sistematizado de medidas preventivas y reactivas que buscan resguardar y proteger la información para mantener su

condición de confidencial, así como su integridad y disponibilidad. Inicia desde el momento mismo de la generación de la información y trasciende hasta el evento de la muerte de la persona.

El deber de confidencialidad respecto a la información de los documentos que contienen información de salud perdurará, incluso, después de finalizada la actividad del establecimiento de salud, la vinculación profesional o el fallecimiento del titular de la información.

- Art. 6.- Secreto Médico. - Es la categoría que se asigna a toda información que es revelada por un/a usuario/a al profesional de la salud que le brinda la atención de salud. Se configura como un compromiso que adquiere el médico ante el/la usuario/a y la sociedad, de guardar silencio sobre toda información que llegue a conocer sobre el/la usuario/a en el curso de su actuación profesional. (Registro Oficial, 2015)

Los profesionales de salud de los establecimientos de salud cumplirán con el deber del secreto médico, para generar condiciones de confianza en la relación con los/as usuarios/as y así garantizar el derecho a la intimidad. El secreto médico es extensible a toda la cadena sanitaria asistencial.

- El Ministerio de Salud Pública (MSP, 2016), en el artículo 4, Derecho a la confidencialidad dispone: "Todo paciente tiene derecho a que la consulta, examen, diagnóstico, discusión, tratamiento y cualquier tipo de información relacionada con el procedimiento médico a aplicársele, tenga el carácter de confidencial"

2.1.3.2 Internacional

Existe la norma internacional para la administración y uso de la información médica denominada HL7 (*Health Level Seven*), misma que establece los lineamientos para la

transmisión de la información médica a través del modelo de mensajería para la comunicación entre sistemas y dispositivos, facilitando la integración, intercambio y recuperación de información electrónica de salud.

La norma muestra varias terminologías que establecen normalización de las bases de datos, identificadores inequívocos, motores de integración y un plan de *work Flow* para la integración.

2.1.4 Familia ISO/IEC 27000

La organización de estandarización ISO/IEC dentro del estándar 27000, agrupa una serie de normas, mismas que se las identifica con un número específico y único. Estas normas poseen definiciones aplicables para ciertas áreas que al utilizarlas generan mejoras en los procesos de la línea del negocio.

Está compuesta por:

ESTANDAR	DETALLE
ISO/IEC 27001.	Requisitos para el desarrollo del Sistema de Gestión de Seguridad de la Información. (27001, 2015)
ISO/IEC 27002.	Buenas prácticas con los objetivos de control y controles para la seguridad de la información. Última edición 2013
ISO/IEC 27003.	Aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC/IEC 27001. Última edición 2017
ISO/IEC 27004.	Desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC/IEC 27001. Última edición 2016
ISO/IEC 27005	Gestión del riesgo en la seguridad de la información. Última edición 2011
ISO/IEC 27006	Acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Última edición 2015
ISO/IEC 27007	Auditoría de un SGSI, como complemento a lo

ESTANDAR	DETALLE
	especificado en ISO/IEC 19011. Última edición 2017
ISO/IEC 27008	auditoría de los controles seleccionados en el marco de implantación de un SGSI. Última edición 2011
ISO/IEC 27009	Requisitos para el uso de la norma ISO/IEC/IEC 27001 en cualquier sector específico. Última edición 2016
ISO/IEC 27010	guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. Última edición 2015
ISO/IEC 27011	Interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC/IEC 27002. Última versión 2016
ISO/IEC 27013	guía de implementación integrada de ISO/IEC/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).
ISO/IEC 27014	Guía de gobierno corporativo de la seguridad de la información. Última versión 2013
ISO/IEC 27015	Guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005
ISO/IEC TR 27016	Guía de valoración de los aspectos financieros de la seguridad de la información.
ISO/IEC 27018	Código de buenas prácticas en controles de protección de datos para servicios de computación en *cloud computing*
ISO/IEC 27019	Guía con referencia a ISO/IEC 27002:2005 para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía. Última edición 2017 referencia
ISO/IEC 27021	Competencias requeridas para los profesionales dedicados a los sistemas de gestión para la seguridad de la información
ISO/IEC 27023	Correspondencias entre las versiones del 2013 de las normas ISO/IEC 27001 y ISO/IEC 27002 como apoyo a la transición de las versiones publicadas en 2005.

ESTANDAR	DETALLE
ISO/IEC 27031	adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio
ISO/IEC 27032	Mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad
ISO/IEC 27034	Norma dedicada la seguridad en aplicaciones informáticas
ISO/IEC 27035	Gestión de incidentes de seguridad en la información.
ISO/IEC 27036	Guía en cuatro partes de seguridad en las relaciones con proveedores
ISO/IEC 27037	Directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales.
ISO/IEC 27038	Especificación para seguridad en la redacción digital
ISO/IEC 27039	guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS).
ISO/IEC 27040	Seguridad en medios de almacenamiento
ISO/IEC 27041	Guía para la garantizar la idoneidad y adecuación de los métodos de investigación.
ISO/IEC 27042	Guía con directrices para el análisis e interpretación de las evidencias digitales
ISO/IEC 27043	Desarrolla principios y procesos de investigación para la recopilación de evidencias digitales
ISO/IEC 27050	información almacenada en dispositivos electrónicos en relación con su identificación, preservación, recolección, procesamiento, revisión, análisis y producción.
ISO/IEC TR 27103:2018	Norma con la orientación sobre cómo aprovechar las normas existentes en un marco de ciberseguridad.
ISO 27799	Directrices para el apoyo de la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes

Tabla 3 *Familia el estándar ISO 27000*

Elaborado por: *investigador*

2.1.5 Selección del estándar de seguridad

El estándar que permitirá el desarrollo de la Política de Gestión de Seguridad de la Información para el área de imagenología del Hospital General Docente de Calderón es el ISO 27001, misma que identificará y evaluará los riesgos existentes y los mitigará o eliminará con los controles que posee.

Cómo el área de aplicación es la salud, se utiliza el estándar ISO 27799, que define las reglas para la interpretación y aplicación en la salud, siendo un complemento del estándar ISO 27001, este presenta en su contenido un conjunto detallado de controles de seguridad para la gestión de la información de la salud.

2.1.6 Estándar ISO 27001

ISO 27001:2013 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y muestra en su contenido los requisitos necesarios para establecer, implementar, y mantener el mejoramiento continuo en sistema de gestión de seguridad de la información.

Es una norma estándar, que permite su implementación dentro de cualquier tipo de organización, independiente de su razón social y de su tamaño.

Gráfico 3 *Factores que influyen en la necesidad de Implementación de un SGSI*
Realizado por: *investigador*

El gráfico 2 muestra los factores que toda organización debe poseer para su desarrollo y deberán ser considerados de forma directa o indirecta dentro de los controles que se implementen para la seguridad de la Información, que se complementarán con el proceso y gestión general de toda la organización.

El estándar utiliza un lenguaje o términos técnicos que presentan una dirección para la implementación de la seguridad, se debe estudiar y analizar los riesgos de la organización que implementará el sistema de gestión de la información determinando las situaciones externas e internas que influyen en el desarrollo del sistema mencionado, como también las necesidades y expectativas de las partes interesadas.

La norma dispone determinar el alcance del sistema de gestión de seguridad de la información, aplicando sus recomendaciones, así como las relaciones y dependencias que realiza la organización y los involucrados que las realizan, estas acciones deberán estar redactadas en un documento de fácil acceso. El objetivo del estándar es que el sistema este en una constante renovación estableciendo, implementando, manteniendo y mejorando su uso.

Renovación que la debe conocer y dirigir personal de la alta gerencia de la organización demostrando liderazgo y compromiso, se deberán establecer políticas de seguridad del sistema de seguridad de la información alineados a los propósitos de la organización, deberá poseer un criterio amplio para la asignación de las responsabilidades y personal que se encargará de cumplir con los roles de seguridad en desarrollo como aplicación.

El desarrollo del sistema además de considerar los aspectos ya expuestos se deberá identificar los riesgos y oportunidades que deben contemplarse para tratarlos y aprovecharlos respectivamente. El tratamiento de los riesgos deberá ser definido y puesto en marcha para determinar los controles para cada proceso y permitirá generar un plan de tratamiento de riesgos de seguridad de la información para obtener su aprobación por parte de los administradores de estos.

Información que deberá estar documentada desde su inicio, proceso y constante actualización, que permitirá establecer los objetivos de seguridad de la información y la planificación para alcanzarlos en las funciones y niveles pertinentes.

Todas las acciones hasta el momento descritas necesitarán de recursos para el establecimiento, implementación, mantenimiento y mejora continua, recursos que las organizaciones deberán determinar y proporcionar para el sistema de gestión de seguridad de la información.

La organización deberá verificar las competencias del personal que desarrollará las actividades bajo su disposición y responsabilidad desde el inicio, durante y la actualización de la información, el personal deberá estar consciente de que su contribución en las labores asignadas dependerá o afectará en la eficacia del sistema de gestión de la seguridad de la información, como las comunicaciones internas y externas relacionadas al proceso como: sobre qué, cuándo, a quién, quién debe, comunicar e identificar los procesos que necesitan la comunicación.

Todo el proceso deberá estar planificado, implementado y controlado para cumplir con los objetivos y requisitos que la norma propone, presentando facilidad para la evaluación del desempeño del sistema, donde realizaran acciones de monitoreo, medición, análisis y evaluación, este proceso generará documentación que servirá como evidencia de las acciones expuestas. Acciones que se ajustan a la necesidad de realizar auditorías internas con la necesidad de saber si el sistema de gestión de seguridad de la información cumple con las necesidades de la organización.

El trabajo de la alta gerencia no concluye, deberá generar revisiones del sistema con intervalos planificados con la finalidad de certificar la conveniencia, adecuaciones y eficacias continuas.

2.1.7 Estándar ISO 27799

La norma internacional ISO 27799 desarrollada por la organización internacional de estandarización en el 2008, proporciona orientación a las organizaciones sanitarias y a otros custodios de información personal sanitaria sobre la mejor forma de proteger la confidencialidad, integridad y disponibilidad de dicha información a través de la implementación de la Norma ISO/IEC 27002/1. Específicamente, esta norma internacional trata sobre las necesidades especiales de gestión de seguridad de la información del sector sanitario y sus entornos operativos únicos.

Mientras que la protección y seguridad de la información personal es importante para todos los individuos, corporaciones, instituciones y gobierno, en el sector sanitario existen requisitos especiales que es necesario cumplir para asegurar la confidencialidad, integridad, trazabilidad y disponibilidad de los datos personales sanitarios.

Como se mencionó en capítulos anteriores que la información hospitalaria al ser la descripción del estado de salud de una persona tiene un alto valor representativo para el propietario y el médico tratante, consideración que asigna a la información grados de confidencialidad con respecto a los demás tipos de datos personales.

Para mantener la privacidad de la información y del paciente luego de los procedimientos médicos de las posibles acciones de delincuentes de la red es esencial proteger esta confidencialidad, así como la integridad de la información sanitaria se debe proteger como el componente importante del ciclo de vida completo de la información por ser totalmente auditable.

La disponibilidad de la información sanitaria también influye en la toma de decisiones por le profesional sanitario (médico). Los sistemas de informática sanitaria deben cumplir demandas únicas para mantenerse operativos ante desastres naturales, fallos de sistema y ataques de denegación de servicio. Por lo tanto, proteger la confidencialidad, integridad y disponibilidad de la información sanitaria requiere de habilidades, consideraciones e implementaciones específicas del sector sanitario.

2.1.8 Fusión de las normas ISO 27001 e ISO 27799

Las normas al ser totalmente integrables una a otra se procura utilizar los beneficios de seguridad de ellas, las generalidades de ISO 27001 y los controles de la ISO 27002 adaptados a un entorno de salud y establecidos como la norma ISO 27799.

La fusión de las normas permite implementar controles alineados a la protección de la información que se genera durante y después de la interacción del profesional de la salud con el paciente, esta es calificada como privada por el grado de influencia que tiene al ser divulgada a terceros.

Este uso confirma que las Tecnologías de la Información y comunicación son parte indispensable para la administración, almacenamiento, transmisión, procesamiento, interpretación y presentación de la información médica de un paciente por un profesional de la salud.

2.1.9 Estándar de comunicación

Las estaciones de trabajo y los equipos poseen un estándar de comunicación denominado DICOM (*Digital Imaging and Communication On Medicine*), describe los medios de formato e intercambio de imágenes médicas de la información, así como para los estudiantes de las diferentes universidades que hacen uso y la información relacionada para facilitar la conectividad de dispositivos y sistemas médicos, el estándar está respaldado por la Asociación de Fabricantes Eléctricos (MENA).

El estándar está en la capacidad de:

- Definir los formatos e intercambiar imágenes, resultados, medidas, reportes y *waveforms* (gráficas).
- Permite la conectividad e intercambio de datos entre: Dispositivos de adquisición de imágenes / Modalidades: rayos X, TC, RM, NM, US; Estaciones de trabajo de diagnóstico; Sistemas de Gestión de Imagen (PACS); Almacenamiento y archivo de productos; Sistemas de Información de Radiología (RIS); Sistemas de Información de Cardiología (CIS); Sistemas de planeación de terapia de radiación.

CAPÍTULO III

ANALISIS SITUACIONAL

3.1. Antecedentes

El estado del Ecuador presento en el 2017 el "Plan Nacional del Buen vivir", cual se apoya en los artículos 280: Plan de desarrollo y 293: Formulación y la ejecución del presupuesto general del estado de la constitución de la república.

El plan nacional del buen vivir es presentado como el deseo de una sociedad en la que las personas puedan satisfacer sus necesidades para alcanzar una vida y muerte digna, con equidad y justicia social, libres de todo tipo de violencia y discriminación, logrando armonía individual, social y con la naturaleza.

El estado como parte del plan nacional del buen vivir implemento infraestructura sanitaria con la construcción de varias casas de salud con la tecnología necesaria para enfrentar los casos necesarios de estados de salud de una persona y el pueblo en general.

Todos los procesos que se realizan dentro de los hospitales en el área administrativa como asistenciales (salud), se los crea, administra y actualiza a través de un software en un computador (PC). Con la inclusión de las tecnologías de la información en las áreas de trabajo y equipos médicos que son parte de una red de datos, los equipos generan gran cantidad de información, por tal razón se debe considerar la implementación de una política de gestión de seguridad de la información.

Las áreas de tecnología de las entidades de salud del país están dirigidas por la Dirección Nacional de Tecnologías de la Información quien debe proponer, implementar y administrar

políticas, normas y procedimientos que optimicen la gestión y administración de las tecnologías de la Información y comunicaciones (TIC'S), garantizando la integridad de la información, optimización de recursos, sistematización y automatización de los procesos institucionales, así como el soporte tecnológico institucional, establecido en el Acuerdo Ministerial 134 del 1 de Noviembre de 2012.

