DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD APLICADA A LA OFICINA DE SISTEMAS DE INFORMACION DEL HOSPITAL REGIONAL DEL LIBANO ESE BASADO EN EL MODELO DE SEGURIDAD PARA LAS ENTIDADES DEL ESTADO APLICANDO LAS GUÍAS DEL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

ROBINSON VARGAS RIVERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANACIA “UNAD”

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

LIBANO – TOLIMA

2018

DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD APLICADA A LA OFICINA DE SISTEMAS DE INFORMACION DEL HOSPITAL REGIONAL DEL LIBANO ESE BASADO EN EL MODELO DE SEGURIDAD PARA LAS ENTIDADES DEL ESTADO APLICANDO LAS GUÍAS DEL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

ROBINSON VARGAS RIVERA

Trabajo de grado para optar el título de:

Especialista en Seguridad Informática

Director de proyecto:

Luis Fernando Zambrano

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANACIA “UNAD”

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

LIBANO – TOLIMA

2018

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Líbano, 15 de Octubre de 2018 Jurado

DEDICATORIA

Este trabajo está dedicado a mi Madre por el apoyo condicional que he tenido, a mis hermanas y hermano que son el motor para lograr mis metas. Al Hospital Regional del Líbano ESE que me brindó su apoyo para crecer profesionalmente

AGRADECIMIENTOS

Al Hospital Regional del Líbano ESE, desde la Dirección del Doctor Manual Alfonso González Cantor por la confianza encomendada en el mejoramiento de los procesos y protección de la información, a la Universidad Nacional Abierta y A Distancia por la formación impartida, y ante todo a mi Familia y a DIOS que me motiva cada día más para cumplir mis sueños y ser cada día Mejor.

CONTENIDO

Pág.

(Continuacion) Pág.

(Continuacion) Pág.

LISTA DE TABLAS

Pág.

LISTA DE GRAFICAS

Pág.

LISTA DE ANEXOS

Pág.

1. GLOSARIO

El Glosario utilizado en el Proyecto aplicado “DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD APLICADA A LA OFICINA DE SISTEMAS DE INFORMACION DEL HOSPITAL REGIONAL DEL LIBANO ESE BASADO EN EL MODELO DE SEGURIDAD PARA LAS ENTIDADES DEL ESTADO APLICANDO LAS GUÍAS DEL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES” fue tomado del Link: *http://www.iso27000.es/glosario.html,* para tener una alineación en los conceptos utilizados por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia en su programa FORTALECIMIENTO DE LA GESTION TI EN EL ESTADO (Link: *https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html*)

ACTIVO INFORMÁTICO: Se define como todo aquello pueda generar valor para la empresa u organización y que éstas sientan la necesidad de proteger. Un activo o recurso informático está representado por los objetos físicos (hardware, como los *routers*, *switches*, *hubs*, *firewalls*, antenas, computadoras), objetos abstractos (software, sistemas de información, bases de datos, sistemas operativos) e incluso el personal de trabajo y las oficinas.

AMENAZA: Es el potencial que un intruso o evento explote una vulnerabilidad específica. Es cualquier probabilidad que pueda ocasionar un resultado indeseable para la organización o para un activo en específico. Son acciones que puedan causar daño, destrucción, alteración, pérdida o relevancia de activos que podrían impedir su acceso o prevenir su mantenimiento.

ATAQUE: Es cualquier intento no autorizado de acceso, uso, alteración, exposición, robo, indisposición o destrucción de un activo.

CONTROL DE SEGURIDAD: Es un conjunto de normas, técnicas, acciones y procedimientos que interrelacionados e interactuando entre sí con los sistemas y subsistemas organizacionales y administrativos, permite evaluar, comparar y corregir aquellas actividades que se desarrollan en las organizaciones, garantizando la ejecución de los objetivos y el logro de las metas institucionales.

EVENTO: Es una situación que es posible pero no certera; es siempre un evento futuro y tiene influencia directa o indirecta sobre el resultado. Un evento se trata como un suceso negativo y representa algo indeseado.

IMPACTO: Es la cantidad de daño que puede causar una amenaza que explote una vulnerabilidad.

POLÍTICA DE SEGURIDAD: Es un documento que define el alcance de la necesidad de la seguridad para la organización y discute los activos que necesitan protección y el grado para el cual deberían ser las soluciones de seguridad con el fin de proveer la protección necesaria

RIESGO INFORMÁTICO: Es la probabilidad de que una amenaza en particular expone a una vulnerabilidad que podría afectar a la organización. Es la posibilidad de que algo pueda dañar, destruir o revelar datos u otros recursos.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: Es un marco de administración general a través del cual las organizaciones identifican, analizan y direccionan sus riesgos en la seguridad de la información. Su correcta implementación garantiza que los acuerdos de seguridad están afinados para mantenerse al ritmo constante con las amenazas de seguridad, vulnerabilidades e impactos en el negocio, el cual es un aspecto a considerar profundamente teniendo en cuenta la competitividad y cambios a los que enfrentan las organizaciones hoy en día.

VULNERABILIDAD: Es una falla o debilidad en los procedimientos, diseño, implementación o controles internos en un sistema de seguridad. Es cualquier ocurrencia potencial que pueda causar un resultado indeseado para una organización o para un activo en específico.

AUTENTICIDAD: La legitimidad y credibilidad de una persona, servicio o elemento debe ser comprobable.

CONFIDENCIALIDAD: Datos solo pueden ser legibles y modificados por personas autorizados, tanto en el acceso a datos almacenados como también durante la transferencia de ellos.

DISPONIBILIDAD: Acceso a los datos debe ser garantizado en el momento necesario. Hay que evitar fallas del sistema y proveer el acceso adecuado a los datos.

GESTIÓN DE RIESGO: Método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. Está compuesta por cuatro fases: 1) Análisis, 2) Clasificación, 3) Reducción y 4) Control de Riesgo.

INTEGRIDAD: Datos son completos, non-modificados y todos los cambios son reproducibles (se conoce el autor y el momento del cambio).

SEGURIDAD INFORMÁTICA: Procesos, actividades, mecanismos que consideran las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

SISTEMA DE INFORMACIÓN: Es un conjunto de elementos orientaos al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (Objetivo). Dichos elementos formarán parte de alguna de categorías. Sus elementos son Personas, Datos, Actividades o técnicas de trabajo, Recursos materiales en general (típicamente recursos informáticos y de comunicación, aunque no tienen por qué ser de este tipo obligatoriamente). Todos estos elementos interactúan entre sí para procesar datos (incluyendo procesos manuales y automáticos) dando lugar a información más elaborada y distribuyéndola de la manera más adecuada posible en una determinada organización en función de sus objetivos.

2. RESUMEN

El Hospital Regional del Líbano ESE, como entidad del estado ve que La información debe fluir entre las oficinas y dependencias sin ningún obstáculo para el desarrollo de las actividades misionales, y evitar toda situación de estancamiento, ya que es la forma más adecuada de sacar el mayor provecho a la información que se obtiene. La información tiene un carácter instrumental y sirve de soporte en todos los ámbitos y decisiones de la empresa. Esta no puede ser considerada como un mero soporte o apoyo de las actividades de la empresa, sino como uno de sus principales recursos o activos.

Es así como la información es un recurso estratégico en la empresa, es decir que la información es vital, hoy el verdadero objetivo de las tecnologías de la información debe ser el aprovechamiento estratégico de la información.

Debemos tener en cuenta además que la información nos permite aprender, asimilar y crear tecnología, la cual los nutren los flujos de información básicos por lo tanto se requiere la información que entra a la Empresa procedente de su entorno (Externa), la información que fluye en la empresa (Interna) y por último la información que la empresa proyecta hacia el exterior (Información Corporativa).

El Sistema de Salud Colombiano se ha caracterizado por no contar con sistemas de información adecuados que permitan obtener datos actualizados de forma rápida y sencilla sobre el estado de salud de la población, a pesar del marco legal existente, el sistema de información de la salud en el país no ha logrado desarrollar de la forma espera y ha permanecido segmentado y con problemas de calidad.

Esta situación hace que sea de especial importancia llevar a cabo una evaluación y diagnóstico, no solo de las características de los sistemas de información de la salud, sino también en la organización, el funcionamiento de estos y los problemas que impiden un correcto funcionamiento.

El Ministerio de TIC ha venido liderando la implementación de programas de desarrollo de tecnologías de la información dentro de las Entidades del Estado. El Plan Nacional de TIC tiene como meta: “en el 2019 todos los Colombianos estarán conectados e informados, haciendo un uso eficiente y productivo de las TIC”.

El desarrollo del sistema de información de la salud está soportado no sólo por la definición de roles en las leyes pertinentes, sino también por un plan nacional de fomento de la utilización de tecnologías de la información. A pesar de la presencia de un marco legal, el Estado no ha tenido la fortaleza institucional para garantizar el cumplimiento de lo contenido en las normas. La reglamentación, implementación y seguimiento es responsabilidad de los entes rectores del sistema, quienes deben tener los recursos y alcance suficiente para hacer entrar la normatividad en vigor.

3. INTRODUCCIÓN

El Hospital regional del Líbano ESE, en su proceso de cumplimientos legales, gestión de la calidad, gestión documental y estrategias como gobierno en línea y gobierno transparente, solo por nombrar algunas, las Empresa Social del Estado se deben cumplir con el objetivo de ser más eficientes y sistemáticos al dar solución a las necesidades de los Usuarios Externos e Interno y partes interesadas, para ello se debe implementar un sistema efectivo en la Seguridad de la Información y activos informáticos, que involucre a todo el personal de la institución, en el Sistema llamado Gestión de la seguridad de la Información basado en las Guías suministradas por el Ministerio de Tecnologías de la Información y las Comunicaciones que establece las guías, procedimientos y procesos para gestionar la información y los activos de información apropiadamente mediante un proceso de mejoramiento continuo.

La oficina de Sistemas de Información del Hospital Regional del Líbano E.S.E, Soporta y Gestiona toda la Infraestructura tecnológica, que ayuda en la toma de decisiones en la institución y fomenta en mejoramientos de los procesos con la implementación y aplicación de soluciones tecnológicas, por tal motivo se hace necesario el inventario de los activos de información digitales y de las tecnologías de la información y las comunicaciones que la soportan, con su respectiva gestión del Riesgo a los que están expuestos los activos informáticos y empleando un enfoque de mejoramiento continuo que permita mitigar o mantener el nivel de aceptabilidad para continuar con las actividades misionales de la entidad.

El presente Proyecto tiene como finalidad, inventariar y gestionar los activos de información digitales y las tecnologías de la información y las comunicaciones de la oficina de sistemas de información del Hospital Regional Del Libano

E.S.E. basado en el modelo de seguridad para las entidades del estado, aplicando las guías del Ministerio De Tecnologías De La Información Y Las Comunicaciones y la selección de una metodología de evaluación de riesgos informáticos, el establecimiento de una política de seguridad informática institucional que sea liderada por gerencia y fortalecida por cada proceso de la institución, además de generar la documentación respectiva para los Planes de Continuidad de Negocio con el fin de mantener y/o restaurar las actividades misionales y el análisis y selección de un modelo de que se ajuste a las necesidades del hospital.

4. PLANTEAMIENTO DEL PROBLEMA

4.1 PROBLEMA GENERAL

El Hospital Regional del Líbano E.S.E., no cuenta con un sistema de gestión de la seguridad de la Información donde se tenga una gestión y clasificación de activos de información que maneja la entidad, un inventario de activos de información donde se pueda determinar que activos posee la entidad, la Clasificación de la información y los Niveles de Clasificación de la Información, para que de esa manera identificar los responsables y administrar los controles efectivos de la seguridad de los activos de información de los procesos misionales del Hospital, alineados a un modelo de Seguridad y Privacidad de la Información acordes a normatividad y estrategias del Gobierno colombiano como Gobierno en línea y las guías de adopción del Ministerio de Tecnologías de la Información y las Comunicaciones para temas de Seguridad y Privacidad de la Información.

4.2 DESCRIPCION DEL PROBLEMA

Desaprovechamiento de las guías de Seguridad y Privacidad de la Información suministradas por el Ministerio de Tecnologías de la Información y las Comunicaciones, para el diseño de un sistema de Inventario General de los Activos de Información del Hospital Regional del Líbano Tolima.

Los activos de Información del Hospital Regional del Líbano ESE ,que soporta los procesos y actividades de la entidad, no se encuentran inventariados y de esa manera no están clasificado, ni gestionados con el fin de protegerlos frente a riesgos de acuerdo a su nivel de clasificación, el propietario y el custodio de

la misma. Por ello se debe realizar un Inventario de Activos de Información Físico y Electrónico de acuerdo a las guías de Seguridad y Privacidad de la Información Suministradas por el Ministerio de Tecnologías de la Información y las Comunicaciones

4.3 FORMULACION DEL PROBLEMA

¿Es necesario un sistema de Seguridad en la Información y activos de información en las entidades de Salud, que proteja la información y los activos de información, los cuales pueden ser importantes para soportar las actividades misionales y en la toma de decisiones administrativas por parte de la alta gerencia? Debido a la falta de un inventario general de los activos de información en el Hospital Regional del Líbano E.S.E. no se ha clasificado que tipo de activo poseen y quien es el responsable de este, para luego poder salvaguardar la información, de igual forma poder valorizar el activo para la entidad y medir los riesgos de no controlarlos, además con el incumplimiento de la normatividad de las guías de Seguridad y Privacidad Suministrada por el Ministerio de Tecnologías de la Información y las Comunicaciones se genera el incumplimiento de la estrategia de Gobierno Digital.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad aplicada a la oficina de sistemas de información del HOSPITAL REGIONAL DEL LIBANO ESE basado en el modelo de seguridad para las entidades del estado aplicando las guías del Ministerio de Tecnologías de la Información y las Comunicaciones

5.2 OBJETIVOS ESPECIFICOS

Realizar el diseño de inventario de activos de información, digitales y las tecnologías de la información y las comunicaciones, gestionar los datos y la información priorizándolos en función de las necesidades, requerimientos y expectativas de información de los clientes, para asegurar la estandarización de la misma durante su captura, el análisis, la transformación, la difusión con seguridad según los niveles de acceso y almacenamiento, con el fin de integrar y estructurar la coherencia de la información de tal manera que se pueda monitorear su tendencia y trazabilidad.

