AUDITORÌA AL SISTEMA DE INFORMACIÓN HOSPITALARIO (SIHOS) DEL HOSPITAL CIVIL DE IPIALES BASADO EN EL ESTÁNDAR COBIT 4.1

LEIDY DORALY SANTANDER CHAMORRO

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2016

AUDITORÍA AL SISTEMA DE INFORMACIÓN HOSPITALARIO (SIHOS) DEL HOSPITAL CIVIL DE IPIALES BASADO EN EL ESTÁNDAR COBIT 4.1

LEIDY DORALY SANTANDER CHAMORRO

Trabajo de Grado presentado como requisito parcial para optar al título de Ingeniero de Sistemas.

DIRECTOR:
Msc JOSÉ JAVIER VILLALBA ROMERO

CO-DIRECTOR:
Msc. FRANCISCO NICOLAS SOLARTE SOLARTE

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2016

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este trabajo de grado, son responsabilidad exclusiva del autor.

Artículo primero del acuerdo No. 324 de Octubre 11 de 1966, emanado del Honorable Consejo Directivo de la Universidad de Nariño.

La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor".

Acuerdo N° 05 de 2010, emanado del honorable Consejo Académico de la universidad de Nariño.

Nota de Aceptación

_____

_____

_____

_____

_____

Firma del Director de Tesis

_____

Firma del Codirector De Tesis

_____

Firma del Jurado

_____

Firma del Jurado

San juan de pasto, enero 2016

AGRADECIMIENTOS

A Dios, el más especial agradecimiento por haberme acompañado y guiado a lo largo de esta carrera porque siempre estuvo conmigo en todo momento permitiéndome lograr mis metas.

A mis padres, que son mis mejores amigos con los que compartimos muchos momentos de tristezas y de alegrías, a ellos que son mi ejemplo de vida y que a través de sus consejos me enseñaron a ser valiente y a salir a delante, por eso solo tengo palabras de agradecimiento a Dios por haberme dado la oportunidad de compartir con los padres más hermosos del mundo, todo lo que soy se los debo a ustedes.

A mis tíos y padrinos Ruby Santander y Alirio Cortes, mi segundos papitos quienes siempre están pendiente de mí, quienes con sus bendiciones, su voz de aliento y a su constante apoyo me han ayudado a escalar peldaño a peldaño de mi vida y a formarme como profesional.

A mi primo, Jhon Fredy Cortes Santander y Amandita Pantoja, quienes siempre están conmigo acompañándome en las situaciones difíciles, escuchándome y motivándome para salir adelante.

A mi prima y madrina Rubí Mercedes Cortes Santander, que a pesar de la distancia también ha estado conmigo en todo momento quien es mi amiga mi confidente, con quien he compartido muchos momentos, una persona incondicional que me brinda todo su apoyo y comprensión, quien se ha preocupa por mi formación como profesional.

A mis hermanos y a toda mi familia, por su apoyo y comprensión.

Al ingeniero José Javier Villalba, quien fue mi apoyo y guía en el desarrollo de este trabajo, por transmitir sus conocimientos e ideas y orientarme en el desarrollo de este trabajo.

Al Ingeniero Francisco Nicolás Solarte, por su apoyo, orientación paciencia y compresión para culminar este trabajo.

Al Ingeniero Nelson Jaramillo, Decano de la Facultad de Ingeniería y al ingeniero Manuel Ernesto Bolaños Gonzales Director del Departamento de Sistemas, por su apoyo y compromiso para culminar de la mejor manera este trabajo.

Al Doctor Eduardo Efraín Narváez, Gerente del Hospital Civil de Ipiales, al Ingeniero José Fernando Mora Jefe de Sistemas, y a todo el equipo de la dependencia de Sistemas, por permitirme el acceso a la información del Hospital Civil de Ipiales, por su colaboración y disposición en todo, lo cual permitió desarrollar el trabajo de acuerdo con lo planteado.

A mis maestros y compañeros, por las enseñanzas, confianza, amistad, tiempo y apoyo dedicado durante la trayectoria de aprendizaje de la carrera.

A la Facultad de Ingeniería de la Universidad de Nariño, por la formación profesional, cimentado en la ética y responsabilidad, que me brindó durante mi etapa como estudiante de Ingeniería de Sistemas.

DEDICATORIA

Este triunfo se lo dedico a Dios, por haberme guiado durante todos estos años, por darme la oportunidad de culminar esta meta con valor y fuerza durante el transcurso de la carrera y por demostrarme su amor incondicional en momentos de dificultades.

De igual manera, se lo dedico a mis padres, por los esfuerzos y los sacrificios que hicieron para formarme como profesional, por su apoyo incondicional y por brindarme cada día su cariño y amor que me motivan para luchar por cada una de mis metas. A ellos, debo toda mi vida y mis logros que no podre pagar nunca lo que han hecho por mí.

A mis hermanos y a toda mi familia, por sus consejos y palabras de aliento, por todo lo que me han brindado y por su constante apoyo y comprensión.

Se lo dedico además a mi asesor el ingeniero José Javier Villalba, por guiarme y compartir su conocimiento y acompañarme durante el desarrollo del trabajo de grado.

Así como también se lo dedico al ingeniero Nelson Antonio Jaramillo, que me guio en momentos de dificultad, por sus consejos y palabras de aliento que me motivaron para continuar con mi trabajo.

.

RESUMEN

Hoy en día la auditoría a Sistemas de Información se ha convertido en una necesidad para el desarrollo y crecimiento en cualquier empresa ya que a través de la evaluación de las distintas áreas; la auditoria permite evaluar la eficiencia y eficacia de cada proceso.

La necesidad de evaluar el Sistema de Información Hospitalario (SIHOS) del Hospital Civil de Ipiales nace a través de la continua búsqueda del mejoramiento del Sistema teniendo como objetivo perfeccionar continuamente la atención de los servicios de salud que se brindan al usuario a través de este sistema.

La auditoría al Sistema de Información Hospitalario (SIHOS) se realizó con el fin de identificar riesgos y vulnerabilidades del sistema, que permitieron establecer algunas recomendaciones que se deben implementar para obtener un buen rendimiento del Sistema de Información Hospitalario (SIHOS) y mejorar la atención de los servicios prestados a los pacientes.

Para llevar a cabo este proceso de auditoria se tomó como referente el estándar Cobit 4.1 se seleccionaron y se evaluaron distintos procesos de acuerdo con cuatro dominios de planear y organizar (PO), adquirir e implementar (AI), entregar y dar soporte (DS), monitorear y evaluar (ME), dentro de cada dominio se escogieron los objetivos de control apropiados para evaluar el Sistema de Información Hospitalario (SIHOS), seguidamente se elaboraron las listas de chequeo y entrevistas para cada dominio y objetivos de control, luego se procedió a realizar análisis con la información recolectada a través de un formato de no conformidades de cada pregunta, así como también se realizó análisis de riesgos utilizando la metodología planteada por Horacio Villa Loboguerrero de los datos recopilados, además se realizó la evaluación del Sistema de Información Hospitalario (SIHOS) de acuerdo con el alcance planteado en el proyecto.

Una vez terminado el proceso de auditoría al Sistema de Información Hospitalario (SIHOS) del Hospital Civil de Ipiales, se plantearon una serie de recomendaciones para fortalecer y mejorar la seguridad y la atención de usuarios a través del Sistema de Información Hospitalario (SIHOS).

ABSTRACT

NOWADAYS, THE INFORMATION SYSTEM AUDITS HAS BECOME A NEED FOR ANY ENTERPRISE DEVELOPMENT AND GROWTH BECAUSE THROUGH THE EVALUATION OF DIFFERENT AREAS, THE AUDITS LET EVALUATE THE EFFICIENCY AND EFFECTIVENESS IN EACH PROCESS.

THE EVALUATION NEED IN THE HOSPITAL INFORMATION SYSTEM (SIHOS) HOSPITAL CIVIL FROM IPIALES WAS BORN DUE TO THE WISH OF IMPROVING THE SYSTEM, HAVING AS AN OBJECTIVE THE IMPROVEMENT OF THE CARE HEALTH SERVICES THAT THE USER IS PROVIDED THROUGH THIS SYSTEM.

THE AUDITS TO THE HOSPITAL INFORMATION SYSTEM (SIHOS) WAS MADE WITH THE PURPOSE OF IDENTIFYING THE RISKS AND VULNERABILITIES THE SYSTEM HAS, THOSE THINGS LET ESTABLISH SOME RECOMMENDATIONS THAT SHOULD BE TAKEN INTO ACCOUNT IN ORDER TO OBTAIN A GOOD PERFORMANCE IN THE HOSPITAL INFORMATION SYSTEM (SIHOS) AND IMPROVE THE CARE SERVICES PROVIDED TO PATIENTS.

TO CARRY OUT THIS AUDIT PROCESS IS TAKEN AS A REFERENCE THE STANDARD COBIT 4.1, DIFFERENT PROCESSES WERE SELECTED AND EVALUATED ACCORDING TO THE FOUR DOMAINS: PLAN AND ORGANIZE (PO), ADQUIRE AND IMPLEMENT (AI), DELIVER AND SUPPORT (DS), MONITOR AND EVALUATE (ME), IN EACH DOMAIN SOME APPROPRIATED CONTROL OBJECTIVES WERE CHOSEN TO EVALUATE THE HOSPITAL INFORMATION SYSTEM (SIHOS). THEN, SOME CHECK LISTS, INTERVIEWS AND OBJECTIVES FOR EACH DOMAIN WERE CREATED. NEXT, THE COLLECTED INFORMATION WAS ANALYZED THROUGH A NONCONFORMITY FORMAT PER QUESTION. ALSO, THE RISKS WERE ANALYZED USING THE METHODOLOGY PROPOSED BY HORACIO VILLA LOBOGUERRERO OF DATA COLLECTED. BESIDES, AN EVALUATION OF THE HOSPITAL SYSTEM INFORMATION (SIHOS) WAS MADE ACCORDING TO THE GOALS PROPOSED IN THIS PROJECT.

ONCE THE AUDITS PROCESS TO THE HOSPITAL SYSTEM INFORMATION (SIHOS), HOSPITAL CIVIL FROM IPIALES HAS FINISHED, SOME RECOMMENDATIONS WITH THE PURPOSE OF IMPROVING AND

STRENGTHENING THE USERS SECURITY AND ATTENTION THROUGH THE HOSPITAL SYSTEM INFORMATION (SIHOS) WERE PROPOSED

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

La informática ha alcanzado un gran desarrollo a lo largo de las últimas décadas convirtiéndose en un pilar fundamental para el desarrollo cognitivo del ser humano lo que influye en la aparición de diferentes herramientas computacionales que manipulan la información, entre ellas el computador indiscutiblemente la herramienta más importante, la cual es utilizada para almacenar, procesar, y comunicar todas las actividades de cualquier organización, para tener un manejo más eficiente de la información.

A raíz del surgimiento de las computadoras, comenzaron a crecer sistemas de información sencillos, tanto con fines administrativos como financieros, posteriormente, se da lugar a los Sistemas de Información Hospitalaria, tan indispensables en la actualidad. Su impacto en las instituciones de salud es fuerte, ya que busca elevar la calidad de la atención del paciente, de los servicios brindados y aplicar la información obtenida a las áreas de la investigación, la clínica, la docencia, la administración y desde luego evadir costos y elevar la productividad.

Actualmente, cualquier institución cuenta con equipos informáticos y sistemas implementados para automatizar sus procesos, lo que ha contribuido a que se brinden servicios rápidos y de calidad, sin embargo, estos avances traen consigo inconvenientes en el manejo de los procesos, creando la necesidad de evaluar los Sistemas Informáticos a fin de determinar si su funcionamiento es el adecuado o descubrir donde se pueden realizar mejoras.

En la actualidad en el Hospital Civil de Ipiales se han presentado situaciones de accesos indebidos a los centros de procesamiento de datos, situaciones referentes a virus, sabotajes, denegación de servicios vulnerabilidades en los sistemas, confidencialidad y privacidad de los datos, que en varias ocasiones colocan en riesgo la disponibilidad, integridad de la información, los niveles de competitividad, rentabilidad, estabilidad y legalidad de los procesos, lo que influye en la prestación de servicios a cada uno de los pacientes y sobre todo en la velocidad con la que se requiere ser atendidos.

Por otra parte, el Sistema de Información Hospitalario (SIHOS) es un sistema que ha implementado el Hospital Civil de Ipiales pero aún no ha sido evaluado es decir se desconoce cómo está funcionando en cuanto a seguridad, integridad, confiabilidad, disponibilidad, funcionalidad y usabilidad, además no se ha identificado si este sistema permite apoyar las actividades a nivel operativo táctico y estratégico dentro del Hospital.

Por lo tanto, se hace necesario realizar la auditoría al Sistema de Información Hospitalario (SIHOS), ya que es de gran importancia que los procesos se desarrollen de una manera eficaz y eficiente buscando mejorar la calidad de los servicios prestados hacia los usuarios finales y usuarios del sistema e implementando planes preventivos contra fallas, amenazas y vulnerabilidades para verificar el correcto funcionamiento de los diferentes módulos, así como también el cumplimiento de los requerimientos de entradas y salidas de los datos, además, evaluar que los módulos del Sistema de Información suplan la necesidades del Hospital Civil de Ipiales y de sus usuarios.

Desde este punto de vista, los beneficios que trae la auditoría al Sistema de Información Hospitalario (SIHOS) es la revisión de controles existentes en cuanto al cumplimiento de los requerimientos de los usuarios de los módulos, como también realizar recomendaciones de implementación de planes, herramientas, políticas, controles para la protección de los activos principales del Hospital Civil de Ipiales, garantizando que el funcionamiento de los módulos sea el óptimo y permita la gestión y administración trasparente para los usuarios.

Hoy en día ninguna organización está exenta de vulnerabilidades, las cuales deben ser detectadas a tiempo para así diseñar controles que las contrarresten, para lo cual existe una serie de normas como lo es COBIT 4.1 (Modelo de Auditoría y Control de Sistemas de Información), es un modelo de evaluación y monitoreo cuyo objetivo es evaluar los criterios de información como la seguridad calidad, gestión y control enfocado a administradores de tecnologías de información.

Para el trabajo se usó el estándar COBIT 4.1 que aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de los recursos TI que necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer

la información pertinente y confiable que requiere una organización para lograr sus objetivos.

En relación con anterior el presente trabajo se orientó a la evaluación del Sistema de Información Hospitalario (SIHOS) en el Hospital Civil de Ipiales basado el estándar COBIT 4.1 con el fin de generar un diagnóstico en el que se identificaron aquellas fallas y riesgos en el proceso, además se formularon las respectivas recomendaciones a seguir, se elaboró un documento que incluye los hallazgos y evidencias encontradas durante el proceso que permitirán a esta entidad desarrollar un plan de mejoramiento que conlleve a una buena toma de decisiones y así optimice sus procesos y para finalizar presentar el informe ante la Gerencia del Hospital Civil de Ipiales.

IDENTIFICACION DEL PROBLEMA

TITULO

AUDITORÍA AL SISTEMA DE INFORMACIÓN HOSPITALARIO (SIHOS) DEL HOSPITAL CIVIL DE IPIALES BASADO EN EL ESTÁNDAR COBIT 4.1

MODALIDAD

El presente trabajo de grado corresponde a la modalidad proyecto de aplicación estipulado por la Facultad De Ingeniería de la Universidad de Nariño.

LINEA DE INVESTIGACIÓN

El trabajo pertenece a la línea de auditoría de Sistemas Computacionales definida por el programa de Ingeniería de Sistemas de la Universidad.

DESCRIPCION DEL PROBLEMA

Planteamiento del problema

Los Sistemas de Información son una combinación de personas, hardware, software, redes de comunicación y recursos de datos que reúne, transforman y disemina información en una organización. Los usuarios finales actualmente

dependen de varios tipos de sistemas que van desde sistemas simples de datos organizados manualmente hasta aquellos en los que se utilizan redes de telecomunicaciones sofisticados para la comunicación. Los cuales están expuestos a un gran número de vulnerabilidades, riesgos y amenazas que pueden tener fuertes impactos en la confidencialidad, integridad y disponibilidad de la información.

El Hospital Civil de Ipiales cuenta en la actualidad con un Sistema de información Hospitalario (SIHOS) encargado del procesamiento de la información de pacientes y empleados. En este sistema se han presentado varias situaciones como accesos indebidos, situaciones referentes a virus, vulnerabilidades en los sistemas, confidencialidad y privacidad de los datos. Esto ha ocasionado problemas tales como lentitud en los procesos, interrupción en la prestación de servicios, inseguridad en los diferentes elementos dentro del Hospital.
Esta problemática aún no ha sido totalmente identificada debido a que no se han realizado procesos de auditoría informática especialmente en la parte de seguridad.

El no contar con estos procesos de auditoría es una pérdida de oportunidad para el Hospital ya que si se llegase a presentar alguna situación de riesgo que afectara la vulnerabilidad de la información las incidencias serian catastróficas.

Por otra parte, el Sistema de Información Hospitalario (SIHOS) maneja distintos módulos como son facturación, contabilidad, inventario, este sistema manipula la información referente pacientes, empleados, profesionales, administrativos y en general de todo el Hospital. Por lo tanto, es indispensable que los datos que se manejen dentro Sistema de Información Hospitalario (SIHOS) estén orientados a preservar la confidencialidad, integridad, disponibilidad de la información y de los sistemas.

En la actualidad, se desconoce cuál ha sido la eficiencia y la eficacia del uso del Sistema de Información Hospitalario (SIHOS) en el Hospital Civil de Ipiales, es decir, no se ha evaluado si el sistema brinda las condiciones de seguridad adecuadas, apoya la consecución de los objetivos, permite una integración confiable hacia sus pacientes y en general, si responde a las necesidades de información de la institución generando un buen servicio hacia todo el Hospital.

Por lo anterior y ante esta problemática es necesario profundizar en los temas de seguridad de la información, que le permitan diagnosticar su situación actual e implementar mecanismos de gestión de riesgos y controles orientados desde estándares internacionales de auditoría.

OBJETIVOS

Objetivo general

Evaluar el Sistema de Información Hospitalario (SIHOS) al Hospital Civil de Ipiales basado en el estándar Cobit 4.1 que permita establecer recomendaciones necesarias para su mejoramiento.

Objetivos específicos

- Identificar el contexto en el manejo del Sistema de Información Hospitalario (SIHOS) en el Hospital Civil de Ipiales.

- Diseñar técnicas e instrumentos de recolección de información que permitan evaluar el desempeño del Sistema de Información Hospitalaria (SIHOS).

- Evaluar la seguridad del Sistema de Información Hospitalario (SIHOS).

- Estructurar el informe final del diagnóstico con los hallazgos, evidencias y recomendaciones.

JUSTIFICACION

La auditoría de sistemas es de gran importancia ya que se encarga de evaluar normas, controles, técnicas y procedimientos para un excelente desempeño de los sistemas de información que permiten apoyar las actividades en los niveles operativos tácticos y estratégicos dentro de cualquier organización y además proporcionan controles necesarios para que los sistemas sean confiables y con un buen nivel de calidad.

En la actualidad, los sistemas de información han transformado la manera en que operan las organizaciones. A través de su uso se logran significativos cambios, se automatizan los procesos operativos, suministran plataformas de información necesaria para la toma de decisiones, además su implantación logra ventajas competitivas que se traducen en beneficios para las organizaciones.

En un Sistema de Información Hospitalario influyen factores internos como externos de la institución como son entidades de supervisión, asociaciones de usuarios, proveedores de servicios, proveedores de medicamentos, proveedores de servicio de mantenimiento, personal administrativo, personal asistencial y por su puesto los pacientes. Cada actor juega un papel fundamental en el Sistema de Información Hospitalario, cada uno produce y consume información primaria o procesada con lo cual activa procesos o procedimientos en otros actores, todos dirigidos a mejorar la calidad de la salud de las personas.