3.2. La institución

Gráfico 4 *Hospital General Docente de Calderón*
Fuente: *Fotografía de Google Maps*

El Hospital General Docente de Calderón tiene como misión en su plan estratégico*:*

*"*Proveer atención integral especializada a la comunidad, complementando la atención en red a través de nuestra cartera de servicios, garantizando accesibilidad y calidad, con talento humano capacitado y motivado, apoyados en la docencia e investigación*"* (HGDC, 2017 - 2020).

El hospital tiene como objetico en su plan estratégico: "Incrementar la eficiencia operacional en el hospital" y la acción para cumplirlo es: Automatizar el sistema de Información de acuerdo a lineamientos de la Dirección Nacional de Hospitales

La automatización de los sistemas de información involucra el uso de varias herramientas del área de TIC'S, como el almacenamiento, alertas, virtualización, seguridad y administración que permitirá mitigar los riesgos de ingresos no autorizados entre otras.

Poseer desarrollada la política de gestión de seguridad de la información que facilitará la automatización y administración de la información una vez que la tengamos ordenada, segura y con procesos definidos para mantenerlos.

Al establecer la articulación entre el Plan Nacional del Buen Vivir y las responsabilidades de la Dirección Nacional de Tecnologías de la Información, se establece que debe tener, mejorar y velar por una comunicación efectiva, eficiente y pertinente para contribuir a la mejora de la cultura de seguridad organizacional.

El hospital posee una estructura organizacional conformada por la Gerencia en un primer nivel, en segundo nivel los comités, en tercer nivel Asesoría Jurídica, Comunicación, Planificación, Gestión de Calidad, Gestión de red, en un cuarto nivel Administrativo Financiero, Admisiones y Estadística, Atención al Usuario, Administrativo, Financiero, Talento Humano, TIC'S, Seguridad, Salud Ocupacional y Ambiente, igual en un primer nivel la Dirección Asistencial y las Subdirecciones Médicas. Como se muestra en la siguiente Imagen.

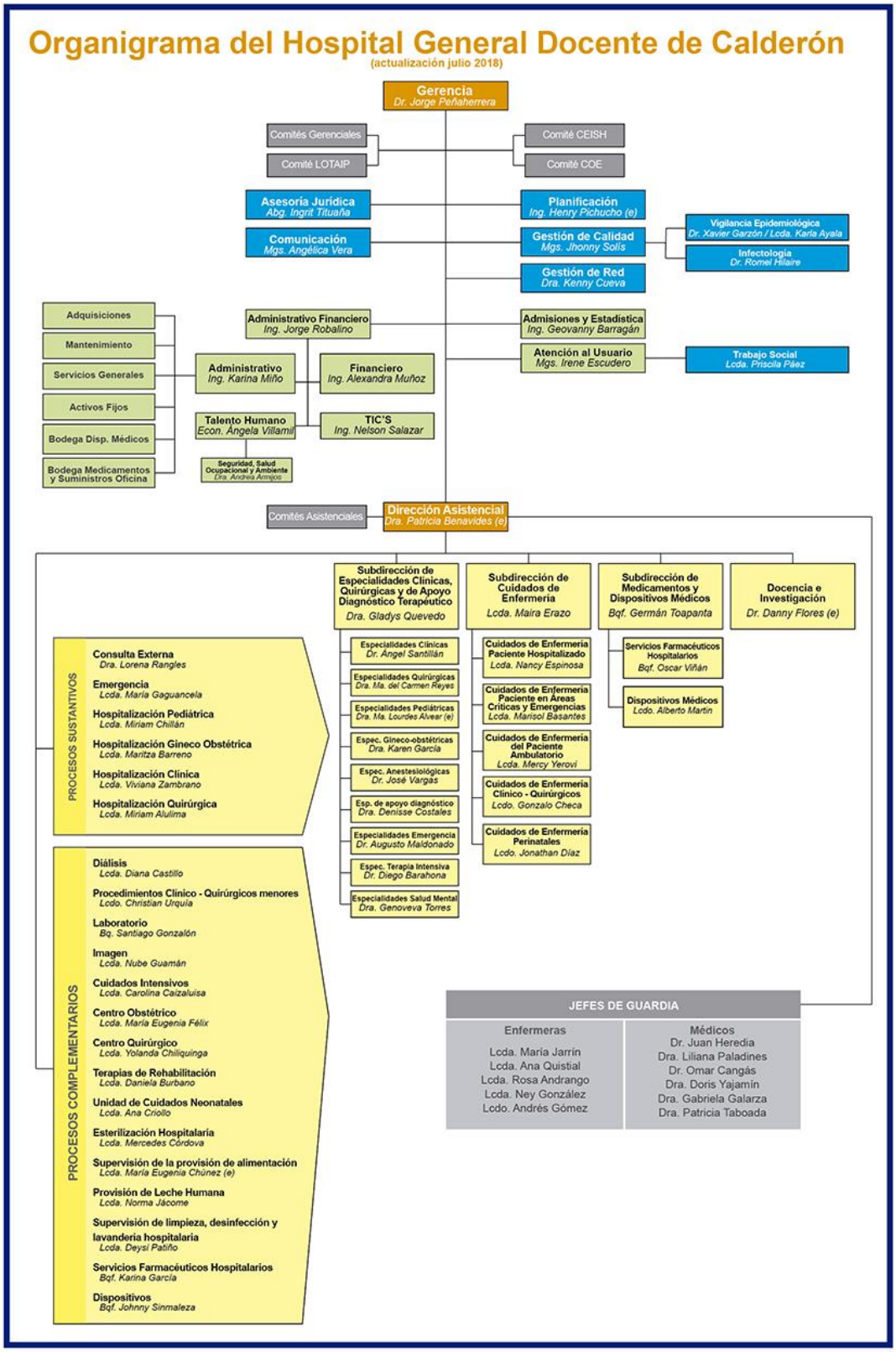


Gráfico 5 *Organigrama del Hospital General Docente de Calderón*
Fuente: *Pagina web del Hospital (https://www.hgdc.gob.ec/index.php/hospital/organigrama)*

3.3. Situación Actual

En referencia a lo expuesto el hospital posee directrices para el tratamiento y administración de las tecnologías de la Información internas, mismas que deben ser aplicadas para garantizar el funcionamiento de las áreas administrativas y de salud, pero no dirigidas a la Seguridad de la Información y específicamente para las áreas médicas como la de Imagenología.

El hospital como se comentó pertenece al MSP (Ministerio de Salud Pública) quien posee un documento con Políticas Uso de Servicios de Red y Servicios Informáticos del Ministerio de Salud Pública, donde en su segmento de seguridad habla del "criterio de configuración de contraseñas, violaciones a la seguridad de cuentas de correo, si fue esta vulnerada, o cuando el usuario no tiene acceso" (DNTICS, 2012). Siendo evidente la falta de directrices o guías para cumplir con la seguridad de la producción de información médica dentro de las unidades hospitalarias a su administración y el incumplimiento de las leyes nacionales e internacionales expuestas en 2.1.4 Marco Regulatorio, con el concepto generalizado del uso de un conjunto de buenas prácticas que posee el estándar ISO 27000 y el objetivo de llegar al establecimiento del Gobierno de TI que en la práctica Oliveira W (2017) la define como:

> La combinación estructurada de un conjunto de directrices, responsabilidades, habilidades y capacidades, compartida y asumida dentro de las empresas por los ejecutivos, gerentes, técnicos y usuarios de TI, con el objetivo de controlar eficazmente los procesos, garantizar la seguridad de la información, optimizar el uso de recursos y dar apoyo para la toma de decisiones, todo eso alineado con la visión, misión y objetivos estratégicos de las organizaciones.

Un primer paso para llegar a cumplir este objetivo es el desarrollo de un SGSI (Sistema de Gestión de Seguridad de la Información) el cual pretende establecer una serie de controles para la gestión de la seguridad de la Información.

Conceptos, criterios y argumentos que impulsan la investigación y selección del área de imagenología del hospital general Docente de Calderón como un área estratégica para implementar controles de seguridad, que permitan el cumplimiento de leyes nacionales en la administración de la información a través del diseño de una política de gestión de seguridad de la información.

3.3.1. Topología de la red

La estructura de la red del hospital de acuerdo con un modelo tipo de unidades médicas para la Sierra, posee una estructura lineal, iniciando desde la conexión a un servicio de datos, un firewall, un equipo de enrutamiento, un controlador de rede Inalámbricas, servidores de correo, sistemas médicos entre otros. Un bosquejo de la red general del HGDC, en el Gráfico 5, y del área en el Gráfico 6 El Hospital General Docente de Calderón posee una topología de red jerárquica:

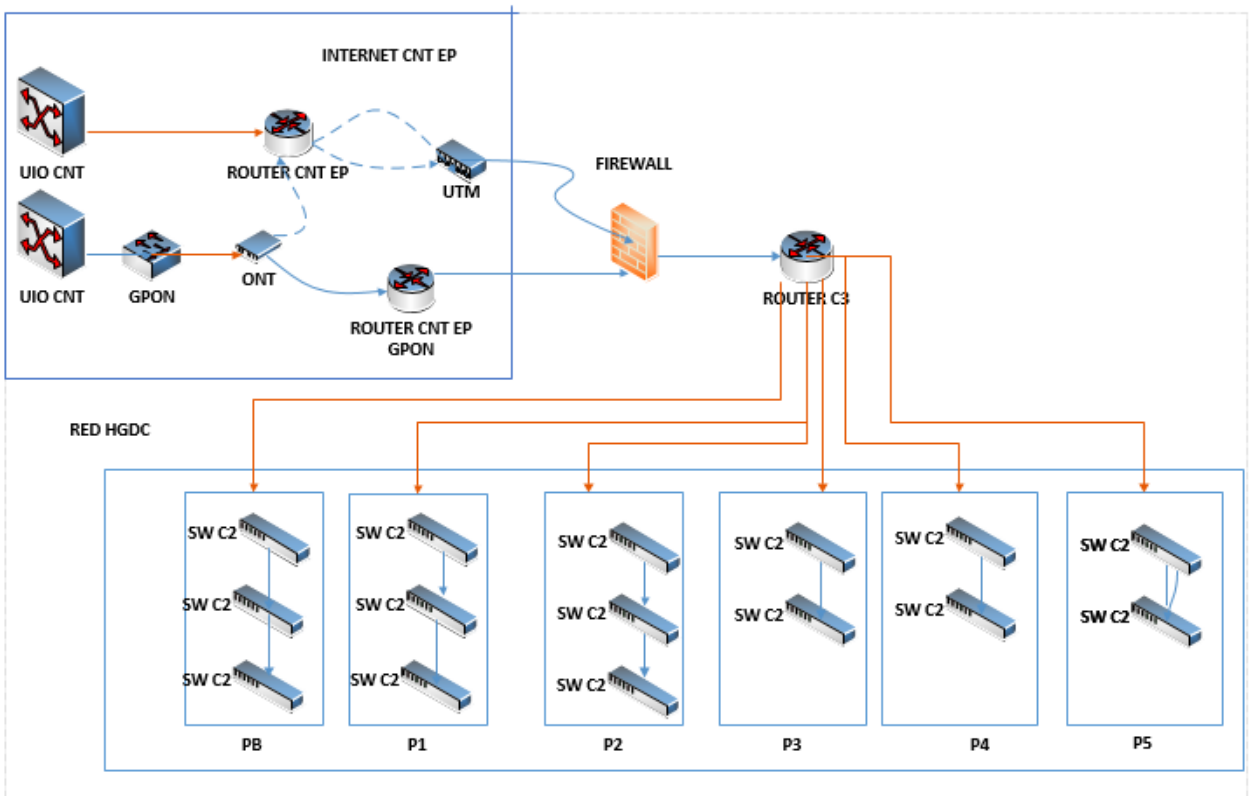


Gráfico 6 *Diagrama de red del HGDC*
Elaborado por: *investigador*

El área de estudio se encuentra en la planta baja y posee la siguiente topología de infraestructura:

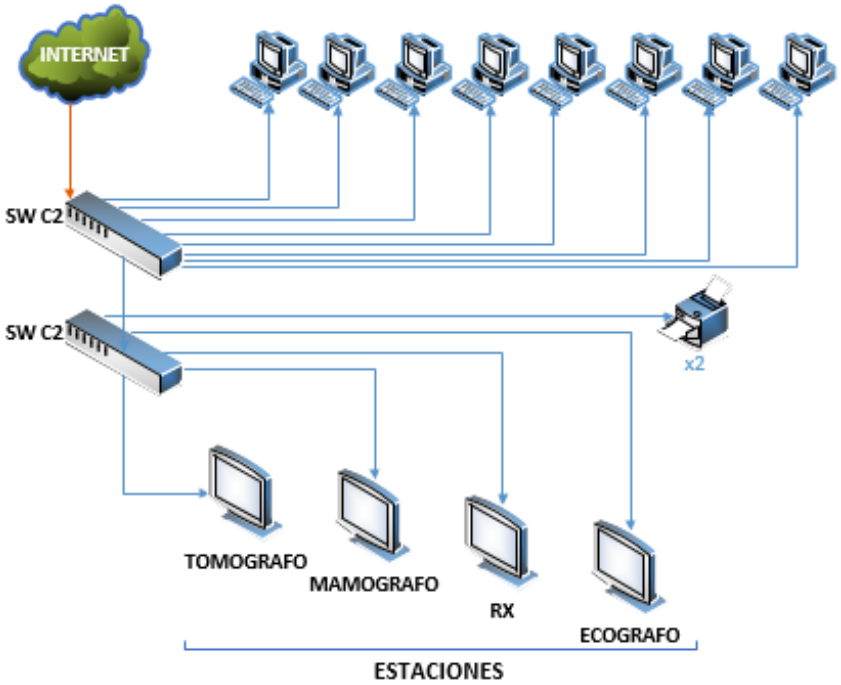


Gráfico 7 *Topografía de red del área de imagenología*

Elaborador por: *investigador*

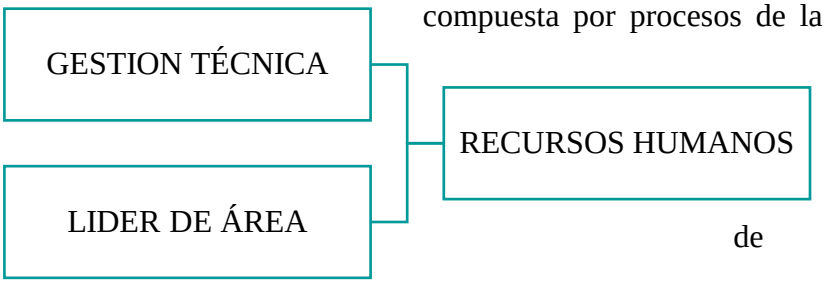
3.3.2. Área de imagenología

El área de imagenología se estructura de acuerdo con los procesos técnicos y administrativos:

Gráfico 8 *Diagrama de procesos imagenología*
Elaborado por: *investigador*

Descripción

El área está compuesta por procesos de la gestión técnica que se encarga de la compra o contratación de equipos y los procesos de gestión y administración del área ejecutados por la líder del área.