Aplicar el Modelo de Seguridad para las entidades del Estado aplicando las guías del Ministerio de Tecnologías de la Información y las Comunicaciones con la valoración de los activos de información.

Realizar el Mapa de Gestión del Riesgo de los activos de Información, Digitales y las tecnologías de la información y las comunicaciones del Hospital Regional del Líbano ESE.

Implementar los controles de la ISO 27001 de 2013 para mitigar el grado de incertidumbre de los RIESGOS.

6. JUSTIFICACION

El Hospital Regional del Líbano Tolima ESE, reconoce la información como un bien público que genera una cultura de la información y como herramienta fundamental en la toma de decisiones, lo cual ayuda a visualizar el panorama de las necesidades de los usuarios, los requerimientos legales, normativos y reglamentarios, es por ello que el diseño de un inventario de activos de información al interior del área de sistemas de información, colaborara en la implementación de las guías que define el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC en el Hospital Regional del Líbano ESE y d esta manera Diseñar el Sistema de Gestión de Seguridad en la Información.

Debido a la problemática de gestión, seguridad y privacidad de la información en el HOSPITAL REGIONAL DEL LIBANO ESE, se debe diseñar un sistema de gestión de seguridad, que resguarde y proteja los activos de información de la Entidad y que garantice la continuidad de las actividades en la empresa.

Como entidad del Estado el Hospital Regional del Líbano E.S.E., debe soportar cada uno de los procesos que desarrolla en fundamento de su objetivo funcional, por tal razón cada proceso que se implemente debe estar salvaguardado con el propósito de mitigar el riesgo de la perdida de información y hardware, debido a los problemas en la materialización del riesgo que se puedan presentar, es por tal razón que se realizará un diseño de inventario y se documentará los activos de información, que en la cual se implementará la metodología que provee el Ministerio de Tecnologías de la Información y las Comunicaciones para dar soporte en la continuidad a las actividades de la empresa alineada a las metodologías para la evaluación e implementación de los Controles.

7. ALCANCE Y DELIMITACIONES

El Diseño del SGSI se en marca en la Norma de Seguridad de Sistemas de Información ISO/IEC 27001 y las Guías que define el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI y la legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, Como entidad pública del estado debe propender por el mejoramiento continuo y tomas acciones preventivas que conduzcan a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos.

En el área de Sistemas de Información del Hospital Regional del Líbano E.S.E., cuenta con varios activos de información que no tienen su respectiva gestión del riesgo y por ende su respectiva clasificación según la información y servicio prestado al interior de la entidad, es por ello que se define varias fases para tener documentados, gestionado y verificado los activos de información del área de sistemas.

Por tal motivo con la implementación de un inventario de activos de información, se identifica las vulnerabilidades y una gestión del riego adecuada, mejorando la confidencialidad, integridad, disponibilidad con el fin de minimizar los riesgos de pérdida de información y hardware, todo esto en base al Modelo de Seguridad para las entidades del Estado aplicando las guías del Ministerio de Tecnologías de la Información y las Comunicaciones.

Al final, el área de sistemas de Información del Hospital regional del Libano ESE, tendrá un inventario de activos de información con su respectiva gestión

del riesgo y el continuo mejoramiento de acuerdo a la metodología PHVA y la actualización de tecnologías y procedimientos que esta área soporta al interior del Hospital brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

8. METODOLOGÍA

El Hospital Regional del Líbano ESE, en el área de Sistemas de información se acobija a la metodología aplicada en las Guías que define el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI y la legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, Como entidad pública del estado para la realización del Inventario de Activos de Información y la Gestión adecuada del Riesgo se alineara con la metodología del Departamento Administrativo de la Función Pública - DAFP para una correcta valorización del activo e identificación de las vulnerabilidades y de esta manera realizar los controles preventivos y correspondientes a cada activo identificado.

Para el Diseño y Recolección del inventario de la Información, frente a los activos de información que soporta los procesos administrativos y misionales del Hospital Regional del Líbano ESE, se aplicaran las Guías de Seguridad y Privacidad de la Información que en conjunto contribuyen al Modelo de Seguridad y Privacidad de la Información del Ministerio de las Tecnologías y las Comunicaciones.

Inicialmente se aplicara la Guía 5 – Guía para la Gestión y Clasificación de Activos de Información, con el diseños de un formulario realizado en Hoja de Cálculo, el cual ayudara en la recopilación de la información por cada área funcional y en la cual tenga procesos misionales y administrativos de la entidad que soporten los procesos del Hospital.

Una vez realizado el Inventario de activos de información del Hospital Regional del Líbano ESE, se aplicara la Guía 7 – Guía de Gestión de Riesgos y la ***GUIA***

PARA LA ADMINISTRACION DEL RIESGO del DEPARTAMENTO DE LA FUNCION PUBLICA – DAFP, para resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros eventos, el cual significa un respaldo de las actividades del Hospital alineados a metodologías de Gestión del Riesgo del Departamento de la Función Pública y Modelo Estándar de Control Interno y normas Internacionales como la ISO/IEC 27001.

De acuerdo a la información recopilada, consolidad, jerarquizada y analizada según su Nivel de Clasificación e importancia, se procede aplicar la Guía 8 – Controles de Seguridad y Privacidad de la Información, para seleccionar los controles para protegerla de amenazas y garantizar la continuidad de los sistemas de información.

9. MARCO REFERENCIAL

Las normas ISO surgen para armonizar la gran cantidad de normas sobre gestión de calidad y seguridad que estaban apareciendo en distintos países y organizaciones del mundo. Los organismos de normalización de cada país producen normas que resultan del consenso entre representantes del estado y de la industria. De la misma manera las normas ISO surgen del consenso entre representantes de los distintos países integrados a la I.S.O.

Uno de los [1]"***activos más valiosos que hoy en día posee las diferentes empresas, es la información y parece ser que cada vez más sufre grandes amenazas en cuanto a su confiabilidad"*** y su resguardo, de igual forma la información es vital para el éxito y sobrevivencia de las empresas en cualquier mercado. Con todo esto todo parece indicar que uno de los principales objetivos de toda organización es el aseguramiento de dicha información, así como también de los sistemas que la procesan.

Para que exista una adecuada gestión de la seguridad de la información dentro de las organizaciones, es necesario implantar un sistema que aborde esta tarea de una forma metódica y lógica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización. Para lograr estos objetivos, existen organizaciones o entes especializados en redactar estándares necesarios y especiales para el resguardo y seguridad de la información, los estándares correspondientes se encuentran en la norma ISO 27000.

La ISO 27000 es una serie de estándares desarrollados, por ISO e IEC. Este estándar ha sido preparado para proporcionar y promover un modelo para

[1] La importancia de la Información, tomado de: http://docslide.net/documents/auditoria-iso-27000.html

establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de Información. La adopción de este estándar diseño e implementación debe ser tomada en cuenta como una decisión estratégica para la organización; se pretende que el SGSI se extienda con el tiempo en relación a las necesidades de la organización. La aplicación de cualquier estándar ISO 27000 necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

El objetivo de desarrollar un sistema de gestión de seguridad de la información para la organización es disminuir el número de amenazas que, aprovechando cualquier vulnerabilidad existente, pueden someter a activos de información a diversas formas de fraude, sabotaje o vandalismo. Las amenazas que pueden considerarse de mayor relevancia en la institución son los virus informáticos, la violación de la privacidad de los empleados, los empleados deshonestos, intercepción de transmisión de datos o comunicaciones y/o fallas técnicas de manera voluntaria o involuntariamente.

La importancia de realizar el análisis referente a la gestión de Recursos Humanos, radica en conocer el manejo de la información correspondiente a esta área y su flujo dentro de la empresa. De esta manera, se establece que personas conocen o manejan que información y se establecen los procedimientos a seguir para resguardar dicha información. Al implementar estos procedimientos se deben realizar controles u observaciones de su funcionamiento dentro del área dispuesta, los cuales permitirán desarrollar cambios en los mismos.

El Hospital Regional del Líbano ESE requiere implementar un sistema de gestión de seguridad de la información con respecto a los activos de información enfocada en la gestión del riesgo, minimización de amenazas y detección de vulnerabilidades

9.1 ANTECEDENTES

En el Hospital Regional del Líbano ESE, no ha tenido ningún estudio o aplicación de un Sistema de Gestión direccionado a la Seguridad Informática, por ende la razón de este proyecto.

10. MARCO TEORICO

Sistema de Gestión de la Seguridad de la Información - SGSI, El Ministerio de Tecnologías de la Información y Comunicaciones provee un ***Modelo de Seguridad y Privacidad de la Información***[2] que permite establecer, implementar, monitorear, revisar, mantener y mejorar la protección de los activos informáticos para lograr los objetivos organizacionales basados en una gestión del riesgo y en los niveles aceptables de riesgos diseñados efectivamente para tratarlos y gestionarlos, analizando los requerimientos para la protección de los activos informáticos y aplicando los controles apropiados para asegurar que la protección de éstos activos contribuyen a la implementación exitosa del mismo, incluyendo para la organización las políticas, la planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

Como Política de Gestión, El HOSPITAL REGIONAL DEL LIBANO ESE implementa la Gestión y análisis del Riesgo de acuerdo a la metodología e instrucciones del DEPARTAMENTO DE LA FUNCION PUBLICA – DAFP con su ***GUIA PARA LA ADMINISTRACION DEL RIESGO***[3] , la cual ayuda al

[2] Modelo de Seguridad y Privacidad de la Información, Tomado de: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

[3] Guía para la Administración del Riesgo, descargada de: http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

conocimiento y mejoramiento de la entidad, contribuye a elevar la productividad y a garantizar la eficiencia y la eficacia en los procesos organizacionales, permitiendo definir estrategias de mejoramiento continuo, brindándole un manejo sistémico a la entidad.

Para realizar mejora continua y seguimiento al Sistema de Gestión de la Seguridad de la Información – SGSI en armonía con el Sistema Obligatorio de Garantía de la Calidad – SOGC, se utiliza el ciclo PDCA[4] (PHVA, Planear, Hacer, Verificar, Actuar), donde esta metodología ha demostrado su aplicabilidad y ha permitido establecer la mejora continua en la entidad. Este modelo consta de varias fases que permiten medir el estado actual del sistema con el fin de realizar un mejoramiento continuo:

Planear (Plan): En esta fase se diseña o planea el SGSI, definiendo las políticas de seguridad generales que aplicarán a la organización, los objetivos que se pretenden y cómo ayudarán a lograr los objetivos misionales. Se realiza el inventario de activos y la selección de la metodología de riesgos a implementar que estén acordes a los objetivos y políticas propuestos.

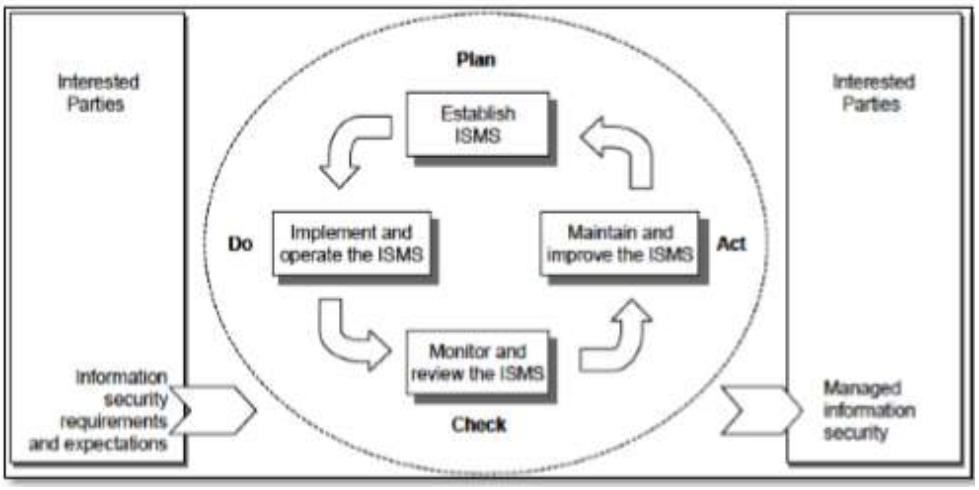
Hacer (Do): Es la fase donde se implementa el SGSI mediante la aplicación de los controles de seguridad escogidos, se asignan los responsables y se ejecutan los procedimientos.

Verificar (Check): Es la fase de monitorización del SGSI donde se verifica y audita que los controles, políticas, procedimientos de seguridad se están aplicando de la manera esperada.

[4] Ciclo PHVA, Tomado de: https://www.isotools.com.co/la-norma-iso-9001-2015-se-basa-ciclo-phva/

Actuar (Act): Esta fase implementa las acciones correctivas y mejoras del SGSI.

Figura 1. Modelo PHVA en los procesos de un SGSI.



Fuente: *ISO/IEC. International Standard ISO/IEC 27000: Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary. Geneva: ISO Copyright Office. 2014.*

10.1. MARCO CONCEPTUAL

10.1.1. RIESGOS INFORMÁTICOS

Riesgos Informáticos. El **riesgo informático** se define como "la probabilidad de que una amenaza en particular expone a una vulnerabilidad que podría afectar a la organización", o como "la posibilidad de que algo pueda dañar, destruir o revelar datos u otros recursos". El riesgo va inherente a una serie de términos que se deben comprender para poder tener una mejor concepción de su significado en el contexto de la seguridad de la información; entre ellos se encuentran:

- **Evento**: Es una situación que es posible pero no certera. En el contexto de la evaluación de riesgos es siempre un evento futuro y tiene influencia directa o indirecta sobre el resultado. Un evento (nuevamente en este contexto) se trata como un suceso negativo y representa algo indeseado.