De allí la importancia de evaluar el Sistema de Información Hospitalario (SIHOS) en el Hospital Civil de Ipiales ya que permitió beneficiar al Hospital, a usuarios del sistema, a usuarios finales, al Hospital porque permite identificar controles, fallas y vulnerabilidades al sistema, que faciliten la implementación de planes de mejoramiento encaminados hacia la eficiencia y eficacia de los procesos y procedimientos que se manejan en el Sistema de Información Hospitalario (SIHOS), así como la implementación de nuevos controles.

De esta manera, también se pueden beneficiar los usuarios del sistema porque tienen control sobre los datos que manejan y la información procesada, lo que permite evitar errores en los módulos como puede ser facturación, contabilidad, atención al usuario, laboratorios clínicos o en ocasiones equivocaciones en los datos, diagnósticos y reclamo de medicamentos.

Igualmente, se pueden beneficiar los usuarios finales de los servicios porque se agilizan los procesos de cada paciente como asignación de citas, urgencias, atención al usuario, resultados clínicos, y se incrementara la calidad de cada uno de los procesos y procedimientos manejados.

Así mismo los administradores del sistema observaran rendimiento en la operatividad del Sistema de Información Hospitalaria (SIHOS).

De igual forma, permitió fortalecer e implementar sistemas de gestión mediante el establecimiento de controles y seguimiento a planes de mejoramiento a procesos institucionales a fin de incrementar la calidad de los servicios al existir mayor disponibilidad de la información, y por consiguiente la satisfacción de sus pacientes por un servicio más eficiente, lo que trasciende en la imagen del Hospital ante la sociedad.

Finalmente, con el informe de auditoría se orientó al Hospital Civil de Ipiales en el seguimiento de la eficacia de las acciones correctivas y preventivas, de esta manera también se analizaron e identificaron los problemas para que la institución pueda corregirlos o prevenirlos, ya que teniendo conocimiento del estado de sus procesos y la forma en que estos son realizados se puede comprobar si los procesos realmente producen los resultados esperados o no, y tomar las medidas necesarias en pro de la institución.

ALCANCE Y DELIMITACION

La auditoría se realizó al Sistema de Información Hospitalario (SIHOS) en el Hospital Civil de Ipiales ubicado en el Departamento de Nariño en la frontera con la República del Ecuador, en el área de Auditoría de Sistemas y se enfocó al sistema de información Hospitalario (SIHOS).

Para evaluar el sistema de Información Hospitalario (SIHOS) se tuvieron en cuenta las características de calidad del estándar COBIT 4.1, como son:

- Funcionalidad
- Usabilidad
- Portabilidad
- Accesibilidad
- Confiabilidad

Para la evaluación del Sistema de Información Hospitalario (SIHOS) se enfatizó en el módulo de historias clínicas en cuanto a evaluación de entradas y salidas, resultado de pruebas realizadas, seguridad del sistema y salida de información

ANTECEDENTES

- El trabajo denominado “AUDITORÌA AL SISTEMA DE INFORMACION DE LA DEPENDENCIA DE OCARA DE LA UNIVERSIDAD DE NARIÑO. se realizó en el año 2013, por los estudiantes de ingeniería de sistemas German Darío Burbano Hualpa y Sandra Milena Ordoñez Cerón con el fin de detectar causas de los problemas que presenta el sistema de información de OCARA en el módulo de matrículas para lo cual se utilizó el estándar COBIT. De este trabajo se tuvo en cuenta la metodología y algunos aspectos de evaluación al sistema de información como son usabilidad, accesibilidad, funcionalidad y confiabilidad.

- El trabajo denominado “AUDITORÍA DE SISTEMAS APLICADA AL SISTEMA INTEGRAL DE INFORMACIÓN EN LA SECRETARIA DE PLANEACIÓN MUNICIPAL DE LA ALCALDÍA DE PASTO” se realizó en el año 2009 por el estudiante de Ingeniería de Sistemas Carlos Julián Estrada Obando con el fin de detectar las vulnerabilidades físicas y lógicas que se presentan en un sistema integral de información (SII) en la secretaria de planeación municipal de Pasto para la cual se utilizó el estándar COBIT.[9]

  De este trabajo se abordaron algunos controles tanto en la parte física como en la lógica además se revisaron algunas pautas para el diseño del informe final en cuanto a su estructura.

- El trabajo denominado “AUDITORÍA DE SISTEMAS DE INFORMACION DE LA IPS INDIGENA GUAITARA DEL MUNICIPIO DE IPIALES “ se realizó en el año 2013 por los estudiantes de ingeniería de sistemas Julio cesar Lagos Chaguezac y Nelson Andrés Cortes Bernal con el fin de identificar vulnerabilidades de seguridad física lógica a las cuales se encuentra expuesta la información, además de evaluar procedimientos, controles, archivos de seguridad con el propósito de lograr una utilización eficiente y segura. Este trabajo utilizo de base para la identificación de pruebas y herramientas para efectuar la auditoría de sistemas.

- El trabajo denominado “AUDITORÍA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACION DE PAGINAS WEB EN INSTITUCIONES OFICIALES DEL DEPARTAMNETO DE NARIÑO, HOSPITAL CIVIL DE IPIALES Y HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE PASTO” desarrollado por Ricardo Alexander Cabrera y Luis Carlos Chávez Yela, el trabajo consistió en aplicar técnicas de auditoría en la contratación de páginas web. La información que se encuentra en este trabajo se empleó para la comprensión de diferentes técnicas y metodología para la auditoría de sistemas.

- El trabajo denominado **“**AUDITORÍA AL PORTAL WEB DEL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E desarrollado por Jeniffer Nathaly Realpe Portilla y Yenifer Adriana Rodríguez Ojeda en la Universidad de Nariño**.**”. Este trabajo hace la evaluación de la página web institucional del hospital y en él se desarrolló un instrumento que fue aplicado a los usuarios internos de la página web y se aplicó una metodología para su evaluación. De este trabajo se tomó como ejemplo los instrumentos y la metodología empleados para la evaluación de la página web.

- PLAN DE SEGURIDAD INFORMATICA realizada por los estudiantes de ingeniería de sistemas María Dolores Cerini, Pablo Ignacio Prá de la UNIVERSIDAD CATÓLICA DE CORDOBA con el fin de evaluar las vulnerabilidades existentes en lo relativo a controles de seguridad como medio para el desarrollo de una política de seguridad donde se definen lineamientos para promover la implementación de un modelo de seguridad en toda la organización. De este trabajo se tuvo en cuenta temas como la seguridad de aplicaciones y seguridad de las comunicaciones.

1. MARCO REFERENCIAL

1.1 MARCO CONTEXTUAL

1.1.2 Reseña histórica del Hospital Civil de Ipiales Nariño: el Hospital Civil de Ipiales E.S.E. está ubicado en el Municipio de Ipiales, al sur del Departamento de Nariño. Su origen se remonta a partir de la Fundación Hospital San Vicente de Paúl como se denominaba anteriormente y la cual fue reconocida con personería jurídica en el año 1921; existe constancia documental de ese reconocimiento en la publicación del diario oficial de Octubre de 1921[1].

También existe la certificación emanada de la Dirección del Archivo Nacional de Colombia, donde se constata que mediante resolución No.001 del 15 de enero de 1970, la Junta Directiva de la Fundación Hospital San Vicente de Paúl expidió nuevos estatutos que fueron aprobados debidamente por el Ministerio de Salud, expresando su carácter de ser institución de utilidad común de origen canónico.

En 1980, se suscribió contrato entre la Fundación Hospital San Vicente de Paúl y el Servicio Seccional de Salud de Nariño vinculándose al Sistema Nacional de Salud y convirtiéndolo en sede de la Unidad Regional de Salud Sur, actualizando sus estatutos para la nueva entidad con el nombre de Hospital Civil de Ipiales.

En 1997 de conformidad con lo dispuesto por la Ordenanza No.018 proferida por la Honorable Asamblea Departamental de Nariño, el 10 de mayo del mismo año, cambia la denominación adoptando el nombre de Hospital Civil de Ipiales Empresa Social del Estado, identificado con Nit Nº 800084362-3, constituyéndose con una categoría especial de entidad pública descentralizada del orden departamental, dotada de personería jurídica, patrimonio propio y autonomía administrativa, sometida al régimen jurídico previsto en el capítulo III, Artículo 194, 195 y 197 de la Ley 100 de 1993 y sus decretos reglamentarios y adscrita al Instituto Departamental de Salud de Nariño. El domicilio es el Municipio de Ipiales, Avenida Panamericana Norte, barrio los Chilcos.

[1] SITIO OFICIAL DEL HOSPITAL CIVIL DE IPIALES NARIÑO, COLOMBIA [En Línea]. <http://www.hospitalcivilese.gov.co/site/index.php/nuestra-empresa/quienes-somos/historia> [Citado el 03 de junio 2015].

Grado de complejidad: El número de camas ha ido incrementando. En la actualidad tiene habilitadas 109 camas y tres quirófanos. Ofrece servicios de I, II y III nivel de complejidad con un portafolio de servicios dado por las siguientes especialidades:

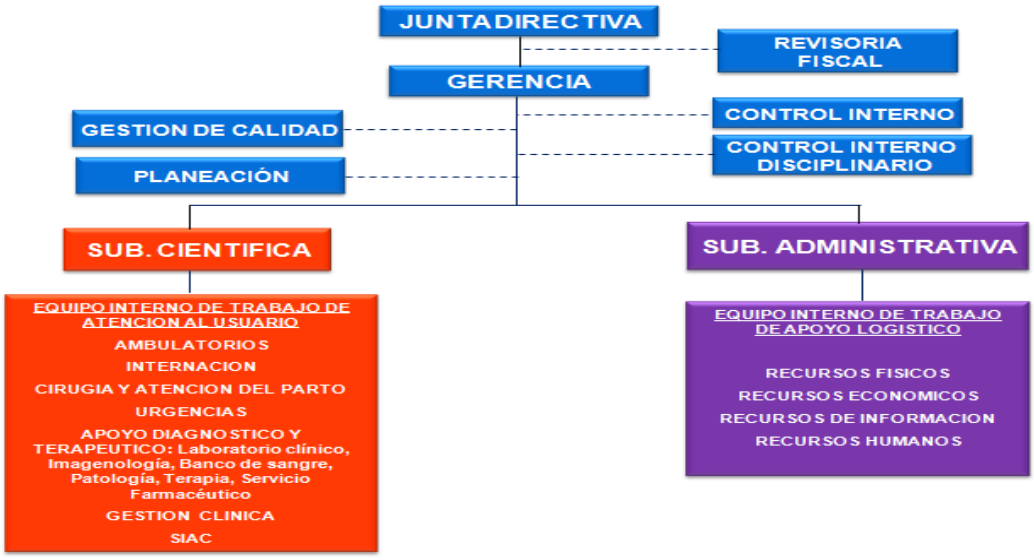
Especialidades: medicina interna, cirugía, pediatría, anestesia y ginecobstetricia, otorrinolaringología, cardiovascular las cuales han tenido continuidad dependiendo del análisis del entorno.

1.1.3 Ubicación: Ipiales, es una ciudad colombiana situada en el departamento de Nariño y cabecera del municipio del mismo nombre. Es puerto aéreo y terrestre fronterizo pues se ubica en la frontera con la república del Ecuador, en el Nudo de los Pastos, en el altiplano andino relativamente cerca a la costa del océano Pacífico, al pie de monte amazónico[2].

1.1.4 Estructura orgánica del Hospital Civil de Ipiales: en la figura 1, se puede apreciar la estructura orgánica de todo el Hospital Civil de Ipiales, en donde se observa a nivel estratégico la junta directiva y la Gerencia, y en el nivel táctico se encuentra la Subgerencia científica y Subgerencia Administrativa dentro de la cual se encuentra el equipo interno de trabajo que incluye recursos físicos, económicos, humanos y de la información dentro del cual se encuentra inmerso el Sistema de Información Hospitalario (SIHOS).

[2] SITIO OFICIAL DEL HOSPITAL CIVIL DE IPIALES NARIÑO, COLOMBIA [En Línea]. <http://www.hospitalcivilese.gov.co/site/index.php/nuestra-empresa/quienes-somos/ubicacion> [Citado en 03 de junio de 2015].

Figura 1. Organigrama del Hospital Civil De Ipiales.



Fuente: Estructura Orgánica HCI

1.2 MARCO TEÓRICO

La investigación requiere de algunos aspectos conceptuales y teóricos que soportan el desarrollo de cada uno de los temas. Por ello es importante abordar diferentes teorías entre las que se encuentran.

1.2.1 Conceptos de auditoría: es una disciplina expresada en conceptos, normas, técnicas, procedimientos y metodologías que tiene por objeto examinar y evaluar críticamente una determinada realidad, para emitir una opinión independiente, sobre un aspecto o la totalidad del objeto auditado [Echenique1992][3]. De igual manera es la evaluación que se realiza a un objeto, bajo ciertos criterios, obteniendo un diagnóstico de una situación o un proceso y generar planes de mejoramiento orientados a proponer soluciones (ANSI – Asociación Americana de Normalización).

[3] ECHENIQUE GARCIA, José Antonio. Auditoría en Informática: McGraw-Hill/interamericana Editores, S.A de C.V., 2001.Pag 2. ISBN 970-10-3356-6.

[AFNOR X50-I09] La define como la cooperación con los interesados, para verificar la concordancia de la realidad con lo preestablecido y la adecuación al objeto buscado, así como una actividad para determinar, por medio de la investigación, la adecuación de los procedimientos establecidos, instrucciones, especificaciones, codificaciones y estándares u otros requisitos, la adhesión a los mismos y la eficiencia de su implantación [ANSI N45.2.10.1973][4].

La recopilación y evaluación de datos sobre información de una entidad para determinar e informar sobre el grado de correspondencia entre la información y los criterios establecidos. La auditoría debe ser realizada por una persona competente e independiente. [Gustavo Alonso Cepeda][5].

Es la revisión independiente de diferentes actividades, funciones, especificas, resultado u operaciones de una entidad administrativa, realizada por un profesional, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones. [Carlos Muñoz Razo][6].

Para la investigación se usó lo definido por Carlos Muñoz Razo ya que se va a realizar una auditoría que permita identificar riesgos vulnerabilidades, amenazas en el Sistema de Información Hospitalaria (SIHOS) y a la vez emitir recomendaciones que sirvan para la adecuada toma de decisiones.

Después de mencionar algunas definiciones de auditoría, es pertinente conocer los tipos de auditoría ya que es importante clasificarla de acuerdo a distintos criterios.

1.2.2 Tipos de auditoría: algunos autores clasifican la auditoría de acuerdo con su lugar de aplicación, otros por su objeto de estudio o área de aplicación, a

[4] RIVAS, Gonzalo Alonso. Auditoría informática: Ediciones Díaz de Santos, S. A. Pág. 18,20. ISBN 84-87189-13.

[5] CEPEDA, Gustavo Alonso. Auditoría y control interno: McGraw-Hill, Editores, S.A de C.V., 1997.Pág 50 ISBN 958-60-060-18.

[6] MUÑOZ RAZO, Carlos. Auditoría en sistemas Computacionales: McGraw-Hill/interamericana, Editores, S.A de C.V., 2002. Pág. 11. ISBN 970-17-0405-3.

continuación se analiza la opinión de Gonzalo Alonso Rivas [2002][7] , quien las clasifica así:

- Auditoría financiera
- Auditoría organizativa
- Auditoría de gestión
- Auditoría informática

Auditoría financiera: es un procedimiento mediante el cual las empresas someten al examen de un experto (sea este de la organización o independiente de ella) su información económica, financiera, contenida esta en los estados financieros, en el estado de origen y aplicación de fondos y justificantes de los mismos, al objeto de asegurar su integridad y razonabilidad, en concordancia con los principios de contabilidad generalmente aceptados.

Auditoría organizativa: en el campo de aplicación de la auditoría organizativa entraría en el análisis de la adecuación de los procedimientos establecidos y de las funciones distribuidas físicamente, según las necesidades y problemas de la empresa.

Cuando diferentes tareas técnicas son ejecutadas por partes diferentes, parece obvia la necesidad de establecer una delimitación para cada tarea y ejercer un control riguroso de su acabado.

Auditoría de gestión: tiene por omisión conocer si las principales decisiones de gestión en la empresa han sido tomadas de una forma consiente. Entre otros aspectos estudia si las informaciones existentes son suficientes y óptimas para apoyar la decisión y si los procesos de estudio son razonables.
También se clasifica la auditoría como:

Auditoría interna:

Objetivos

[7] RIVAS, Gonzalo Alonso. AUDITORIA INFORMATICA: Ediciones Díaz de Santos, S. A. Pág. 18,20. ISBN 84-87189-13-X

- Revisión y evaluación de controles contables, financieros y operativos.
- Determinación de la utilidad de políticas, planes y procedimientos, así como su nivel de cumplimiento.
- Custodia y contabilización de activos.
- Examen de la fiabilidad de los datos.
- Divulgación de políticas y procedimientos establecidos.
- Flujo descendente desde la alta dirección hacia la dirección operativa.
- Información exacta a la gerencia.

Auditoría externa:

Objetivos

- Obtención de elementos de juicio fundamentados en la naturaleza de los hechos examinados para garantizar que han quedado significativamente probados.
- Medición de la magnitud de un error ya conocido, detección de errores
- Supuestos o confirmación de la ausencia de errores.
- Propuesta de sugerencias, en tono constructivo, para ayudar a la Gerencia.
- Detección de los hechos importantes ocurridos tras el cierre del ejercicio, teniendo en cuenta la previsible evolución de la empresa.
- Control de las actividades de investigación y desarrollo.

Auditoría informática: es la revisión técnica, especializada que se realiza a los sistemas computacionales, software, hardware e información utilizados en una empresa, sean individuales, compartidos y de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo.

Según Carlos Muñoz Razo [2002][8] en su libro: Auditoría en Sistemas Computacionales, menciona la siguiente clasificación de los tipos de auditoría:

[8] MUÑOZ RAZO, Carlos. Auditoría en sistemas Computacionales: McGraw-Hill/Interamericana editores, S.A de C.V., 2001. Pág. 12-25. ISBN 970-17-0405-3.

1.2.3 Auditoría por su área de aplicación:

Auditoría financiera: es la revisión sistemática, explicativa y critica que realiza un profesional de la contabilidad a los libros y documentos contables, a los controles y registros de las operaciones financieras y la emisión de los estados financieros de una empresa con el fin de evaluar y opinar sobre la razonabilidad, veracidad, confiabilidad y oportunidad en la emisión de los resultados financieros obtenidos durante un periodo especifico o un ejercicio fiscal.

Auditoría administrativa: es la revisión sistemática y exhaustiva que se realiza a la actividad administrativa de una empresa, en cuanto a su organización, las relaciones entre sus integrantes y el cumplimiento de las funciones y actividades que regulan sus operaciones. Su propósito es evaluar tanto el desempeño administrativo de las áreas de la empresa como la planeación y control de los procedimientos de operación, y los métodos y técnicas de trabajo establecido en la institución, incluyendo la observancia de las normas, políticas y reglamento que regulan el uso de todos sus recursos.

Auditoría operacional: en un principio formo parte de la evaluación a las operaciones contables y administrativas de las empresas, pero su peso e importancia fueron tales que fue necesario hacer auditorías a las operaciones de toda la institución, dándose así una nueva especialidad, no solo en el campo de los administradores, si no en otras ramas que la utilizan para evaluar las operaciones de cualquier área de una institución.