Mapa de procesos del área:

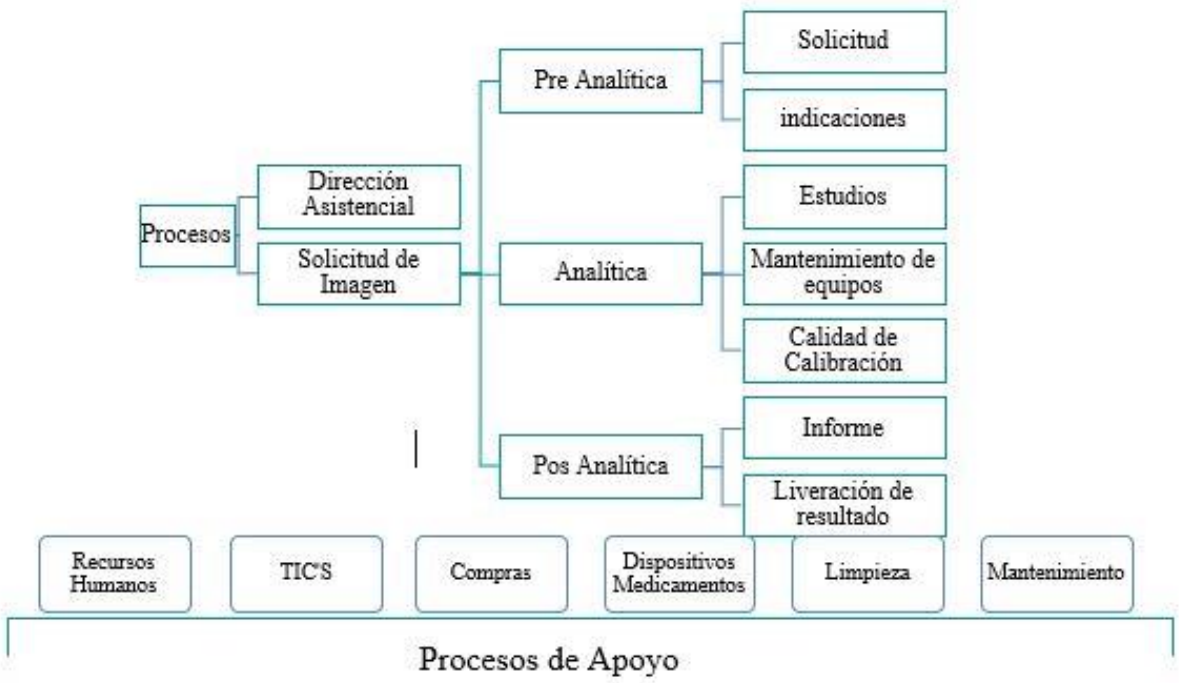


Gráfico 9 *Mapa del proceso de examen de imagen*
Elaborado por: *investigador*

Personal del área:

El área se encuentra conformada por 3 grupos de profesionales con un total de 19 personas que desempeñan sus funciones en el área, los grupos se describen en la siguiente tabla:

DENOMINACIÓN	PERFIL	N°
Médico/a Especialista de Imagenología/Radiología 1	El profesional interpreta y entrega los resultados de los exámenes realizados por los tecnólogos médicos de	4

	Imagen, además asisten en los procedimientos invasivos para los pacientes.	
Tecnólogo Médico de Imagenología 2 y 3	Profesional que realiza los procedimientos técnicos, manipula los equipos para generar los exámenes a ser interpretados por el médico.	12
Administrativos	Personal que se encuentra en la entrega de exámenes, turnos entre otras.	3

Tabla 4 *Personal del área de imagenología del HGDC*
Elaborado por: *investigador*

3.3.3. Descripción técnica de equipos

El área de Imagenologías del hospital Docente de Calderón posee el siguiente equipamiento:

3.3.3.1. Computadores de las áreas de trabajo

Estos equipos son utilizados para redactar los informes de los exámenes realizados a los pacientes, así como las funciones administrativas.

Los equipos poseen las siguientes Características:

EQUIPO	AREA	N°
Procesador: Core i5; Memoria: 4 GB Procesador core i5; Disco Duro: 500 GB; Sistema Operativo: Win7; Monitor: 19,5"	Recepción y entrega de Exámenes	2
	Área de Interpretación	5
	Oficina Líder de área	1

Tabla 5 *Número de equipos y su ubicación*
Elaborado por: *Investigador*

3.3.3.2. Estación de trabajo del tomógrafo

El equipo se lo utiliza para visualización e impresión de las imágenes, es un equipo tipo servidor tipo torre de la serie HP ProLiant ML310e Gen8 v2:

EQUIPO	AREA	N°

Procesador: Intel Xeon E3-1240V3 / 3,4 GHz. Memoria: 32 GB / DDR3 SDRAM – ECC Disco Duro: 8GB / SATA 6Gb/s / 7200 rpm / HDD Monitores: 2 de resolución 2560 x 1440 píxeles/contraste1000/brillo de 350 cd/m^2	Área de visualización	2

Tabla 6 *Número de equipos y su ubicación*
Elaborado por: *Investigador*

Para la transmisión y visualización de las imágenes generadas por el Tomógrafo, este posee un computador adicional propio del equipo, mismo que posee un *software* llamado Singo.via, que es el que permite la visualización en conjunto con la calidad del monitor.

3.3.3.3. Estación de trabajo del mamógrafo

El equipo se lo utiliza como visualizador de las imágenes de los exámenes, consta de un equipo *Dell Precision* T5600 con las siguientes características:

EQUIPO	AREA	N°
Procesador: Intel Xeon E5-2630 Memoria: 16GB de Memoria DDR3 a 1333 MHz (4 DIMMs x 4GB ECC UDIMM) Disco Duro Capacidad: 2 DISCOS DE 1000 GB ARREGLO RAID 1 (espejo) Monitores: 2 de resolución 2560 x 1440 píxeles/contraste1000/brillo de 350 cd/m^2	Área de visualización	1

Tabla 7*Número de equipos y su ubicación*
Elaborado por: *Investigador*

3.3.3.4. Tomógrafo

Imagen 1 *Tomógrafo*
Fuente*: AG and Medical (2006)*

El equipo posee las siguientes características:

- Marca SIEMENS
- MODELO: SOMATOM *Definition* AS, Siemens ha establecido un escáner que, por primera vez, es capaz de adaptarse a prácticamente todos los pacientes y todas las preguntas clínicas.

Con su gran flexibilidad, el sistema ha demostrado ser la opción correcta cuando se trata de imágenes de tomografía computarizada de alta calidad, sin importar si está configurado para ser usado en diagnósticos de rutina.

Imágenes, ajustes cardíacos de alta gama o para agregar información funcional y material a la morfología con Dual Energy o conjuntos de datos dinámicos. Además, el sistema puede adaptarse a entornos clínicos especializados, como cirugía de alto nivel, una solución de cuidado agudo de dos salas con un pórtico deslizante, un escenario de planificación de radioterapia dedicado con un gran calibre o un entorno de intervención altamente eficiente con capacidades 3D excepcionales. Todo esto viene junto con la exclusiva tecnología FAST CARE de Siemens.

Resultados clínicos sobresalientes y más tiempo con sus pacientes: simplemente se hace para maximizar los resultados clínicos y la productividad centrada en el paciente. Siemens-Healthcare-Headquarters (2016) Mamógrafo

Imagen 2 *Componentes de Mamógrafo*
Fuente*: AG and Medical (2006)*

El mamógrafo es de la marca *General Electric*, modelo *Senographe DS* que pertenece a la familia de sistemas de mamografía digital, con la capacidad de utilizar la tecnología digital, dispositivos de visualización digital, redes de datos, sistema de archivos y se elimina el uso de casetes de película.

El equipo posee la capacidad de mostrar en su pantalla imágenes procesadas como no procesadas tras pasar unos cuantos segundos de ser generada.

El equipo posee un componente adicional que es la estación de revisión, al que consta de un computador con características de manejo de imágenes y 2 monitores verticales.

Toda la transferencia de imágenes se la realiza con el estándar de comunicación DICOM, la capacidad de almacenamiento es de 195 GB

Imagen 3 *Elementos de una estación de revisión*
Fuente: *AG and Medical (2006)*

3.3.3.5. Rayos x

Imagen 4 *Rayos X*
Fuente: *AG and Medical (2006)*

El *PEDS 600* es un sistema de radiografía brazo en U para radiología análoga o digital, en combinación con las mesas XP es la solución ideal para trabajar en espacios pequeños, modernos con un solo Bucky.

3.3.3.6. Rayos X móvil

Imagen 5 *Rx Móvil*
Fuente: *GE.Healthcare (2011)*

Los sistemas AMX de última generación son equipos de rayos X móviles y completamente digitales que llevan las tecnologías de adquisición de imágenes digitales hasta los pacientes.

Marca: *General Electric*
Posee las siguientes características:

Interfaz de usuario

- Interfaz gráfica de usuario (GUI) optimizada: técnica, adquisición de imagen y herramientas de visualización en una única interfaz de usuario integrada. La pantalla de previsualización de imágenes abarca el 50% de la pantalla.

- Paleta con las herramientas más utilizadas disponible en todas las pantallas de procesamiento de imágenes.

- Edición/copia de exámenes para volver a procesar las imágenes sin exposiciones de un paciente adicionales.

- Reprocesamiento de imágenes que permite seleccionar varias apariencias con parámetros de representación configurables.

- Técnicas opcionales según la anatomía y tamaño del paciente.

- Se admiten anotaciones de texto en imágenes con posibilidad de configurar el tamaño de la fuente para la visualización e impresión.

- Uso de herramientas de generación de informes por parte de usuarios individuales y grupos de usuarios.

- Panel de mandos del estado del sistema.

- Indicadores independientes de carga de la batería del sistema y del estado del sistema.

Productividad

- El modo en espera evita los ciclos de inicio y permite realizar radiografías 25 segundos después de activar el sistema.

- Se pueden realizar y procesar exposiciones mientras la unidad está conectada y se está cargando.

- Los algoritmos de carga automática de la carga inteligente permiten que el sistema se vuelva a cargar, aunque las baterías no estén completamente agotadas.

- El sistema se puede desplazar 4 segundos después de su activación.

Detector digital

- Conectividad inalámbrica del detector al sistema.

- El diseño ligero de la carcasa del detector, específica para un uso móvil, pesa menos de 4,5kg (10 libras) con la batería.

- El detector funciona con baterías recargables e intercambiables. Se incluye cable de conexión de reserva, dos baterías y un cargador.

- La batería del detector se carga automáticamente mientras el detector está en el receptáculo.

- El sistema se puede utilizar sin el detector para realizar exposiciones de CR o filmaciones analógicas.

Flujo de trabajo

- Paso del procedimiento realizado de la modalidad (MPPS; SPS/PPS configurable)
- Transferencia de imágenes automática y personalizable a PACS e impresoras.
- Actualización automática de la lista de trabajo (configurable).
- Las imágenes se pueden volver a procesar después de la adquisición y durante un examen.
- MWL permanece visible hasta la siguiente actualización, aunque se pierda la conexión a la red.

Comunicación. –

La lista de trabajo puede recuperarse de los sistemas HIS/RIS y las imágenes se pueden transmitir a través de la interfaz DICOM a impresoras, dispositivos de almacenamiento de archivos (PACS), servidores o estaciones de trabajo de revisión.

- Puerto Ethernet Base T RJ45 10/100/1000 o conexión inalámbrica opcional 802.11 a/b/g/n
- Servicios compatibles con IHE y DICOM 3.0:
- DICOM IOD generado: DX
- Envío/transferencia automáticos de imágenes: DX o CR (compatibles con varios destinos)
- Almacenamiento DICOM: SCU
- SCP de confirmación de almacenamiento DICOM, cuando se proporciona una dirección fija de IP (función programable de eliminación automática)
- Lista de trabajo de modalidad DICOM para los sistemas HIS/RIS: SCU (con actualización automática programable)
- Impresión en escala de grises DICOM: manual y automática (con opciones de disposición de impresión)
- Impresión de formatos múltiples
- Intercambio de soportes CD-R DICOM (sólo DX)
- Verificación de la conectividad para los servicios SCU y SCP
- Comentarios del Paso del procedimiento realizado de la modalidad (MPPS) DICOM a los sistemas HIS/RIS (SPS PPS) (configurables)
- VOI LUT graba al enviar (configurable) General-Electric-Company (2015)

3.3.3.7. Ecógrafo 1

Imagen 6 *Ecógrafo Móvil*
Fuente: *Philips (2019)*

El equipo posee las siguientes características:

- Marca: Philips
- Modelo: Affiniti 50
- *Software* cardiógico para Aplicaciones de Imágenes Generales.
- Arquitectura con 4.718.592 canales de Procesamiento
- Rango dinámico de 280 dB
- SonoCT Composición de imágenes en tiempo real.
- XRES Analiza patrones de imágenes a nivel de los píxeles, proporciona reducción de artefactos.
- La optimización iSCAN con la pulsación de un solo botón, ajusta de forma rápida y automática los parámetros
- Optimización inteligente iOPTIMIZE
- Modo en Imagen Panorámica
- AutoSCAN con compensación de ganancia adaptativa
- Imágenes armónicas tisulares (THI) con tecnología de pulso invertido
- Capacidad WideSCAN para ampliar el campo de visión
- Función QuickSAVE permite guardar con rapidez los ajustes preferidos como tipos de examen individuales
- Conectividad y Manejo de Datos. Módulo de CD/DVD
- DICOM 3.0 Conectividad con impresoras y servidores.
- pantalla LCD de alta definición de 21,5″. Con articulación oscilobatiente independiente en Brazo articulado.

- Capacidad de almacenamiento combinada de 512 GB
- Puerto USB
- Puerto Ethernet
- Conectividad inalámbrica

El Affiniti 50 de Philips es una máquina de ultrasonido de servicio compartido de gama media que se desarrolló en 2014 a partir de la prima Epiq 7. El Affiniti 50, El Affiniti 50 tiene características de la tecnología de la serie Epiq, incluyendo el asombroso QLAB a bordo del conjunto de cuantificación, Si no necesita sondas de cristal único, o elastografía de Shearwave entonces el Affiniti 50 ofrece una opción menos costosa.