- **Activo**: Representa el objetivo directo o indirecto de un evento. El resultado siempre tiene una consecuencia directa el cual es aplicado al activo. Un activo es algo valioso para una organización y en el contexto de seguridad informática están constituidos por el software, el hardware, las aplicaciones, las bases de datos, las redes, copias de seguridad e incluso las personas.

- **Resultado**: Es el impacto del evento. En el contexto de la seguridad informática siempre será una circunstancia no deseada como una pérdida o pérdida potencial. Esta pérdida siempre tiene un efecto directo en una mayor parte del activo.

- **Gestión del Riesgo:** Aplicación sistemática de políticas, procedimientos y prácticas de gestión para analizar, valorar y evaluar los riesgos.

- **Políticas de la Seguridad de la Información:** Es la confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información; su integridad, asegurando que la información y sus métodos de proceso son exactos y completos; su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran. La seguridad de la información se consigue implantando un conjunto adecuado de controles, tales como políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles han sido establecidos para asegurar que se cumplen los objetivos específicos de seguridad de la empresa.

- **Estándar ISO/IEC 27001:2013:** Es un estándar para la seguridad de la información, aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como Planificar, Hacer, Verificar, Actuar.

- **Planes de Continuidad del Negocio:** Es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcialmente o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

- **Gobierno de Tecnología Informática:** consiste en una estructura de relaciones y procesos destinados a dirigir y controlar la empresa, con la finalidad de alcanzar sus objetivos y añadir valor mientras se equilibran los riesgos y el retorno sobre TI y sus procesos.

11. MARCO LEGAL

CONSTITUCIÓN POLÍTICA DE COLOMBIA
Derechos: Artículo 2, 20, 74
El secreto profesional es inviolable: Artículo 79, 103, 123, 270
Deberes: Artículo 23, 209

Ley 100 de 1993: Por la cual se crea el Sistema Integral de Seguridad Social Integral y se dictan otras disposiciones.

Ley 594 de 2000: Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.

Ley 134 de 1994: Por la cual se dictan normas sobre mecanismos de Participación Ciudadana.

Ley 190 de 1995: Establece que las quejas y reclamos se resolverán o contestarán siguiendo los principios, términos y procedimientos dispuestos en el Código Contencioso Administrativo para el ejercicio del derecho de petición, según se trate de interés particular o general. (Estatuto Anticorrupción)

Ley 962 de 2005: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de las Particulares que Ejercen Funciones Públicas o Prestan Servicios Públicos.

Ley 1474 de 2011: Estatuto Anticorrupción. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Ley 1450 de 2011: Plan Nacional de Desarrollo. "Mejorar la oportunidad, accesibilidad y eficacia de los servicios que provee la Administración Pública al Ciudadano.

Ley 1680 de 2013: Por la cual se garantiza a las personas ciegas y con baja visión, acceso a la información, a las comunicaciones, al conocimiento y a las tecnologías de la información y de las comunicaciones.

Decreto 1011 de 2006: Por el cual se establece el Sistema Obligatorio de Garantía de Calidad de la Atención de Salud del Sistema General de Seguridad Social en Salud.

Decreto 2232 de 1995: Reglamenta la Ley 190 de 1995 en materia de bienes y rentas e informe de actividad económica así como el Sistema de Quejas y Reclamos.

Decreto 210 de 2003: Recibir y atender oportunamente las quejas y reclamos que se presenten en relación con la institución

Decreto 1151 de 2008: Establece los lineamientos generales de la Estrategia Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005 y se dictan otras disposiciones.

Decreto 2623 de 2009: Por el cual se crea Creó el Sistema Nacional de Servicio al Ciudadano.

Decreto 4485 de 2009: Adopta la actualización de la Norma Técnica de Calidad de la Gestión Pública.

Decreto 26 93 de 2012: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia.

Decreto 1510 de 2013: Por el cual se reglamenta el sistema de Compras y Contratación Pública.

Decreto único reglamentario 1078 de 2015: se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

Decreto 1080 de 2015: Por medio del cual se expide el Decreto Único del Sector Cultura

Resolución 1446: Por el cual se define el Sistema de Información para la Calidad y se adoptan los indicadores de monitoria del Sistema Obligatorio de Garantía de Calidad de la Atención en Salud.

Resolución 2433 de 2003: Adopta el Manual de Procedimientos del sistema de Quejas y Reclamos.

Resolución 2507 de 2006: Por la cual se definen los mecanismos de publicidad en el Portal Único de Contratación en desarrollo de lo dispuesto en el Decreto 2434 de 2006.

Resolución 1926 de 2005: Reglamenta la tramitación interna a que deben someterse las actuaciones administrativas relacionadas con el ejercicio del Derecho de Petición, ésta debe aplicarse al trámite de quejas y reclamos de la entidad.

Resolución 108 de 2006: De la tramitación interna a que deben someterse las actuaciones administrativas relacionadas con el ejercicio del Derecho de Petición.

Resolución 1495 de 2006: Adopta la Política de Información y Comunicación y el Procedimiento.

Resolución 195 de 2009: Crea el Comité de Gobierno en Línea.

CONPES 3649 de 2010. Establece la Política Nacional de Servicio al Ciudadano. Objetivo Central: contribuir a la generación de confianza y al mejoramiento de los niveles de satisfacción de la ciudadanía respecto de los servicios prestados por la Administración Pública en su orden nacional.

CONPES 3650 de 2010. La Estrategia Gobierno en Línea tiene por objeto contribuir, mediante el aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC), a la construcción de un Estado más eficiente, más transparente, más participativo y que preste mejores servicios a los ciudadanos y las empresas, lo cual redunda en un sector productivo más competitivo, una administración pública moderna y una comunidad más informada y con mejores instrumentos para la participación.

CONPES 3654 de 2010. Política de rendición de cuentas de la Rama Ejecutiva a los ciudadanos.

CONPES 3701 de 2011. Lineamientos de Política para la Ciberseguridad y Ciberdefensa.

CONPES 3785 DE 2013. Política Nacional de eficiencia administrativa al servicio del ciudadano y concepto favorable a la Nación para contratar un Empréstito Externo con la Banca Multilateral hasta por la suma de USB 20 millones destinado a financiar el proyecto de eficiencia al servicio del ciudadano.

NTCGP100:2009: Norma Técnica de Calidad en la Gestión Pública.

MECI 1000: 2005: Modelo Estándar de Control Interno.

Norma ISO 9001:2008: Requisitos para un Sistema de Gestión de Calidad.

Norma ISO 14001: 2004: Sistema de Gestión Ambiental, requisitos para su uso.

Norma ISO 26000:2010: Guía de Responsabilidad Social

Norma ISO 27001:2013: Seguridad de la Información

Norma ISO 25000:2005: Requisitos y Evaluación de Calidad de Productos de Software

Manual para la implementación de la estrategia de Gobierno en Línea de la República de Colombia 2008.

Fortalecimiento de la Gestión TI en el Estado – Modelo de Seguridad, Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC

12. MARCO CONTEXTUAL

12.1. NUESTRA HISTORIA

En 1964 se inicia la construcción del Hospital Regional del Líbano, en terreno cedido por el municipio del Líbano, en 1975 se inaugura la obra siendo presidente el doctor Alfonso López Michelsen. En 1977 se expiden los primeros estatutos de funcionamiento.

En su primera etapa de actividad asistencial, se consolida como el más grande prestador de servicios de salud del norte del Tolima y demuestra su capacidad operativa directa en los municipios de su área de influencia, siendo inclusive un importante protagonista en la resolución de la tragedia de Armero sucedido el 13 de noviembre de 1985.

En 1991 por Ordenanza 013 de la Asamblea Departamental fue creado como establecimiento público del orden departamental con autonomía y patrimonio independiente adscrito a la Secretaría de Salud del Departamento, asignándole el Segundo Nivel de Atención.

En 1994 mediante Ordenanza 085, la Honorable Asamblea del Tolima transforma al Hospital Regional del Líbano en Empresa Social del Estado, adoptándose y desarrollándose un proceso de planeación estratégica.

En 1998 el Hospital Regional del Líbano realizó un autodiagnóstico detectándose que no había seguimiento y definición de indicadores, por lo que

se determinaron metas apoyándose en los planes operativos de cada área e iniciando un modelo de Planeación estratégica para la institución.

En 2000 y 2001 fue postulado al premio de calidad del Centro de Gestión Hospitalaria, constituyéndose esto en un alto nivel de exigencia, obteniendo durante los dos años un reconocimiento especial y una moción de felicitación por sus avances en calidad, pese a la crisis de la I.P.S. Públicas y fundamentalmente de las de segundo nivel de atención.

Debido a los embates del Sistema de Salud y a la necesidad de transformación profunda, aunado a la mayor crisis financiera de su historia, el Hospital Regional debió Reestructurarse y modernizar su planta de personal en el año 2003. Sin embargo, a pesar de ese esfuerzo, el año 2004 se ahonda la crisis al no haber desarrollado eficientemente esta estrategia de cambio hacia empresa auto sostenible.

Desde el año 2005 y hasta la fecha, el hospital inicia su verdadera transformación entendiendo que la administración es responsabilidad de todos los trabajadores de la empresa, empoderando al cliente interno y aplicando la planeación estratégica hacia el cumplimiento de objetivos comunes.

Aprovechando su historia, se reactivó el mercadeo de servicios, aprovechando como la imagen institucional, el posicionamiento en el mercado y el conocimiento de la E.S.E por parte de la población del área de influencia, enfocando la oferta de servicios hacia la atención materno infantil, con la estructuración de estrategias encaminadas a incrementar el nivel de complejidad y la capacidad resolutiva suscribiendo el contrato de asociación con la IPS MEINTEGRAL que inicio la operación en el año 2006 con servicios de unidad de cuidados intensivos neonatales, pediátricos y en el año 2009 de apertura a la UCI adultos.

En el trienio junio de 2005 al 2008 se mejoran y se ofrecen nuevos servicios en el portafolio, con la adquisición de nuevos equipos y actualización de la tecnología del Laboratorio, del área de sistemas, fisioterapia, quirófano, urgencias y hospitalización, donde mención especial merece la inauguración de una Sala de Atención Materna Especial o cuidados intermedios maternos así como la renovación del parque automotor con la adquisición de dos nuevas ambulancias con tecnología de punta.

En el año 2013 el hospital regional del Líbano rediseño su plataforma estratégica enmarcada en un modelo de atención preferencial al binomio madre hijo mediante la adopción de las estrategia de la atención primaria en salud con la reinauguración de los centros y puestos de salud de los corregimientos de convenio san Fernando, santa teresa y tierra adentro que fueron entregados en comodato por la administración municipal por 5 años.

Actualmente podemos resaltar nuestras fortalezas en todos los ámbitos; contamos con una Infraestructura nueva y moderna en los servicios de Urgencias, Central de Facturación, Farmacia, Atención al Usuario, Fisioterapia, Promoción y Prevención, Unidad Intermedia; realidad que nos permite brindar servicios en términos de calidad y seguridad en los procesos de atención a nuestros usuarios y sus familias, cumpliendo con nuestro objetivo principal como es lograr la satisfacción de necesidades y expectativas de nuestra población usuaria.

Se ha reactivado la difusión del Portafolio de Servicios, con nuevas estrategias de mercadeo, haciendo uso de nuestras fortalezas en Infraestructura, avances tecnológicos, adquisición de nuevos equipos biomédicos, así como la actualización de equipos industriales de apoyo.

Nuestro reto se enfoca al cumplimiento del rol asignado al hospital regional del Líbano en el modelo Red de prestación de servicios de salud de la red pública del departamento del Tolima, como institución de referencia para la atención en mediana complejidad y sub especialización en ginecología, obstetricia y pediatría para el norte del departamento del Tolima; para lo cual en el marco de la crisis financiera del sistema de salud colombiano con la adopción del plan de saneamiento fiscal y financiero se garantizara el cumplimiento de esta responsabilidad.