Auditoría integral: es la revisión exhaustiva, sistémica y global que realiza un equipo multidisciplinario de profesionales a todas las actividades y operaciones de una empresa, con el propósito de evaluar de manera integral, el correcto desarrollo de la funciones en todas sus áreas administrativas, cualesquiera que estas sean, así como de evaluar sus resultados conjuntos y relaciones de trabajo, comunicaciones y procedimientos interrelacionados que regulan la realización de las actividades compartidas para alcanzar el objetivo institucional.

1.2.4 Auditoria Por áreas específicas y especializadas:

Auditoría al área médica: es la evaluación sistemática y especializada que se realiza a las ciencias médicas y de la salud, aplicada solo por especialistas de disciplinas médicas o similares, con el fin de emitir un dictamen especializado

sobre el correcto desempeño de las funciones y actividades del personal médico, paramédico, técnicos en salud y similares, así como la atención que las dependencias y del personal de esta especialidad presentan a pacientes, familiares y proveedores.

Auditoría al desarrollo de obras y construcciones: es la revisión técnica especializada que se realiza a la edificación de construcciones y revisiones, obra negra, acabados y servicios urbanísticos complementarios de casas, edificios, puentes, caminos, presas, y cualquier otro tipo de construcción, ya sea de tipo civil o de tipo arquitectónico; cálculos y programas de obra, así como al cumplimiento y desarrollo de las mismas.

Auditoría fiscal: es la revisión pormenorizada y completa que se realiza a los registros y operaciones contables de una empresa, así como la evaluación de la correcta elaboración de los resultados financieros de un ejercicio fiscal, con el propósito de dictaminar sobre el correcto ejercicio financiero y razonabilidad en la prestación de los estados de resultado, y como consecuencia de ello , comprobar el correcto pago de los impuestos y demás contribuciones tributarias tanto de la empresa como los empleados, acreedores y compradores.

Auditoría laboral: es la revisión y evaluación especializadas que se realizan a las actividades, funciones y operaciones relacionadas con el factor humano de una empresa; su propósito es dictaminar sobre el adecuado cumplimiento en la selección , capacitación y desarrollo del personal, la correcta aplicación de las prestaciones sociales y económicas, la elaboración de los contratos colectivos e individuales de trabajo, los reglamentos internos de trabajo, normas de conducta y demás actividades que intervienen en la gestión del personal de una empresa.

1.2.5 Auditoría a los Sistemas Computacionales

Auditoría con la computadora: es la auditoría que se realiza con el apoyo de los equipos de cómputo y sus programas para evaluar cualquier tipo de actividades y operaciones, no necesariamente computarizadas, pero si susceptibles de ser

automatizadas. Dicha auditoría se realiza también a las actividades del propio centro de sistemas y a sus componentes.

Auditoría sin la computadora: es la auditoría cuyos métodos, técnicas y procedimientos están orientados únicamente a la evolución tradicional del comportamiento y validez de las transacciones económicas, administrativas y operacionales de un área de computo, y en sí de todos los aspectos que afectan a las actividades en las que se utilizan sistemas informáticos, pero dicha evaluación se realiza sin el uso de los sistemas computacionales.

Auditoría al sistema de cómputo: es la auditoría técnica y especializada que se enfoca únicamente a la evaluación del funcionamiento y uso correcto de los equipos de cómputo, su hardware, software, y periféricos asociados. Esta auditoría también se realiza a la composición y arquitectura de las partes físicas y demás componentes del hardware incluyendo equipos asociados, instalaciones y comunicaciones internas o externas así como el diseño, desarrollo y uso del software de operación, de apoyo y de aplicación, ya sean sistemas operativos, lenguajes de procesamiento y programas de desarrollo o paquetería de aplicación institucional que se utiliza en la empresa.

Auditoría a la gestión informática: es la auditoría cuya aplicación se enfoca exclusivamente a la revisión de las funciones y actividades de tipo administrativo que se realizan dentro de un centro de cómputo, tales como la planeación, organización, dirección y control de dicho centro. Esta auditoría se realiza también con el fin de verificar el cumplimiento de funciones y actividades asignadas a los funcionarios, empleados, y usuarios de las áreas de sistematización, así como para revisar y evaluar las operaciones del sistema, el uso y protección de los sistemas de procesamiento, los programas y la información.

Auditoría de la seguridad de sistemas computacionales: es la revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema de cómputo, sus áreas y personal, así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a salvaguardar la seguridad de los equipos computacionales, las bases de datos, redes, instalaciones y usuarios del sistema. Es también la revisión de planes de contingencia y medidas de protecciones para la información, los usuarios y los propios sistemas computacionales.

Auditoría a los sistemas de redes: es la revisión exhaustiva, especifica y especializada que se realiza a los sistemas redes de una empresa, considerando en la evaluación los tipos de redes, arquitectura, topología, sus protocolos de comunicación, las conexiones, accesos, privilegios, administración y además aspectos que repercuten en su instalación, administración. Funcionamiento y aprovechamiento. Es la revisión del software institucional, de los recursos informáticos e información de las operaciones, actividades y funciones que permiten compartir las bases de datos, instalaciones, software y hardware de un sistema en red.

Con las anteriores clasificaciones se puede decir que la auditoría es muy extensa y cada autor la puede clasificar de diferente manera, de acuerdo con el ambiente en el que se encuentre.

El trabajo por su objeto de estudio abordará temas de auditoría informática desde el estándar COBIT 4.1 ya que se evaluará la eficiencia y la eficacia del Sistema de Información Hospitalaria (SIHOS) analizando ciertas características como son confiabilidad funcionalidad usabilidad portabilidad accesibilidad que son de gran importancia para el buen desempeño de los sistemas de información pues proporcionan los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.

Después de haber estudiado los tipos de auditoría es necesario profundizar en el tema de auditoría informática.

Auditoría Informática: Gonzalo Alonso Rivas [1988][9] define la auditoría informática como un examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual y de modo discontinuo, a instancias de la Dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia, y la rentabilidad del servicio, o del sistema, que resultan auditados.

Echenique García José Antonio [2001][10], define la auditoría en informática como la revisión y evaluación de los controles, sistemas y procedimientos de la informática, de los equipos de cómputo, su utilización, eficiencia y seguridad de la

[9] RIVAS, Gonzalo Alonso. Auditoría Informática: Ediciones Díaz de Santos, S. A. Pág. 39-40. ISBN 84-87189-13-X.

[10] ECHENIQUE GARCIA, José Antonio. Auditoría en Informática: McGraw-Hill/Interamericana editores, S.A de C.V., 2001. Pág. 2. ISBN 970-10-3356-6.

organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de recursos alternativos se logre una utilización más eficiente, confiable y segura de la información que servirá para una adecuada toma de decisiones.

Este trabajo se ubica dentro de una auditoría informática ya que permite detectar de forma sistemática el uso de los recursos y los flujos de información dentro de cualquier organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, que obstaculizan el manejo de información. Su objetivo es verificar y asegurar que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología informática en la organización se realicen de manera eficiente y eficaz.

Teniendo en cuenta que la información es de suma importancia para cualquier organización, un sistema de información es una herramienta muy útil para todas las empresas, ya que con su aplicación se logra obtener un mejor manejo de la toda la información que se genere para poder utilizarla cuando se crea necesario. De allí se hace necesario enfatizar en los temas de Sistemas de Información a fin de tener conceptos acertados de la utilidad y el funcionamiento de estos en cualquier empresa.

1.2.6 Fases de la auditoría: Echenique define que la auditoría se sigue por las siguientes fases:

Visita Preliminar: en esta etapa se obtiene un marco contextual que incluye toda la información relativa de la empresa a auditar como la ubicación de la empresa, su estructura organizacional, sus planes y proyectos, recursos etc.

Planeación de la auditoría: en esta fase se definen los objetivos de la auditoría, el alcance o las áreas a cubrir en la realización de esta, los recursos tecnológicos, económicos, el talento humano además se define el cronograma, el presupuesto y los resultados esperados con la auditoría.

Ejecución de la auditoría: se ejecutan el plan de auditoría, se hace el levantamiento de hallazgos y evidencias.

Síntesis y diagnóstico: se analiza e interpreta los datos obtenidos en la fase anterior y se compara o se realizan estadísticas de lo encontrado. En esta fase

quedan definidos los puntos débiles, los riesgos y las fortalezas de la organización.

Informe final: en esta fase se elabora un documento que contiene los hallazgos y evidencias, las conclusiones de los hallazgos debidamente argumentadas y soportadas. Se debe realizar la carta de presentación del documento, la introducción del informe, las principales observaciones, recomendaciones.

También cabe destacar la importancia de realizar estas fases de auditoría que permitirán realizar un diagnóstico más ordenado y detallado de la auditoría al Sistema de Información Hospitalaria (SIHOS).

1.2.7 Definición de sistemas de información: el Sistema de Información es un proceso de planificación diseño análisis y control de los datos, que afecta a todo el núcleo de la actividad empresarial y es el encargado de coordinar los flujos y registros de la información tanto internas, como la proveniente del entorno, que son necesarias para realizar las operaciones básicas y toma de decisiones para conseguir los objetivos de la empresa. Este proceso se realiza de forma conjunta con el proceso de actividades propias de la empresa y sirve de apoyo a las decisiones de planificación, diseño, ejecución, y control que realiza.

1.2.7.1 Tipos de sistemas de información:

Los tipos de sistemas de información son los siguientes:

- Sistemas Económicos-financieros.
- Sistemas Administrativos.
- Sistemas para Registro Central de pacientes.
- Sistema de Manejo de Materiales.

Los sistemas económico-financieros en medicina, llamados sistemas de economía Médica se clasifican en:

- Sistemas de nómina y de personal.
- Sistema de manejo de materiales.
- Sistema de cargos y cobros.
- Sistema de pagos.
- Sistema de contabilidad.

Los sistemas administrativos, según Huesing[11], se clasifican en:

- Sistema para registro central de pacientes.
- Sistema para admisión, altas y transferencias de pacientes.
- Sistema para el control de citas y programación de servicios.
- Sistema para el procesamiento y edición de documentos (historias clínicas, reportes, recetas, etc.).

1.2.7.2 Funciones de un sistema de información: el Sistema de Información lleva a cabo una serie de funciones que se pueden agrupar en cuatro grandes grupos[12]:

- Funciones de captación y recolección de datos.
- Almacenamiento de la información.
- Tratamiento de la información.
- Distribución de la Información.

Captación y recolección de datos: recoge la información externa (o del entorno) e interna, enviando dicha información a través del SC a los órganos del SI, encargados de reagruparla, para evitar duplicidades e información inútil o ruido, la captación de información depende del tipo de empresa o del destino que se espera de la información.

Almacenamiento: una vez filtrada la información relevante, ésta se almacenará, puede ser en un lugar único (archivo central, sistema informático), accesible a todos los usuarios, o bien en los distintos departamentos, pero igualmente accesible a cualquier usuario que la necesite.

Tratamiento de la información: es la función clave del Sistema de Información tiene por objeto transformar los datos de la información almacenada en información significativa, para ofrecérsela a quien la necesite, en la medida y formato que el usuario requiera. Generalmente en esta función, se utilizan medios informáticos por su capacidad de almacenar y velocidad en el tratamiento, así como la reducción de costes que representan.

[11] Huesing, S.A., Administrative and Financial Systems, North-Holland, 1983, pág. 208-211.

[12] CORPORACIÓN UNIVERSITARIA DEL CARIBE. Dirección de Educación abierta y a distancia y virtualidad: Equipo de Edición SIERRA, Kadi, GONZALES, Rafael. MARQUINEZ, Leidy, 2013.Pág 20-23

Distribución y diseminación: es muy importante para la empresa que cada usuario posea la información requerida en el momento preciso y de una forma normalizada para su correcta interpretación, además existe la necesidad de que alguna información acerca de la empresa y su entorno sean conocidas por diferentes miembros de la organización, para hacer frente con rapidez de forma conjunta a las situaciones que se presenten.

1.2.7.3 Objetivos de los sistemas de información: durante los próximos años, los Sistemas de Información cumplirán tres objetivos básicos dentro de las organizaciones:

- Automatización de procesos operativos.
- Proporcionar información que sirva de apoyo al proceso de toma de decisiones.
- Lograr ventajas competitivas a través de su implantación y uso.

En este trabajo es necesario presentar algunos fundamentos generales en el tema que comprende al surgimiento y evolución y que han venido sufriendo los Sistemas de Información en la sociedad.

1.2.7.4 Historia y evolución de los Sistemas de Información Hospitalarios:

Según Kaplan [1988][13] la historia de los Sistemas de Información Hospitalarios es en realidad la historia de los Sistemas de Información en el campo de la salud, ya que fue el entorno hospitalario donde primero se implantaron.

Durante las décadas de los 50 y de los 60, los sistemas de información se introdujeron casi exclusivamente por necesidades financieras y de gestión económica de los centros. Estos sistemas se centraban en recoger datos demográficos del paciente y mezclarlos con datos de costes para producir facturas. Así pues, se desarrollaron sistemas de facturación y de contabilidad.

Este período viene caracterizado por los grandes sistemas informáticos (mainframes), que a su vez eran muy costosos. La incapacidad de muchos Hospitales para soportar estos costos tan altos, llevaron a la necesidad y al éxito de los sistemas compartidos.

Un Sistema de Información Hospitalario típico de los 60 tenía poco de sistema clínico, ya que el énfasis estaba puesto en la contabilidad, nóminas y recursos humanos. Los únicos sistemas clínicos que se desarrollaron fueron sistemas de registros de pacientes que recogían sobre todo datos con los que estudiar diagnósticos y tomar decisiones para mejorar la precisión diagnóstica, para tomar decisiones clínicas más fiables y para aumentar la comprensión de la estructura del conocimiento médico de tal manera que se pudieran tomar mejores decisiones y mejores métodos de diagnóstico.

En la década de los 70, comenzaron a dejarse sentir con más fuerza las necesidades clínicas, pero principalmente como un producto de las necesidades financieras. Estas cuestiones financieras se centraban en maximizar los ingresos y capturar los costes, y los sistemas de atención al paciente eran capaces de servir como vehículo para documentar las órdenes y peticiones, e indirectamente, sus costes. Sin embargo, con este objetivo financiero continuo, se hizo poco esfuerzo para tratar las necesidades de los médicos y enfermeras implicados en la atención directa al paciente. El crecimiento de los sistemas departamentales coincidió con la disponibilidad de los miniordenadores, de menor coste que los mainframes. Los hospitales estaban ya experimentando una necesidad creciente de datos de servicios específicos y del hospital en conjunto.

[13] KAPLAN B. Development and acceptance of Medical Information systems,1988.Pág. 9-29.

La década de los 80, impulsó un cambio dramático de maximizar los ingresos a maximizar el reembolso. Se comenzó a presionar para mejorar la coordinación entre diferentes servicios y para reducir la estancia. Cada vez cobraba mayor importancia la contención de costes, los sistemas de pago prospectivo, la revisión de utilización. Los servicios clínicos comenzaron a recibir mayor presión para mejorar la productividad. Pero un hecho clave en el crecimiento de los sistemas departamentales fue el desarrollo de los microordenadores y de los lenguajes de programación de 4ª generación, que trajeron un mayor acceso a los datos a un menor coste. Un sistema de Información Hospitalario típico de los 80 estaba formado por un sistema de contabilidad y un sistema de atención al paciente.

En la década de los 90, los sistemas se mueven en la dirección de centrarse sobre el paciente y estar orientados clínicamente, estos sistemas no ven al paciente como una colección de números o episodios, sino como un flujo continuo de datos. Se podrá conseguir más información desde el punto mismo de asistencia, y los sistemas mejorarán la comunicación proveedor-paciente.

Los sistemas clínicos de atención al paciente deben de tratar sobre los procesos clínicos y servir de apoyo a la toma de decisiones de los médicos.

[Dowling, 1989][14], declaró que “el proceso de producción principal de un Hospital es la asistencia al paciente, no el proceso financiero”. De aquí, que el núcleo de la arquitectura de los sistemas de información deba de ser los procesos clínicos: valoración, planificación del alta, planificación del tratamiento, entrada de peticiones y órdenes, informes de resultados, acceso a datos clínicos del paciente, historias clínicas electrónicas y acceso a la literatura médica.

Por lo tanto, la conexión en el Hospital de diferentes puestos de trabajo a través de redes informáticas es el presente/futuro esta conectividad permitirá transferir datos o compartirlos entre diferentes aplicaciones. El elemento principal de la

[14] SALVADOR OLIVÁN, José Antonio. El sistema de Información CMBD como Herramienta de Control y Gestión Hospitalaria, Tesis Doctoral, Univ. de Zaragoza, 1997.Pág 6.

estructura de estas redes será la fibra óptica, de gran velocidad de transmisión. Existirán nodos para acceder a bases de datos externas y para comunicarse con otros hospitales u otras instalaciones; se podrán transmitir imágenes entre diferentes ciudades y países.

Sistema de información hospitalaria: es un sistema de información orientado a satisfacer las necesidades de generación de información, para almacenar, procesar e interpretar datos médicos-administrativos de cualquier institución hospitalaria. Permitiendo la optimización de los recursos humanos y materiales, además de minimizar los inconvenientes burocráticos que enfrentan los pacientes.[15]

Todo Sistema de Información Hospitalaria genera reportes e informes dependiendo del área o servicio para el cual se requiera, dando lugar a la retroalimentación de la calidad de la atención de los servicios de salud.

Objetivos de los sistemas de información hospitalarios: de acuerdo con [Collen 1988][16], los objetivos básicos de un Sistema de Información Hospitalario son los siguientes:

Establecer una base de datos capaz de proporcionar un registro médico integrado de datos asistenciales para todos los pacientes, y que sea accesible para todos los profesionales médicos y de la salud debidamente autorizada.

Posibilidad de comunicar los datos del paciente desde todos los servicios administrativos y clínicos del Hospital.

Soportar todas las funciones del proveedor de asistencia sanitaria, incluyendo la entrada de órdenes, informes de resultados, historia del paciente, informes de procedimientos, y comunicar datos individuales del paciente a los profesionales sanitarios.

Proporcionar apoyo en la toma de decisiones clínica y administrativa.

---

[15] LARA, Florina, FERNANDEZ PUERTO, Fernando. Sistema de Información Hospitalaria: Edición Lic. Ana María Hernández López, México, D.F., 200. Pág. 1.

[16] COLLEN, M.F. (1988). HIS concepts, goals and objectives: Towards new Hospital Information systems. The Netherlands: Elsevier Science Publishers, 1988. Pág. 3-9.

Establecer y mantener ficheros para las funciones administrativas y de gestión hospitalaria, incluyendo aplicaciones de personal, recursos, programación y registro.

Ayuda en la evaluación de la calidad, acreditación y requisitos reguladores.
Apoyo a la investigación y educación.

La auditoría se realiza teniendo en cuenta algunas fases, que se deben comprender y seguir de manera ordenada. Para ello, se hace necesario apoyarse en estándares que guían la planificación y ejecución de la auditoría.

1.2.8 Estándares internacionales de auditoría: para todo tipo de trabajos enfocados en la auditoría informática se han implementado diferentes estándares que apoyan la ejecución de auditorías y permiten a cualquier empresa alinear sus estrategias con las tecnologías de información entre ellas se encuentran:

1.2.8.1 Coso (Committee Of Sponsoring Organizations) : Según Yeimi Karina Reyes Morales [2013][17], es una iniciativa conjunta de las cinco organizaciones que dedica a proveer liderazgo a través del desarrollo de los marcos y directrices sobre la gestión del riesgo, control interno y la disuasión del fraude. La gestión de riesgos empresariales es un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos y está completamente ligado con el COSO, las mejoras en la gestión de riesgo permitirán mejorar, aún más, sobre la inversión ya realizada en control interno bajo las disposiciones de la Ley Sarbanes Oxley.