Imagen 7 *Panel de Control del Ecógrafo*
Fuente: *Philips (2019)*

Este es equipo que permite atender tal demanda es preciso disponer de funciones avanzadas y de información de diagnóstico con toda rapidez, pero no a costa de la precisión ni de la facilidad de manejo. El sistema ha de ser ergonómico y, al mismo tiempo, lo suficientemente resistente para dar respuesta a un elevado número de pacientes.

Tecnología

La función de formación de haces de precisión, las preconfiguraciones específicas de tejidos (TSP) y las herramientas eficientes y automáticas de Affiniti 50, aumentan la productividad y la fiabilidad. La tecnología proporciona un rango dinámico y amplio para una excelente resolución espacial y de contraste, una extraordinaria uniformidad de los tejidos, menos artefactos y disminución de las perturbaciones de la imagen.

Las preconfiguraciones específicas para tejidos (TSP) ajustan más de 7500 parámetros a fin de optimizar el transductor para cada tipo de examen, lo que permite generar imágenes de gran calidad. A esta calidad de imagen superior se suman funciones clínicas avanzadas como la elastografía, el ultrasonido con contraste (CEUS) y *Anatomical Intelligence Ultrasound* (AIUS). d sin apenas realizar ajustes.

Valoración dinámica de órganos y tumores en tiempo real

Con Affi niti 50, puede agregar la capacidad de contraste mejorado (CEUS) a prácticamente cualquier examen. Además, proporciona un rendimiento excepcional con numerosas aplicaciones, lo que permite llevar a cabo una evaluación dinámica de la perfusión de órganos y tumores en tiempo real. (KPI.HEALTHCARE.INC., 2019)

3.3.3.8. Ecógrafo 2

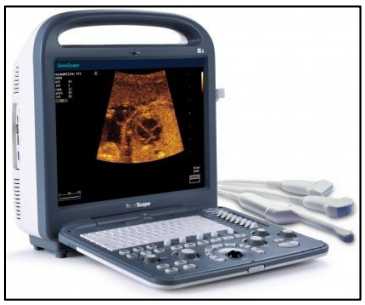


Imagen 8 *Ecógrafo Portátil*
Fuente: *SonoScape* (2014)

El equipo Posee las siguientes características:

- S2: Sistema Inteligente de Color
- Diseño ergonómico
- Diseño Portátil que permite su uso a cualquier tiempo y en cualquier lugar
- Monitor HD LCD de 15 pulgadas con amplios ángulos de visualización
- Teclado estándar PC
- Dos conectores y soportes ergonómicos para transductor
- Batería recargable de Litio, con posibilidad de escaneo de 1 hora sin fuente de alimentación

- Varios sistemas de salida de imagen: DICOM3.0, VGA, video out, USB, S-Video, Footswitch etc.

Funciones sobresalientes:

Modos de trabajo completos, sobresaliente desempeño 2D, imagen de flujo sanguíneo sensitiva, tecnología de imagen 4D, paquete interno con las mejores funciones de su clase.

Modos de trabajo completos:

- B Mode, Dual B, 4B
- M Mode, Steer M,
- Color Mode, DPI Mode
- PW Mode, CW Mode (opcional)

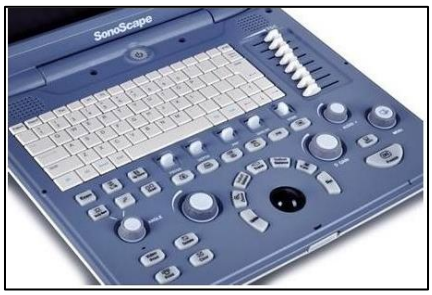


Imagen 9 *Panel y Teclado*
Fuente: *SonoScape* (2014)

Tecnología avanzada de imagen:

- THI
- μ-Scan Speckle Reduction (opcionall)
- Compound Imaging (opcional)
- Panoramic Imaging (opcional)
- Trapezoid Imaging (opcional)

- 4D imaging (opcional)

Amplia gama de aplicaciones clínicas:

- Practica general: gastroenterología, ginecología y obstetricia, Cardiovascular, Urología
- *Software* de paquetes para cálculos y post medidas
- Reportes profesionales para diferentes exámenes

Múltiples transductores:

Convexo, Linear, Transvaginal, Transrectal, Intraoperativo, Micro-convexo, Volume 4D

Optimización en la práctica diaria:

- Flujo de trabajo mejorado, manejo inteligente de información, sistema Doppler color con interfaz amigable e intuitiva.
- Define tu propio estilo de trabajo: Configuraciones de trabajo totalmente ajustables
- Sistema de fácil revisión de imagen
- Diferentes soluciones de almacenamiento de información: disco duro de 320Gb, puerto
- DICOM 3.0 LAN, VGA Flash disk, Disco duro externo, DVD externo, impresora de video, USB laser/jet printer (ADIEMED)

3.3.4 Administración de la información médica en el área de imagenología

Actualmente, la producción del área de imagenología con respecto a la información resultante de la práctica de los exámenes a los pacientes no posee un medio de almacenamiento centralizado como recomiendan los estándares de seguridad de la Información de la salud estudiados, al momento la producción se está almacenando en los discos de los mismos equipos y estaciones de monitoreo, incumpliendo una de las normas de almacenamiento que las norma

nacional dispone de 7 años, los equipos de las áreas de trabajo (computadores), carecen de perfiles, no poseen claves de acceso a la cuenta de usuario, el área maneja y genera información confidencial, por tal razón el hospital deberá generar documentación legal que garantice y comprometa la confidencialidad de la información por temas académicos.

La red del área se encuentra segmentada a través de una VLAN, que se propaga para todos los equipos de la planta que incluyen otras áreas médicas como administrativas.

Los equipos de imagen y las estaciones de monitoreo se encuentran dentro de la red del hospital y a la ves comparten de manera interna para la transmisión de las imágenes con el formato de comunicación DICOM.

El personal médico para visualizar y analizar los resultados de los exámenes, utilizan la estación de monitoreo, misma que cuenta con un solo perfil de usuario.

El hospital al poseer su área de docencia, estudiantes de diferentes universidades del país utilizan resultados de exámenes como material académico, incumpliendo el hospital con la confidencialidad de la información médica del paciente.

3.3.5 Gestión de cambios en *software* y *hardware*

Gestión que las establece las dos normas de estudio como un eje fundamental para la seguridad de la información, haciendo hincapié con la información de la salud como lo dispone la ISO 27799. Las acciones que involucran cambios son: la creación, modificación de aplicativos, reportes, configuraciones de equipos, instalaciones y muchos más, que de no ser planificados y documentados pueden interferir en la integridad y continuidad de la información.

Las normas establecen que se debe establecer un proceso de solicitud a las áreas de administración de tecnología (TIC´S), para que sea informado y aprobado por el jefe inmediato o

que al momento se encuentre encargado, sabiendo que tiene la responsabilidad de aceptar o rechazar lo solicitado.

Al momento dentro de las instalaciones del hospital Docente de Calderón estas se las solicita a través de la mesa de ayuda, misma que es asignada a un Analista de Soporte Técnico, con la debilidad de que en casos el Administrados del área desconoce de las acciones solicitadas. El cumplimiento de estas depende de la existencia de material necesario para lo solicitado.

3.3.6 Seguridad física

Las estaciones de monitoreo al momento son de fácil acceso a cualquier personal del hospital sea este médico como administrativo, aumentando las vulnerabilidades de la información, estas poseen clave de acceso mínima, misma que está expuesta por estar escrita al reverso de un calendario. El acceso al área de imagenología posee 2 ingresos uno con control de acceso magnético y la otra totalmente abierta para el ingreso de las camillas misma que esta junto a los ascensores.

Los equipos de cómputo poseen dos cuentas de administrador y de cliente, este último no posee seguridad alguna, todo el personal médico los utiliza para redactar los informes de los exámenes realizados.

3.3.7 Producción

Dentro del ámbito médico y en general un área produce y se lo representa cuantitativamente con datos estadísticos ya analizados, el área de imagenología contempla sus 4 tipos de exámenes con una sala de tomografía, dos salas de radiografía y tres salas para ecografía, además de dos

equipos de Rayos X portátiles que se encuentran a disposición de todos los servicios del hospital como de varias áreas de salud de referencia (externas).

La producción anual se la cuantifica de acuerdo con:

Examen / año	2015	2016	2017	2018
Rayos x	3694	24149	36018	
Tomografías	1459	13824	18689	
Ecografías	2504	15464	17884	
Mamografías	-	975	1306	
Total, Placas	7657	54412	73897	
Procedimientos			836	
Placas por día		286	2383	

Tabla 8 *Estadísticas de Producción del Área de Imagenología*
Fuente: *Por investigador*

AÑO	2015	2016	2017	2018
Total, Pacientes	5003	35074	44336	
Promedio x mes	416	2923	3695	
Promedio x día	21	146	19	

Tabla 9 *Estadísticas de Pacientes*
Fuente: *Por investigador*

Esta producción son imágenes que se encuentran con extensión DICOM, y cada una genera un tamaño:

TIPO DE ESTUDIO	PROMEDIO DE TAMAÑO POR IMAGEN
Rayos X	91,66 KB
Tomografías	514 KB
Ecografías	3,16 KB
Mamografías	14,39 KB

Tabla 10 *Tamaño de Imagen en KB*
Fuente: *Por investigador*

3.4. Criterio de evaluación del riesgo

La evaluación del riesgo es el proceso de identificar la magnitud de la pérdida o daño posible y la probabilidad que dicho daño o pérdida suceda u ocurra, este concepto se lo tiene presente en toda actividad de la organización que de materializarse afectará a productos y/o servicios que esta ofrece.

La evaluación e identificación del riesgo en el campo de la Información existe la norma ISO 27001 cual posee 133 controles cuales son seleccionados luego de identificar los riesgos existentes en la organización con la finalidad de cumplir con el tratamiento del riesgo que es eliminarlo, mitigarlo o transferirlo.

Los riesgos en el campo de la salud se los puede tratar con la norma ISO 27799, en su capítulo 6.4.4 Evaluación del riesgo, donde hace referencia a la norma ISO/IEC 27002 además presenta directrices a considerar para proceder con la evaluación e identificación de los riesgos que existen en el campo de la salud.

3.5. Objetivos de la seguridad de la información de la salud

La norma tiene como objetivo “Mantener la confidencialidad, disponibilidad y la integridad de la información” (BRITISH, 2008), e incluye la autenticidad, responsabilidad y la capacidad de auditoría, esta última con la característica de que la política se encuentre en constante actualización, acción que permitirá cada vez afianzar la aplicación de los controles para la seguridad de la información.

Las normas al ser la recolección de buenas prácticas, posee objetivos y para que se cumplan debemos contemplar ciertas consideraciones:

- Cumplir con obligaciones legislativas.

- Aplicar las mejores prácticas para seguridad en informática de la salud
- Identificar las obligaciones de la entidad como de los profesionales de la salud
- Incentivar la implementación de la gestión de riesgos en las casas de salud
- Cumplir con todas las necesidades de seguridad identificadas.
- Utilizar la tecnología para apoyo en las actividades de salud.
- Generar niveles de confianza con el uso y aplicación de la tecnología.
- Garantizar la ética profesional del personal técnico que administra la información.
- Implementar un entorno de seguridad para los sistemas electrónicos de información de salud.
- Garantizar la interoperabilidad entre sistemas de salud.

De cumplir con cada una de las recomendaciones y otras consideraciones, la casa de salud poseerá una herramienta de administración de seguridad de la información garantizando el cumplimiento de los aspectos que la información debe poseer.

3.6. Identificación de las amenazas y riesgos en el área de imagenología

Una vez definido el concepto de política el item 2.1.3, y uno de los objetivos de la investigación de establecer los controles que permitan cumplir con las normas nacionales e internacionales ya nombras enfocados a la integridad, disponibilidad y confidencialidad como la generación de respaldos de la información sanitaria generada en el área de estudio, recurriendo a las recomendaciones de la ISO 27799.

Con la finalidad de identificar las amenazas y los riesgos la investigación define a los mismos como:

- **Amenaza. –** es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan.
- **Riesgo.** – es la acción que esta relaciona con la presencia de amenazas que pueden atentar contra la seguridad de recursos, información o peor aún con la continuidad de la empresa.

Como ya se estableció al riesgo se lo debe cuantificar en relación con la probabilidad de la Amenaza y la magnitud de daño que pueda ocasionar.

3.6.1. Amenazas en el área de imagenología

La norma ISO 27799 posee una lista de amenazas ya definida para él sector sanitario o de la salud, la investigación definirá a cada una de ellas y en base al número de soportes realizados en el área de imagenología, que se encuentran registrados en la herramienta de gestión de servicios GLPI establecida en el hospital. (**Anexo 1** Lista de Tiques dentro del área de imagenología, plataforma GLPI).

Amenazas definidas por la Norma:

- **Enmascararse por los internos. –** esta consiste en el uso de cuentas existentes, pero no propias.
- **Enmascararse por los proveedores de servicios. –** son acciones desleales por parte de los proveedores de servicios que, al poseer accesos totales a él o los sistemas, hacen uso de esta posibilidad para acceder a la información reservada.
- **Enmascararse por extraños. –** procedimiento realizado por una persona externa a la compañía obtiene los accesos infiltrándose de tal forma que llega a ser un usuario autorizado de forma ilegal.

- **El uso no autorizado de una solicitud de información de salud. –** Acción ejecutada por personal interno que posee un perfil de usuario, hace uso de su capacidad para alterar información de salud, auto beneficiándose.
- **Introducción del *software* dañino o perjudicial. –** El talón de Aquiles de la seguridad de la información como de los sistemas que los generan y almacenan, son los virus informáticos, que a través de la acción básica como instalar un *software*, al ser este dañino o perjudicial, evidencia la falta de protección de un antivirus o el mismo control de cambio de *software*.
- **El mal uso de los recursos del sistema. –** es una de las amenazas comunes en el campo laboral, que utilizan su equipo que posee *software* sanitario propios de la casa de salud, para beneficios propios, ingresando al internet y descargando información, creando aplicaciones no alineadas con las labores de la institución o trabajo, lo que genera una degradación de las capacidades de procesamiento y almacenamiento del equipo.
- **La infiltración de las comunicaciones. –** es la acción de interrumpir el flujo continuo y normal de los datos con la finalidad de obtener información y beneficiarnos de ella.
- **Interceptación de comunicaciones. –** es la interrupción de la transmisión de información cifrada, para realizar cambio alguno sobre ellas.
- **Repudio. –** es la acción de negación de haber enviado como recibido un mensaje.
- **Fallo en la conexión. –** Toda red de datos tiene la probabilidad de que los servicios que se distribuyen a través de ella fallen, para minimizar esta probabilidad se debe establecer niveles de calidad de servicio que influyen en el campo de la salud por valor para el bienestar de un paciente. Los fallos pueden generar accesos no deseados dejando la información disponible a ser extraída o alterada.