12.2. LOCALIZACION DE LA EMPRESA

El Hospital Regional del Líbano es una Empresa Social del Estado que pertenece al Segundo nivel de atención de mediana complejidad que atiende la población del Municipio del Líbano (42.000 habitantes) tiene como referencia la población del Norte del Departamento y debido a su capacidad resolutiva actualmente atiende todos los municipios del Tolima e incluso pacientes de otros Departamentos. Su naturaleza jurídica es pública; cuenta en la actualidad con una oferta habilitada hospitalaria de 45 camas en hospitalización y 13 más en el servicio de urgencias, para un total de 58 camas. Cuenta con una sede única ubicada en la Calle 4 Número 2– 111 Avenida fundadores, en una planta física de seis pisos y terraza, con una construcción de 11.000 metros cuadrados. En la actualidad se han realizado intervenciones de remodelación en el servicio de Urgencias, Imagenología y Facturación. Las áreas en las cuales se han realizado intervenciones cuentan con unas especificaciones que están orientadas a satisfacer las necesidades de nuestros clientes en cuanto a: seguridad, confort, amenidades y tecnología de última generación en cuanto a redes hidráulicas, sanitarias, neumáticas, de gases y de comunicaciones en sistemas de información, las cuales fueron cambiadas y actualizadas para ser compatibles con las ultimas normas y especificaciones técnicas necesarias. El código de identificación inscrito en el Registro Especial Nacional de Prestadores de Servicios de Salud es

734110068701. Nuestro Correo Electrónico gerenciahrl2012@gmail.com. Nuestra Página Web hospitallibano.gov.co. Líneas Telefónicas: 2564496-2564537-2564755

12.3. PORTAFOLIO DE SERVICIOS

TABLA N° 1: PORTAFOLIO DE SERVICIOS- HOSPITAL REGIONAL DEL LIBANO

Tabla N° 1 (Continuación)

PROCESO	DESCRIPCION	CAPACIDAD INSTALADA	UBICACIÓN
URGENCIAS	Consulta las 24 horas, todos los días del año, se prestan los siguientes servicios: Consulta Médica General, Consulta Especializada, Observación y Procedimientos.	Área Triage, Sala de Observación con 12 camillas adulto y 4 pediátricas, Sala de yesos, Sala de Curaciones, Sala de reanimación, Salas IRA, Salas EDA, Sala de pequeños procedimientos, oficina con los servicios de Facturación, de Referencia y Contrareferencia	**1 PISO**
TRASLADO ASISTENCIAL DE PACIENTE	Disponibilidad 24 horas del día de traslado asistencial básico y traslado asistencial medicalizado.	2 ambulancias equipadas para el traslado asistencial básico. Y ambulancias completamente equipadas para el traslado asistencial medicalizado: tota 4 ambulancias	

Tabla N° 1 (Continuación)

PROCESO	DESCRIPCION	CAPACIDAD INSTALADA	UBICACIÓN
PROTECCION ESPECIFICA Y DETECCION TEMPRANA	ACTIVIDADES, PROCEDIMIENTOS E INTERVENCIONES DE PROTECCION ESPECÍFICA EN: • Vacunación según esquema de programa ampliado de inmunizaciones (PAI). • Salud oral. • Control prenatal y atención del recién nacido. • Planificación familiar. ACTIVIDADES, PROCEDIMIENTOS E INTERVENCIONES PARA DETECCION TEMPRANA DE: • Control de crecimiento y desarrollo. • Consulta de planificación familiar. • Consulta prenatal para determinar alteraciones del embarazo. • Atención del joven. (De 10 a29 años). • Atención al adulto. (Mayores de 45 años). • Medición de la agudeza visual. • Tamización de Cáncer de cuello uterino. • Tamización de Cáncer de seno. • Higiene Oral.	(edificio adyacente frente a Urgencias) Coordinación PE y DT, consultorios de Control prenatal, control de enfermedades crónicas, crecimiento y desarrollo, atención al joven y planificación familiar, sala de Vacunación, cava de vacunas, sala de salud oral, consultorio rosado y Sala AIEPI, dos unidades de odontología para la realización de actividades de salud oral.	

Tabla N° 1 (Continuación)

PROCESO	DESCRIPCION	CAPACIDAD INSTALADA	UBICACIÓN
ACTIVIDADES EXTRAMURALES	Contamos con un equipo multidisciplinario que recorre los barrios, visita los colegios del municipio en el área rural al igual que en el área urbana. • Servicios de Apoyo Ambulatorio. • Consulta Médica General, cuanta con 9 consultorios de medicina general. • Vacunación. • Sala AIEPI. • Odontología. • Programa Crónicos: Diabetes e Hipertensión arterial	4 unidades odontológicas portátiles. Equipo de atención extramural.	
ATENCION MEDICA AMBULATORIA	***Consulta Médica General*** ***Consulta Médica Especializada*** • *Cirugía* • *Ginecología y Obstetricia* • *Ortopedia y Traumatología* • *Anestesiología* • *Pediatría* • *Medicina Interna* • *Urología* • *Radiología* • *Oftalmología*	4 consultorios de medicina general y 5 consultorios de medicina especializada, estación de enfermería.	

Tabla N° 1 (Continuación)

PROCESO	DESCRIPCION	CAPACIDAD INSTALADA	UBICACIÓN
PSICOLOGIA	Consulta de psicología	consultorio de psicología	
TRABAJO SOCIAL	consulta de trabajo social	consultorio de trabajo social	
OPTOMETRIA	Consulta de Optometría	consultorio de Optometría	
FISIOTERAPIA	SERVICIOS DE: • Fisioterapia • Terapia Respiratoria • Espirómetro Simple	sala del Terapia Física y salada Terapia Respiratoria completamente equipadas, Espirómetro y nebulizadores	
IMÁGENES DIAGNOTICAS	Rayos X. Urografía. Ecografía. Ecografía de detalle 3D y 4D. Tomografía y urotac Mamografía.	2 salas de RX, 1 sala de tomografo,1 sala de ecografía ,1 mamógrafo, 2 Rx portátiles. Telemedicina, digitalizador de imágenes diagnósticas.	

Tabla N° 1 (Continuación)

PROCESO	DESCRIPCION	CAPACIDAD INSTALADA	UBICACIÓN
LABORATORIO CLINICO	Servicio 24 horas: laboratorios de primer nivel laboratorios especializados. Química sanguínea, uro-coproanalisis, microbiología, hematología, laboratorio especializado. Unidad transfusional	Área remodelada con las condiciones y equipos requeridos para garantizar las fases pre-analítica, analítica y post-analítica.	
ODONTOLOGIA	Servicio de consulta externa y pyp, en horario hábil, realización de todos los procedimientos de odontología general: operatoria, endodoncia, periodoncia, exodoncia	4 unidades completamente dotadas para la prestación del servicio.	
QUIRURGICAS	BLOQUE QUIRURGICO • Cirugía • Ginecología y Obstetricia • Ortopedia y Traumatología • Anestesiología • Urología • Oftalmología	Cuenta con dos salas de cirugía, sala de Recuperación, sala de atención de parto y legrados, 1 Sala de Pequeños Procedimientos y 1 salas de procedimiento incruentos.	**2 PISO**
ESTERILIZACION	Proceso de esterilización	2 autoclaves 1 esterilizador Sterrad	

Tabla N° 1 (Continuación)

PROCESO	DESCRIPCION	CAPACIDAD INSTALADA	UBICACIÓN
INTERNACION	Unidad de cuidado especial materno	1 habitación de 4 camas dotada con tecnología de punta que permite la monitorización de gestantes de alto riesgo obstétrico	
	SEGUNDO PISO SUR	2 Habitación de 4 camas (8 camas) destinadas a parto y postparto, 3 habitaciones de 4 camas (12 camas), 3 habitaciones unipersonales (3 camas) y 1 habitación de 3 camas (3 camas) para hospitalización gineco-obstétrica Total de camas: 26 camas totalmente equipadas con insumos y muebles de hotelería y Bombas de Infusión, Monitores fetales, Oxímetros de pulso, Monitores Multiparamétricos requeridos par ala atención integral del binomio madre -hijo.	
	CUARTO PISO NORTE	12 habitaciones bipersonales (24 camas) y 2 habitaciones unipersonales (2 camas) para hospitalización adulto, Total camas:26 camas totalmente equipadas con insumos	**4 PISO**

Tabla N° 1 (Continuación)

PROCESO	DESCRIPCION	CAPACIDAD INSTALADA	UBICACIÓN
		y muebles de hotelería y Bombas de Infusión,, Oxímetros de pulso, Monitores Multiparamétricos requeridos para la atención integral del binomio madre -hijo.	
	QUINTO PISO SUR	4 habitaciones bipérsonales (8 camas) Total camas:26 camas totalmente equipadas con insumos y muebles de hotelería y Bombas de Infusión,, Oxímetros de pulso, Monitores Multiparamétricos requeridos para la atención integral del binomio madre -hijo.	**5 PISO**
BLOQUE ADMINISTRATIVO	bloque administrativo	oficinas, muebles y enseres requeridos para la gestión administrativa de la empresa	**3 PISO**
SERVICIO FARMACEUTICO	Servicio 24 horas: suministro de medicamentos hospitalarios y ambulatorios.	Áreas de recepción, almacenamiento, dispensación y bodega.	**SOTANO**

Tabla N° 1 (Continuación)

PROCESO	DESCRIPCION	CAPACIDAD INSTALADA	UBICACIÓN
SERVICIOS DE HOTELERIA	Alimentación y cafetería. Lavandería. Vigilancia. Mantenimiento. Almacén. Morgue. Servicios generales. Planta de gases medicinales. Concentrador de oxígeno. Concentrador de aire plata eléctrica. Procesos admistrativos	Insumos, muebles e inmuebles requeridos para garantizar condiciones óptimas de hostelería.	

Fuente: Portafolio De Servicios- Hospital Regional Del Líbano

12.4. DESCRIPCIÓN DEL TALENTO HUMANO

Talento humano suficiente del orden asistencial y administrativo que garantizan la plena operación de su portafolio de servicios, en el cual se destacan los servicios del modelo de atención primaria con la presencia de recurso humano técnico y profesional capacitados en cada uno de los puestos y centros de salud extramural, llevando actividades de promoción en salud y prevención de la enfermedad.

Igualmente se destaca la oferta permanente de especialidades no quirúrgicas como son las de medicina interna y pediatría que junto con las especialidades quirúrgicas permanentes: anestesia, cirugía general, ortopedia,

ginecobstetricia, y las especialidades programadas de oftalmología y urología, suplen gran parte de la demanda de la atención en salud de la población usuaria.

En la tabla N° 2 se discrimina el personal que el HRL tiene contratado en la actualidad para el desarrollo de su labor asistencial.

TABLA No: 2 Recurso Humano Asistencial- Hospital Regional Líbano

Tabla N° 2 (Continuación)

CARGOS	**AREA FUNCIONAL**	**TOTAL**
ANESTESIOLOGO	CONSULTA E. - CIRUGIA	2
AUXILIAR DE CONSULT.ODONT	ODONTOLOGIA	1
AUXILIAR DE ENFERMERIA	TODOS LOS SERVICIOS	97
AUXILIAR DE ENFERMERIA	CENTROS Y PUESTOS DE SALUD	3
BACTERIOLOGA	LABORATORIO	5
BACTERIOLOGA 4 HORAS	LABORATORIO	2
BATERIOLOGO S.S.O	LABORATORIO	1
CIRUJANO	CIRUGIA Y C.E	2
COORDINADOR DE CALIDAD	COORD. CALIDAD	1
ECOGRAFISTA	TODOS LOS SERVICIOS	1
ENFEREMERO S.S.O	URGENCIAS	1
ENFERMERO	ATENCION PRIMARIA	8
FISIOTERAPEUTA	TERAPIAS	3
GINECOLOGO	CONSULTA EXTERNA HOSPITALIZACION URGENCIAS	2
HIGIENISTA ORAL	CONSULTA EXTERNA	2
INSTRUMENTADOR	CIRUGIA	2
MEDICO GENERAL	TODOS LOS SERVICIOS	12
MEDICO S.S.O	TODOS LOS SERVICIOS	7
ODONTOLOGO	ODONTOLOGIA	5
ODONTOLOGO S.S.O	ODONTOLOGIA	1
OFTALMOLOGO	C.E Y CIRUGIA	1

Tabla N° 2 (Continuación)

CARGOS	AREA FUNCIONAL	TOTAL
OPTOMETRA	CONSULTA EXTERNA	1
ORTOPEDISTA	CONSULTA EXTERNA HOSPITALIZACION URGENCIAS	2
PATOLOGO	CONSULTA EXTERNA	1
PEDIATRA	CONSULTA EXTERNA HOSPITALIZACION URGENCIAS	1
PROFESIONAL ESP. AREA SALUD	COORDINACION MEDICA	1
PSICOLOGA	CONSULTA EXTERNA	1
RADIOLOGO	CONSULTA EXTERNA	1
REGENTE DE FARMACIA	FARMACIA INTERNA Y EXTERNA	2
TECNOLOGO DE RX	RAYO X	3
TRABAJADORA SOCIAL	ATENCION AL USUARIO	1
UROLOGO	CONSULTA E. - CIRUGIA	1
TOTAL		**174**

Fuente: Oficina de Talento Humano – Hospital Regional del Líbano E.S.E

Prestando apoyo directo a los servicios asistenciales se cuenta con personal administrativo de oficina, mantenimiento, servicios generales, facturación, lavandería auditoria, cocina, vigilancia, atención al usuario y call center, y otros procesos trasversales y esenciales para el normal funcionamiento de una unidad hospitalaria, el personal administrativo se relaciona detalladamente en la tabla Nº 3:

TABLA Nº 3: RECURSO HUMANO ADMINISTRATIVO- HOSPITAL REGIONAL LIBANO

CARGOS	**AREA FUNCIONAL**	**TOTAL**
ASESEOR JURIDICO	JURIDICA	1
ASESOR FINANCIERO	GERENCIA	1
AUDITOR	AUDITORIA	2
AUX. SERVICIOS GENERALES	TODOS LOS SERVICIOS	20
AUXILIAR ADMINISTRATIVO	TODOS LOS SERVICIOS	12
AUXILIAR DE FACTURACION	FACTURACION	20
AUXILIAR DE LAVANDERIA	LAVANDERIA	3
AUXILIAR DE MANTENIMIENTO	MANTENIMIENTO	1
CONDUCTOR	REMISIONES	5
CONDUCTOR ADMINISTRATIVO	GERENCIA	1
CONTADOR	CONTABILIDAD	1
COORDINADOR DE FACTURACION	FACTURACION	2
GERENTE	GERENCIA	1
INGENIERO DE SISTEMAS	SISTEMAS	1
JEFE DE CONTROL INTERNO	CONTROL INTERNO	1
MANIPULADORA DE ALIMENTOS	NUTRICION Y DIETA	8
PROFESIONAL ESPECIALIZADO	TALENTO HUMANO	1
PROFESIONAL UNVIERSITARIO	FINANCIERA	1
PROFESIONAL UNVIERSITARIO	GTAF	1
PROFESIONAL UNVIERSITARIO	CONTRATACION	2
REVISOR FISCAL	GERENCIA	1
SECRETARIA	FATURACION P Y P	1
TECNICO	TODOS LOS SERVICIOS	23
TECNICO ELECTROMECANICO	MANTENIMIENTO	1
TECNOLOGO	TODOS LOS SERVICIOS	9
TRABAJADOR OFICIAL	AREAS COMUNES	4
VIGILANTE	TODOS LOS SERVICIOS	11
TOTAL		**135**

Fuente: Oficina de Talento Humano – Hospital Regional del Líbano E.S.E

El talento humano del hospital está comprometido con la calidad de la Atención En salud, está capacitado para ofrecer una atención idónea bajo estándares de humanización, pertinencia y seguridad del paciente.