La misión es proporcionar liderazgo a través del desarrollo de los marcos generales y orientación sobre la gestión del riesgo empresarial, control interno y la disuasión del fraude diseñada para mejorar el desempeño organizacional y la gestión y reducir el alcance del fraude en las organizaciones.
El Informe COSO[18], es un documento que contiene las principales directivas para la implantación, gestión y control de un sistema de Control Interno. Debido a la gran aceptación de la que ha gozado, desde su publicación en 1992, el Informe

[17] REYES MORALES, Yeimi Karina, Universidad de San Carlos de Guatemala. Pàg. 66.
[18] LUPPI, Heddy. Control Interno Hoy. [En línea] < http://controlinternohoy.blogspot.com/2010/10/el-informe-coso.html> [consulado 8 marzo de 2015].

COSO se ha convertido en el estándar de referencia en todo lo que concierne al Control Interno.

COSO define el Control Interno como un proceso que garantice, con una seguridad razonable (y por lo tanto no absoluta), que se alcanzan los tres objetivos siguientes:

- Eficacia y eficiencia de las operaciones
- Fiabilidad de la información financiera
- Cumplimiento de las leyes y normas que sean aplicables.

A la hora de realizar una auditoría es conveniente descomponer los tres objetivos anteriores en los siguientes:

- Eficacia de las operaciones
- Eficiencia de las operaciones
- Fiabilidad de la información financiera
- Fiabilidad de la información operativa y de gestión
- Salvaguardia de los activos

Los cinco elementos del Control Interno interactúan entre sí, y forman un sistema. Este sistema debe estar integrado (no solo simplemente superpuesto) a las actividades operativas de la empresa. Cuanto más integrado esté el sistema de Control Interno con las actividades de la empresa, tanto mayores serán las posibilidades de éxito del mismo.

Todos los miembros de la organización son responsables de la implantación y correcto funcionamiento del sistema de Control Interno.

El Informe COSO consta de dos partes:

- Un resumen para la Dirección, que introduce los principales conceptos.
- Un marco integrado de referencia, donde se analizan en detalle los cinco pilares del Control Interno como son: entorno de Control, evaluación de los riesgos, actividades de control, información y comunicación, supervisión.

1.2.8.2 Iso (International Standart Organization): ISO[19] (**International Organization for Standardization**) e IEC (Comisión Internacional de Electrotecnia) conforman un sistema especializado para los estándares mundiales, Organizativos nacionales que son miembros de ISO o IEC participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos por la organización respectiva para tratar con los campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en relación con ISO e IEC, también forman parte del trabajo.
ISO es una organización especializada en el desarrollo y difusión de los estándares a nivel mundial.

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Muchos de ellos no están aún publicados, pero la estructura ya está definida.

ISO/IEC 27000[20] fue diseñada para Sistemas de Gestión de Seguridad de la Información, generalidades y vocabulario, publicada en Abril del 2009, en la que se recogen los términos y conceptos relacionados con la seguridad de la información, una visión general de la familia de estándares de esta área, una introducción a los SGSI, y una descripción del ciclo de mejora continua.

Esta norma se basa en que “La información es un activo importante vital para el éxito y continuidad en el mercado de cualquier organización”. El aseguramiento de dicha información y de los sistemas que la procesan, es por tanto un objetivo de primer nivel para la organización. Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una manera metódica, documentada y basada en unos objetivos claros de seguridad y

[19] HEREDIA VIVEROS Nora Ligia. Gerencia de Compras la nueva Estrategia Competitiva Ediciones primera Edición Bogotá D.C., ISBN 978-958-648-842-6.

[20] CORLETTI ESTRADA, Alejandro. Seguridad por Niveles. Ediciones primeras Edición, Pág. 511. Madrid, septiembre de 2011.[en línea] <http://www.DarFe.es>.

una evaluación de los riesgos a los que está sometida la información de la organización. ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO/IEC que proporcionan un marco de gestión de seguridad de la información utilizable por cualquier tipo de organización, pública o privada grande o pequeña.

UNE-ISO/IEC 27001 Especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) de acuerdo a la Norma ISO 27002 dentro del contexto de los riesgos identificados por la Organización. Esta es la norma fundamental, ya que contiene los requerimientos del sistema de gestión de seguridad de la información y es la norma con arreglo a la cual serán certificados los SGSI de las organizaciones que lo deseen.

Asimismo está basada en un enfoque por procesos y en la mejora continua, por lo tanto es perfectamente compatible e integrable con el resto de sistemas de gestión que ya existan en la organización. La Norma asume que la organización identifica y administra cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas, puede ser considerada como un "proceso". A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos. Estos procesos se someten a revisiones para detectar fallos e identificar mejoras, por lo que se encuentran dentro de un proceso de mejora continua.

La Norma recoge:

- Los componentes del SGSI, es decir, en qué consiste la parte documental del sistema: qué documentos mínimos deben formar parte del SGSI cómo se deben crear, gestionar y mantener y cuáles son los registros que permitirán evidenciar el buen funcionamiento del sistema.
- Cómo se debe diseñar e implantar el SGSI.
- Define los controles de seguridad a considerar. Se requiere que se escojan los controles del Anexo A, que recoge todos los controles detallados en la Norma ISO/IEC 27002.
- Cómo debe realizarse la revisión y mejora del SGSI.

La ISO 27001 adopta un proceso para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI en una organización.

ISO/IEC27002[21], nace como modelo para gestionar la seguridad de la información y, no se refiere a un contexto específico, es decir, que el modelo también es aplicable fuera de los sistemas informáticos, siendo la información entendida como independiente de los soportes y de las infraestructuras.

En general se puede afirmar que el modelo es aplicable a cualquier contexto productivo y a cualquier tipo de organización simple o compleja, pública o privada, informatizada o no.

El estándar ISO/IEC 27001:05 define los requisitos aplicativos para un SGSI. Dichos requisitos son utilizables tanto para la implementación como para la auditoría de los SGSI.

ISO/IEC 27003[22], se centra en los aspectos críticos necesarios para el exitoso diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con la norma ISO / IEC 27001:2005. Describe el proceso de delimitación de un SGSI, y el diseño y puesta en marcha de diferentes planes de implementación. Igualmente incluye el proceso para obtener la aprobación de la Gerencia para implementar un SGSI, define un alcance inicial del SGSI, y proporciona una guía de cómo hacer desde la planeación inicial hasta la Implementación final de un proyecto SGSI.

ISO27004 tiene por objeto ayudar a las organizaciones a medir, informar y, por tanto, mejorar sistemáticamente la eficacia de sus sistemas de gestión de seguridad de información.

Ofrece orientación sobre el desarrollo y uso de las medidas y la medición con el fin de evaluar la eficacia de un sistema de gestión de seguridad de la información en práctica (ISMS) y controles o grupos de controles, como se especifica en la norma ISO/IEC 27001 . Esto incluiría la política, la información gestión de riesgos de seguridad, objetivos de control, controles, procesos y procedimientos, y apoyar el proceso de su revisión, lo que ayuda a determinar si alguno de los SGSI procesos o controles tienen que ser cambiado o mejorado.

[21] ISO I/IEC 27002. [En línea] <http://orcilatam.com/isoiec-27002/> [consultado 08 marzo 2015].

[22] Guía para la Implementación de un Sistema de Gestión de Seguridad de la Información. [En línea] <http://seguridadinformacioncolombia.blogspot.com/2010/02/publicada-la-iso-27003-2010-guia-para.html> [citado 10 de marzo de 2015].

1.2.8.3 Cobit:[23] (Objectives for Information Systems and Related Technology), es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información, (ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992.

El objetivo principal de COBIT consiste en proporcionar una guía a alto nivel sobre puntos en los que establece controles internos con tal de asegurar el buen gobierno, proteger los intereses de los stakeholders (clientes, accionistas, empleados, etc.) garantizar el cumplimiento normativo del sector al que pertenezca la organización, mejorar tanto en eficacia como en eficiencia de los procesos y actividades de la organización, y garantizar la confidencialidad, integridad y disponibilidad de la información.

COBIT brinda buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control. Estas prácticas ayudan a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindan una medida contra la cual juzgar cuando las cosas no vayan bien.

Para que TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

- Establece un vínculo con los requerimientos del negocio
- Organiza las actividades de TI en un modelo de procesos generalmente aceptado.
- Identifica los principales recursos de TI a ser utilizados.
- Define los objetivos de control gerenciales a ser considerados.

[23] IT Governance Institute. COBIT 4.1. 2007. [En línea] <http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf> [citado 15 de marzo de 2015].

La orientación al negocio que enfoca COBIT consiste en alinear las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de la TI. Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infra-estructura y personas.

"La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyan al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

Criterios de información COBIT: para satisfacer los objetivos de negocio, la información necesita dar conformidad a ciertos criterios de control, a los cuales COBIT se refiere como requerimientos de información de negocios, se define siete criterios de información.

- **Eficiencia:** Información relevante a los procesos de negocios y su entrega a tiempo, correcta, consistente y usable.

- **Integridad:** Exactitud y completitud de la información y su validez de acuerdo a los valores y expectativas de negocio.

- **Disponibilidad:** Que la información esté disponible en el momento requerido por el proceso de negocios.

- **Conformidad:** Se ocupa de cumplir con las leyes, regulaciones y contratos a los cuales están sujetos los procesos de negocios.

- **Confiabilidad:** Provisión de información apropiada a la gerencia para manipular la organización.

COBIT define las actividades de TI en un modelo de procesos genéricos que son cuatro dominios.

- **PLANEAR Y ORGANIZAR (PO)**: Este dominio cubre estrategias y tácticas, y se preocupa en identificar la manera en que las TI pueden contribuir, mejorar y alcanzar sus objetivos.

- **ADQUIRIR E IMPLEMENTAR (AI):** Para realizar la estrategia de TI, se necesita identificar soluciones de TI así como también implementarlas e integrarlas en el proceso de negocio.

- **ENTREGAR YSOPORTAR (DS):** Esta dominio trata de la entrega real de los servicios requeridos, lo cual incluye entrega, gestión de seguridad y continuidad, soporte de servicios, gestión de datos y suministros operativos.

- **MONITOREAR Y EVALUAR (ME):** Este dominio trata de la gestión funcionamiento, monitoreo de control interno, conformidad regulatoria y gobierno de aprovisionamiento.

1.2.8.4 Magerit: Según Fernando García Rubio[24] MAGERIT es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las administraciones públicas, ha sido elaborado por un equipo multidisciplinar del comité técnico de seguridad de los sistemas de información y tratamiento automatizado de datos personales, SSITAD, del Concejo Superior de Informática, siendo sus objetivos: estudiar los riesgos que se encuentren en el sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la valoración del impacto de seguridad en las organizaciones, señalar riesgos existentes identificando las amenazas que acechan al sistema de información y determinan la vulnerabilidad del sistema de producción de dichas amenazas, obteniendo unos resultados. Los resultados del análisis de riesgo permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir y controlar los riesgos identificados y así reducir a lo mínimo su potencialidad o sus posibles perjuicios.

[24] GARCIA RUBIO, Fernando. Las Nuevas Tecnologías ante el Derecho y la Organización administrativa. Instituto Nacional de Administración Pública, 2003. Pág. 80. ISBN 8470887343

El Congreso Superior de informática ha elaborado la metodología de análisis y Gestión de Riesgos de los sistemas de información de las Administraciones Publicas, MAGERIT, cuya utilización promueve, como respuesta a la dependencia creciente de estas (y en general de toda la sociedad) de las tecnologías de información.

Así mismo, Juan Desongles Corrale[25] define MAGERIT como un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

La aplicación de MAGERIT, permite:

- Aportar racionalidad en el conocimiento del estado de seguridad de los Sistemas de Información y en la introducción de medidas de seguridad.
- Ayudar a garantizar una adecuada cobertura en extensión, de forma que no haya elementos del sistema de información que queden fuera del análisis, y en intensidad, de forma que se alcance la profundidad necesaria en el análisis del sistema.
- Para hallar las insuficiencias de los sistemas vigentes.
- Asegurar el desarrollo de cualquier tipo de sistemas, reformados o nuevos, en todas las fases de su ciclo de desarrollo, desde la planificación hasta la implantación y el mantenimiento.

MAGERIT responde a las necesidades de un espectro amplio de intereses de usuarios con un enfoque de adaptación a cada organización y a sensibilidades diferentes en seguridad de los Sistemas de Información. Las diferencias residen en tres cuestiones fundamentales:

- Situación dentro del “ciclo de estudio”: Marco estratégico, planes globales, análisis de grupos de múltiples activos, gestión de riesgos de activos concretos, determinación de mecanismos específicos de salvaguarda.
- Envergadura: Complejidad e incertidumbre relativas del sistema estudiado, tipo de estudio más adecuado a la situación: corto, simplificado, etc.

[25] DESONGLES CORRALE, Juan. Ayudante técnico de Informática de la junta de Andalucía. Editorial MAD, S.L, 2005. Pàg. 363-366. ISBN: 84-665-201-39N.

- Problemas específicos a solventar: Seguridad lógica, Seguridad de Redes y Comunicaciones, Planes de Emergencia y Contingencia, Estudios técnicos para homologación de sistemas o productos, Auditorías de seguridad.
- El modelo normativo de MAGERIT se apoya en tres submodelos: El submodelo de elementos proporciona los componentes que el submodelo de eventos va a relacionar entre sí, mientras que el submodelo de procesos será la descripción funcional del proyecto de seguridad a construir.

Para realizar esta evaluación y el posterior diagnóstico, al Sistema de Información Hospitalaria (SIHOS) dispone de una metodología que toma COBIT 4.1 como marco de referencia ya que es un modelo para auditar la gestión y control de los sistemas de información y tecnología orientados a todos los sectores de cualquier organización y permite la definición de prioridades de implementación, mejora y aseguramiento del gobierno de las TI, que se basa en metas corporativas de la institución y el riesgo relacionado. Además propone un ciclo de vida de mejoramiento continuo es decir una guía para evitar los obstáculos, aprovechar las mejores prácticas y ayudar en la creación de resultados satisfactorios.

Tomando como referente COBIT 4.1 para seguir el proceso de planeación y ejecución de la auditoría se procederá a implementar las fases de auditoría.

1.3 MARCO CONCEPTUAL

Para la presente investigación es necesario contribuir con conceptos que se usan dentro trabajo y que requieren ser explicados. Entre ellos se tienen:

Amenaza: representa un peligro latente asociado con un fenómeno físico de origen natural que puede presentarse en un sitio específico y en un tiempo determinado, los bienes y/o el medio ambiente. Se debe tener en cuenta entre otros aspectos su dinámica, características, comportamiento histórico, potencialidad y área de influencia.

Según [ISO/IEC 13335-1:2004] Causa potencial de un incidente no deseado, el cual puede causar daño a un sistema.

Una amenaza informática es un posible peligro del sistema. Posibles atacantes o factores que aprovechan las debilidades del sistema.

En sistemas de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, maquinas o sucesos) que de tener la oportunidad atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad.

Análisis de Riesgos: es una herramienta de diagnóstico que permite establecer la exposición real a los riesgos por parte de una organización. Este análisis tiene como objetivos la identificación de los riesgos (mediante la identificación de sus elementos), lograr establecer el riesgo total y posteriormente el riesgo residual luego de aplicadas las contramedidas en términos cuantitativos o cualitativos.

El riesgo total es la combinación de los elementos que lo conforman, calculando el valor del impacto por la probabilidad de ocurrencia de la amenaza y cuál es el activo que ha sido impactado. Presentado en una ecuación matemática para la combinación válida de activos y amenazas:

RT (riesgo total) = probabilidad x impacto

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel del riesgo asumido.

El control es el proceso de verificar el desempeño de distintas áreas o funciones de una organización. Usualmente implica una comparación entre un rendimiento esperado y un rendimiento observado, para verificar si se están cumpliendo los objetivos de forma eficiente y eficaz y tomar acciones correctivas cuando sea necesario.

Existen tres clases de control los cuales son control correctivo, detectivo y preventivo

Confiabilidad: la capacidad para mantener su nivel de desempeño cuando es utilizado bajo condiciones especificadas (durante un determinado período de tiempo). El producto será confiable siempre y cuando el usuario pueda tener siempre la certeza de que su información estará protegida ante cualquier tipo de falla, garantizando que los datos estarán disponibles en el momento en el que se requieran. Entre las características de la confiabilidad están

- Madurez.
- Tolerancia a fallas.
- Recuperabilidad.
- Conformidad.

Disponibilidad: la información puede estar sana y salva en el sistema, pero de poco sirve si los usuarios no tienen acceso a ella. La disponibilidad significa que los recursos del sistema, tanto de hardware como de software, se mantendrán funcionando de forma eficiente, y que los usuarios lo podrán utilizar en el momento que lo necesiten. También significa que el sistema sea capaz de recuperarse rápidamente en caso de ocurrir un problema de cualquier índole.

Eficiencia: capacidad para proporcionar un desempeño apropiado, en relación con la cantidad de recursos utilizados, bajo condiciones establecidas en determinado momento del tiempo.

La eficiencia evalúa el comportamiento en el tiempo al igual que el consumo de los recursos y los estándares establecidos.

Las características que se evalúan en la eficiencia son: comportamiento en el tiempo, consumo de recursos y conformidad.

Seguridad informática: la seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización información. Es el objeto de mayor valor para una organización es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico programas maliciosos programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema.

Según Harold F y Micki Krause[26] La seguridad informática puede ser definida, básicamente, como la preservación de la confidencialidad, la integridad y la disponibilidad de los sistemas de información. Dependiendo del entorno de la organización, se puede tener diferentes amenazas que comprometan a los

[26] HAROLD F, MICKI KRAUSE Tipton (ends), Information Security Management Handbook, 5th Ed, CRC Press, 2006.

objetivos. Ante un riesgo la organización tiene tres alternativas, aceptar el riego, hacer algo para disminuir la posibilidad de ocurrencia del riesgo o transferir el riego, mediante un contrato de seguro.

Usabilidad: la capacidad del producto para ser comprendido, aprendido, utilizado y ser atractivo para el usuario cuando es utilizado bajo condiciones especificadas. La usabilidad de un sistema pretende determinar qué tan fácil es para un usuario, independiente del tipo de usuario que sea, enfrentarse al producto de software.

Capacidad de un producto de software para permitirle al usuario conocer cómo puede utilizar el sistema, qué tareas puede llevar a cabo, cuáles son sus condiciones de uso y cuáles de ellas son necesarias para que pueda desenvolverse de una manera adecuada cuando se encuentre navegando en el mismo.

Las características que hacen parte de la usabilidad son:

- Comprensibilidad.
- Facilidad de aprendizaje.
- Operatividad.
- Conformidad.

Vulnerabilidad: predisposición intrínseca de un sujeto o elemento a sufrir daño debido a posibles acciones externas. Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004][27].

Son ciertas condiciones inherentes a los activos, o presentes en su entorno, que facilitan que las amenazas se materialicen y los llevan a la condición de vulnerabilidad. Las vulnerabilidades son de diversos tipos como por ejemplo: la falta de conocimiento de un usuario, la transmisión a través de redes públicas, entre otros.

Dentro de la investigación se utilizó estos conceptos por lo que es importante mencionarlos y realizar una descripción breve de estos.

[27] Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la tecnología de la información y las comunicaciones. ISO/IEC 13335-1,2004

1.4. MARCO LEGAL

El trabajo de investigación contiene algunos aspectos de tipo legal como son la ley de delitos informáticos, ley 1273 de 2009, la ley de protección de datos que se las menciona a continuación.

1.4.1 Ley 1273 de 2009: por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se reservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se protejan jurídicamente para evitar incurrir en alguno de estos tipos penales.