- **Incrustación de código malicioso. –** es una de las amenazas con mayor probabilidad de producirse debido al uso de correo electrónico y de descargas de páginas desconocidas, a través de estas acciones se infecta el *software* evidenciando la falta de antivirus o procedimientos de prevención de real de intrusiones.
- **Fallo técnico del anfitrión, instalaciones de almacenamiento o infraestructura de red.** Son amenazas que están directamente relacionadas con fallos en *Hardware* (storage), infraestructura (red de datos), que se provocan por la falta de control y seguimiento en los procesos de mantenimiento.
- **El fracaso de apoyo ambiental. –** amenaza no contemplada e influyente en las condiciones del entorno, infraestructura civil.
- **Sistema o *software* de red falla. –** es el foco principal de los atacantes utilizando la denegación de servicio, gracias a malas configuraciones existentes en los equipos de capa 2 y 3, así como de los equipos de usuarios finales con el uso de *software* no licenciado.
- **Falla de *software* de aplicaciones. –** estos son fallos en el *software* de equipos relacionados con servidores de aplicaciones internas, de ejecutarse el ataque la información sería de fácil acceso.
- **El error del operador. –** Son las ejecuciones no mal intencionadas de procedimientos en los equipos activos, que tiene la probabilidad de dejar expuesta la información. Este error es un fallo en el control de operaciones, seguridad del personal y recuperación de desastres.
- **Error de mantenimiento. –** Es una de las amenazas presente en los mantenimientos de los equipos activos que conforman la red, hechos por personal propio o por personal de la marca o empresa del equipo o sistema.

- **Error del usuario. –** Estas es una amenaza que encaja con una de las formas de obtener información que es la ingeniería social, todo usuario posee cierta información que a propio criterio no influye para la integridad de la información.
- **Escasez de personal. -** Es una amenaza que pertenece el cumplimiento a la alta gerencia, en contratar el número necesario de personal y con el conocimiento necesario para la administración y ampliación de la infraestructura existente.
- **Robo por los internos. –** Es una acción desleal de beneficiarse de la información que está a la administración y cuidado.
- **Robo por parte de personas ajenas. –** al ser lugares de alta circulación de personas un hospital debe contar con un gran sistema de seguridad, para la protección de la infraestructura e información, de consumarse un robo la fuga de información es la principal acción de disolución de la seguridad.
- **Daño intencional por los internos. –** Son acciones ejecutadas con premeditación por personal interno, calificados como actos de vandalismo, afectando al equipamiento y al entorno donde estos se alojan.
- **Daño intencional por personas ajenas. -** Son acciones ejecutadas con premeditación por personas externas, calificados como actos de vandalismo, afectando al equipamiento y al entorno donde estos se alojan.
- **Terrorismo. –** es una de las amenazas que no podemos controlar, que de suceder no solo destruyen la información o infraestructura involucra a todo el entorno.

3.6.2. Evaluación del riesgo

Con el Criterio de evaluación de riesgo y las amenazas identificadas por la norma, descritas en la sección anterior, se las ajusta a las condiciones del área de Imagenología del Hospital General Docente de Calderón para determinar niveles de riesgo, tomando en cuenta la frecuencia e impacto.

En la investigación se utilizó la matriz de riesgos, herramienta que nos permitió identificar los riesgos más significativos inherentes para el área de estudio, para ello las variables son la frecuencia que autores la toman como una probabilidad de ocurrencia y otros como la frecuencia de ocurrencia, así también al impacto representado como el nivel de gravedad que producirá la amenaza de ejecutarse en la producción del área. Dentro del campo de la salud la información es un aspecto crucial de protección, debido a que la perdida de esta no solo generaría desprestigio al hospital, procesos legales, también incide en la salud de una persona.

Con referencia en la Guía para la administración del riesgo institucional de la fiscalía general del estado suscrita el 21 de marzo del 2016, la matriz de calor de riesgo representada en la siguiente tabla:

MAPA DE CALOR DEL RIESGO						
FRECUENCIA	**Muy Probable (5)**	Alto (5)	Alto (5)	Extremo (15)	Extremo (20)	Extremo (25)
	Probable (4)	Moderado (4)	Alto (8)	Alto (12)	Extremo (16)	Extremo (20)
	Posible (3)	Baja (3)	Moderado (6)	Alto (9)	Extremo (12)	Extremo (15)
	Irregular (2)	Baja (2)	Baja (4)	Moderado (6)	Alto (8)	Extremo (10)
	Improbable (1)	Baja (1)	Baja (2)	Moderado (3)	Alto (4)	Alto (5)
IMPACTO		**Insignificante (1)**	**Menor (2)**	**Moderado (3)**	**Mayor (4)**	**Catastrófico (5)**

Tabla 11 *Mapa de calor del riesgo*
Fuente: *Guía para la administración del riesgo institucional de la fiscalía general del estado*

De acuerdo con la Tabla 7 se procede con la evaluación de las amenazas expuestas en el literal 3.6.1 en correlación a la realidad del área de Imagenología del Hospital General Docente de Calderón, se ha extraído información de la herramienta de administración de servicios GLPI, estadísticas de las atenciones que el área ha generado durante todo el 2018, información que permite ser objetivos en la evaluación de las amenazas.

Identificador de la Amenaza	Amenaza Evaluada	Frecuencia	Impacto	Riesgo
ASI-1	Enmascararse por los internos	**Probable (4)**	**Mayor (4)**	Extremo (16)
ASI-2	Enmascararse por los proveedores de servicios	**Probable (4)**	**Catastrófico (5)**	Extremo (20)
ASI-3	Enmascararse por extraños	**Improbable (1)**	**Catastrófico (5)**	Alto (5)
ASI-4	El uso no autorizado de una solicitud de información de salud	**Irregular (2)**	**Catastrófico (5)**	Extremo (10)
ASI-5	Introducción del *software* dañino o perjudicial	**Improbable (1)**	**Catastrófico (5)**	Alto (5)
ASI-6	El mal uso de los recursos del sistema	**Improbable (1)**	**Menor (2)**	Baja (2)
ASI-7	La infiltración de las comunicaciones	**Posible (3)**	**Moderado (3)**	Alto (9)
ASI-8	Interceptación de comunicaciones	**Posible (3)**	**Moderado (3)**	Alto (9)
ASI-9	Repudio	**Posible (3)**	**Insignificante (1)**	Baja (3)
ASI-10	Fallo en la conexión	**Muy Probable (5)**	**Mayor (4)**	Extremo (20)
ASI-11	Incrustación de código malicioso	**Probable (4)**	**Catastrófico (5)**	Extremo (20)
ASI-12	Fallo técnico del anfitrión, instalaciones de almacenamiento o infraestructura de red	**Posible (3)**	**Moderado (3)**	Alto (9)
ASI-13	El fracaso de apoyo ambiental	**Improbable (1)**	**Insignificante (1)**	Baja (1)
ASI-14	Sistema o *software* de red falla	**Muy Probable (5)**	**Mayor (4)**	Extremo (20)
ASI-15	Falla de *software* de aplicaciones	**Irregular (2)**	**Mayor (4)**	Alto (8)
ASI-16	El error del operador	**Posible (3)**	**Moderado (3)**	Alto (9)
ASI-17	Error de mantenimiento	**Irregular (2)**	**Catastrófico (5)**	Extremo (10)
ASI-18	Error del usuario	**Muy Probable (5)**	**Moderado (3)**	Extremo (15)
ASI-19	Escasez de personal	**Irregular (2)**	**Moderado (3)**	Moderado (6)
ASI-20	Robo por los internos	**Irregular (2)**	**Moderado (3)**	Moderado (6)
ASI-21	Robo por parte de personas ajenas	**Improbable (1)**	**Moderado (3)**	Moderado (3)
ASI-22	Daño intencional por los internos	**Irregular (2)**	**Catastrófico (5)**	Extremo (10)
ASI-23	Daño intencional por personas ajenas	**Improbable (1)**	**Moderado (3)**	Moderado (3)
ASI-24	Terrorismo	**Probable (4)**	**Catastrófico (5)**	Extremo (20)

Tabla 12 *Evaluación de las amenazas de ISO 27799 en HGDC*
Elaborado por: *investigador*

Trasladando los datos a un diagrama de calor se observa la tendencia de las amenazas dentro del área de imagenología del Hospital General Docente de Calderón.

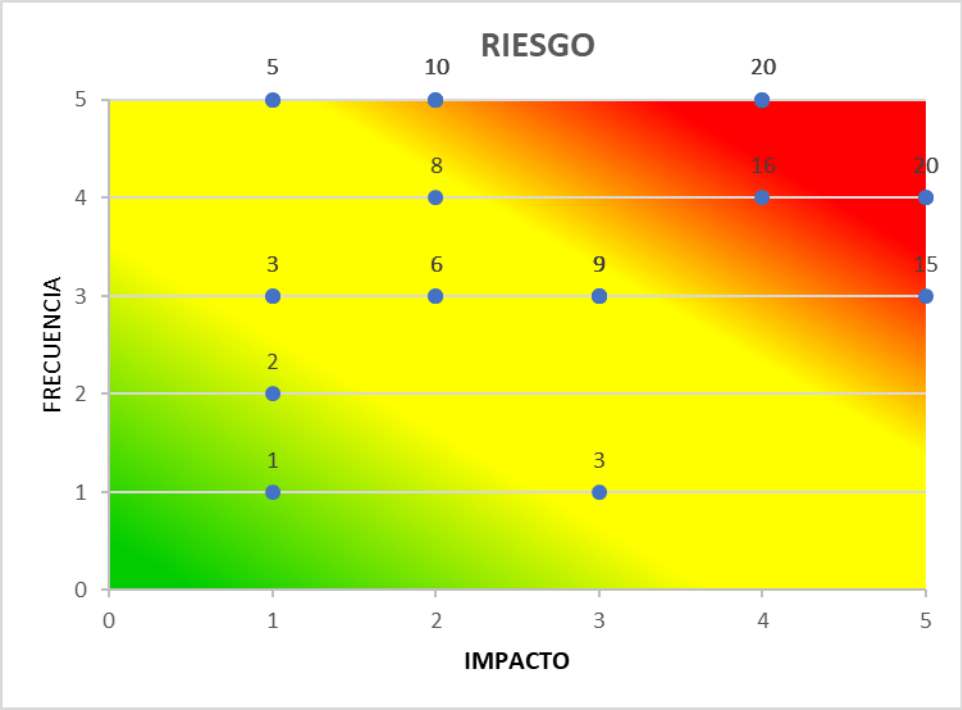


Gráfico 10 *Análisis de las amenazas en el HGDC*
Elaborado por: *investigador*

La investigación en su desarrollo ha permitido identificar que las amenazas establecidas por la norma ISO 27799, se las puede analizar de acuerdo con la incidencia del servicio en el área, análisis realizado y con incidencia a procesos y procedimientos con influencia en la determinación, control y tratamiento de enfermedades por el médico tratante. Situación que comprueba y afirma la importancia de ejecución del examen solicitado por el especialista al paciente y la entrega oportuna de los mismos.

Con esta perspectiva la materialización de una amenaza dentro del área de imagenología incrementa el riesgo como en el impacto o consecuencia en la detección, control o determinación del avance de la enfermedad que el paciente posee y el tiempo se acorta para fijar el tratamiento para su recuperación.

Para este análisis se aplicará la técnica de análisis de riesgo Análisis Modal de Fallos definida por Martinez (2018) que permite cuantificar los riesgos fundamentándose en conceptos como:

- La severidad del efecto del riesgo
- La probabilidad de ocurrencia
- La capacidad de su detección y prevención

Esta técnica pondera a las variables de severidad, ocurrencia y por detección en una escala de 1 a 10, siendo 1 el nivel más bajo y 10 el nivel más alto, al multiplicarlos obtenemos el valor de la prioridad del riesgo como mínimo 1 y máximo 1000, que nos servirá para priorizar las acciones a llevar a cabo.

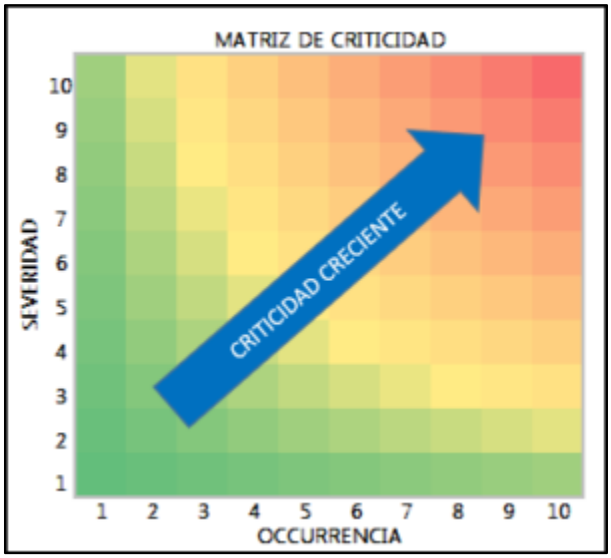


Gráfico 11 *Matriz de Criticidad*
Fuente: *Martinez (2018)*

Matriz de índice de prioridad:

Se tomará en cuenta el segundo criterio de la influencia con respecto a procesos y procedimientos médicos.