12.5. ANÁLISIS DE ENTORNO.

Antes de que la organización formule su plataforma estratégica, debe analizar el entorno externo para identificar posibles oportunidades y amenazas, así como el entorno interno para detectar sus fortalezas y debilidades. En análisis de Entorno trata de la vigilancia, evaluación y difusión de información desde entornos externo e interno hasta el personal clave de la organización, el objetivo fundamental de esta fase es evitar sorpresas estratégicas y asegurar su salud a largo plazo.

El Hospital Regional del Líbano ha decidió utilizar como herramienta análisis del entorno externo el modelo PESTEL (análisis de factores políticos, Económicos, sociales, Tecnológicos, ecológicos y legales) y para el entorno interno el modelo FODA (Fortalezas, Oportunidades, Debilidades y Amenazas). Ambos modelos uno complementario del otro permiten tener un panorama claro del estado del entorno de la institución y permiten enfocar esfuerzos y diseñar estrategias tendientes a los resultados del análisis.

12.6. IDENTIFICACION DE LAS PARTES INTERESADAS.

Las partes interesadas son las personas que importan en un sistema. El análisis de poder de las partes interesadas es una herramienta que ayuda al entendimiento de cómo las personas afectan a las políticas e instituciones, y de cómo las políticas e instituciones afectan a las personas. Resulta particularmente útil para la identificación de ganadores y perdedores y para destacar los desafíos que se deben enfrentar para cambiar el comportamiento, el desarrollo de capacidades y enfrentar desigualdades.

Cada organización debe identificar sus propios stakeholders (partes interesadas), pues en función de su tamaño, ámbito de actuación, actividad, se

relacionará más con unos grupos y otros y la intensidad de esas relaciones será variable. Sin embargo, los stake holder con los que el Hospital Regional del Líbano (HRL) se relaciona son en general los que se relacionan a continuación.

12.7. JUNTA DIRECTIVA

Son quieres asumen la gestión de la empresa y generan también ciertas expectativas sobre la misma. Son quizás la parte que más podríamos identificar con la empresa en sí, en tanto que nodo gestor de relaciones. El Hospital Regional del Líbano debe articular mecanismos para armonizar las decisiones que tome la junta directiva sean acorde con la realidad de la institución y en beneficio de la comunidad, usuarios y sus familias y colaboradores y el de otros stakeholders.

12.8. EMPLEADOS Y TRABAJADORES

Siendo el principal activo de la organización y sin duda, uno de los grupos de interés más cercanos a la organización, el HRL propende por que se brinde un trato justo independiente con la modalidad de contratación, escrupulosamente respetuoso con sus derechos como personas y con la legislación laboral de aplicación. Más allá de esto, una gestión responsable de TTHH evaluará y recompensará las contribuciones de cada uno de los miembros de la organización y facilitará, más allá de la profesional, el cultivo de todas las dimensiones de la persona.

12.9. PROVEEDORES Y CONTRATISTAS.

Una empresa socialmente responsable debe garantizar el cumplimiento de los derechos humanos con la misma diligencia con que se garantiza el suministro. El HRL debe asegurar un escrupuloso respeto de los derechos humanos y de

las obligaciones legales en su cadena de suministro. En contrapartida, los proveedores deberían poder esperar cierto compromiso por parte del Hospital consolidando relaciones que, yendo más de perspectivas cortoplacistas, les permitan mejorar su operatividad y consolidar su responsabilidad social.

12.10. USUARIO Y SU FAMILIA.

Más allá de los derechos que garantizan las diferentes legislaciones a consumidores y usuarios de bienes y servicios y de los requisitos para la protección de los mismos que se imponen a las empresas, éstas, tanto por manifestación de su responsabilidad social como por necesidad de mejorar sus resultados, se debe prestar constante atención a las legítimas expectativas de los sus usuarios y sus familias y ser coherentes con los compromisos que adquieren con éstos a través de la publicidad y la atención brindada a los mismos.

12.11. ENTIDADES ADMINISTRADORAS DE PLANES DE BENEFICIOS.

Las entidades adaptadas de planes de beneficios conocidas como EPS (empresas promotoras de salud) del régimen contributivo y subsidiado, aseguradoras, ARL (administradora de riesgos laborales), son entidades con quienes establecemos constante comunicación y con quienes tenemos una vinculación directa puesto que el sistema de seguridad social está diseñado de esta manera, es por eso que para el HRL es importante conocer que expectativas y necesidades tiene esta parte interesada que pueda aportar al mejoramiento de la empresa.

12.12. COMPETENCIA Y MERCADOS.

La competencia es el elemento regulador del mercado que debería contribuir a que cada vez los bienes y servicios producidos sean mejores, se produzcan de forma más eficiente y respondan más adecuadamente a las necesidades y demandas de los consumidores. Más allá del deber regulador que compete a los gobiernos y del escrupuloso cumplimiento de la legislación al respecto que debe caracterizar la actuación de las empresas, de éstas se espera lealtad y buena fe, un comportamiento ético que, a través del juego limpio, alimente una sana competencia que contribuya a la mejora continua de todos los oferentes de bienes y servicios. Además de tener en cuenta la red de prestación de servicio que también el HRL debe conocer las necesidades y expectativas de aquellas IPS de la cual somos centro de referencia.

12.13. ENTORNO SOCIAL CERCANO (VECINDARIO)

Nos referimos aquí al entorno inmediato el lugar donde está ubicado el Hospital, que pueden sufrir tanto externalidades negativas (contaminación, impacto paisajístico, fluctuaciones en el valor del suelo…) como positivos (mejoras en las vías de comunicación, aumento de la renta disponible…).

Una empresa socialmente responsable es consciente de su capacidad de impacto en su entorno y estableciendo cauces de diálogo y cooperación con él, identifica estos impactos e intenta implementar mecanismos para minimizar o compensar los negativos y potenciar los positivos.

Este compromiso con su entorno social cercano crea vínculos muy estrechos entre la empresa y la comunidad de la que forma parte, que repercutirán positivamente en la organización tanto por la identificación y compromiso de los miembros de esa comunidad que la empresa incorpore como trabajadores como por la especial atención que cabe esperar le brinden las administraciones que representan a la misma.

12.14. MEDIO AMBIENTE

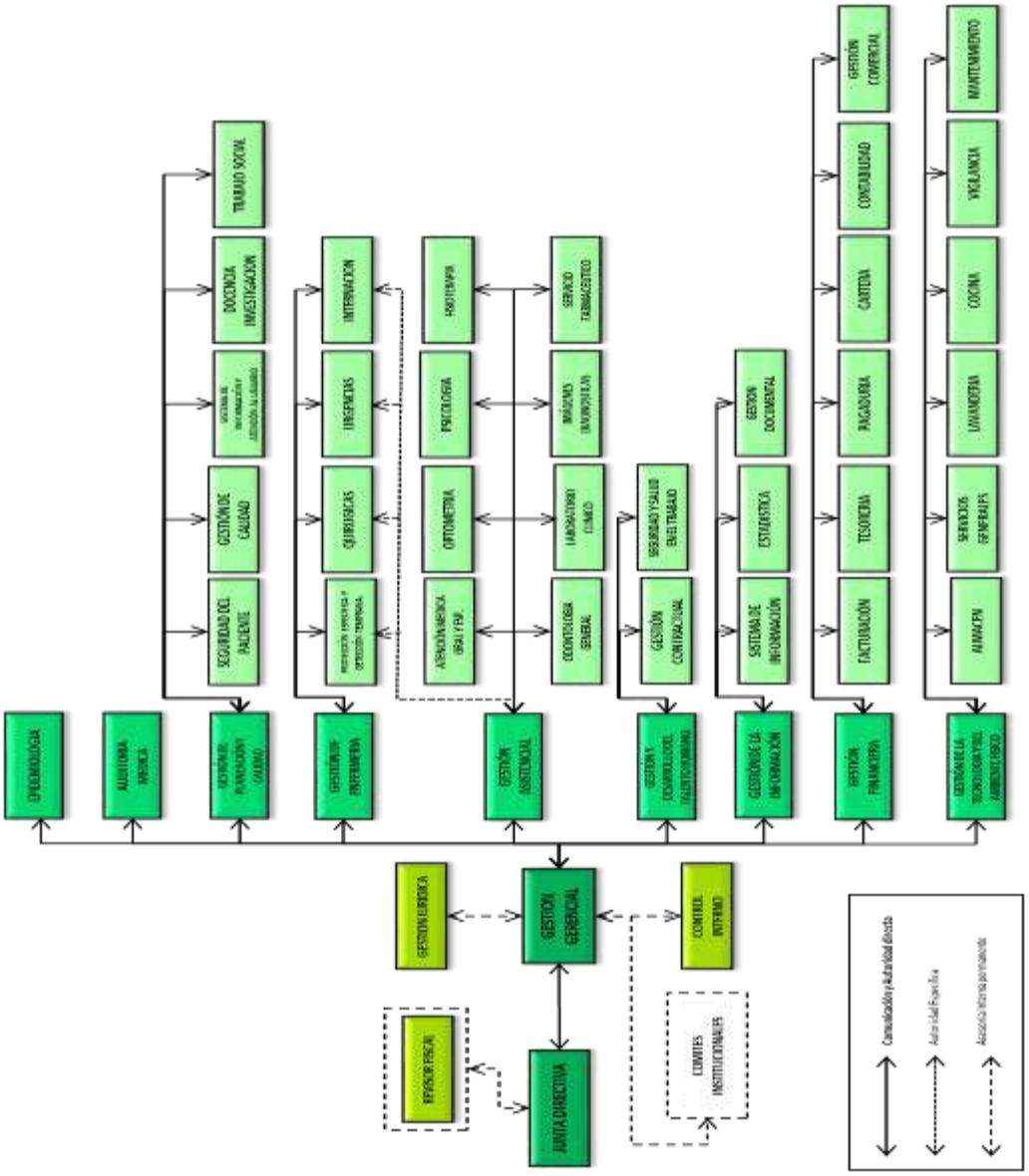
Una de las definiciones que pueden darse de “sostenibilidad” es aquella que la considera como la capacidad de satisfacer las necesidades presentes sin comprometer la capacidad de satisfacción de las necesidades de las generaciones futuras; definición especialmente pertinente cuando consideramos el impacto ecológico de la actividad industrial y económica. La huella ecológica de dichas actividades se pone de manifiesto en hechos como el calentamiento global, la disminución de la biodiversidad. La única apuesta posible es un desarrollo ecológicamente sostenible y para que esto sea posible sin renunciar a las cotas de bienestar alcanzadas, es más, para que estas cotas pueden extenderse a las poblaciones de áreas geográfica menos privilegiadas que el primer mundo desarrollado, es necesario un desarrollo tecnológico que se oriente a la explotación de fuentes de energía alternativas.

12.15. MEDIOS DE COMUNICACIÓN SOCIAL

En el ámbito empresarial, los medios de comunicación desarrollan una labor de control y crítica contribuyendo a la higiene del sistema y jugando un papel de gran relevancia. Una empresa socialmente responsable debe aceptar y respetar este papel que juegan los medios de comunicación encarando su política de comunicación desde el diálogo y la transparencia yendo así más allá de encuadra su relación con estos desde una estrategia de “marketing social” que lejos de ser manifestación de sus valores se convierte un trabajo estético vacío de contenido.

13. ORGANIGRAMA

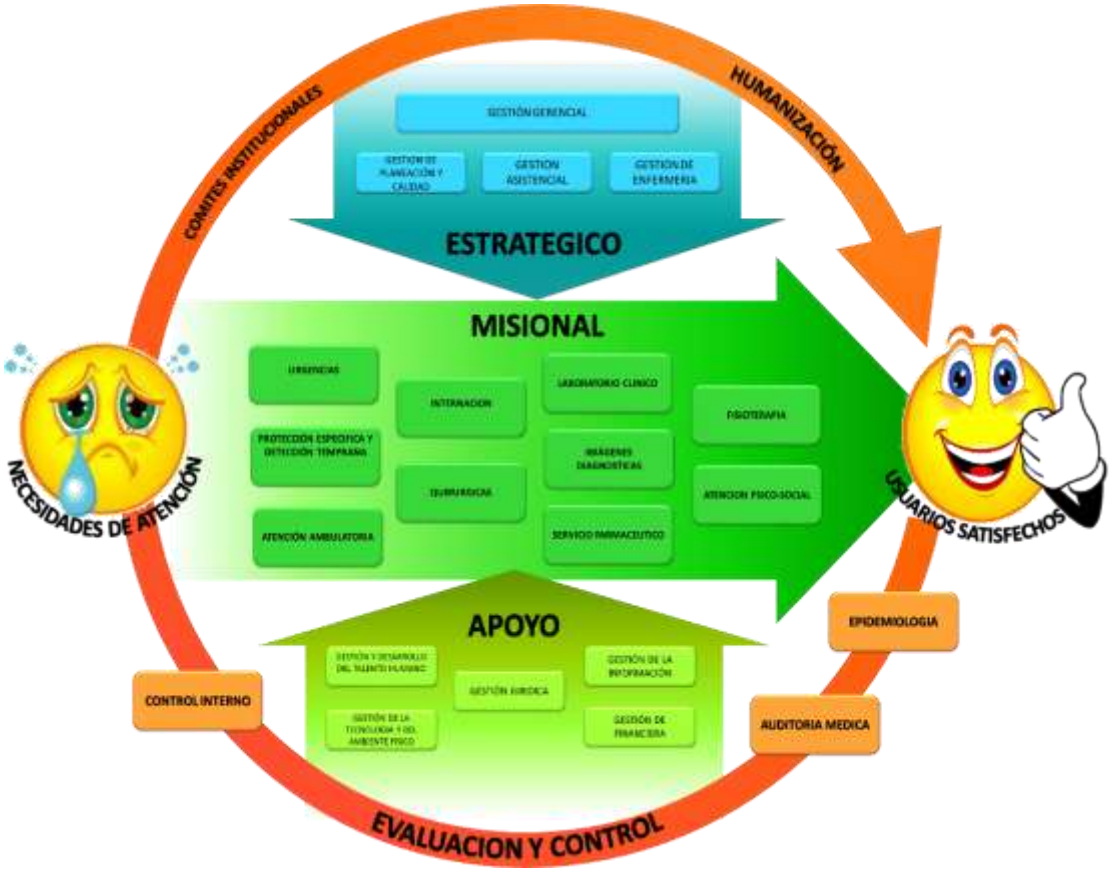
Figura 1 Organigrama Institucional



Fuente: Organigrama Institucional del Hospital Regional del Líbano

14. MAPA DE PROCESOS

Figura 2. Mapa de Procesos Institucional



Fuente: Mapa de Procesos Institucional del Hospital Regional del Líbano

15. DIRECIONAMIENTO ESTRATEGICO

El direccionamiento Estratégico Institucional es el camino orientador del crecimiento y desarrollo de la Entidad él debe estructurar una metodología clara, alcanzable, medible y participativa con el seguimiento periódico pertinente que generen oportunidades de mejoras y de ajustes en el tiempo requerido para alcanzar de los objetivos trazados por la administración.