Cabe destacar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo.

De ahí la importancia de esta ley, ya que consiste en controlar la integridad, confidencialidad y la disponibilidad de los datos y de los sistemas informáticos de los atentados informáticos y otras infracciones.

Esta ley contribuye a la investigación ya que permite establecer un marco de trabajo a fin de proteger los activos informáticos estipulados dentro de esta ley. Además los posibles riesgos y vulnerabilidades que se identifiquen al Sistema de Información Hospitalaria (SIHOS), permitirán a la institución tomar decisiones basados en dicha ley.

1.4.2 Ley 1581 de 2012: por la cual se dictan disposiciones generales para la protección de datos personales". Que busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada.

Esta Ley tiene como fin esencial salvaguardar los derechos y deberes fundamentales, así como los procedimientos y recursos para su protección. La Jurisprudencia Constitucional trató desde el inicio el derecho al hábeas data como una garantía del derecho a la intimidad, de allí que se hablaba de la protección de los datos que pertenecen a la vida privada y familiar, en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir. Actualmente el hábeas data es un derecho autónomo, compuesto por la autodeterminación informática y la libertad (incluida la libertad económica). Este derecho como fundamental autónomo, requiere una efectiva protección de mecanismos que lo garanticen.

Dentro de los contenidos que se desprenden del derecho de hábeas data se encuentra que las personas tienen la facultad de conocer el acceso a la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las mismas donde se encuentra dicha información; tienen además, el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular, salvo las excepciones previstas en la norma.

La ley tiene como objetivo facilitar la implementación y el cumplimiento del reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, entre otros.

Además obliga a todas las entidades públicas y empresas privadas a revisar el uso de los datos personales contenidos en sus sistemas de información y replantear sus políticas de manejo de información y fortalecimiento de sus herramientas, como entidad responsable del tratamiento (persona natural o jurídica, pública o privada, que por sí misma o en asociación, decida sobre la base de datos y/o el tratamiento de los datos) deben definir los fines y medios esenciales para el procesamiento de los datos de los usuarios y/o titulares.

Es importante para la auditoría al Sistema de Información Hospitalaria tratar aspectos relacionados con el procesamiento de la información y garantizar la manipulación de manera segura.

1.4.3 Ley de derechos de autor: los derechos de autor se aplican a obras originales de propiedad intelectual, en virtud de cual se otorga protección a las distintas creaciones expresadas a través de los géneros literarios, artísticos y de cualquier medio tangible. El autor de la obra es propietario de los derechos de autor.

Los autores de obra literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente ley.

Son titulares de los derechos reconocidos por la ley:

- El autor de su obra
- El artista, intérprete o ejecutante, sobre su interpretación o ejecución;
- El productor, sobre su fonograma
- El organismo de radiodifusión sobre su emisión
- Los causahabientes, a título singular o universal, de los titulares anteriormente citados, y la persona natural o jurídica que, en virtud de contrato obtenga por su cuenta y riesgo, la producción de una obra científica, literaria o artística realizada por uno o varios autores en las condiciones previstas en el artículo 20 de esta ley.

El artículo 21 de la Ley 23 de 1982 establece el plazo de protección de los derechos de autor, aplicable: la vida del autor y ochenta años después de su muerte.

2.4.3.1 Criterios de protección

- Protección a la Forma y no a las Ideas
- La Originalidad
- El mérito y la destinación de la obra
- Ausencia de formalidades para la protección
- Se protege la obra independientemente del objeto material en el que se encuentra fijada.

2. METODOLOGÍA

2.1 TIPO DE INVESTIGACION

El trabajo se ubica dentro de las investigaciones descriptivas ya que según Hernández [2007][28] , consiste en indicar todas las características del fenómeno que se estudia.

Otros precisan aún más esto señalando que "Desde el punto de vista científico, describir es medir". Esta última definición es importante, por cuanto implica por parte del investigador la capacidad y disposición de evaluar y exponer, en forma detallada, las características del objeto de estudio. Además, estos estudios permiten poner de manifiesto los conocimientos teóricos y metodológicos del autor del estudio, ya que evidencia el nivel cognitivo y operativo de conceptos y categorías relacionados con el tema.

Ander - Egg [1977: 40][29] , advierte, además, que "Los estudios exploratorios y los estudios descriptivos son los dos niveles en los que habitualmente han de trabajar quienes están preocupados por la acción, puesto que permiten elaborar un marco de estudio a partir del cual se deduce una problemática, o bien formular un diagnóstico con el fin de conocer carencias esenciales y sugerir una acción posterior".

En el trabajo de investigación se describió todo el proceso de hallazgos encontrados durante la auditoría al Sistema de información Hospitalario (SIHOS), además de las recomendaciones que se realizaron a dicho sistema.

De igual manera, es aplicativa ya que Murillo [2008][30], define la investigación

[28] HERNANDEZ SAMPERI, Roberto. Metodología de la investigación: McGraw-Hill /Interamericana de México, S.A de C.V., ISBN 968-422-931-3.

[29] TESIS DE INVESTIGACION [En línea] <http://tesisdeinvestig.blogspot.com/2011/11/tipos-de-investigacion-segun-ander-egg.html> [citado el 8 de marzo de 2015].

[30] MURILLO, W. La investigación científica. [En línea] <http//www.trabajos15/investigación científica/investcientíficas.htm> [consultado marzo 8 de 2015].

aplicativa como una característica que busca la aplicación o utilización de los conocimientos adquiridos, a la vez que se adquieren otros, después de implementar y sistematizar la práctica basada en investigación. El uso del conocimiento y los resultados de investigación que da como resultado una forma rigurosa, organizada y sistemática de conocer la realidad.

Por su parte, Boggino y Rosekrans [2004][31], mencionan la investigación aplicativa vista como un proceso investigativo científico, serio y riguroso, y como una forma necesaria y óptima para conocer las realidades desde la misma evidencia.

Hernández [2007][32], la investigación aplicativa o práctica se caracteriza por la forma en que se analiza la realidad social y aplica sus descubrimientos en la mejora de estrategias y actuaciones concretas, en el desarrollo y mejoramiento de éstas, lo que, además, permite desarrollar la creatividad e innovar.

La investigación aplicativa refiere al empleo de otros tipos de estudio y técnicas, entre las que se mencionan, estudios de mercado, sondeos de opinión pública, entrevistas y grupos focales. Todos con miras a responder con propuestas estratégicas de mejoramiento o cambio de una situación problema o para documentar experiencias basadas en situaciones reales.

Por lo anterior el trabajo se ubica dentro de una investigación descriptiva aplicativa por lo que se evaluó y explico en forma detallada, distintas características del Sistema de Información Hospitalario (SIHOS), además se elaboró un marco de estudio a partir del cual se deduce una problemática y se formular un diagnóstico con el fin de conocer carencias esenciales y sugerir un plan de acción posterior.

Teniendo en cuenta los conceptos de investigación descriptiva aplicativa en el trabajo de auditoría se evaluaron y expusieron los procesos, las etapas el análisis, los hallazgos mediante la aplicación creativa e innovadora de diferentes técnicas, métodos y estándares que permitieron obtener un diagnostico detallado de la

[31] VARGAS CORDERO, Zoila Rosa. La investigación aplicada: Una nueva forma de conocer la realidad. En Revista Educación 33(1), 155-165, ISSN: 0379-7082, 2009.

[32] Cívicos, A, Hernández, M. Algunas reflexiones y Aportaciones en torno a los Enfoques Teóricos y Prácticos de la Investigación en Trabajo social. Revista Acciones e Investigaciones Sociales, 2007, 23, 25-55. Disponible en <http://www.acofipapers.org/index.php/ei/2014/paper/viewFile/997/349> [Citado el 1 de Febrero de 2016].

situación en la institución es decir detectar conformidades y no conformidades en el manejo del sistema y con ello se elaboró un informe con recomendaciones que son el resultado de aplicar la auditoría al Sistema de Información Hospitalaria al (SIHOS).

2.2 ENFOQUE Y PARADIGMA DE LA INVESTIGACION

2.2.1 Enfoque: la investigación se ubica dentro de un enfoque empírico analítico, ya que según Restrepo [1999]33, empírico se refiere a la denominada investigación científica clásica, que consiste en plantear situaciones problemáticas a partir de hipótesis de trabajo para demostrarlas, además busca el dominio y conocimiento a través de la experiencia y se interesa por controlar y predecir los hechos que se estudian para ser modificados.

Y analítico ya que consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar las causas, la naturaleza y los efectos. El análisis es la observación y examen de un hecho en particular. Es necesario conocer la naturaleza del fenómeno y objeto que se estudia para comprender su esencia. Este método permite conocer más del objeto de estudio, con lo cual se puede explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías.

El enfoque empírico – analítico como un modelo de investigación científica, que se basa en la lógica empírica y es el más usado en al campo de las ciencias descriptivas y en las ciencia sociales. Su aporte al proceso de investigación es resultado fundamentalmente de la experiencia. Este enfoque posibilita revelar las relaciones esenciales y las características fundamentales del objeto de estudio, accesibles a la detección, a través de procedimientos prácticos con el objeto y diversos medios de estudio. Su utilidad destaca en la entrada en campos inexplorados o en aquellos en los que destaca el estudio descriptivo.

El enfoque del trabajo de investigación que se utilizó es empírico – analítico ya que este enfoque permite conocer más el objeto de estudio, con lo cual se puede explicar, analizar y comprender mejor el comportamiento y establecer

[33] RESTREPO, María Consuelo. PRODUCCION DE TEXTOS EDUCATIVOS. Ediciones Bogotá D.C. Colombia. Pág. 8 .ISBN: 978-958-20-0850-4.

recomendaciones que permitan mejorar la eficiencia y la eficacia del Sistema de Información Hospitalaria (SIHOS).

2.2.2 Paradigma de investigación: García Estebaranz [1994][34], define el paradigma cuantitativo objetivista, edificado sobre la autoridad de los evaluadores para intervenir se identifica con la autoridad del experto, basada en una imagen dualista del mundo (sujeto/objeto), estática, de datos, en el que la ciencia es el único camino de conocimiento y la "realidad" como el único objeto posible del conocimiento. La evaluación "acrítica", "neutral", "desinteresada" se fundamenta en el interés por el control y en los valores de eficiencia, eficacia, certidumbre y predictibilidad.

Además de lo antes expuesto, vale decir que la investigación cuantitativa estudia la asociación o relación entre las variables que han sido cuantificadas, lo que ayuda aún más en la interpretación de los resultados.

Haciendo énfasis en el concepto de paradigma cuantitativo el trabajo de auditoría se dedica a recoger, analizar, y procesar datos cuantitativos, es decir este va más allá de un listado de datos organizados. Para ello se apoya en distintos instrumentos de recolección de información y técnicas de auditoría asistidas por computador pues estos datos se muestran en él informa final y los resultados obtenidos brindarán una realidad específica a la que están expuestos.

2.4 POBLACION Y MUESTRA

2.4.1 Población: el trabajo se enfocó a la población de las áreas de informática del Sistema de Información Hospitalaria (SIHOS) en donde se encuentran involucrados personal profesionales en el área de sistemas, profesionales en el área contable, empleados, usuarios, quienes almacenan, procesan y comunican información y datos dentro del Sistema de Información Hospitalaria (SIHOS).

Entre ellos se encuentran.

- 1 Ingeniero de sistemas Jefe de sistemas
- 1 Ingeniera de sistemas

[34]ESTEBARANZ GARCÍA, Araceli. Didáctica e Innovación Curricular. Universidad de Sevilla, Primera edición 1994, Pág. 374. ISBN: 84-472-0534-7.

- 3 Técnicos de sistemas
- 2 Ingenieros de desarrollo
- Comité de proyectos investigación

2.4.2 Muestra: La muestra para este trabajo es la misma población ya que representa las características del objeto estudiado como son los diferentes funcionarios del Hospital Civil de Ipiales.

2.5 INSTRUMENTOS DE RECOLECCION DE INFORMACIÓN

Los instrumentos de recolección de información ayudan a obtener datos que permiten el control, análisis y medición de procesos y procedimientos en los Sistemas de Información. Para el proceso de auditoría se usaron diferentes instrumentos de recolección de información entre los que se encuentran:

2.5.1 Observación directa: consiste en verificar en la entidad auditada, en forma directa y paralela, lo que ocurre en una situación real como se desarrollan y documentan los procesos, procedimientos, controles, las instalaciones físicas, los movimientos diarios, la relación con el entorno, el accionar de sus directivos, y trabajadores, permitiendo tener una visión de la organización desde la perspectiva que el auditor necesita. La acción de observar es el hecho de examinar, analizar, advertir, o estudiar algo en este caso el auditor observa todo lo relacionado con el Sistema de Información Hospitalaria (SIHOS). En el Hospital Civil de Ipiales se implementó esta técnica para colocarse en contacto con el sistema de Información Hospitalaria (SIHOS), y con las personas y la administración.

2.5.2 Entrevista: consiste en la comunicación interpersonal establecida entre el investigador y el sujeto de estudio a fin de obtener respuestas a los interrogantes planteados sobre el problema propuesto. Permite estudiar aspectos de cualquier índole en el tema que se desee profundizar, con una información más precisa y uniforme, igualmente permite procesar la información de una manera más sencilla obteniendo datos cuantitativos y cualitativos. Este trabajo será valioso ya que se podrá entablar conversaciones sobre la investigación obteniendo información desde el punto de vista de cada funcionario en general y en su área de trabajo.

Se utiliza para recabar información en forma verbal, a través de preguntas que propone el investigador o entrevistador a fin de aclarar dudas, orientar las situaciones o problemas que pueda tener cualquier institución.

Quienes responden a la entrevista pueden ser gerentes, empleados, los usuarios actuales del sistema, usuarios potenciales o aquellos que proporcionan datos.

2.5.3 Encuesta: es una técnica destinada a obtener datos de varias personas cuyas opiniones impersonales interesan al auditor. Para ello se utiliza un cuestionario de preguntas escritas que se entregan a las personas encuestadas, a fin de que las contesten por escrito.

Es impersonal ya que el cuestionario no lleva el nombre ni alguna identificación de la persona que lo responde, ya que esos datos no interesan.

Para el desarrollo de este trabajo de auditoría se aplicó encuestas a algunos funcionarios que hacen uso del Sistema de Información Hospitalaria (SIHOS) en el Hospital Civil de Ipiales.

En el desarrollo de este trabajo todos estos elementos son necesarios ya que permiten identificar, analizar y tratar los datos que ayudan al auditor a realizar un trabajo eficiente. Cabe resaltar que el manejo es importante ya que obedece a la veracidad de la información, de manera correcta.

3.5.4 Listas de chequeo: es un tipo de instrumento en el que se muestra la presencia de un aspecto, a ser analizado. Su estructura debe especificar todos los aspectos antes nombrados, que se pretendan observar y la presencia o no de estas. La investigación utilizó este instrumento como técnica de verificación de conformidades y no conformidades en el manejo de la seguridad de la información en las áreas del Sistema de Información Hospitalaria (SIHOS).

3. RESULTADOS DE LA INVESTIGACION

3.1 ANÁLISIS DEL ENTORNO AUDITABLE

El Hospital Civil de Ipiales de acuerdo con su estructura organizacional cuenta con el proceso llamado recursos de la información dentro del cual se encuentra ubicada la dependencia de sistemas en donde está funcionando el Sistema de Información Hospitalario (SIHOS). Además cabe mencionar que existen algunos recursos como son hardware, software, comunicaciones, y red de datos que facilitan la comunicación entre diferentes procesos y por supuesto el Sistema de Información Hospitalario (SIHOS). En la Tabla 1,2 y 3 se sintetiza la organización de los activos.

Tabla 1. Inventario de los recursos informáticos del área de sistemas.

NOMBRE PC	TIPO DE EQUIPO		MARCA	DESCRIPCION
SISTEMAS1-PC	COMPUTADOR	PORTATIL	ASUS	INTEL I7
SISTEMAS5	COMPUTADOR	PORTATIL	LENOVO	INTEL I5
SISTEMAS3-	COMPUTADOR	PORTATIL	LENOVO	INTEL I5
SISTEMAS4	COMPUTADOR	PORTATIL	LENOVO	INTEL I5
SISTEMAS	COMPUTADOR	PORTATIL	LENOVO	INTEL I5

Fuente: ésta investigación.

Tabla 2. Inventario de servidores de la dependencia de sistemas.

SERVIDORES	UBICACIÓN
SERVIDOR HEWLETT-PACKARD ML11G6 GENERATION 6 SERVER	SISTEMAS
SERVIDOR HEWLETT-PACKARD ML11G6 GENERATION 7	SISTEMAS

SERVER	
HEWLETT-PACKARD ML11G6	SISTEMAS
IBM SYSTEM 3400	SISTEMAS
JANUS I3	SISTEMAS
COMPAQ V117388	SISTEMAS
DELL POWERADGE R720	SISTEMAS
SWICTH	UBICACIÓN
SWITCH HEWLETT-PACKARD PROCURVE NETWORKING INTERRUPTOR 2910AL-48G	SISTEMAS
HP PROCURVE SWITCH 2510-24G J9279A 24 PORT GIGABIT MANAGED - HP E2510-24G	SISTEMAS

Fuente Inventario 2015 del Hospital Civil de Ipiales.

Tabla 3. Inventario de UPS de la dependencia de sistemas.

NOMBRE	DESCRIPCION	SERIE
UPS	VANGUARD serie ll	V116803
UPS	DELTA GES303H	E0012C00024WD
UPS	UPS/R TURBO UPS	V111568
UPS	UPS/R TURBO UPS	V114689
UPS	DELTA 40KVA EDO13C000 TRIFASICA	
UPS	SPECTRONIC	V120813

Fuente: Plan mantenimiento 2015 del Hospital Civil de Ipiales.

El anterior inventario de recursos informáticos incluye la parte de hardware en donde se puede observar que el área de sistemas cuenta con un total de 5 portátiles, 7 servidores, 2 swicth, 6 UPS.

A continuación se describirá el software y aplicaciones instaladas en los equipos del área de Sistemas ya permite tener un conocimiento más amplio de las

herramientas y procesos que se manejan dentro de cada equipo del Área de Sistemas (Ver Tabla 4).

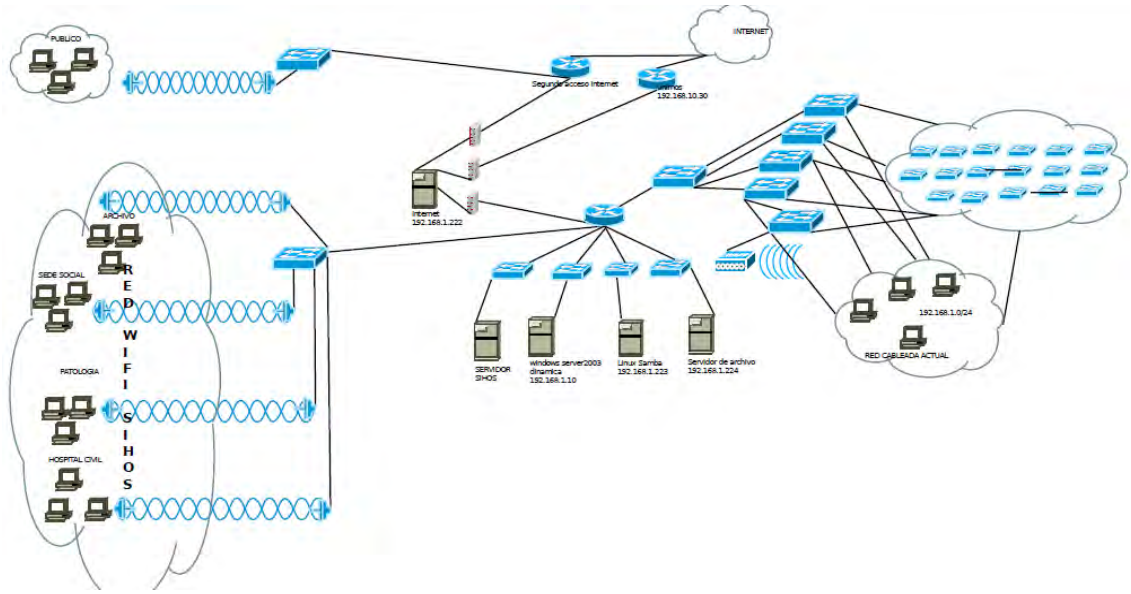
Tabla 4. Inventario de software y aplicaciones del área sistemas.