AMFE							
Elemento / Función	**Modo de Fallo**	**Efecto**	**S**	**O**	**D**	**NPR=S*O*D**	**Acciones Propuestas**
Uso de contraseñas ajenas	Enmascararse por los internos	Ingreso a otras cuentas o perfiles	6	4	4	96	Control de Acceso Físico al área de trabajo
Uso de contraseñas ajenas	Enmascararse por los proveedores de servicios	Ingreso a otras cuentas o perfiles	8	5	4	160	Cronograma de mantenimientos y control por personal interno
Uso de contraseñas ajenas	Enmascararse por extraños	Ingreso a otras cuentas o perfiles	8	5	4	160	Control de Acceso Físico al área de trabajo
Uso de información sin autorización	El uso no autorizado de una solicitud de información de salud	Alteración de la Información	9	3	7	189	Asignación de perfiles para control de
Instalación de *Software*	Introducción del *software* dañino o perjudicial	Daño de *software* y *hardware* existente	10	7	6	420	Perfiles de Usuario en Acceso al Equipo
Software	El mal uso de los recursos del sistema	Generación de información no médica o relacionada al trabajo	9	8	8	576	Cronograma de Revisión de contenido de los equipos
Ruptura de Seguridades	La infiltración de las comunicaciones	Manipulación de la Información	10	8	9	720	Monitorización de la Red de Datos
Ruptura de Seguridades	Interceptación de comunicaciones	Manipulación de la Información	10	8	9	720	Monitorización de la Red de Datos
Acciones del Personal	Repudio	Complicidad, fuga de información	10	8	10	800	Supervisión de Tareas
Equipos	Fallo en la conexión	Falla de la Tx de información entre equipos	10	10	9	900	Plan de Contingencia (Acciones alternativas para extracción de Información)
Infección de equipos	Incrustación de código malicioso	Perdida de información y funcionalidad de las aplicaciones médicas	10	9	8	720	Campañas de concientización de riesgos informáticos, Instalación de Antivirus, firewalle
Acciones de Personal Técnico	Fallo técnico del anfitrión, instalaciones de almacenamiento o infraestructura de red	Fallos en *hardware*, en red, en equipos de almacenamiento.	10	10	6	600	Plan de Contingencia
Condiciones de Infraestructura civil y el entorno	El fracaso de apoyo ambiental	Daños en los sistemas que soportan las aplicaciones médicas	10	9	10	900	Plan de Contingencia
Hardware y *Software*	Sistema o *software* de red falla	Perdida de información y funcionalidad de las aplicaciones médicas	10	9	9	810	Plan de Contingencia

AMFE							
Elemento / Función	**Modo de Fallo**	**Efecto**	**S**	**O**	**D**	**NPR=S*O*D**	**Acciones Propuestas**
Hardware y *Software*	Falla de *software* de aplicaciones	Perdida de información y funcionalidad de las aplicaciones médicas	9	9	9	270	Plan de Contingencia
Usuario	El error del operador	Develamiento de información médica no intencionadas por parte de TI	7	8	4	224	Informes de Actividades
Proveedores e Internos	Error de mantenimiento	Perdida de información y funcionalidad de las aplicaciones médicas	10	9	8	720	Manual de Procedimientos
Personal Médico	Error del usuario	Entrega de Información confidencial involuntariamente	10	9	9	810	Manual de manejo de información de acuerdo con el perfil de usuario
Contratación de Personal	Escasez de personal	Poca resolución de problemas y demora en la resolución de estos	10	9	4	360	Generalización de Manual de funciones con Autoridades
Personal Interno	Robo por los internos	Perdida divulgación de información,	10	8	4	320	Control de Uso y acceso a Equipos de monitoreo médico
Personas Externas	Robo por parte de personas ajenas	Perdida divulgación de información	10	9	8	720	Control de acceso al área física de imagenología
Personal Interno	Daño intencional por los internos	Perdida de información y funcionalidad de las aplicaciones médicas	10	5	5	250	Registro de accesos y actividades del personal
Personas Externas	Daño intencional por personas ajenas	Perdida de información y funcionalidad de las aplicaciones médicas	10	9	8	720	Control de acceso al área física de imagenología y áreas de equipos del hospital
Personas Externas	Terrorismo	Pérdida total de la infraestructura Informática y Civil del hospital	10	10	10	1000	Plan de Contingencia

Tabla 13 *Tabla de Riesgos con relación a procedimientos de salud*
Fuente: *Por investigador*

3.6.3. Tratamiento del riesgo

En la Tabla 10, en la columna de acciones propuestas, se establece las acciones a seguir por cada una de las amenazas en caso de que se materializarse.

3.6.4. Aceptación del riesgo

El concepto de aceptación del riesgo se basa en que ningún riesgo es totalmente eliminable, y es algo ambiguo que también es necesario para obtener la mejora continua en la administración de la información como de su seguridad. Con respecto a la seguridad de la información sanitaría no se podría establecer niveles de aceptación de riesgo, debido a la importancia que esta, luego de procesarla y generarla toma para la recuperación o identificación del tratamiento que el paciente debe seguir.

3.6.5. Comunicación del riesgo

Es una de las acciones primordiales y principales que se la establece como política de seguridad de la información, que es la comunicación de los riesgos al personal del área, ya que se convierten en el primer punto de origen de la inseguridad por acciones voluntarias como involuntarias.

3.6.6. Validación de la implementación de la política de gestión de la seguridad de la información

En el apartado 4.3.2 se analizan las amenazas que dicta la norma ISO 27799 para el campo de la salud, aplicándolas a las condiciones e información del área de imagenología del Hospital General Docente de Calderón.

El Análisis se lo realizó con 2 perspectivas: el impacto que genera la materialización de la amenaza en el área como servicio y el impacto que genera para los procesos y procedimientos médicos que el paciente es beneficiario.

Los análisis permiten confirmar la importancia de la implementación de una política de gestión de la Seguridad de la Información en el área de estudio, por la criticidad de la información y los riesgos que ocasiona de ser modificada o peor aún eliminada o extraviada.

Las metodologías de estudio de las amenazas, la estimación del riesgo entre las variables de la frecuencia y el impacto de materializarse y la determinación del índice de prioridad de fallo manejando las variables de severidad, probabilidad de incidencia y probabilidad de no detección, que establece una prioridad de acuerdo con su gravedad y así se establecerán los controles.

La última técnica de determinación del riesgo permite identificar si las circunstancias actuales del área permiten detectar la materialización de la amenaza o el inicio de ellas, la identificación de las deficiencias de no poseer herramientas de detección se convierte en los controles a implementar.

3.7. Diseño de la política de gestión de la seguridad de la información

La investigación se realiza dentro de un área del hospital por cuanto se limita a una política de esta para luego replicar el estudio acoplando a cada una de las áreas del hospital y poder obtener el documento de Sistema de Gestión de Seguridad de Información global. Se tomó las amenazas identificadas para el área de la salud de la norma ISO 27779, que se las definió como riesgos cuantificándolas mediante dos métodos de determinación del riesgo, esto permitió identificar las amenazas más incidentes en el área como para los procesos y procedimientos médicos y la recuperación del paciente.

La política de seguridad será el documento guía y a aplicarse dentro del área de imagenología para el uso y generación de la información desde los equipos médicos hasta las computadoras de áreas de trabajo en la redacción del informe del examen realizado. Este documento deberá ser generalizado y aceptado por cada integrante del área y personal nuevo, y de detectarse la materialización de una amenaza con a violación de la seguridad el desconocimiento de la política no eximirá de culpa.

La norma ISO 27779 a más de establecer las amenazas para el área de la salud posee 14 criterios para la seguridad de la información integral:

- Política de seguridad de la información.
- Política de seguridad de la organización.
- Seguridad de los recursos humanos
- Gestión de activos
- Control de Acceso
- Criptografía
- seguridad física y ambiental
- seguridad de operaciones
- seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas.
- Relación de proveedor
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información de la gestión de la continuidad del negocio.
- Cumplimiento

De generar cada documento se logrará poseer un sistema de seguridad de la información garantiza, lo importante de cada documento es que debe ser generalizado y comprendido por cada integrante del hospital.

CAPÍTULO IV

PROPUESTA

4.1. Objetivo

Generar un documento con la información necesaria para el personal médico y administrativo del área de imagenología del Hospital General Docente de Calderón, para el tratamiento de la información su seguridad como la integridad del *hardware* apoyado en normas y controles.

4.2. Alcance

El presente documento contiene la política y controles para garantizar la seguridad de la información del área de imagenología del Hospital General Docente de Calderón, desde su generación, transmisión y almacenamiento, luego de ser aprobada por la máxima autoridad, será de fiel cumplimiento por parte de usuarios internos y externos al área que manejen información médica y administrativa.

4.3. Controles para la seguridad de la información

El estándar posee 116 controles segmentados en 14 áreas o subtemas, de los cuales se presentarán los que el área necesita.

Los controles que se utilizan de la norma se los seleccionó, con la perspectiva de influencia directa a la información del área y sin que estos dependan de otros procesos u área que dejen inconcluso la aplicación de este, así como del análisis de riesgo realizado en las Tablas 9 y 10, tomadas en cuenta los análisis.

4.4. Política de seguridad de la información

Control 1. – Todos los controles de la política deberán estar en una constante actualización, el período de revisión será de seis meses o de existir una materialización de una de las amenazas, el control deberá ser corregido de tal manera que la política se ajuste a las variaciones de las vulnerabilidades.

4.4.1. Organización de la seguridad de la información

Control 2. – El personal de la alta gerencia del HGDC deberá inmiscuirse en el conocimiento de la política y gestionarla de tal forma que se cumpla dentro del área de imagenología.

Control 3. – La infraestructura tecnológica del hospital y en el área de imagenología estará disponible necesariamente para actividades correspondientes al desempeño de cada área, administrativa y médica en cumplimiento con el giro del negocio.

Control 4. – La dirección del área de imagenología deberá informarse de la política, con el objetivo de dar fiel cumplimiento e identificar las actualizaciones que se deben hacer.

Control 5. – El desarrollo de los proyectos del área deberán ser realizados con suma discreción y con conocimiento de la alta gerencia y personal del área de TICS, aplicando los procedimientos de seguridad de la información.

Control 6. – El uso de equipos móviles dentro del área estará restringido para la transmisión de imágenes y audio, de ser necesario su uso será utilizando la infraestructura del hospital, el control estará a cargo del departamento de TICS quien deberá generar un registro de ingreso y egreso de usuarios. El registro deberá ser aprobado por el líder del área de Imagenología justificando su necesidad.

4.4.2. Seguridad de recursos humanos

Control 7. – De acuerdo con los procesos administrativos el personal es contratado por el área de Talento Humano del HGDC, donde aplicarán sus procesos y procedimientos, con la coordinación previa de conocimiento de perfiles necesarios para la contratación de personal para el área de imagenología.

Control 8. – El Hospital en coordinación con el área de Recursos Humanos deberá solicitar al personal nuevo documentación relacionada a su identidad, domicilio actual, referencias de empleos anteriores, sobre todo a quienes manipularan información como dispositivos médicos.

Control 9. – El área de Talento Humano deberá implementar una política que permita informar al nuevo personal sobre la Política de Seguridad de la Información existente en el área de Imagenología siempre que esta trabajare ahí.

Control 10. – La información generada, procesada o almacenada en la infraestructura del hospital por el empleado es de propiedad exclusiva del Hospital General Docente de Calderón, la que no podrá ser revelada a personas externas de la institución.

Control 11. – El personal del área de Tecnologías de la Información con una debida planificación deberá generar campañas de capacitación sobre temas de seguridad de la información a todo el personal del área de Imagenología.

Control 12. – El área de Talento Humano en conjunto con personal del TIC deberá generar y entregar un manual de usuario, así como la respectiva inducción sobre las políticas y estándares de seguridad de la información, a todo personal nuevo del área de imagenología y el respectivo registro

Control 13. – Al detectar alteración de la información por un empleado dentro de las instalaciones del hospital en el área de imagenología será responsabilidad de este, el hospital se

deslinda de responsabilidad alguna en caso de generar procesos legales, por el propietario de la información (paciente).

Control 14. – Una vez que el presente documento sea entregado al empleado y tenga la inducción respectiva, es obligatorio cumplir con las disposiciones de este, de no hacerlo o generar un riesgo en la infraestructura o información sanitaria, deberá responder a procesos administrativos.

Control 15. – Si el área de imagenología o el empleado deciden dar por terminada la relación laboral, en conjunto con el área de recursos humanos debe notificar al área de TICS de la finalización de las actividades laborales para proceder con la eliminación del usuario y accesos al *hardware* como *software* del área.

4.4.3. Gestión de activos

Control 16. – El líder del área de Tecnología deberá designar a un responsable miembro de su equipo para realizar un control cada semestre de los activos de *hardware* como de *software* de las aplicaciones médicas dentro del área de imagenología del hospital, este deberá llevar un registro digital del control.

Control 17. – El líder del área de TICS del hospital deberá designar a un responsable miembro de su equipo para realizar un control de la integridad física de los equipos de almacenamiento pertenecientes el área de imagenología del HGDC, control que deberá presenta una bitácora con el estado de cada trimestre del equipo y aplicaciones.

Control 18. – De adquirir el área de imagenología un equipo médico nuevo, un representante del área de TICS, deberá ser capacitado y solicitar información, manuales de este antes y para su uso.

Control 19. – La clasificación de la información del área de imagenología del hospital estará netamente a criterio del área médica, se deberá establecer un formato único en el área, mismos que se deberá socializar y solicitar manejen las mismas variables en el *software* propietario

Control 20. – La infraestructura tecnológica al ser calificada como activo fijo del Hospital General Docente de Calderón, se debe asignar una ponderación de acuerdo con el grado de exposición o vulnerabilidad entre equipos médicos.

Control 21. – El uso de medios extraíbles en los equipos médico y estaciones de trabajo se permitirá el su uso previa autorización del líder del área de imagenología y tan solo como medio contingente de no existir la transmisión de datos.

4.4.4. Control de acceso

Control 22. – Todo personal del área de imagenología deberá ser identificado para generar el control de acceso físico como lógico, con la asignación de *tags* de acceso a las diferentes secciones del área, proceso que deberá ser realizado al ingreso de este.

Control 23. – La administración del control de acceso del personal del área de imagenología se coordinará entre las tres áreas TICS, Talento Humano y Líderes del Área de imagenología, información que deberá estar en constante actualización, llevando un registro de estos.

Control 24. – Todo usuario será responsable del uso de sus credenciales asignadas de acceso a *software* y *hardware*, si se detecta el uso mal intencionado de estos, se procederá con sanciones administrativas.

Control 25. –Toda estación de visualización o trabajo tendrá configurado los accesos a la raíz de aplicativos médicos, para garantizar su funcionalidad y garantías.

4.4.5. Criptografía

Control 26. – La transmisión de información médica del área se utilizará el protocolo de encriptación y transmisión DICOM, que es propio del *hardware* como del *software*.

Control 27. – Las credenciales asignadas o generadas por los usuarios para el ingreso a *software* y equipos médicos estarán bajo la supervisión de un responsable del área de TICS, mismas que deberán ser cambiadas cada 3 meses.

4.4.6. Seguridad física y ambiental

Control 28. – Garantizar la integridad física de los equipos como de los usuarios, al manejar información médica susceptible, con la delimitación del acceso a los equipos médicos, estaciones de visualización y de trabajo (equipos de oficina). **Anexo 2** (Aplicación de control)

Control 29. – Se deberá coordinar acciones con personal de seguridad para proteger las áreas destinadas para entrega y descarga de insumos para el área de imagenología, del ingreso de personas extrañas.

Control 30. – Estará a cargo la configuración de la fiabilidad de imagen de los monitores de las áreas de trabajo (computadores), del personal de TICS.

4.4.7. Seguridad de las operaciones

Control 31. – Se realizará monitorización por parte del personal del área de TICS a la manipulación de información digital e impresa, su transmisión, acciones de cambio y producción, para poder dimensionar el almacenamiento centralizado.