Ubicada el área informática o departamento de sistemas, la estructura organizacional del área informática, los cargos y funciones.

una descripción del área informática o departamento de sistemas identificando los activos informáticos, los procesos que se realiza dentro del área y los servicios que presta a las demás áreas de la organización.

Determinar las vulnerabilidades, amenazas y riesgos de seguridad del área informática o departamento de sistemas en cada uno de los activos informáticos categorizados de acuerdo al activo donde se presentan (talento humano, hardware, seguridad física, redes de datos, sistemas operativos, bases de datos, seguridad lógica, entre otros) y se debe entregar un cuadro con las categorías de los activos, las vulnerabilidades, amenazas de seguridad encontrados en dicha organización.

El cuadro de las vulnerabilidades y amenazas, se adjunta los riesgos de seguridad a que se ven expuestas las organizaciones y se debe diseñar un cuadro donde aparezcan clasificados los riesgos por activo informático (talento humano, hardware, seguridad física, redes de datos, sistemas operativos, bases de datos, seguridad lógica, entre otros), describiendo claramente como se están presentando los riesgos y la valoración del impacto y la probabilidad de ocurrencia.

Para el caso de los riesgos se debe tener en cuenta que al describirlos se relacione la amenaza con el riesgo y se dé una breve descripción de cómo se presenta en la organización o en el sistema. Por ejemplo, si la vulnerabilidad es

la falta de personal de seguridad, la amenaza puede ser el acceso no autorizado de personal a los equipos donde se procesa información y el riesgo sería el robo de información confidencial debido al acceso libre de personal no autorizado a los equipos terminales en la empresa. Al finalizar deberá mostrar una sola lista de riesgos y elaborar la matriz de riesgos donde se muestre gráficamente el impacto y probabilidad de acuerdo a la escala de valoración para probabilidad que puede tener los valores (bajo, medio, alto), y para impacto los valores de (leve, moderado, catastrófico), esta valoración debe hacerla el grupo de acuerdo a la probabilidad de ocurrencia de riesgos (número de veces por periodo de tiempo) y el impacto (las consecuencias de llegar a concretarse el riesgo).

15.1. TECNOLOGÍA

Tabla 1 Sistemas de Información – Hospital Regional Líbano E.S.E

SISTEMA DE INFORMACION	CARACTERISTICAS
SISTEMA ADMINISTRATIVO HOSPITALARIO INTEGRAL – SAHI	N.A
SISTEMA INTEGRAL DE FACTURACIÓN EN SALUD - SIFAS	N.A
SISCAFE	N.A

Fuente: propia

Tabla 2 Cableado Estructurado y Eléctrico

CONEXIONES	CARACTERISTICAS
CABLEADO ESTRUTURADO	**CABLE UTP CATEGORIA 5E**
SISTEMA ELECTRICO CONECTADO A UNA UPS	N.A
PLANTAS ELECTRICAS	N.A
CONEXIÓN FIBRA OPTICA	N.A

Fuente: propia

15.2. PROCESOS DEL ÁREA DE SISTEMAS

Tabla 3 Procesos Internos- Hospital Regional del Líbano

ÍTEM	DESCRIPCIÓN DE LA ACTIVIDAD	**CARGO ESPONSABLE**
1	ADMINISTRACIÓN DEL CABLEADO ESTRUCTURADO Y TOPOLOGÍA DE LA RED DE DATOS	
1.1	Verificación de la Ruta y lugar donde se van a Instalar más punto de Red	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS
1.2	Verificación e instalación en el Rack de primer o tercer piso, el lugar donde se va conectar en el patch panel el punto de red a Instalar	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS
1.3	Configuración del Punto de red con configuración 568A en el área	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS
1.4	Pruebas de conectividad y conexión a la base de datos del Sistema de información	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS
1.5	Identificaron del punto de red con su respectiva identificación en el patch panel del rack	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS
1.6	PUNTOS DE CONTROL	

Tabla N° 3 (Continuación)

1.6.1	1.1, 1.2, 1.3,1.4 y 1.5	
1.7	INDICADORES	
1.7.1	*evento*	
2	CONFIGURACION DE MODULOS	
2.1	Recepción del Requerimiento de los hallazgos detectados o Actualizaciones en el Funcionamiento del Sistema de Información	Responsable del Proceso
2.2	Notificación a la empresa desarrolladora del Sistema de Información el Requerimiento presentado	DESARROLLADORES DEL SISTEMA DE INFORMACIÓN
2.3	Verificación de los cambios	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS
2.4	Registro de Control de Cambios	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS
2.5	Notificación de los Cambios y Mejoras o Actualizaciones realizadas	Responsable del Proceso
2.6	PUNTOS DE CONTROL	
2.6.1	2.1, 2.3, 2.4 y 2.5	

Tabla N° 3 (Continuación)

2.7	INDICADORES	
2.7.1	Cambios Solicitados/Cambios Realizados *100 Actualizaciones o mejoras planteadas/ Actualizaciones o mejoras realizadas *100	
3	REGISTRO DE COPIAS DE SEGURIDAD DEL SISTEMA DE INFORMACION DEL HOSPITAL REGIONAL DEL LIBANO E.S.E	
3.1	Programación del Sistema Manejador de la Base de Datos para la generación Automática de la copia de seguridad	**Sistemas de Información**
3.2	Generación Automática de la Copia de Seguridad de la base de Datos o Información	**Sistemas de Información**
3.3	Comprimir la copia de seguridad generada	**Sistemas de Información**
3.4	Trasladar la copia de seguridad comprimida a la ubicación de almacenamiento y almacenamiento alterno como resguardo de la Información.	**Sistemas de Información**
3.5	Registrar los datos de la copia de seguridad en la bitácora de Registro de Copia de Seguridad del sistema de Información	**Sistemas de Información**
3.6	Custodiar la ubicación de la copiad e seguridad	**Sistemas de Información**
3.7	PUNTOS DE CONTROL	

Tabla N° 3 (Continuación)

3.7.1	3.1, 3.2 y 3.5	
3.8	INDICADORES	
3.8.1	Número de Copias de Seguridad Generadas/Numero de Copias de seguridad Registradas * 100	
4	ADMNISTRACION DE BASES DE DATOS	
4.1	Recibir la solicitud o requerimiento de información que puede ser suministrada por la Base de datos del Sistema de Información.	Sistemas de Información
4.2	Determinar y analizar la viabilidad del requerimiento de Base de datos. Si es viable: realizar diagnóstico de base de datos o requerimiento	Sistemas de Información
4.3	Diagnostico de Base de Datos: Recopilar la información de una variedad de fuentes tales como: vistas del diccionario de datos. Vistas dinámicas de rendimiento. y el sistema operativo. Requerimiento: Ejecutar cada una de las actividades registradas en la Solicitud de Requerimiento o las registradas en número de caso en el SAC.	Punto exe
4.4	Aplicar correctivos a situaciones anómalas derivadas del resultado de diagnostico.	Punto exe
4.5	Realizar las pruebas derivada de aplicar los correctivos a la base de datos o de ejecutar las actividades de la solicitud de requerimiento	Punto exe

Tabla N° 3 (Continuación)

4.6	A través del SAC se documenta la respuesta realizada y se reporta al funcionario que solicito el caso.	Sistemas de Información
4.7	PUNTOS DE CONTROL	
4.7.1	4.1, 4.4 y 4.5	
4.8	INDICADORES	
4.8.1	Actividad del área de Sistemas	
5	MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS INFORMÁTICOS.	
5.1	Proyectar e Implementar el Plan de Mantenimiento Preventivo de Recursos Informáticos de la institución	Sistemas de Información
5.2	Aplicación del protocolo de Mantenimiento Preventivo o Correctivo.	
5.3	Diligenciar el Formato de RUTINA DE MANTENIMIENTO de acuerdo al periodo y fecha del Cronograma	TÉCNICOS EN SISTEMAS.
5.4	Administración de las Hojas de Vida de los Recursos Informáticos	TÉCNICOS EN SISTEMAS
5.5	Diligenciar el Formato de Mantenimiento Preventivo o Correctivo	TÉCNICOS EN SISTEMAS
5.6	Diligenciar el Informe de Baja de Inventario en el formato.	
5.7	Generación de Análisis de Conveniencia en el formato	

Tabla N° 3 (Continuación)

5.8	PUNTOS DE CONTROL	
5.8.1	5.1, 5.3, 5.5,5.6 y 5.7	
5.9	INDICADORES	
5.9.1	Numero de Recursos Informáticos/Numero de Mantenimientos Realizados * 100	
6.	ANÁLISIS DE CONVENIENCIA PARA LA ADQUISICIÓN DE ELEMENTOS INFORMÁTICOS	
6.1	Estudio de la Necesidad para dar respuesta en la adquisición de un elemento Informático	INGENIERO DE SISTEMAS
6.2	Verificación de las especificaciones técnicas de los Dispositivos informáticos en las diferentes casas matrices o proveedores	INGENIERO DE SISTEMAS
6.3	Diligenciamiento del Formato de Análisis de Conveniencia y Adquisiciones con las especificaciones técnicas del Elemento Informático a adquirir	INGENIERO DE SISTEMAS
6.4	Envió En Medio Físico y Digital del Análisis de Conveniencia y Adquisiciones diligenciado al área de Almacén para ser presentados a Gerencia	ALMACEN
6.5	Aprobación del Análisis de Conveniencia y Adquisiciones	GERENCIA
6.6	Realización de la Gestión con los proveedores o empresa que suministre	ALMACEN

	dicho elemento informático	
6.7	PUNTOS DE CONTROL	
6.7.1	6.2,6.3,6.4,6.5	
6.8	INDICADORES	
6.8.1	Necesidades presentadas / análisis de conveniencia realizados *100	
7	PLAN OPERATIVO ANUAL DE SISTEMAS DE INFORMACION	
7.1	Proyectar e planificar las actividades de acuerdo al os ejes temáticos que se realizaran durante la vigencia proyectada del plan	INGENIERO DE SISTEMAS
7.2	Ejecución de las actividades proyectadas de acuerdo al Cronograma dispuesto en el plan operativo	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS
7.3	Seguimiento y monitoreo de los recursos informáticos según los servicios que prestan y las actividades que se desarrollan con ellos	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS
7.4	Cumplimiento de los Indicadores del Plan Operativo de acuerdo al numeral 7.1	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS
7.5	PUNTOS DE CONTROL	
7.5.1	7.1, 7.2 y 7.4	

Tabla N° 3 (Continuación)

7.6	INDICADORES	
7.6.1	Actividades realizadas /actividades proyectadas *100	
8	PEDIDO DE SUMINISTROS / INSUMOS / MATERIALES AL ALMACÉN	
8.1	Listar los SUMINISTROS / INSUMOS / MATERIALES necesarios para las actividades internas del Área de Sistemas de Información con sus respectivas cantidades	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS
8.2	Diligenciar el Formato A-GTAF-A-05-EEIDE- F-PA-04 de GESTION DE LA TECNOLOGIA Y DEL AMBIENTE FISICO – ALMACÉN con los SUMINISTROS / INSUMOS / MATERIALES con sus respectivas cantidades para realizar el pedido	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS
8.3	Envió del Formato A-GTAF-A-05-EEIDE-F-PA-04 diligenciado al correo institucional de Almacén almacenhrl@gmail.com	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS
8.4	Recepción y alistamiento de lo solicitado por parte del almacén	ALMACEN
8.5	Entrega de lo Solicitado con su respectivo vale	ALMACEN
8.6	Verificación del Pedido	INGENIERO DE SISTEMAS, TÉCNICOS EN SISTEMAS

Tabla N°3 (Continuación)

8.7	PUNTOS DE CONTROL
8.7.1	8.1, 8.2, 8.4,8.5
8.8	INDICADORES
8.8.1	Artículos Solicitado / Artículos despachado *100
9	DISPONIBILIDAD DE LOS FUNCIONARIOS DEL AREA DE SISTEMAS
9.1	Realización del Cronograma de Disponibilidades para los fines de Semana y días festivos de los Funcionarios del área e Sistemas para atender la Disponibilidad
9.2	Publicación en los ENTIS de la persona Responsable de la Disponibilidad para el Fin de Semana
9.3	Entrega del Teléfono Celular del Área de Sistemas de Información a la persona responsable de la disponibilidad
9.4	Atender el llamado a las Dificultades presentadas en el Hospital, mediante los canales de Comunicación Oficiales de la entidad
9.5	Realización de la Solución vía Telefónica a la persona solicitante o caso contrario el desplazamiento del personal al Hospital Regional del Libano Tolima ESE del Funcionario de Sistemas
9.6	PUNTOS DE CONTROL
9.6.1	9.2, 9.4 Y 9.5
9.7	INDICADOR

Tabla N° 3 (Continuación)

9.7.1	Número de casos reportados por los medios de comunicación Oficiales / soluciones efectuadas * 100

Fuente: Procesos del Área de Sistemas de Información – Hospital Regional del Libando