DERSCRIPCION
Paquetes Microsoft Office
Sistema Operativo Windows
Navegador Google Chrome
Navegador Mozilla Firefox
Navegador Internet Explorer
Antivirus Node
Visor de pdf (Adobe Reader)
Descompresor de archivos (Winrar)

En el Hospital Civil de Ipiales en el área de sistemas manejan 2 tipos de redes, la red cableada e inalámbrica, las cuales permite el acceso a las aplicaciones y sistemas de Información que se maneja en la Área incluyendo el Sistema de Información Hospitalario (SIHOS).

En la figura 2 se puede apreciar el diseño de la red que tiene implementado el Hospital Civil de Ipiales.

Figura 2. Diseño lógico de la wlan



Fuente: plan de Continuidad del Hospital Civil de Ipiales.

En la figura anterior, se puede observar los distintos servidores que maneja el Hospital Civil de Ipiales como son servidor dinámica, servidor SIHOS, servidor samba y el servidor de archivos. Además al lado derecho también se puede apreciar que se maneja una red cableada y al lado izquierdo se está implementando la red wifi del Sistema de Información Hospitalario (SIHOS).

En la tabla 5, se muestra los empleados que se encuentran dentro del Área de sistemas del Hospital Civil de Ipiales que hacen parte del Sistema de Información Hospitalario (SIHOS).

Tabla 5. Talento humano.

	NOMBRE COMPLETO	CARGO
Ingeniero de Sistemas	José Fernando Mora Montenegro	Jefe de Recursos de la Información
Ingeniera de sistemas	Alejandra Escobar	Ingeniera de Sistemas
Ingeniero de sistemas	Ricardo Tapia	Desarrollador

Ingeniero de sistemas	John Barrios	Desarrollador
Ingeniero de Sistemas	Marco Patiño	Técnico en sistemas
Técnico en Sistemas	Biki Cerón	Técnico en sistemas
Técnico en Sistemas	Diego Sánchez	Técnico en sistemas

En la tabla anterior, se puede apreciar el talento humano que hace parte de la dependencia de Sistemas entre los cuales se encuentra el jefe de sistemas, una ingeniera de sistemas, dos desarrolladores del Sistema de Información Hospitalario (SIHOS) y 3 Técnicos en sistemas.

3.1.1 Descripción del sistema de información hospitalario: un Sistema de Información es el conjunto formal de procesos de análisis, que operando sobre una colección de datos estructurados de acuerdo a las necesidades de la empresa, recopila elabora y distribuye, la información necesaria para realizar las operaciones básicas y la toma de decisión en cualquier empresa, que sirva para desempeñar las funciones de negocio de acuerdo con sus estrategias. Por lo tanto cualquier sistema que se encuentre dentro del sector de la salud está dirigido a ayudar la gestión Hospitalaria de centros médicos que requieran un eficiente control administrativo y financiero, que permita mejorar la eficiencia y rendimiento de la institución. Los sistemas de Información Hospitalarios son un producto especializado para el sector de salud, ya que la salud juega un papel fundamental en cada uno de los usuarios, y es importante el tiempo en el cual los pacientes son atendidos, de allí la importancia de un sistema de Información Hospitalario abarque todo el proceso del paciente desde la admisión hasta la salida y permita eliminar errores que se presentan en los diferentes módulos del sistema que repercuten en la salud de cada usuario y por ende mejorar la calidad de prestación de servicios.

3.1.2 Descripción del (SIHOS) en el Hospital Civil de Ipiales: el sistema de Información Hospitalario (SIHOS) es un sistema integrado de información que reúne en un solo ambiente de trabajo, información de tipo clínico, administrativo, contable, financiero, por lo que se constituye en una solución para la institución.

El Hospital Civil de Ipiales cuenta con varias plataformas software y sistemas de información como se puede apreciar en la Tabla 6, que muestra el nombre del sistema y una breve descripción del mismo.

Tabla 6. Sistemas de información del Hospital Civil de Ipiales ESE.

SISTEMAS DE INFORMACIÓN HOSPITAL CIVIL DE IPIALES	
NOMBRE	**DESCRIPCION**
SIHOS	Sistema de Información Hospitalaria para el de Historia Clínica electrónica y procesos financieros.
ANNAR LAB	Software de laboratorio Clínico.
DARUMA -D	Software para manejo del sistema de gestión de calidad.
AM INGENIERIA	Software de mantenimiento hospitalario y gestión de la tecnología.
CARESTREAM HEALTH	Software de digitalización de imágenes diagnósticas.
WIRECAST	Software para el manejo de circuito cerrado de televisión.
CMS SMART DVR	Software para el manejo de circuito de cámaras de seguridad internas.
LED EDITTOR V9.0	Software para el manejo de información en Pantallas LED Informativas.
HEXABANK	Software de Banco de Sangre.

Fuente: Plan de Contingencia Sistemas de Información y comunicaciones HCI.

El Sistema de Información Hospitalario (SIHOS) se implementó en el Hospital Civil de Ipiales hace tres años y maneja toda la parte de atención al usuario y la parte administrativa y financiera, es el sistema que más lo utiliza el Hospital ya que en

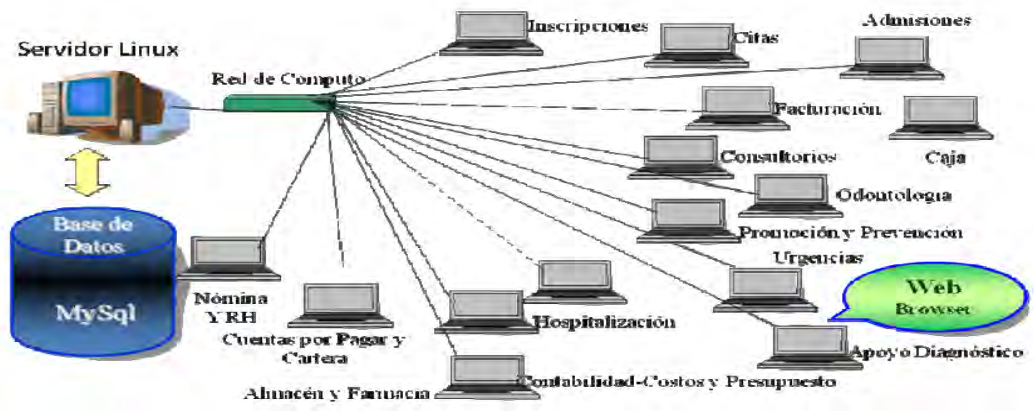
este se encuentran involucrados Médicos especialistas, Médicos Generales, Enfermeras Jefes, Auxiliares, Administrativos y de esta manera la mayor parte del Hospital se involucra en este sistema.

El Sistema de Información Hospitalario (SIHOS) está construido bajo un esquema de Base de Datos integrando las áreas asistenciales y administrativas buscando la reducción de costos, tiempos de espera y elaboración de tareas complejas y redundantes, además incorpora el manejo integral del paciente en la Institución, registrando la información desde la admisión del paciente hasta la generación de la cuenta por pagar.

El Sistema de Información está instalado aproximadamente 240 equipos del Hospital civil de Ipiales de acuerdo a cada dependencia, este Sistema de Información Hospitalario (SIHOS) se maneja a través de la web por lo tanto funciona en cualquier equipo, y se utiliza el navegador Internet Explorer 7, fue desarrollado en los lenguajes Php, Ajax, JavaScript y su base de datos está diseñada Mysql.

En el siguiente grafico se observa como está organizado el Sistema de Información Hospitalario (SHOS).

Figura 3. Diseño lógico del sistema de información hospitalario.



Fuente: Manual de Usuario del Sistema de Información Hospitalario (SIHOS).

Está compuesto por los siguientes módulos interconectados y vinculados a una Base de Datos.

- Admisión del Paciente
- Administración
- Caja
- Citas
- Consulta externa
- Contabilidad
- Contratos
- Facturación y cartera
- Gestión de pacientes
- Glosas y objeciones
- Imagen logia
- Inscripción y comprobación de derechos
- Inventario
- Laboratorio clínico
- Liquidación de servicios de salud
- Nomina
- Observación e interacción
- Patología
- Presupuesto
- Procedimientos
- Promoción y prevención
- Tesorería
- Triage
- Urgencias

Figura 4. Sistema de información hospitalario (SIHOS)

Fuente: Sistema de Información Hospitalario del HCI.

3.1.3 Descripción del módulo de historias clínicas: el módulo de Historias Clínicas permite un almacenamiento y consulta en línea de la historia del paciente facilitando un resumen total de las atenciones realizadas por el Hospital Civil de Ipiales,

Módulo de admisiones.

Este módulo se utiliza para abrir la historia clínica de cada paciente que va a ingresar por urgencias, este módulo genera un número automático por cada paciente.

Como parte del funcionamiento y operatividad del módulo de admisión de los servicios a desarrollar se ha identificado los siguientes procesos.

- Inscripción del usuario en caso de que no se encuentre e l a base de datos y una vez verificada la información en las bases de datos enviadas por las entidades administradoras se autoriza su inscripción.
- Generar un número único de admisión por cada atención de paciente
- Abrir historia clínica del paciente en el sistema

- Registrar el ingreso del paciente al nivel de urgencias
- Realizar búsquedas de pacientes de acuerdo al número de admisión
- Guardar la información consignada en cada admisión
- Modificar la admisión una vez guardada
- Imprimir la admisión

Cabe destacar que la elaboración de la admisión se realiza a partir de los siguientes escenarios:

- Consulta por urgencias ambulatorias
- Referido por otra IPS

Como información generada del módulo de admisión de servicios de salud se encuentra los siguientes reportes que pueden ser personalizados o específicos.
Reporte de admisiones: causa de atenciones condición, entidad administradora, contratos tipo de usuario, pacientes en un rango de fecha determinado.

Módulo de urgencias.

El sistema va generando de acuerdo con los eventos asistenciales la historia clínica del paciente conforme a la reglamentación existente, este módulo permite alimentar la historia clínica con los hallazgos y seguimientos de exámenes clínicos realizado por el médico, lo cual permite acceder de una forma rápida y confiable del estado de salud del usuario en cuanto a : triage, consultas, prescripción, ordenación, notas de enfermería, notas médicas, medicamentos, procedimientos, materiales, consentimiento informado , plan de manejo, cambio de atención, incapacidad, remisiones. Además la historia clínica queda guardada y puede ser consultada por el médico tratante.

3.2 DISEÑO DE TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE EVIDENCIAS

Para iniciar el proceso de auditoria se diseñó una matriz dominio para planificar de manera ordenada la etapa de recolección de información.

Tabla 7. Matriz dominio / instrumentos de recolección de información.

INSTRUMENTO / DOMINIO	OBSERVACION DIRECTA	LISTA DE CHEQUEO	ENCUESTA	ENTREVISTA
PLANEACION Y ORGANIZAR	↔	↔		↔
ADQUIRIR E IMPLEMENTAR	↔	↔		↔
ENTREGAR Y DAR SOPORTE	↔	↔		↔
MONITOREAR Y EVALUAR	↔	↔		↔

En la tabla N° 7, se indica en la parte superior de izquierda a derecha se ubicaron los instrumentos de recolección de información como son observación directa listas de chequeo encuesta y entrevista, y en la primera columna se ubicaron los dominios de acuerdo con estándar COBIT como son planear y organizar, adquirir e implementar, entregar y dar soporte, monitorear y evaluar, de acuerdo a cada uno de estos dominios se diseñaron los instrumentos de recolección de información es decir los recuadros que están marcados con las flechas indican que se aplicara dicho instrumento de acuerdo a cada dominio de COBIT.

Teniendo en cuenta esta matriz, se realizó los instrumentos de recolección de información como son listas de chequeo y entrevistas que se planteó en la matriz dominio dirigidas al Jefe de Recursos de la Información, ingenieros desarrolladores del Sistema de Información Hospitalario (SIHOS) basados en el estándar Cobit 4.1, además se realizó algunas pruebas de análisis y ejecución

permitiendo obtener mayor claridad del Sistema de Información Hospitalario (SIHOS).(Ver Anexo N° 1, Anexo N° 2, Anexo N° 3,Anexo N° 4, Anexo N°5, Anexo N° 6. Anexo N° 7, Anexo N° 8)

Las listas de chequeo y las entrevistas contienen el logo del Hospital Civil de Ipiales y los ítems relacionados con la auditoria se describen a continuación.

REF: Espacio para identificación del cuestionario.

ENTIDAD AUDITADA: En este espacio se indica el nombre de la entidad a la cual se le está realizando la auditoría.

AREA AUDITADA: En este espacio se indica el nombre del área a la cual se le aplica la auditoria.

DIRIGIDO A: Personal al cual se les aplica la entrevista y lista de chequeo.

OBJETIVO: En este espacio se indica el objetivo del proceso establecido dentro de los dominios COBIT.

MATERIA DE SOPORTE: Nombre del estándar aplicado en la auditoria en este caso COBIT 4.1.

DOMINIO: Nombre del Dominio de COBIT que se está evaluando.

PROCESO: Nombre del proceso que se está evaluando dentro de cada Dominio.

PREGUNTAS: Listado de preguntas a evaluar.

SI, NO N/A: Posibilidades de respuesta cumple no cumple no aplica para la entidad.

OBSERVACION: Notas importantes de cada pregunta.

AUDITOR RESPONSABLE: Nombre de la persona que está llevando a cabo el proceso de Auditoria.

Tabla 8. Formato de lista de chequeo.

HOSPITAL CIVIL DE IPIALES EMPRESA SOCIAL DEL ESTADO		LISTA DE CHEQUEO			REF
ENTIDAD AUDITADA					
AREA AUDITADA					
DIRIGIDO A					
OBJETIVO					
MATERIAL SOPORTE					
DOMINIO			**PROCESO**		
Nº	**PREGUNTAS**	**SI**	**NO**	**N/A**	**OBSERVACION**
AUDITOR RESPONSABLE					

.

Tabla 9. Formato de entrevista

HOSPITAL CIVIL DE IPIALES EMPRESA SOCIAL DEL ESTADO		**ENTREVISTA**		**REF**
ENTIDAD AUDITADA				
AREA AUDITADA				
DIRIGIDO A				
OBJETIVO				
MATERIAL SOPORTE				
DOMINIO			**PROCESO**	
Nº	**PREGUNTAS**			

AUDITOR RESPONSABLE	

Después de haber aplicado los instrumentos de recolección de información se realiza un formato de no conformidades encontradas en el Sistema de Información Hospitalario (SIHOS), en el cual se describe la no conformidad de acuerdo a cada dominio del estándar cobit y de la misma manera se describe la acción correctiva que se debe tomar con respecto a la misma. (Ver Anexo N° 9 a Anexo N° 40.)

Los ítems que contiene el formato de no conformidades se describen a continuación

HOJA DE NO CONFORMIDADES: Número de hojas de la no conformidad.

CIUDAD: Nombre de la ciudad.

FECHA: Día y mes en el que se diligencia el formato de no conformidad.

AUDITOR: Nombre del Auditor.

PREGUNTA: Número de la correspondiente pregunta.

DEPENDENCIA: Centro de cómputo principal.

N°: Número consecutivo de las no conformidades.

REPORTE DE LA NO CONFORMIDAD: Explicación y documentación de la no conformidad de la pregunta correspondiente encontrada en el Sistema de Información Hospitalario (SIHOS) en el Hospital Civil de Ipiales.

ACCION CORRECTIVA: Descripción completa de la acción correctiva realizada por la auditora responsable.

MATERIAL SOPORTE Nombre del estándar aplicado en la auditoria en este caso COBIT 4.1.

DOMINIO: Nombre del dominio de COBIT que se está evaluando.

Tabla 10. Formato de no conformidades.

HOJA DE NO CONFORMIDADES (1/_) REPORTE NC CIUDAD_____
FECH_/_/2015 AUDITOR _____

FORMATO DE REPORTE DE NO CONFORMIDAD			
	PREGUNTA Nº	**DEPENDENCIA**	**Nº__ _**
REPORTE DE NO CONFORMIDAD		**FECHA __/__/__ HORA ___**	
MATERIAL DE SOPORTE			
DESCRIPCION DE LA NO CONFORMIDAD			
DESCRIPCION DE LA ACCION CORRECTIVA		**FECHA __/__/__/ HORA__**	

3.3 ANÁLISIS Y EVALUACIÓN DE RIESGOS, DE ACUERDO CON LOS DOMINIOS DEL COBIT 4.1 AL SISTEMA DE INFORMACION HOSPITALARIO (SIHOS) EN EL HOSPITAL CIVIL DE IPIALES.

Este evaluación se inicia tomando como referente los resultados de la aplicación del instrumento de recolección de información tipo entrevista y listas de chequeo aplicado al Jefe de recursos de la información y funcionarios de la dependencia de sistemas, en donde se investiga sobre controles y riesgos que se presentan frente al manejo del Sistema de Información Hospitalario (SIHOS) basados en el estándar COBIT 4.1.

La apreciación de los funcionarios de la dependencia de Sistemas con respecto a la seguridad del Sistema de Información Hospitalario (SIHOS) se encuentra en una seguridad básica es decir que falta implementación de herramientas y

políticas que garanticen la seguridad del sistema así como la manera informal que se realizan actividades, procesos, funciones, desarrollo y actualización del Sistema de Información Hospitalario (SIHOS), de esta manera también se puede observar el deficiente control de acceso a las instalaciones de la Dependencia ya que se encuentran algunos servidores, y copias de seguridad que no se encuentran en un lugar seguro, además no se encuentra instalado cámaras de seguridad dentro de la dependencia en caso de accesos indebidos a esta área.

Con estos datos se procede a cruzar las opiniones de los funcionarios con la observación directa, aplicando las listas de chequeo basados el estándar COBIT.

3.3.1 Análisis de riesgos: con la aplicación de las listas de chequeo y entrevistas se observa que existen riesgos y vulnerabilidades que son evidentes en el manejo de la información en la dependencia.

En la tabla 11 se describen los riesgos clasificados de acuerdo a los dominios de COBIT 4.1

Tabla 11. Listado de riesgos.