Control 32. – Se deberá proteger a los equipos de escritorio de código malicioso con la instalación de antivirus y sus actualizaciones, para lograr la detección y prevención de alteraciones o perdidas en el *software* como *hardware*.

Control 33. – Se deberá dimensionar uno o varios equipos para respaldo de información, con la necesidad de precautelar la integridad de esta y cumplimiento de normas nacionales. **Anexo 3 (**dimensionamiento de Storage para el área)

Control 34. – El líder del área de imagenología deberá asignar a un(a) profesional del área de imagenología que, al existir una novedad, reportarla al área de tics y generar una bitácora con el registro de la novedad y su solución.

Control 35. – Los equipos de escritorio y de uso médico deberán ser configurados de tal forma que no permitan instalar programas médicos o no médicos por los usuarios sin autorización o previa autorización.

Para la instalación de *software*, se deberá presentar la respectiva justificación al área de TICS, por la líder del área.

4.4.8. Seguridad de las comunicaciones

Control 36. – Personal del área de TICS realizará monitoreo del funcionamiento de los servicios de red (datos), así como de su seguridad, Guiados por los acuerdos de servicio establecidos por el área, como el uso de los servicios para uso netamente médico.

Control 37. – Se deberá verificar la estabilidad de los medios de comunicación o transmisión, con la implementación de políticas de seguridad de navegación web, bloqueando el acceso a páginas de: pornografía, redes sociales, de infringir lo dispuesto el usuario enfrentará acciones administrativas por violación de una política de seguridad.

Control 38. – Los usuarios del área de Imagenología del hospital con respecto a las descargas de archivos desde el internet deberán ser ligados con temas laborales y con mesura, los equipos con esta posibilidad serán las estaciones de trabajo (computadoras), se restringirá la posibilidad en las estaciones de visualización.

4.4.9. Adquisición, desarrollo y mantenimiento de sistemas de información

Control 39. – El área de imagenología administrará los contratos, donde se establecerá los mantenimientos y actualizaciones de los equipos y *software* médico. Tomando en cuenta de que el área de TICS deberá ser informada de las fechas de mantenimiento y deberá estar un representante presente.

4.5. INFORMÁTICA MEDICA

Al no ser desconocido que la transmisión de datos a través de cualquier tipo de infraestructura sea esta guiada o no, llega a cada proceso o procedimiento con la ayuda de los avances de la tecnología (electrónica), generando la automatización de estos, no es la excepción en el campo de sanitario (salud).

La tecnología en el área de la salud genera mejoras considerables en el estado del paciente, en los resultados médicos, y la calidad de vida. Es de conocimiento general y empírico que la tecnología está inmersa en el ciclo de vida del ser humano, desde que está en desarrollo hasta cuando necesita ser monitorizados sus signos vitales.

El mercado ofrece para el área de Imagenología una plataforma de administración de la información cumpliendo con los aspectos que establece la norma de estudio ISO 27799 en

cuanto a la seguridad de la información que involucra a la transmisión, almacenamiento, seguridad, y los tres criterios de la seguridad Integridad, Confidencialidad y la Disponibilidad.

4.5.1. SOFTWARE

Empresas grandes y pequeñas reconocidas en el campo de la salud, desarrollan un *software* de administración para el área de Imagenología denominado RIS/PACS.

El *software* se encuentra estructurado en dos partes:

- RIS: Sus siglas en ingles *Radiology Information System* (Sistema de Información de Radiología), es la parte del *software* que gestiona todos los datos, exámenes e imágenes desde el registro del turno hasta la entrega del informe al paciente como al médico especialista.
    - El *software* trabaja con los estándares HL7 y DICOM, que proveen de la seguridad en la transmisión de la información y la visualización respectivamente.
- PACSes un sistema de almacenamiento y distribución de imagen. Esta definición corresponde a la traducción literal de sus siglas Picture Archiving and Comunications System. Normalmente asociamos este sistema a Radiología, debido a que este servicio es el principal generador de imagen de un hospital y además el de mayor consumo. En un sentido más estricto lo podríamos considerar como un sistema de almacenamiento de imagen radiológica, normalmente recibida de las distintas modalidades. Entendemos por Modalidad, cada una de las técnicas usadas para la obtención de imagen: Tac, Resonancia, Ecografía. El protocolo específico que utilizan los sistemas PACS esel DICOM (*Digital Imaging Communication on Medicine*),aunque también se pueden usar otros protocolos específicos para capturar las imágenes (Bordils y Chavarría, 2004).

Al fusionarlos obtenemos el *software* de administración y la interacción es del RIS al PACS proporcionando la información sobre las citaciones (turnos), a consecuencia el PACS podrá crear un estudio si y solo si RIS posea los datos registrados del paciente, esta información es bidireccional.

Cada desarrollador incluye funciones extras para hacer del *software* más novedoso, como el acceso web a los informes e imágenes específicas, acceso total al estudio en la intranet.

El *Software* al incluir los estándares DICOM y HL7 garantizan que la transmisión de la información sea interna o externa será cifrada.

CAPITULO V

CONCLUSIONES

- La investigación permitirá establecer un antes y un después en la administración de la información dentro del Hospital Docente de Calderón, especialmente en el campo de la salud, garantizando la integridad, disponibilidad y confidencialidad de la información médica del paciente y la continuidad de su tratamiento, sin necesidad de incurrir en gastos adicionales.
- El área de la salud en el país se encuentra en crecimiento y dentro de un marco legal que no está muy definido, mismo que debe ser aplicado para garantizar la confidencialidad, integridad y disponibilidad de la información del paciente que se produce con los procedimientos médicos realizados durante el tratamiento.
- Al diseñar la política de Gestión de Seguridad de la Información para el área de imagenología del Hospital General Docente de Calderón e identificar los riesgos, analizarlos con las técnicas de valoración de riesgos, determinar los controles para mitigarlos, con los lineamientos que establece la norma ISO 27799 y la estructura de ISO 27001, se confirma de la implementación de controles para cada uno de los procesos informáticos existentes es necesaria.
- El desarrollo y el uso de las tecnologías de la Información en el área de la salud ha permitido que se creen varias herramientas tanto de *hardware* y *software* que cumplan con varios procesos administrativos como: el registro de un paciente, de sus signos vitales, etc. Que de fallar deja al médico imposibilitado para proceder con las acciones médicas, mientras la

estabilidad del individuo decae, por cuanto el paso a seguir es establecer un plan con medios y acciones de contingencia.

- Identificar las amenazas establecidas por la norma ISO 27799 dentro del área de imagenología del Hospital General Docente de Calderón, permite confirmar la importancia de generar un Sistema de Gestión de la Seguridad de la Información integrado.

RECOMENDACIONES

- Es recomendable que el documento de la política de gestión de seguridad de la información sea revisado y aprobado por la conformación del comité de seguridad de la información, mismo que estará constituido por la alta gerencia: Gerente, Asesor jurídico, adm. Financiero, adm. Estadística, Dirección asistencial, Gestión técnica y líder de imagenología.
- Se recomienda replicar la política en todas las áreas del hospital con las consideraciones necesarias para cada una y lograr establecer el Sistema de Gestión de Seguridad de la Información aplicando los controles de acuerdo con el área.
- Asignar el tiempo suficiente de implementación y pruebas de la presente política, debido a que representan varios cambios en la perspectiva laboral del personal interno y externo.
- Generar revisiones periódicas de la política con la finalidad de mejorarla y mantener actualizada a cambios realizados dentro del área como de normativa nacional e interna.
- Designar a una persona del área de TICS con conocimientos de seguridad para el seguimiento y definición de nuevas directrices, con la finalidad de no generar ambigüedades en la aplicación y control.
- La implementación de normas ISO de seguridad de la Información requiere del respaldo de la alta gerencia como de la necesidad de establecer un comité de Seguridad de la Información dentro del Hospital General Docente de Calderón, quienes se encargarán del

desarrollo e implementación del SGSI mismos que poseerán el privilegio de acceso a toda la información médica y administrativa.

- Las actividades del personal médico como administrativo están sujetos a la funcionalidad, estabilidad y desempeño de las Tecnologías de la información, por cuanto se recomienda establecer un plan de contingencia en cuanto estos llegaran a fallar.

BIBLIOFRAFÍA

27001, N. I.-I. I. (2015). NORMA TECNICA ECUATORIANA *Objeto y campo de Aplicación* (pp. 1).

ADIEMED, S. Ecógrafo 4D Sonoscape S2. Retrieved from http://www.adiemed.es/index.php?id_product=157&controller=product

AG, S., & Medical, S. (2006). *SOMATOM Definition* E. d. validated information (Ed.) Retrieved from www.siemens.com/medical

Asamblea Nacional República del Ecuador. (2014). *Código orgánico integral penal*.

Bertolín y Areitio. (2008). *Seguridad de la información. Redes, informática y sistemas de información*: Editorial Paraninfo.

Bordils y Chavarría. (2004). Almacenamiento y transmisión de imágenes. PACS,. Retrieved from http://webcache.googleusercontent.com/search?q=cache:http://www.conganat.org/seis/is/is45/is45_54.pdf

Borghello. (2017). Políticas de Seguridad. Retrieved from http://www.evaluandosoftware.com/politicas-de-seguridad/

BRITISH, S. (2008). Health informatics — Information security management in health using ISO /IEC 27002 (ISO 27799:2008).

DNTICS. (2012). Políticas Uso de Servicios de Red y Servicios Informáticos del Ministerio de Salud Pública. In MinisteriodeSaludPúblicadelEcuador (Ed.).

Eset. (2014). SEGURIDAD INFORMÁTICA PARA ENTIDADES DE SALUD. Retrieved from https://empresas.eset-la.com/novedad/soluciones-de-seguridad-para-entidades-de-salud

Estrada. (2017). Red de hospitales de Inglaterra afectada también por ataque informático. *FayerWayer*.

GE.Healthcare. (2011). Mobile X-ray Systems.

General-Electric-Company. (2015). *Optima XR220amx*

Sistema de rayos X.

Gutiérrez y Brenner. (2017). Ataques cibernéticos, la nueva amenaza de muerte en los hospitales del mundo. *Infobae.*

HGDC. (2017 - 2020). Hospital General Docente de Calderón,. Retrieved from https://www.hgdc.gob.ec/index.php/hospital/mision-y-vision

Hodge, James, Gostin, Lawrence, Gostin, & Jacobson. (1999). Legal Issues Concerning Electronic Health InformationPrivacy, Quality, and Liability. *JAMA, 282*(15), 1466-1471. doi:10.1001/jama.282.15.1466

Jara y Pacheco. (2012). Implementación de un sistema para la Gestion de la Seguridad. *Ethical Hacking 2.0,* 15.

KPI.HEALTHCARE.INC. (2019). Ecógrafo Philips Affiniti 50. 2019 KPI Healthcare - All Rights Reserved. Retrieved from https://www.equipo-ultrasonido.com/ecografo-philips-affiniti-50.html

López, Barreras, & Fernández. (2014). *Implementación de estándares DICOM SR y HL7 CDA para la creación y edición de informes de estudios imagenológicos* (Vol. 6).

Martinez. (2018). AMFE: ¿Ideas claras? Riesgo y criticidad. Retrieved from http://kailean.es/amfe-ideas-claras-riesgo-y-criticidad/

MSP. (2016). LEY DE DERECHOS Y AMPARO DEL PACIENTE

(Vol. Ley 77): Registro Oficial Suplemento 626 de 03-feb.-1995.

MVINF. (2015). Entienda la importancia de la seguridad de la información en la gestión hospitalaria. Retrieved from http://www.mv.com.br/es/blog/entienda-la-importancia-de-la-seguridad-de-la-informacion-en-la-gestion-hospitalaria

Oliveira W. (2017). Qué es el Gobierno de TI y cuál es su importancia para la toma de decisiones en las empresas. Retrieved from https://www.heflo.com/es/blog/gobernanza/gobierno-ti/

Philips, N. V. (2019). *Affiniti 50, Sistema de Ultrasonido* Retrieved from https://www.centralamerica.philips.com/healthcare/product/HC795208/philips-affiniti-50-ultrasound-system

Ramos, V. (2007). Las TIC en el sector de la salud., 41-45. 163. Retrieved from https://www.researchgate.net/publication/28168792

Registro Oficial. (2015). *REGLAMENTO DE INFORMACION CONFIDENCIAL EN SISTEMA NACIONAL DE SALUD*.

Sánchez, Fernández, Ambrosio, Hernández, & Geaa, C. d. (2013). *Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria* (elsevier Ed. Atención Primaria ed.).

Secretaría Nacional de Planificación y Desarrollo. (2017). Plan Nacional para el Buen Vivir 2017 2021.pdf,.

Siemens-Healthcare-Headquarters. (2016). Maximize Outcome. Minimize Dose.

SonoScape. (2014). *Ecógrafo* d. d. Medical (Ed.) Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&cad=rja&uact=8&ved=2ahUKEwj84efd7afgAhVHyYMKHXiPDH4QFjAIegQIChAC&url=http%3A%2F%2Fmeddevicedepot.com%2FPDFs%2FS2-Sonoscape-Datasheet.pdf&usg=AOvVaw0F5o_BCPrJfJUEAoGInZr7

Sunyaev, Kaletsch, Mauro, & Krcmar. (2010). *Open security issues in german healthcare telematics.* Proceedings of the 3rd International Conference on Health Informatics: INSTICC, 2010.

Thompson. (2019). Definición de información - Promonegocios.net. Retrieved from http://www.promonegocios.net/mercadotecnia/definicion-informacion.html

Vidal, Gonzalo, & Cazes. (2005). Seguridad, Información y Salud. *Revista Cuban de Informática Médica*. Retrieved from http://www.rcim.sld.cu/revista_7/articulo_htm/segurinfsalud.htm

ANEXOS

ANEXO 1.-

Tabla de Tiques de daños en el área de imagenología del Hospital se muestran una imagen de los datos debido a que el total de datos son 13 hojas.