16. MARCO METODOLOGICO

Para lograr el objetivo Propuesto y generar la Documentación respectiva en los productos, es necesario aplicar las Guías expuestas por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, se implementaran por fases las actividades para la Implementación del Inventario de Activos de la Información:

16.1. FASE 1: PLANEACIÓN

Fase 1. Obtención del apoyo de la alta gerencia, mediante la generación de una circular informativa donde se adopte el sistema de Gestión de Seguridad de la Información y la elaboración del inventario de Activos de Información alienados a las Guías expuestas por el Ministerio de Tecnologías de la Información y las Comunicaciones.

a. Generación de una Política de Sistema de Gestión de la seguridad de la Información.

b. Documentación

16.2. FASE 2: HACER

Fase 2. Documentación e identificación de los Activos de Información según las Guías para Inventario de Activos de Información del Hospital Regional del Líbano ESE

a. Realización de Formatos e Instructivos para el correcto diligenciamiento según las Guías expuestas por el Hospital Regional del Líbano ESE y Ministerio de Tecnologías de la Información y las Comunicaciones

b. Capacitación a todos los Funcionarios jefes y coordinadores de área del Hospital Regional del Líbano ESE para el diligenciamiento de los formatos

c. Identificación de los Activos de Información del área funcional sistemas de Información del Hospital.

d. valoración de los Activos de Información del área funcional sistemas de Información del Hospital.

e. Definición de la metodología para el Análisis y Evaluación del Riesgo.

f. Identificación de los factores de amenazas y Riesgos

g. Creación del SOA - Declaración de aplicabilidad

h. Creación del PTR - Plan Tratamiento Riesgos

i. Realización del Manual de Seguridad de la Información

16.3. FASE 3: VERIFICAR

Fase 3. Realización del análisis de las vulnerabilidades y amenazas de cada activo de información para el Análisis y Evaluación del Riesgo

a. vulnerabilidades y amenazas de cada activo de información

b. Identificar el riesgo teniendo en cuenta el impacto y la probabilidad

Fase 4. Tratamiento del Riesgo de cada uno de los Activos de Información según la metodología aplicada

a. Aplicación de los Controles y salvaguardas por cada amenaza detectada de acuerdo al Plan de Tratamiento de Riesgos

16.4. FASE 4. ACTUAR

Implementación

Fase 5. Definición de la Política de Seguridad

Fase 6. Aplicación de los Controles de Seguridad de la Información

Generación del Manual de Sistema de Gestión de la seguridad de la Información

17. PRODUCTOS ESPERADOS Y RESULTADOS A ENTREGAR

Documentar e inventariar los activos de información físicos (equipos de las tecnologías de la información y las comunicaciones) y digitales (bases de datos) aplicando el Modelo de Seguridad para las entidades del Estado empleando las guías del Ministerio de Tecnologías de la Información y las Comunicaciones la valoración de los activos de información.

Entregables:

Inventario de activos de Información del Hospital Regional de Líbano ESE del área de Sistema de Información

Valoración de los activos de información según el Modelo de Seguridad para las entidades del Estado aplicando las guías del Ministerio de Tecnologías de la Información y las Comunicaciones la valoración de los activos de información.

Formatos de:

a. Inventario de Activos de Información

b. Identificación de los factores de amenazas y Riesgos

c. Creación del SOA - Declaración de aplicabilidad

d. Creación del PTR - Plan Tratamiento Riesgos

Gestión del Riesgo de los activos de Información

Políticas y controles de Seguridad en los activos de Información según la ISO 27001 de 2013

Manual de Sistema de Gestión de la seguridad de la Información

18. CONCLUSIONES

Con La Aplicación De Este Proyecto en el Hospital Regional del Líbano Tolima, con llevo a la identificación y protección a los activos de información con la documentación necesaria para la creación del SISTEMA DE GESTION DE SEGURIDAD INFORMATICA, con el mejoramiento de los procesos, actividades misionales e identificación de la información importante para el área de Sistema de Información.

La documentación de un Sistema de Gestión de Seguridad Informática, mejora la calidad de los procesos y la identificación de los activos de información, las amenazas que poseen los activos de información de la entidad, realizando un tratamiento al riesgo adecuado y optimo con el fin de minimizar la materialización de algún riesgo identificado.

El Sistema de Gestión de Seguridad de la Información se alinea al Sistema de Gestión de la Calidad que el Hospital Regional del Líbano ESE a través de las metodologías utilizadas para la gestión de activos de información, gestión del riesgo y aplicación de controles a través de Guías como la Guía Para La Administración Del Riesgo del DAFP y las guías que suministra el Ministerio de Tecnologías de la Información y Comunicaciones para la realización del Sistema de Seguridad de la Información para entidades públicas del estado.

Con la implementación del Sistema de Seguridad de la Información a través de la gestión de los activos de información y la aplicación de controles en base a estándares y normas internacionales que poseen buena documentación para la implementación en empresas donde la información y las personas es bien

más preciado para la organización, El Hospital Regional del Líbano ESE, a través de la implementación de controles de la ISO/IEC 27000 y las Guías del Ministerio de las TICS, trabajo de manera armónica con el Sistema de Gestión de la Calidad que posee la entidad para mejorar los procesos, engranado de manera óptima ambos sistemas de gestión, salvaguardando los activos de información y haciendo que los procesos al interior de la entidad tengan mejoramiento continuo.

19. BIBLIOGRAFIA

COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Acuerdo 027 de 2006 “por el cual se modifica el Acuerdo No. 07 de 29 de junio de 1994”. En: Diario Oficial No. 46.528 (ene., 2007) p. 40-43.

COLOMBIA. CONGRESO DE COLOMBIA. Ley 594 del 2000 “por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”. En: Diario Oficial. No. 44084.

Ley 1712 de 2014 “por medio de la cual se crea la Ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones”. En: Diario Oficial. No. 49.084 (mar., 2014) p. 1-61

COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA Norma Técnica de Calidad en la Gestión Pública. Bogotá D.C.: Departamento Administrativo de la Función Pública, 2009. 88 p. (NTCGP 1000:2009). Disponible en http://portal.dafp.gov.co/form/formularios.retrive_publicaciones?no=628.

Manual técnico del Modelo Estándar de Control Interno para el Estado Colombiano MECI 2014. Bogotá D.C.: Departamento Administrativo de la Función Pública, 2009. 132 p. Disponible en http://portal.dafp.gov.co/form/formularios.retrive_ publicaciones?no=2162>

COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 2573 de 2014 “por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones”. En: Diario Oficial No.49.363 (dic., 2014) p. 23-26

Decreto Nacional 103 de 2015 “por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”. Disponible en http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/DECRETO_103_DE_2015.pdf

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES et. al. Documentos electrónicos. Bogotá D.C.: Minitc, 2015?. 19 p.:il. (Guía de Activos de Información, Guía No. 5) Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES et. al. Documentos electrónicos. Bogotá D.C.: Minitc, 2013?. 19 p.:il. (Cero papel en la administración pública, Guía No. 3) Disponible

en: <http://programa. gobiernoenlinea.gov.co/apc-aa-files/Cero_papel/guia-3-documentos-electronicos-v1.pdf>

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, Estrategia de Gobierno en Línea. <http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf>

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Información y Documentación: Gestión de Documentos. Parte 1: Generalidades. Bogotá D.C.: ICONTEC, 2012, 50 p.:il. (NTC-ISO 15489-1).

Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá D.C.: ICONTEC, 2013. 37p.: il. (NTC-ICO/IEC 27001)

Tecnología de la información. Técnicas de seguridad. Guía de implementación de un sistema de gestión de la seguridad de la información. Bogotá D.C.: ICONTEC, 2012. 72?p.: il. (GTC-ISO/IEC 27003)

Fortalecimiento de la Gestión TI en el Estado – Modelo de Seguridad, Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC Disponible en: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

Decreto 1078 de 2017, “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

20. ANEXOS

Anexo 1 Guía Inventario De Activos De Información

Adapta al Hospital Regional del Líbano ESE de la Guía 8 – Guía para la gestión y Clasificación de Activos de la Información de MINTIC

Anexo 2 Formato activos de la información

Anexo 3 Formato plan de tratamiento del riesgo

Anexo 4 Formato declaración de aplicabilidad - SOA

Anexo 5 Plan de tratamiento de riesgo

Anexo 6 Plan de contingencia sistemas de información

Anexo 7 Manual de seguridad de la información

21. LISTA DE CHEQUEO

21.1. PLANEAR

ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
1	La entidad cuenta con un auto diagnóstico realizado para medir el avance en el establecimiento, implementación, mantenimiento y mejora continua de su SGSI (Sistema de Gestión de Seguridad de la información?	0		Diligenciar auto diagnosticó de seguridad de la información.
2	La entidad creó un caso de estudio o plan inicial del proyecto, donde se incluyen las prioridades y objetivos para la implementación del SGSI?	1	Se identifico que la entidad no ha tenido un estudio sobre SGSI	Crear caso de estudio o plan inicial del proyecto que incluya prioridades y objetivos del SGSI, estructura del SGSI.
3	La entidad contó con la aprobación de la dirección para iniciar el proyecto del SGSI?	1	Si, carta de solicitud de realización de Proyecto	Debe existir un documento preliminar de aprobación firmado por parte de la dirección donde se aprueba el inicio del proyecto.
4	La entidad ha identificado los aspectos internos y externos que pueden afectar en el desarrollo del proyecto de implementación del sistema de gestión de	1	Con la creación de la Política de Seguridad de la Información identifico los aspectos interno y externos	Se deben identificar los temas tanto externos como internos que pueden afectar el desarrollo de los resultados del sistema.

ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
	seguridad de la información?			
5	La entidad ha identificado las partes interesadas, necesidades y expectativas de estas respecto al Sistema de Gestión de Seguridad de la Información?	1	Si, en el proyecto se encuentra las partes interesadas	Se requiere que se identifiquen las partes interesadas tanto internas como externas, detallando cuáles son sus necesidades y expectativas en la implantación del Sistema de Gestión de Seguridad de la Información.
6	La entidad ha evaluado los objetivos y las necesidades respecto a la Seguridad de la Información?	1	El Asesor del Proyecto	Realizar la identificación de los objetivos y las necesidades que tiene la entidad respecto a la seguridad de la Información.
7	En la entidad se ha definido un Cómite de Seguridad de la Información?	1	El comité de Gestión de la Información desarrolla las actividades del Comite de Seguridad de la Información	Actualizar mediante acto administrativo el comité de Gestión de la información que describa las responsabilidades de los integrantes, reuniones entre otros, sobre el tema de seguridad de la Información
8	La entidad cuenta con una definición del alcance y los límites del Sistema de Gestión de Seguridad de la Información?	1	El proyecto cuenta con un alcance	Crear un documento de alcance del Sistema de Gestión de Seguridad de la Información y sus respectivos límites en cuanto a TIC, límites físicos, temas internos y externos.
9	En la entidad existe un documento de política del Sistema de Gestión de	1	Política de Seguridad y Confidencialidad de la Información	Crear un documento que defina la política general del Sistema de Gestión de Seguridad de la Información y sus

ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
	Seguridad de la Información, el cual ha sido aprobado por la Dirección?			respectivos límites. Tener en cuenta objetivos del SGSI, marco regulatorio, el cual debe estar debidamente documentado y socializado.
10	En la entidad existe un documento de roles, responsabilidades y autoridades en seguridad de la información?	0		Se deben definir roles y responsabilidades para cada etapa de la Implementación.
11	La entidad tiene establecido algún proceso para identificar, analizar, valorar y tratar los riesgos de seguridad de la información?	1	Se cuenta con una metodología basada en el DAFP	Se debe seleccionar una metodología para gestionar los riesgos y describir en una matriz de riesgos los resultados de acuerdo a los criterios de aceptación de los mismos. Nota: Si la entidad ya tiene una matriz de riesgos, se deben identificar los riesgos que apunten a la seguridad de la información.
12	La entidad ha realizado una declaración de aplicabilidad que contenga los controles requeridos por la entidad?	1	Se cuenta con la documentación sobre la aplicabilidad de los controles	Crear documento de declaración de aplicabilidad donde se justifique la inclusión y exclusión de controles del Anexo A de la norma ISO27001 versión 2013.
13	La entidad ha evaluado las competencias de las personas que realizan, bajo su control, un trabajo que afecta el desempeño de la	1	Existe un proceso documentado para la selección del personal	Se debe conservar la información que evidencie las competencias del personal que se encuentre involucrado con la seguridad de la

ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
	seguridad de la Información?			información de la entidad. Se debe definir un plan de capacitación con el fin de que dichas personas adquieran las competencias respectivas.
14	La entidad tiene definido un modelo de comunicaciones tanto internas como externas respecto a la seguridad de la información?	1	Se esta documentado por parte del área de gestión Documental	Se debe desarrollar un modelo que indique el contenido de la comunicación; fechas, a quién se comunica y quién comunica.
15	La entidad tiene la información referente al Sistema de Gestión de Seguridad de la Información debidamente documentada y controlada?	1	Existe la documentación y formatos realizados para el levantamiento de la informacion	Toda la documentación generada del Sistema de Gestión de Seguridad de la Información debe estar debidamente documentada.