N° RIESGO	RIESGO	PROBABILIDAD			IMPACTO			DOMINIO
		B	M	A	B	M	A	
R1.	No se ha realizado el registro Nacional de base de datos la superintendencia de industria y comercio.			X			X	PO
R2.	No existe un diccionario de datos del Sistema de Informacion Hospitalario (SIHOS).		X			X		PO
R3.	No tiene un modelo		X			X		PO

	relacional de la base de datos del Sistema de Información Hospitalario (SIHOS).							
R4.	No se realizan revisiones de aseguramiento de calidad y son evaluados teniendo en cuenta estándares de calidad.			X		X		PO
R5.	No se realizan evaluaciones en cuanto al desempeño de los funcionarios de la dependencia de sistemas.		X		X			PO
R6.	Existe perdida de información por errores.			X			X	PO
R7.	No existe un modelo de arquitectura de información.		X			X		PO
R8.	El sistema de información Hospitalario (SIHOS) no siempre está disponible en el momento requerido.		X				X	PO
R9.	No existe un plan de pruebas al Sistema de		X				X	AI

	Informacion Hospitalario (SIHOS).							
R10.	No existe un plan de mantenimiento al sistema de Información Hospitalario (SIHOS).		X				X	AI
R11.	No existe un manual para el personal que realiza mantenimiento a la infraestructura tecnológica.			X		X		AI
R12.	No se lleva una documentación en bitácoras del proceso de cambios en el sistema de Información Hospitalaria (SIHOS).		X			X		AI
R13.	No se realiza almacenamiento de respaldo dentro y fuera de las instalaciones del Hospital Civil de Ipiales.			X			X	AI
R14.	Existe perdida de información por actualizaciones mal hechas, y mantenimiento inadecuado.			X			X	AI
R15.			X				X	AI

	No existe total documentación de la red.							
R16.	No se ha establecido ambientes de prueba que evalúen la efectividad al Sistema de Información Hospitalario (SIHOS).	X				X		AI
R17.	No se lleva cabo capacitaciones de manera periódica con respecto a lo que se debe hacer con incidentes no planeados del Sistema de Información Hospitalario (SIHOS).			X			X	DS
R18.	No existen cámaras de seguridad dentro de la dependencia			X			X	DS
R19.	No existe un documento de la administración de cuentas de usuarios.	X			X			DS
R20.	No existe un análisis de las fallas encontradas en el Sistema de Información Hospitalario (SIHOS).		X			X		DS
		X			X			DS

R21.	El personal encargado del desarrollo del Sistema de Información Hospitalario (SIHOS) no lleva un registro de las actualizaciones y mejorías realizadas sobre el sistema.							
R22.	No existen procedimientos de seguridad para el acceso y salida de las personas que ingresan a la dependencia de Sistemas.			X			X	DS
R23.	No Se cuenta con salidas de emergencia dentro de la dependencia. No existen señalizaciones.		X		X			DS
R24.	En la Dependencia de Sistemas existen dificultades con el espacio para movilizarse.			X			X	DS
R25.	No se tiene un plan de contingencia en caso de que fallen los extintores.			X			X	DS
R26.	Perdida de información por accesos indebidos a las instalaciones.			X			X	DS

R27.	El personal no conoce las políticas de monitoreo de la seguridad física de los equipos de cómputo.		X			X		ME
R28.	No existen políticas relacionadas con el proceso de monitoreo de las actividades encaminadas a brindar la seguridad al sistema de información Hospitalario.			X			X	ME

Estos aspectos se tuvieron en cuenta para realizar el análisis de riesgos del Sistema de Información Hospitalario (SIHOS) en el Hospital Civil de Ipiales.

En la tabla 12, se muestra la valoración de riesgos encontrados y de esta manera se planean actividades de monitorización y acciones de control que permiten minimizar el impacto de los riesgos identificados.

La tabla se encuentra ordenada de la siguiente manera.

N° DE RIESGO: hace referencia al número consecutivo de los riesgos de la tabla 11.

DESCRIPCIÓN: se realiza una breve descripción de cada riesgo o vulnerabilidad encontrada.

MONITORIZACIÓN: se establecen actividades de control para monitorear los riesgos identificados.

ACCIÓN: se plantean lo que se debe hacer para reducir o minimizar el impacto del riesgo o vulnerabilidad**.**

PROBABILIDAD: Probabilidad de ocurrencia del riesgo que puede ser baja, media o alta.

IMPACTO: se establece el nivel de impacto que causaría los riesgos si llegarán materializarse.

RESPONSABLE: Personal responsable del riesgo**.**

Tabla 12. Identificación y clasificación de riesgos.

N° RIESGO	DESCRIPCION	MONITORIZACION	ACCION	P	I	RESPONSABLE
R1.	No se ha realizado el registro Nacional de base de datos la superintendencia de industria y comercio.	Mantener actualizados de las leyes y reglamento vigente para los sistemas.	Realizar el Registro de la base de datos a la superintendencia de industria y comercio.	A	A	Ing. José Fernando Mora.
R2.	No existe un diccionario de datos del Sistema de Informacion Hospitalario (SIHOS).	Actualizar de manera permanente el diccionario de datos del Sistema de Información Hospitalario (SIHOS).	Diseñar un diccionario de datos del Sistema de Información Hospitalario (SIHOS).	M	M	Ing. José Fernando Mora.
R3.	No tiene un modelo relacional de la base de datos del Sistema de Información Hospitalario (SIHOS).	Actualizar de manera periódica el modelo relacional de la base de datos del Sistema de Información Hospitalario (SIHOS)	Elaborar un modelo relacional de las Bases de Datos del Sistema de Información Hospitalario (SIHOS).	M	M	Ing. José Fernando Mora.

R4.	No se realizan revisiones de aseguramiento de calidad.		Planear evaluaciones en las cuales se tenga en cuenta estándares para el aseguramiento de la calidad.	M	M	Ing. José Fernando Mora.
R5.	No se realizan evaluaciones en cuanto al desempeño de los funcionarios de la dependencia de sistemas.	Realizar seguimiento a las actividades asignadas a cada uno de los funcionarios de la dependencia	Establecer un plan que permita medir el desempeño de los funcionarios de acuerdo a sus actividades asignadas en el manual de funciones. Establecer un proceso disciplinario formal para empleados que hayan cometido alguna violación de la seguridad	M	B	Ing. José Fernando Mora.
R6.	Existe perdida de información por errores.	Al realizar actividades tener en cuenta los manuales.	Realizar capacitaciones e implementar planes de mejoramiento.	A	A	Ing. José Fernando Mora.
R7.	No existe un modelo de arquitectura de información.		Diseñar un modelo de arquitectura de información que facilite el	M	M	Ing. José Fernando Mora.

			desarrollo de aplicaciones y de soporte a la toma de decisiones.			
R8.	El sistema de información Hospitalario (SIHOS) no siempre está disponible en el momento requerido.	se deben verificar periódicamente el Sistema de Información Hospitalaria (SIHOS) para determinar el cumplimiento de las normas de implementación de seguridad.	Adquirir tecnología necesaria para que el Sistema de Información Hospitalario (SIHOS).	M	A	Ing. John Barrios - Ricardo Tapia.
R9.	No existe un plan de pruebas al Sistema de Informacion Hospitalario (SIHOS).	Monitorear la respuesta a la implementación de las pruebas que se diseñaron para el Sistema de Información Hospitalario	Diseñar un plan de pruebas al Sistema de Información Hospitalario (SIHOS).	M	A	Ing. John Barrios - Ricardo Tapia.
R10.				M	A	Ing. John Barrios

	No existe un plan de mantenimiento al sistema de Información Hospitalario (SIHOS).	Implementar y actualizar el plan de mantenimiento al Sistema de Información Hospitalario (SIHOS)	Diseñar un plan de mantenimiento al Sistema de Información Hospitalario (SIHOS).			- Ricardo Tapia.
R11.	No existe un manual para el personal que realiza mantenimiento a la infraestructura tecnológica.	Monitorear si el personal encargado de realizar mantenimiento ejecuta sus actividades teniendo en cuenta este manual.	Diseñar un manual para todo el personal encargado de realizar mantenimiento a la infraestructura tecnológica.	A	M	Técnicos Biki cerón Marco Patiño, Diego Sánchez
R12.	No se lleva una documentación en bitácoras del proceso de cambios en el sistema de Información Hospitalaria (SIHOS).	Actualizar de manera permanente el documento de cambios realizados al Sistema.	Establecer un documento en donde se incorporen todos los cambios que se realizan al Sistema de Información Hospitalario (SIHOS).	M	M	Técnicos Biki cerón Marco Patiño, Diego Sánchez. Ing. John Barrios, Ricardo Tapia.
R13.	No se realiza almacenamiento de respaldo dentro y fuera	Asignar responsables de estar al tanto de las	Asignar un espacio dentro de la dependencia donde se establezcan	A	A	Ing. José Fernando Mora.

	de las instalaciones.	estrategias de seguridad de las copias almacenadas dentro de la dependencia y de las tecnologías que implementadas en la nube.	parámetros de seguridad. Proponer e implementar planes de tecnologías en la nube que permitan obtener mayor seguridad.			
R14.	Existe perdida de información por actualizaciones mal hechas, y mantenimiento inadecuado.	Monitorear las actividades de mantenimiento que realiza el personal. Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.	Para realizar mantenimiento a equipos tener en cuenta la guía o documento en donde proponen actividades para realizar un mantenimiento adecuado.	A	A	Técnicos. Ing. John Barrios – Ricardo Tapia
R15.	No existe una documentación de la red total.	Adquirir Información de la red por cada dependencia.	Elaborar un documento en donde incluya la documentación de toda la red del Hospital Civil de Ipiales.	M	A	Ing. José Fernando Mora.

R16.	No existe un estándar de adquisición y desarrollo del Sistema de Información Hospitalario (SIHOS).	Monitorear el desempeño de los estándares implementados.	Implementar estándares existentes que permitan guiar la adquisición de tecnologías.	B	M	Ing. John Barrios – Ricardo Tapia
R17.	No se lleva cabo capacitaciones de manera periódicas con respecto a lo que se debe hacer con incidentes no planeados del Sistema de Información Hospitalario (SIHOS).	Realizar evaluaciones al personal a fin de determinar lo que captaron de las capacitaciones. Todos los empleados de la organización contratistas usuarios deben recibir formación adecuada de concientización y actualizaciones regulares sobre las políticas y los procedimientos que afectan la seguridad	Establecer capacitaciones en las cuales se dé a conocer al personal los incidentes no planeados que afectan al Sistema de Información y además se tenga en cuenta el plan de continuidad de tecnologías de información.	A	A	

		del Sistema y que no se han contemplado en el plan de continuidad.				
R18.	No existen cámaras de seguridad dentro de la dependencia	Asignar personal responsable de la vigilancia de las cámaras de seguridad que se instalen	Adquirir elementos de infraestructura tecnológica teniendo en cuenta el estudio de factibilidad y estándar de adquisición de los elementos a que se van a conseguir.	A	A	Ing. José Fernando Mora
R19.	No existe un documento de la administración de cuentas de usuarios. No se exige el cambio de contraseñas	Restringir y controlar la asignación y uso de privilegios a cada Usuario del Sistema. Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la	Elaborar un documento en donde se encuentren los usuarios roles y permisos asignados a cada usuario del Sistema de Información Hospitalario (SIHOS). Establecer procedimientos formales de revisión periódica de los derechos de acceso	B	B	Técnico Biki Cerón

		selección y el uso de las contraseñas	de los usuarios.			
R20.	No existe un análisis de las fallas encontradas en el Sistema de Información Hospitalario (SIHOS).	Actualizar de manera permanente el plan de administración de riesgos. Evaluar la exposición del Sistema de Información a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	formular un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad del Sistema de Información Hospitalario (SIHOS)	M	M	Ing. José Fernando Mora.
R21.	El personal encargado del desarrollo del sistema de información Hospitalario (SIHOS) no lleva un registro de las actualizaciones y mejorías realizadas al Sistema	Solicitar al personal el registro de las actualizaciones y desarrollos realizados sobre el sistema.	Implementar actualizaciones y mejorías que se han realizado, en el manual del Sistema de Información Hospitalario y los demás documentos	B	B	Ing. John Barrios Ricardo Tapia.

			existentes.			
R22.	No existen procedimientos de seguridad para el acceso y salida de las personas que ingresan a la dependencia de Sistemas.	Realizar un registro de las personas y elementos que ingresan a la dependencia	Establecer políticas de ingreso con el fin de controlar el acceso de las personas a la dependencia.	A	A	Ing. José Fernando Mora.
R23.	No Se cuenta con salidas de emergencia dentro de la dependencia. No existen señalizaciones.		Diseñar señalizaciones para salidas de emergencia dentro de la dependencia de sistemas.	M	B	Ing. José Fernando Mora.
R24.	En la Dependencia de Sistemas existen dificultades con el espacio para movilizarse.		Adecuar el espacio de la dependencia de sistemas con el fin de garantizar un ambiente de trabajo apropiado.	A	A	Ing. José Fernando Mora.
R25.		El plan de		A	A	Ing. Alejandra

	No se tiene un plan de contingencia en caso de que fallen los extintores.	continuidad de sistemas de información y comunicaciones deben ser sometido a pruebas y revisiones periódicas para asegurar su actualización y eficacia.	En el plan de continuidad de sistemas de información y comunicaciones se debe plantear alternativas de seguridad en caso de que los extintores instalados en la oficina de sistemas fallen.			Escobar.
R26.	Perdida de información por accesos indebidos a las instalaciones.		Implementar estrategias que permitan obtener seguridad al ingresar a las instalaciones.	A	A	Ing. José Fernando Mora.
R27.	El personal no conoce las políticas de monitoreo de la seguridad física de los equipos de cómputo.	Realizar seguimiento a las capacitaciones que se realicen.	Dar a conocer estrategias de seguridad e cuanto a la seguridad de cada uno de los equipos.	B	B	Ing. José Fernando Mora.
R28.	No existen políticas	Cuantificar y	Establecer un marco de	A	A	Ing. John Barrios Ricardo Tapia.

	relacionadas con el proceso de monitoreo de las actividades encaminadas a brindar la seguridad del Sistema de Información Hospitalario (SIHOS).	monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información	trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para medir la solución y la entrega de servicios, así como también monitorear la contribución de Tecnologías de Información al Hospital Civil de Ipiales.			

I: Impacto
P: Probabilidad

Tomando como referente los procesos, procedimientos y la información que maneja el Sistema de Información Hospitalario (SIHOS), en el Hospital Civil de se procede a realizar análisis de vulnerabilidad de los activos informáticos, para ello se identifica las amenazas usando la Metodología de Matriz de Gestión de Riesgos de Horacio Villa Loboguerrero.

3.3.2 Matriz de control de riesgos: la matriz control de riesgos es un método definido por Horacio Villa Loboguerrero [1994][35] en él expresa un técnica para mostrar gráficamente las amenazas a las cuales está expuesto cualquier sistema, así como los objetos que lo comprenden, en este caso la evaluación al Sistema de Información Hospitalario (SIHOS), para lo cual se procedió a elaborar la matriz de control de riesgos escribiendo en la fila superior, identificando la columna a partir de la segunda los nombres de las amenazas y en la columna extrema izquierda, identificando la fila a partir de la segunda los nombres de los objetos, y dentro de cada celda se colocó los controles que mitigan o detienen una amenaza o salvaguardan un objeto. (Ver Anexo 41).

En Anexo 41, se especifican diferentes amenazas del Sistema de Información Hospitalario (SIHOS) como son perdida de datos, documentación desactualizada, acceso ilegal, violación de la privacidad, suspensión del SIHOS, acceso a las bases de datos así como también los objetos y los controles que se encuentran ubicados en cada celda de acuerdo al número que corresponde a la lista de controles que se encuentran debajo de la matriz de control de riesgos.

De este Anexo, se resaltan algunas vulnerabilidades como son instalaciones inadecuadas, suspensión del Sistema de Información Hospitalario (SIHOS), y el acceso a las bases de datos por la mayoría de los funcionarios del sistema, las cuales representan riesgos que deben ser detectados y evaluados a tiempo con el fin de prevenir pérdidas y mejorar la atención de los pacientes y elevar la calidad del Sistema de Información Hospitalario (SIHOS).

Este anexo sirve para implementar los controles existentes que permitan minimizar las amenazas y riesgos que está expuesto el sistema de Información Hospitalario (SIHOS), además se utiliza como base para realizar las siguientes matrices como son matriz de categorización de riesgo, matriz de sensibilidad de objetos, matriz de control de riegos sensibilidad.

[35] VILLA LOBOGUERRERO Horacio. Guía de Fundamentos De Auditoria De Sistemas, 1994. Pág. 39-42

3.3.3 Matriz de categorización de riesgos: para categorizar los riesgos se identifican las áreas de alto, mediano y bajo riesgo, clasificándolas en orden de nivel de exposición. La ejecución de este paso se realiza utilizando el método Delphi y la comparación de niveles de riesgo, que consiste en realizar la categorización individual de las amenazas y los objetos mediante el empleo de comparación de niveles de riesgo. Para categorizar las amenazas se usa como criterio la percepción que tenga cada auditor sobre cuál amenaza de cada pareja de amenazas puede causar mayor pérdida económica en un año.

Al evaluar el Sistema de información Hospitalario (SIHOS) con respecto a la matriz de categorización de riesgos la pérdida de datos obtuvo un puntaje de 5, la suspensión del Sistema de Información Hospitalario (SIHOS) un puntaje de 5, acceso ilegal obtuvo un puntaje de 4, el modelo de arquitectura de información un puntaje de 4, violación de la privacidad un puntaje de 3, almacenamiento de copias de seguridad un puntaje de 5, registro de base de datos un puntaje de 3, y espacios de movilidad obtuvo un puntaje de 1. (Ver Anexo 42).

De este anexo, se puede concluir que la perdida de datos, la suspensión del Sistema de Información Hospitalario (SIHOS) y almacenamiento de copias en lugares no seguros son los criterios que más riesgos pueden producir en el Hospital Civil de Ipiales.

3.3.4 Matriz de categorización de sensibilización de objetos: a continuación se realizó la categorización de la sensibilidad de objetos, este proceso inicia copiando los objetos que registra la matriz de control de riesgos en una hoja de comparación de los mismos, para ello se utiliza como criterio la percepción que tenga el auditor sobre cuál objeto de cada pareja de objetos puede causar mayor pérdida económica si se daña o causa demoras en el procesamiento.

La categorización de objetos se obtiene sumando las fracciones superiores derechas de la diagonal de cada columna, seguidamente se cuentan las filas sumando los votos de las fracciones inferiores izquierdas de la diagonal de la columna, después se suman los dos votos para obtener un total final para cada amenaza, resultado que se utiliza para producir una lista de categorización de amenazas por niveles de riesgo de mayor a menor. (Ver Anexo 43).

De esta matriz, se puede concluir que los objetos que obtuvieron mayor impacto son archivos de datos con un puntaje de 3 seguidamente instalaciones con un

puntaje de 2, así como también el software obtuvo un puntaje de 1 y hardware un puntaje de 0.

3.3.4 Matriz de control de riesgos riesgo/sensibilidad: una vez terminada la categorización de las amenazas y objetos, se procede a elaborar una matriz de control de riesgos para obtener el nivel de riesgo/sensibilidad. En esta matriz se combinan las dos categorizaciones, escribiendo en la fila superior, identificando las columnas a partir de la segunda, los nombres de las amenazas y sus respectivos totales en el orden de mayor a menor que registra la lista de categorización de amenazas por niveles de riesgo, y en la columna extrema izquierda, identificando las filas a partir de la segunda, los nombres de los objetos y sus correspondientes totales en el orden de mayor a menor que registra el detalle de categorización de sensibilidad de objetos, seguidamente, se multiplican los correspondientes valores y el producto se coloca en cada celda, terminada esta operación, se procede a obtener el nivel de riesgo/sensibilidad de las celdas de acuerdo con el valor del producto. (Ver anexo 44).

Al realizar el análisis de esta matriz se obtiene que el almacenamiento de archivos de datos en lugares no seguros presenta el mayor riesgo en el Hospital Civil de Ipiales, esto es pertinente debido a que en la dependencia de Sistemas no se han establecido controles que permitan disminuir los riesgos.