Lugar = %Imagenología% AND Fecha de apertura > 2018-01-01 00:00 AND Fecha de apertura < 2019-01-01 00:00

ID	Título	Entidad	Fecha de apertura	Última modificación	Prioridad	Estado	Lugar	Solicitante - Solicitante	Asignado a - Técnico	Tiempo en resolver + Progreso
11 717	COMPUTADOR SE CUELGA NO RESPONDE (11717)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-12-12 08:17	2019-01-15 15:55	Baja	Cerrado	IMAGENOLOGÍA	PAULINA ELIZABETH VILLACIS ESCOBAR (933)	RAY RICARDO ROBINSON CASIERRA (1416)	
11 987	CONFIGURACIÓN DE LA IMPRESORA (11987)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-12-26 10:03	2018-12-26 10:59	Baja	Cerrado	IMAGENOLOGÍA	NUBE ROCIO GUAMAN CUNDURIN (395)	RAY RICARDO ROBINSON CASIERRA (1416)	
11 817	ACCESO A LA RED INALÁMBRICA HGDC (11817)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-12-17 08:08	2018-12-20 15:39	Baja	Cerrado	IMAGENOLOGÍA	LYLIAN ROCIO VILLAGOMEZ MAQUILON (1423)	CRISTIAN EDUARDO PUGA JACOME (1143)	
11 814	Re: falla de sistema singovia (11814)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-12-14 17:35	2018-12-17 13:19	Media	Cerrado	IMAGENOLOGÍA	NUBE ROCIO GUAMAN CUNDURIN (395)	CRISTIAN EDUARDO PUGA JACOME (1143)	
11 818	Acceso a Zimbra (11818)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-12-17 08:11	2018-12-17 08:12	Baja	Cerrado	IMAGENOLOGÍA	LYLIAN ROCIO VILLAGOMEZ MAQUILON (1423)	GEOMARA MARIBEL TAMBACO TIPANTIZA (1013)	2018-12-17 08:21
11 247	CPU MANTENIMEINTO (11247)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-11-22 10:18	2018-12-12 16:55	Media	Cerrado	IMAGENOLOGÍA	NUBE ROCIO GUAMAN CUNDURIN (395)	RAY RICARDO ROBINSON CASIERRA (1416)	
11 686	COMPUTADOR SE CUELGA (11686)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-12-11 09:16	2018-12-12 09:17	Baja	Cerrado	IMAGENOLOGÍA	PAULINA ELIZABETH VILLACIS ESCOBAR (933)	JURGEN GAVINO ZAMBRANO ZAMBRANO (973)	
11 727	Acceso a Zimbra (11727)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-12-12 08:54	2018-12-12 08:54	Baja	Cerrado	IMAGENOLOGÍA	LETICIA ESTHELA VACA CAÑIZARES (889)	GEOMARA MARIBEL TAMBACO TIPANTIZA (1013)	2018-12-12 09:04
11 152	Solicitud para colocación puerto de red (11152)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-11-19 13:18	2018-11-29 15:56	Media	Cerrado	IMAGENOLOGÍA	NUBE ROCIO GUAMAN CUNDURIN (395)	CRISTIAN EDUARDO PUGA JACOME (1143)	
11 293	Instalación de Office (11293)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-11-23 10:05	2018-11-27 11:48	Media	Cerrado	IMAGENOLOGÍA	NUBE ROCIO GUAMAN CUNDURIN (395)	RAY RICARDO ROBINSON CASIERRA (1416)	
11 280	Cambio de Ubicación de Computadora (11280)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-11-23 07:28	2018-11-26 11:24	Media	Cerrado	IMAGENOLOGÍA	NUBE ROCIO GUAMAN CUNDURIN (395)	CHRISTIAN SAMUEL ESPINOSA CARRILLO (129)	

GLPI PDF export - 2019-01-22 - 126 elementos - 1/13

Anexo 1 *Lista de Tiques del área de Imagenología*

Lugar = %imagenologia% AND Fecha de apertura > 2018-01-01 00:00 AND Fecha de apertura < 2019-01-01 00:00

ID	Titulo	Entidad	Fecha de apertura	Última modificación	Prioridad	Estado	Lugar	Solicitante - Solicitante	Asignado a - Técnico	Tiempo en resolver + Progreso
11 327	Cambio de Tóner (11327)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-11-26 10:15	2018-11-26 11:05	Media	Cerrado	IMAGENOLOGÍA	NUBE ROCIO GUAMAN CUNDURIN (395)	MAYRA GUISELLA DIAZ MORA (1016)	2018-11-26 11:15
10 961	Ausencia de Datos compartidos ventanilla de estadistica (10961)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-11-12 14:53	2018-11-22 11:41	Media	Cerrado	IMAGENOLOGÍA	NUBE ROCIO GUAMAN CUNDURIN (395)	RAY RICARDO ROBINSON CASIERRA (1416)	
11 162	Recuperar información PC (11162)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-11-20 12:00	2018-11-20 13:37	Media	Cerrado	IMAGENOLOGÍA	NUBE ROCIO GUAMAN CUNDURIN (395)	CHRISTIAN SAMUEL ESPINOSA CARRILLO (129)	
11 148	Tinta de Impresora de Sala de Interpretación (11148)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-11-19 12:41	2018-11-19 13:43	Media	Cerrado	IMAGENOLOGÍA	NUBE ROCIO GUAMAN CUNDURIN (395)	CHRISTIAN SAMUEL ESPINOSA CARRILLO (129)	2018-11-19 13:41
10 305	COMPUTADOR NO ENCIENDE (10305)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-10-18 09:43	2018-11-19 13:21	Media	Cerrado	IMAGENOLOGÍA	MARIA AUGUSTA AYALA ESTRELLA (97)	CHRISTIAN SAMUEL ESPINOSA CARRILLO (129)	
11 083	Cambio de CPU (11083)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-11-16 08:10	2018-11-16 08:39	Media	Cerrado	IMAGENOLOGÍA	NUBE ROCIO GUAMAN CUNDURIN (395)	PAOLA ELIZABETH CANDO CAMISAN (173)	
10 352	Fwd: TOMOGRAFO (10352)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-10-19 12:45	2018-11-15 08:38	Media	Cerrado	IMAGENOLOGÍA	NUBE ROCIO GUAMAN CUNDURIN (395)	CRISTIAN EDUARDO PUGA JACOME (1143)	
10 319	SOPORTE URGENTE TOMOGRAFO HGDC - OCTUBRE 2018 (10319)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-10-18 13:36	2018-11-15 08:37	Media	Cerrado	IMAGENOLOGÍA	DAVID ESTEBAN TAMAYO GUTIERREZ (1477)	CRISTIAN EDUARDO PUGA JACOME (1143)	
11 026	SIN ACCESO A INTERNET (11026)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-11-14 13:25	2018-11-14 15:15	Media	Cerrado	IMAGENOLOGÍA	PAULINA ELIZABETH VILLACIS ESCOBAR (933)	JURGEN GAVINO ZAMBRANO ZAMBRANO (973)	
10 913	FIRMA ELECTRÓNICA (10913)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-11-09 15:48	2018-11-14 12:46	Media	Cerrado	IMAGENOLOGÍA	NUBE ROCIO GUAMAN CUNDURIN (395)	JURGEN GAVINO ZAMBRANO ZAMBRANO (973)	

GLPI PDF export - 2019-01-22 - 126 elementos - 2/13

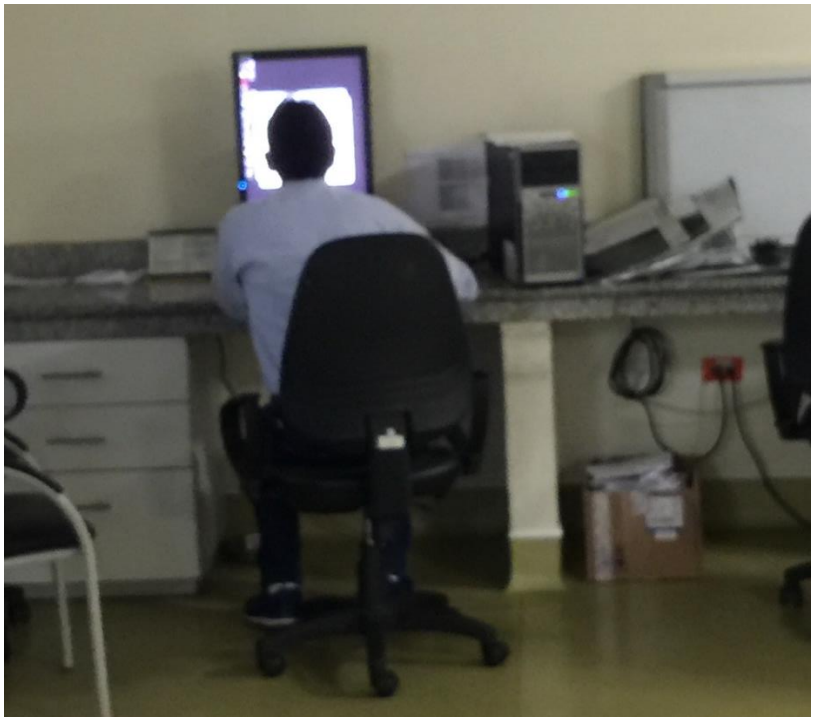
Lugar = %imagenologia% AND Fecha de apertura > 2018-01-01 00:00 AND Fecha de apertura < 2019-01-01 00:00

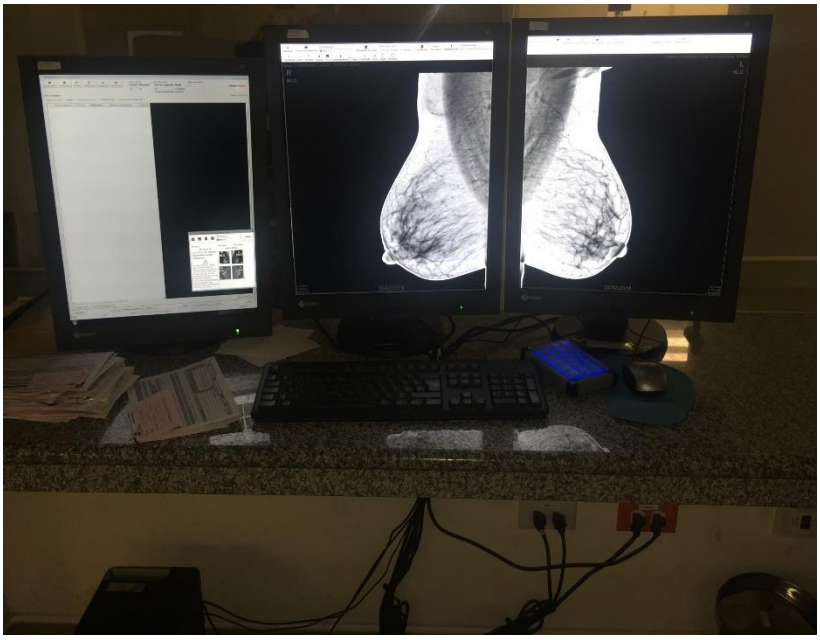
ID	Titulo	Entidad	Fecha de apertura	Última modificación	Prioridad	Estado	Lugar	Solicitante - Solicitante	Asignado a - Técnico	Tiempo en resolver + Progreso
3 625	INSTALACAION DELPROGRAMA DEIMAGENES (3625)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-01-15 09:59	2018-01-15 12:04	Media	Cerrado	IMAGENOLOGÍA	SOFIA ALEJANDRA LLORE QUEZADA (479)	MAYRA GUISELLA DIAZ MORA (1016)	
3 411	CAMBIO DE SISTEMA OPERATIVO EN COMPUTADORAS DEL SERVICIO DE IMAGEN (3411)	HOSPITAL GENERAL DOCENTE DE CALDERON	2018-01-04 14:17	2018-01-08 10:59	Media	Cerrado	IMAGENOLOGÍA	BYRON DAVID FAREZ BUENAÑO (317)	JURGEN GAVINO ZAMBRANO ZAMBRANO (973)	

Se visualizan las fechas desde el 4 de enero hasta el 12 de diciembre del año pasado

ANEXO 2. –

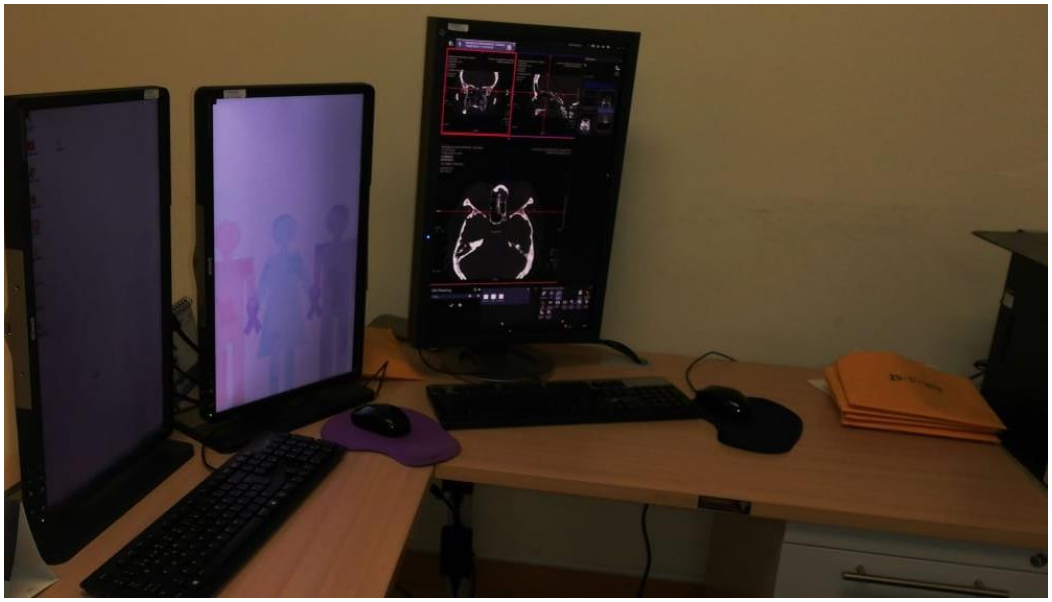
Antes de la implementación de controles, estación de visualización de mamógrafo y tomógrafo.





Aplicando el control 28

Preparando el área para las estaciones de monitoreo de mamógrafo y ecógrafo



Anexo 2 *Aplicación de control 28 Protección física*

ANEXO 3. –

Dimensionamiento de Storage

	TAMAÑO DE IMAGEN	# DE IMAGEN * EXAMEN	1 EXAMEN COMPLETO	1 EXA. COMPLETO
Rayos X	91.66 KB	2	183.32 KB	0.179 MB
Tomografías	514 KB	500	257000 KB	250.977 MB
Ecografías	3.16 KB	5	15.80 KB	0.015 MB
Mamografías	14.39 KB	4	57.56 KB	0.056 MB

# EXA. * DIA	TAMAÑO DE EXA. COMPLETO * DIA	EXA. COMPLETO * MES	EXA. COMPLETO * MES
91	16682.12 KB	500464 KB	488.73 MB
40	10280000 KB	308400000 KB	301171.88 MB
100	1580 KB	47400 KB	46.29 MB
15	863.4 KB	25902 KB	25.29 MB

EXA. COMPLETO * AÑO
5864.81 MB
3614062.50 MB
555.47 MB
303.54 MB

3620786.32	MB
3535.92	GB
3.45	TB

Anexo 3 *Calculo de Storage para el área de Imagenología*

Para la producción necesitamos 3.45 TB al año, descuerdo a la normativa la información se almacena 7 años por lo tanto se necesita un Storage de 25 TB.