21.2. VERIFICAR

ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
1	La entidad tiene una metodología para realizar seguimiento, medición y análisis permanente al desempeño de la Seguridad de la Información?	1		Se debe tener en cuenta que se desea medir, cuando, quien realizará la medición y cuando se analizaran los resultados.
2	La entidad ha realizado auditorías internas al Sistema de Gestión de Seguridad de la Información?	0		Se deben programar auditorias en un intervalo de tiempo con el fin de evaluar y verificar la conformidad y cumplimiento del Sistema de Gestión de Seguridad de la

ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
				Información.
3	La entidad cuenta con programas de auditorías aplicables al SGSI donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes?	0		Se debe planificar, establecer, implementar y mantener uno o varios programas de auditoría donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes.
4	La alta dirección realiza revisiones periódicas al Sistema de Gestión de Seguridad de la Información?	0		Se deben realizar revisiones a intervalos planificados del Sistema de Gestión de Seguridad de la Información.
5	En las revisiones realizadas al sistema por la Dirección, se realizan procesos de retroalimentación sobre el desempeño de la seguridad de la información?	0		El área de Control interno como área imparcial al interior de la entidad, realiza un informe el informe con su respectiva retroalimentación sobre el desempeño de la Seguridad de la Información.
6	Las revisiones realizadas por la Dirección al Sistema de Gestión de Seguridad de la Información, están debidamente documentadas?	0		Se debe documentar las revisiones realizadas por la Alta Dirección con el fin de verificar el estado del sistema de seguridad de la información, cambios que se presenten a nivel interno o externo que puedan afectar la seguridad de la información y evaluación de las no conformidades y acciones correctivas. Esta revisión debe incluir las decisiones

ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
				relacionadas con las oportunidades de mejora

21.3. ACTUAR

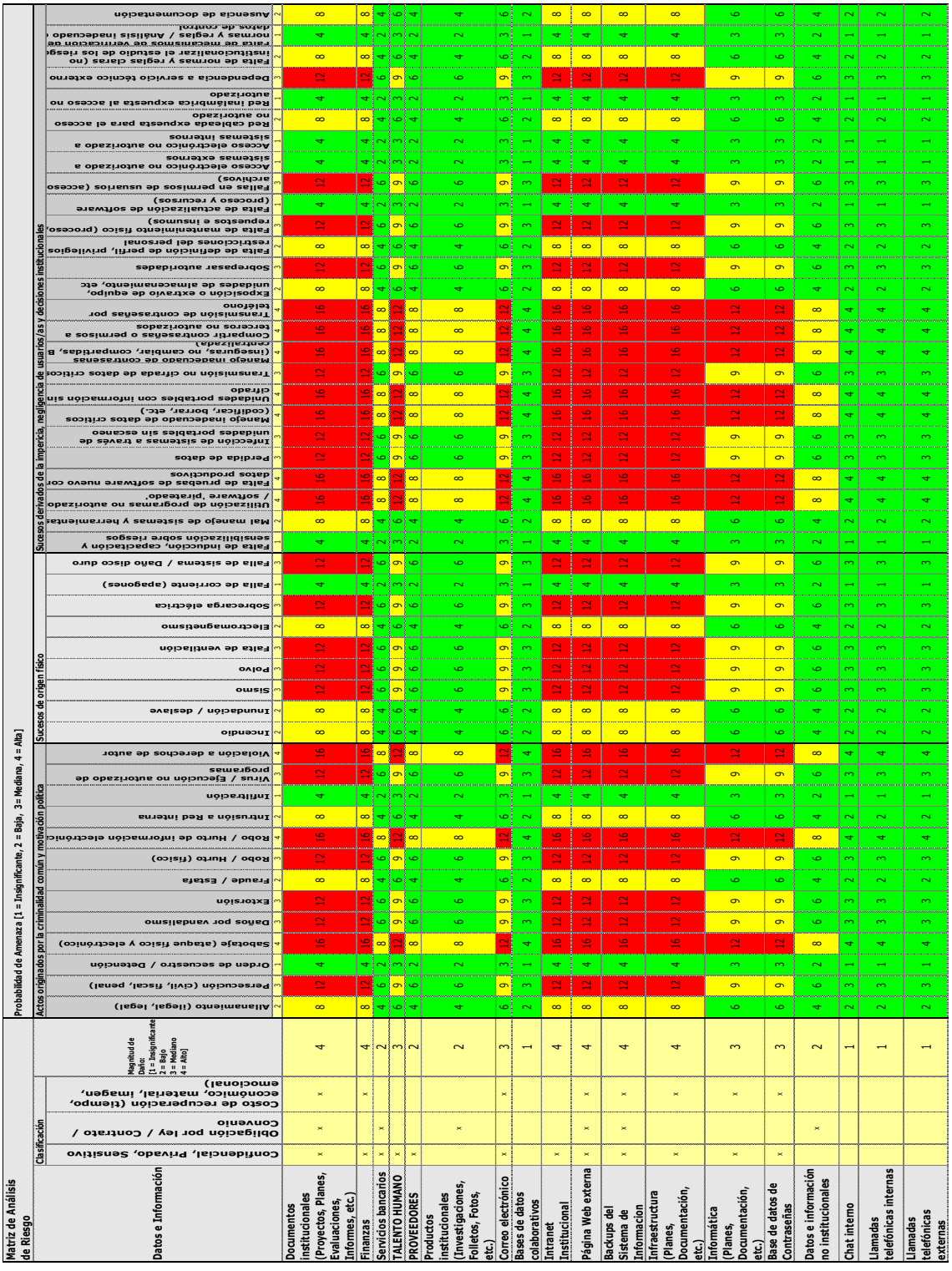
ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
7	La entidad da respuesta a las no conformidades referentes a la seguridad de la información presentadas en los planes de auditoría?			Se deben tomar acciones para eliminar las causas de las no conformidades, para que no vuelvan a ocurrir.
8	La entidad ha implementado acciones a las no conformidades de seguridad de la información presentadas?			Toda la información de acciones realizadas al Sistema de Gestión de Seguridad de la Información debe ser documentada.
9	La entidad revisa la eficiacia de las acciones correctivas tomadas por la presencia de una no conformidad de seguridad de la información?			Se debe evaluar la eficacia de las acciones correctivas con el fin de verificar que la no conformidad no se vuelva a presentar.
10	La entidad realiza cambios al Sistema de Gestión de Seguridad de la Información despues de las acciones tomadas?			Toda la información de cambios al Sistema de Gestión de Seguridad de la Información debe ser documentada.
11	La entidad documenta la información referente a las acciones correctivas que toma respecto a la seguridad de la información?			Toda la información de cambios al Sistema de Gestión de Seguridad de la Información debe ser documentada.

ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
12	La entidad realiza procesos de mejora continua para el Sistema de Gestión de Seguridad de la Información?			Toda la información de mejora al Sistema de Gestión de Seguridad de la Información debe ser documentada.

Fuente: propia

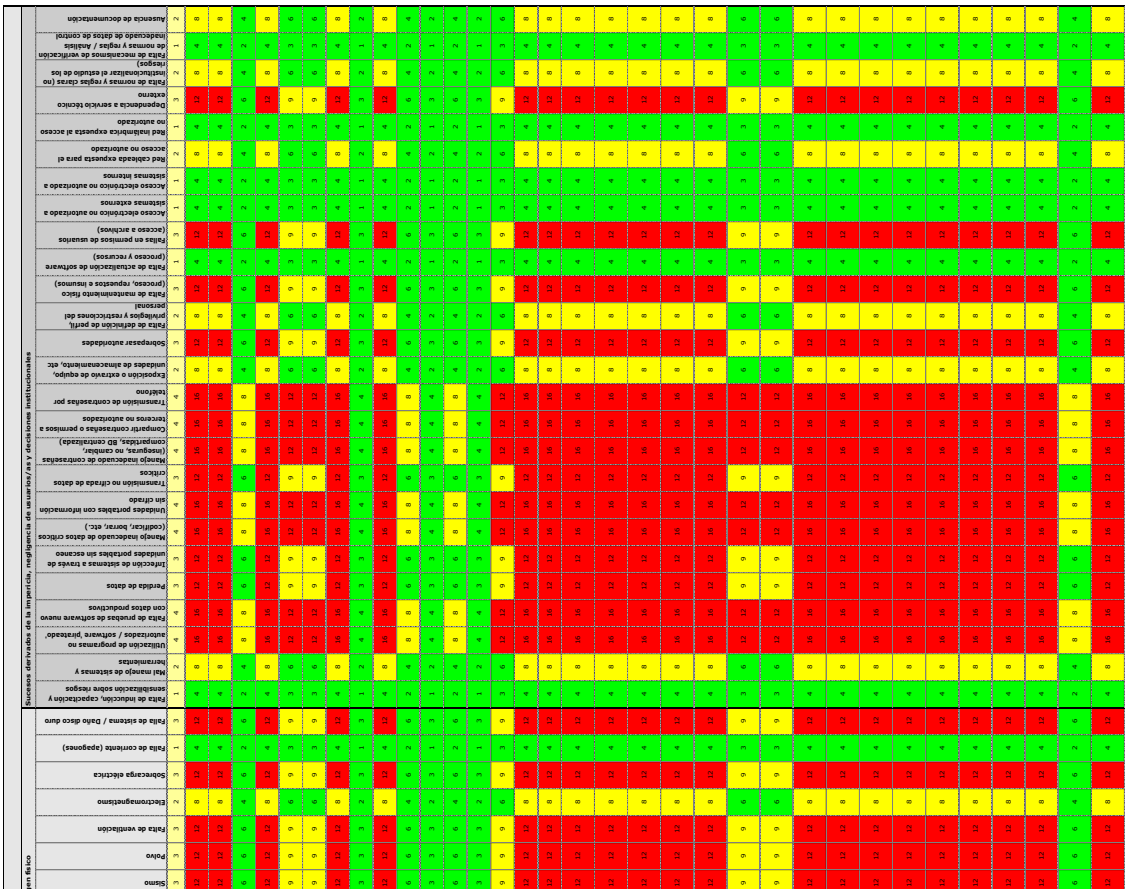
22. MATRIZ DE RIESGO

Figura 4. MATRIZ DE RIESGO DATOS



Fuente: propia

Figura 5. MATRIZ DE RIESGO SISTEMAS

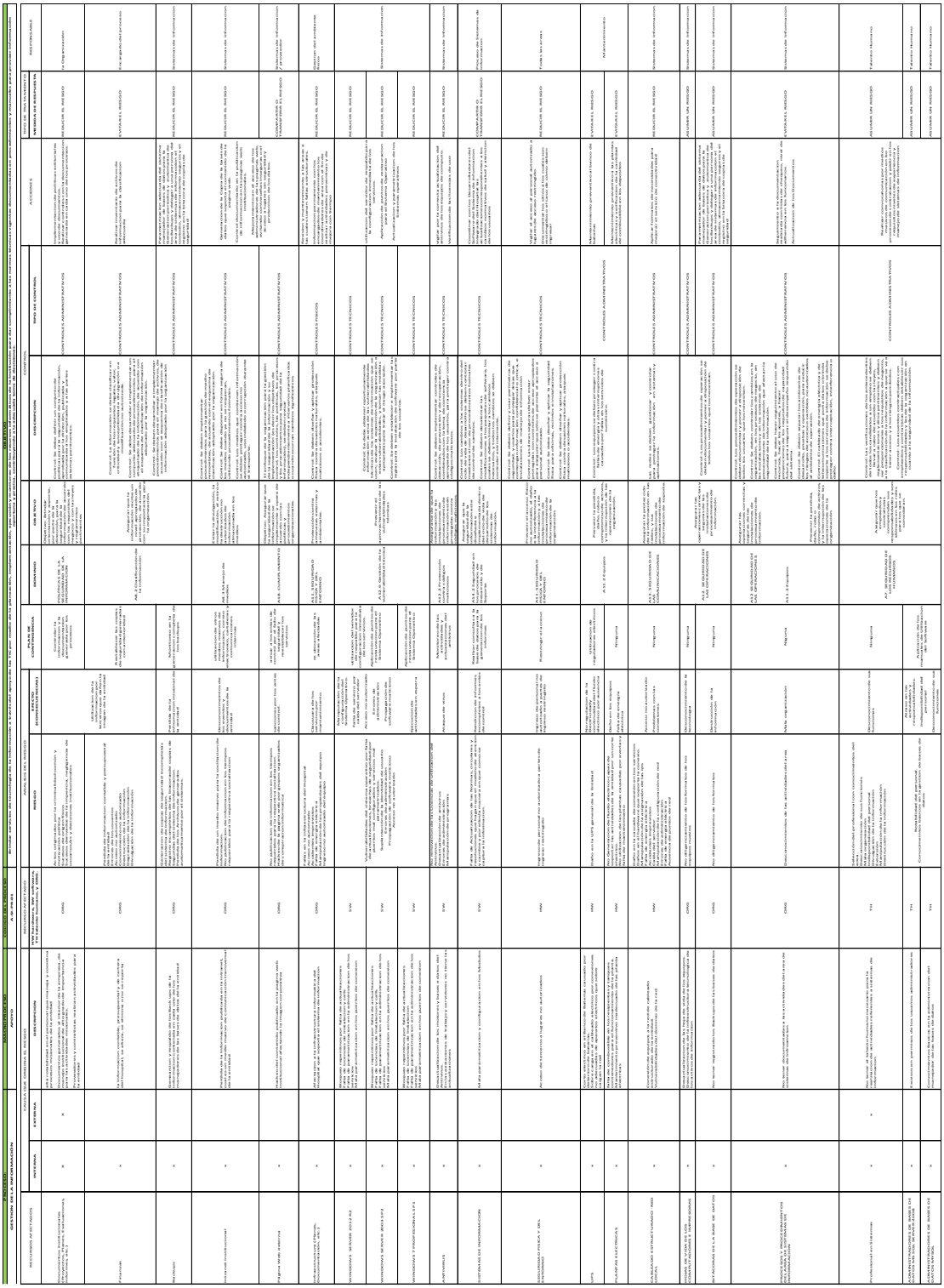


Fuente: propia

Figura 6. MATRIZ DE RIESGO PERSONAL

Fuente: propia

Figura 7. FORMATO TRATAMIENTO DEL RIESGO



Fuente: propia

23. AVISO LEGAL

Este proyecto de grado es realizado conforme al Sistema de Gestión de Seguridad Informática, suministrados por Ministerio de Tecnologías de la Información y las Comunicaciones, junto a las Guías de Seguridad de la información para la Empresas del Estado adaptadas al HOSPITAL REGIONAL DEL LIBANO TOLIMA ESE como entidad prestadora de servicios de Salud.