3.3.5 Matriz de clasificación de regiones de riesgo: a continuación se procede a la clasificación de regiones de riesgo, para lo cual se toma una valoración de alto, mediano y bajo riesgo, este proceso se realiza dividiendo la cantidad de niveles de riesgo/sensibilidad entre 4, el cociente se utiliza para indicar cuales celdas son de mayor riesgo, mediano riesgo y bajo riesgo. Así las celdas con niveles de riesgo/sensibilidad inferiores o iguales al cociente son las celdas de mayor riesgo, las celdas con niveles de riesgo/sensibilidad superiores al cociente e inferiores o iguales a tres veces el cociente son las de mediano riesgo, y las celdas con niveles de riesgo/sensibilidad superiores a tres veces el cociente son las celdas de bajo riesgo. (Ver Anexo 45).

En esta matriz se puede observar las distintas zonas como son alto riesgo que se encuentra de color rojo, mediano riesgo de color amarillo y bajo riesgo de color verde.

Entre las zonas de alto riesgo se encontraron perdida de archivos de datos, pérdida de equipos o herramientas que se encuentran dentro de las instalaciones,

suspensión del Sistema de Información Hospitalario (SIHOS), almacenamiento de copias de seguridad en las instalaciones, almacenamiento de archivos de datos en lugares no seguros, acceso ilegal a archivos de datos, modelo de arquitectura de información de los datos del Hospital Civil de Ipiales de la dependencia de sistemas, y del Sistema de Información Hospitalario (SIHOS).

3.4. EVALUACIÓN DE LA SEGURIDAD DEL SIHOS

3.4.1 Evaluación en cuanto funcionalidad del SIHOS: al realizar las entrevistas con varios usuarios que manejan el Sistema de Información Hospitalario (SIHOS) se encontró que:

Existen algunos inconvenientes al diligenciar el formato de AIEPI de los niños de 0-2 meses de 2-5 años y de las pacientes embarazadas ya que al diligenciar este formato no permite guardando continuamente los datos ingresados de manera que si el usuario comete algún error en cualquier casilla de los datos que se están diligenciando, el Doctor tiene que volver a llenar todo el formato lo que implica mayor tiempo de atención de cada paciente.

Existen errores en la prescripción de medicamentos por lo que la lista de medicamentos está incompleta así como el buscador de diagnósticos también está incompleto y en la evolución de imágenes diagnósticas los códigos son erróneos por lo que los Doctores escriben una nota aclaratoria en donde colocan el diagnóstico, los medicamentos que se le debe aplicar, y las imágenes diagnósticas de cada paciente.

Existen varios errores al diligenciar la historia clínica de los pacientes, por lo tanto cada paciente se ven obligado a acudir a la oficina de sistemas para que puedan cambiar datos y poder continuar con los diferentes tratamientos a cada diagnóstico y a realizar trámites que implican gastos a cada usuario.

3.4.2 Evaluación en cuanto Accesibilidad del SIHOS: en esta sección se evalúa el personal que tiene acceso a estos módulos y los permisos que tiene cada funcionario.

Al evaluar la accesibilidad al Sistema de Información Hospitalario (SIHOS) se encontró que todos los funcionarios de la dependencia acceden a todos los módulos del Sistema de Información, así como a las bases de datos sin existir permisos y restricciones a tablas o partes del sistema y de las bases de datos, lo

que implica que en el Sistema de Información Hospitalario se comentan varios errores y se pierda la confidencialidad.

Además no existe un documento de la administración de cuentas de usuarios que maneja el Sistema de Información Hospitalario (SIHOS).

No se ha realizado actualización periódica al Sistema de Información Hospitalario (SIHOS).

Dentro del sistema existe una sección de administración de cuentas de usuarios de todos los funcionarios que manejan el Sistema de Información. (Ver figura 5).

Figura 5. Administración de cuentas de usuarios del SIHOS.

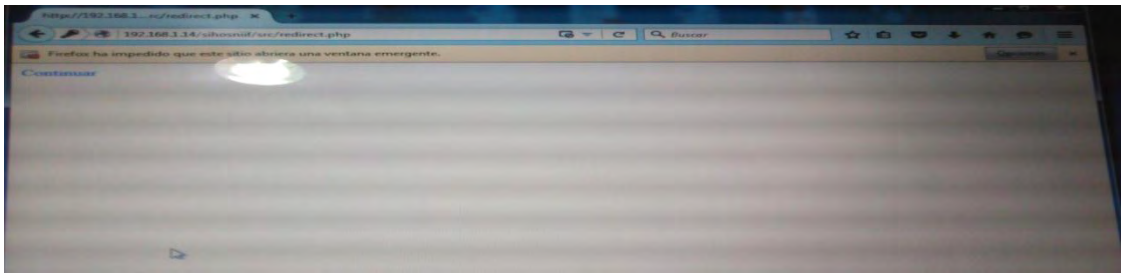
Fuente: Sistema de Información Hospitalario (SIHOS).

En la anterior figura se puede observar los distintos usuarios que tiene el Sistema de Información los cuales son Médicos Generales, Médicos Especialistas, auxiliares de enfermería, jefe de enfermería y los administrativos los cuales tienen permisos distintos de acuerdo al cargo que desempeñan como por ejemplo las auxiliares de enfermería solo tienen acceso al módulo de inscripción y comprobación de derechos y a el módulo de admisiones y los médicos tienen acceso al Sistema de acuerdo a la dependencia donde se encuentren si están en urgencias en consulta externa, o en cirugía tienen acceso a la historia clínica del paciente, nivel de triage, prescripción de medicamentos, ordenación de medicamento, procedimientos y laboratorio clínico.

3.4.3 Evaluación en cuanto portabilidad del SIHOS: al evaluar la portabilidad del Sistema de Información Hospitalario (SIHOS) se encontró que el sistema no funciona en los sistemas operativos de Linux y las distribuciones ya que solo trabaja en el navegador internet Explorer y en los demás navegadores como Mozilla Firefox, Google Chrome, Icewesel el Sistema de Información Hospitalario (SIHOS) no funciona.

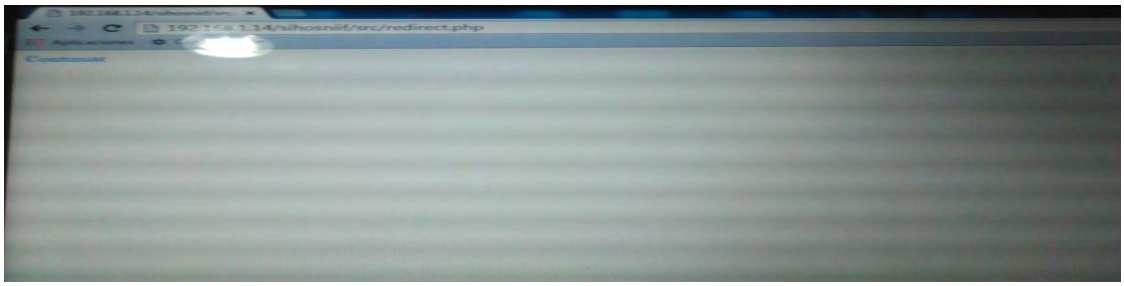
En las siguientes figuras se muestra que el Sistema de Información Hospitalario (SIHOS) no permite ingresar desde otros navegadores diferentes a internet Explorer. (Ver figuras 6,7,8)

Figura 6. De Navegabilidad a través Mozilla Firefox del SIHOS.



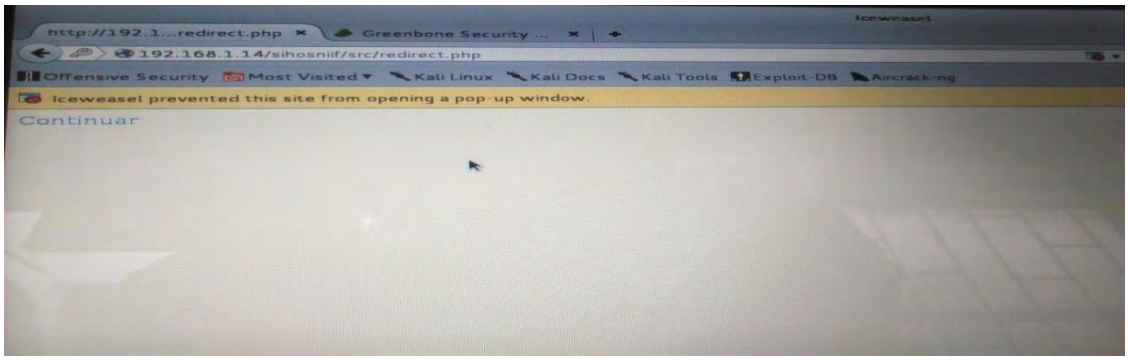
Fuente: Sistema de Información Hospitalario (SIHOS)

Figura 7. De Navegabilidad a través google Chrome del SIHOS.



Fuente: Sistema de Información Hospitalario (SIHOS)

Figura 8. De Navegabilidad a través Iceweasel del SIHOS.



Fuente: Sistema de Información Hospitalario (SIHOS)

De las figuras 6, 7 Y 8, se puede concluir que el Sistema de Información Hospitalario (SIHOS) no es portable ya que no se ejecuta en diferentes plataformas esto hace que el sistema se limite a trabajar en algunos navegadores y en varias ocasiones se hace necesario que el Sistema de Información permita trabajar desde distintos plataformas y poder remplazar el trabajo que se está ejecutando a través de otros navegadores e implementar un plan de contingencia sólido y ofrecer mayor portabilidad

3.4.4 Evaluación en cuanto confiabilidad del SIHOS: en este aspecto hace referencia a la confiabilidad del Sistema de Información Hospitalario (SIHOS) garantizando seguridad a los usuarios y los procesos que se manejan lo que incluye ausencia de errores, utilización de estándares, existencia de vínculos externos.

Los ítems que se evaluaron fueron:

- ✓ Deficiencia de errores
- ✓ Actualización periódica del Sistema de Información Hospitalario (SIHOS)

Al evaluar estos ítems se encontró que el sistema no es confiable ya que al obtener algunos reportes de los pacientes no son confiables porque cada día salen diferentes valores que hacen que el usuario no conozca el valor exacto de los distintos tipos de reportes para realizar investigaciones y trabajar en informes.

Por ejemplo, cuando el equipo médico pide el reporte de los índices morbilidad cada día salen reportes con diferentes resultados que hacen que no se pueda

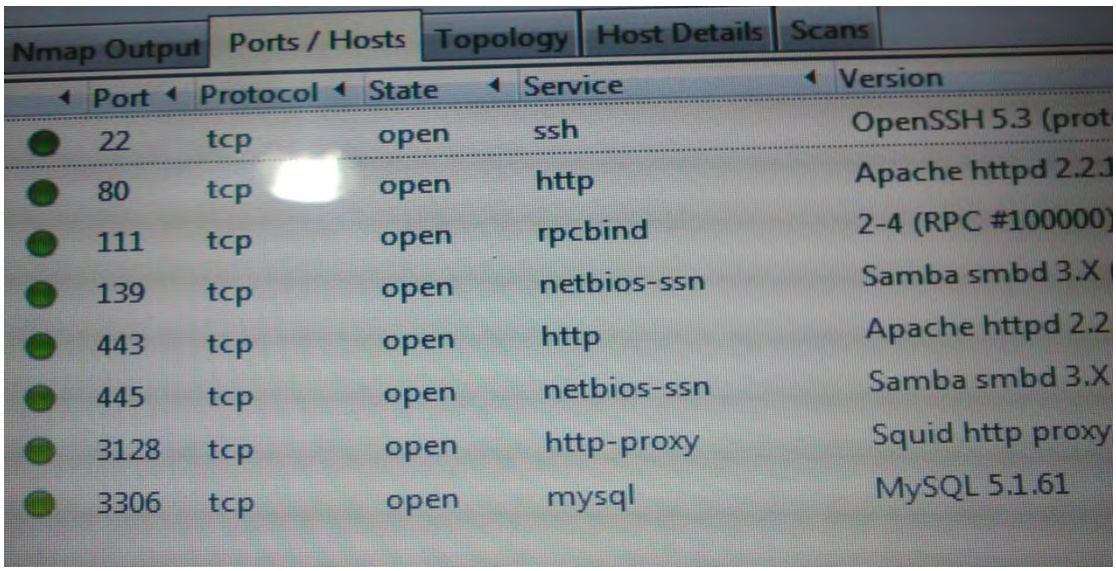
trabajar con dicha información por lo que no es confiable y de esta manera se retrasen actividades pendientes por desarrollar.

Para evaluar este ítem también se realizó algunas pruebas con algunas herramientas que permiten detectar vulnerabilidades a cualquier sistema de información, en este caso se realizó el escaneo al servidor que maneja el Sistema de Información Hospitalario (SIHOS), en el cual se pudo detectar algunas vulnerabilidades del sistema como son:

Puertos abiertos como el puerto 22 ssh , puerto 80 Http, puerto 139 de Samba, puerto 3128 de servicios Squid, puerto 3306 Mysql que en cualquier momento se podría iniciar un ataque través de estos puertos abiertos y entrar a cualquier servicio y adueñarse del Sistema.

A continuación, se muestra una figura del escaneo con la herramienta Zenmap.(Ver figura 9)

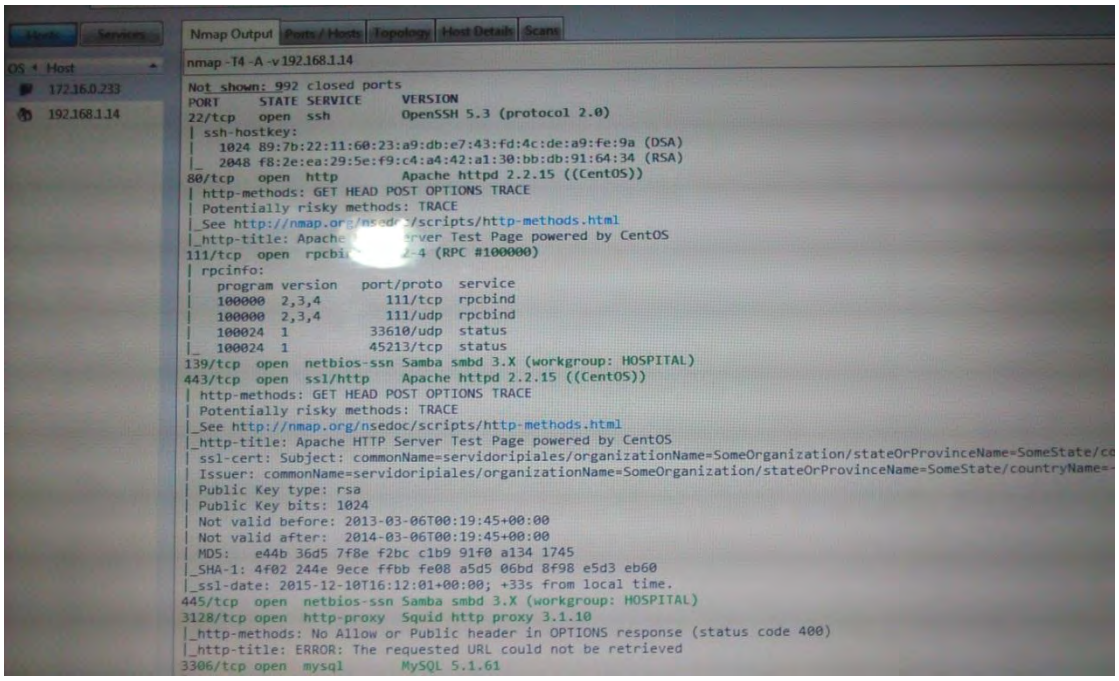
Figura 9. Escaneo de Puertos con Zenmap.



Fuente: Sistema de Información Hospitalario (SIHOS).

En la figura 9 se observar los distintos puertos que se encuentran abiertos lo que puede provocar inseguridad en el Sistema de Información Hospitalario (SIHOS), debido a que cualquier atacante puede intentar ingresar al sistema y obtener información sensible que maneja el sistema.

Figura 10. Versión de cada uno de los servicios instalados.

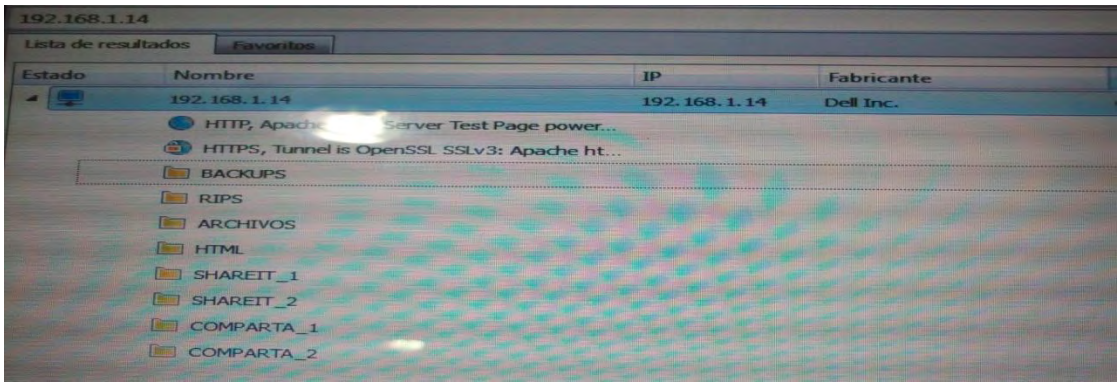


Fuente: Sistema de Información Hospitalario (SIHOS)

Además se accedió a algunos documentos almacenados en el servidor del Sistema de Información Hospitalario (SIHOS) en donde se observó algunas copias de seguridad almacenadas dentro de este servidor.

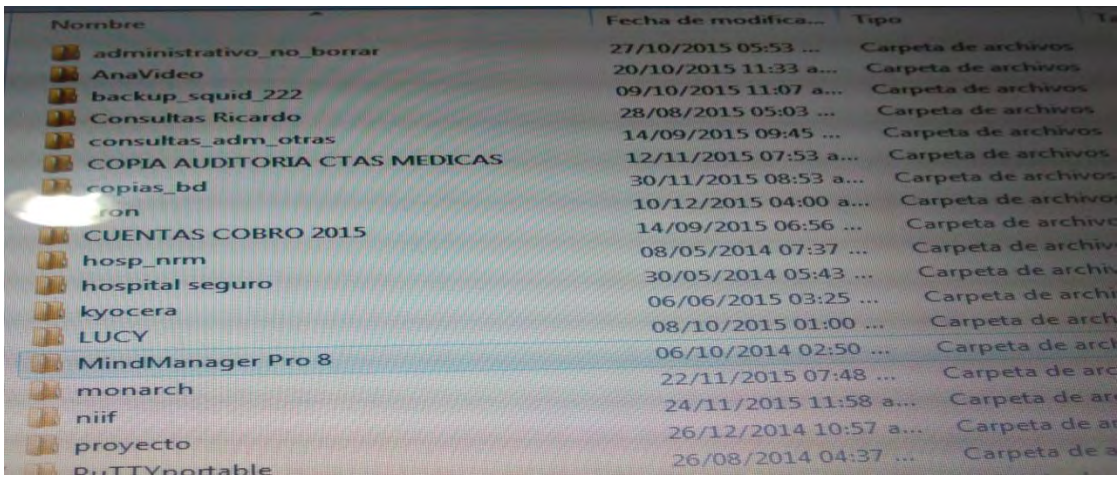
En la figura 11, se puede observar el acceso a los documentos del servidor del Sistema de Información Hospitalario (SIHOS).

Figura 11. Acceso a documentos del servidor del SIHOS.



Fuente: Sistema de Información Hospitalario (SIHOS)

Figura 12. Acceso a la carpeta de backups del servidor del SIHOS.



Fuente: Sistema de Información Hospitalario (SIHOS)

En las anteriores figuras, se muestra como se accedió a algunas copias de seguridad y documentos del servidor del Sistema de Información Hospitalario (SIHOS), lo que puede inducir a que intrusos accedan a estas copias puedan consultar, modificar y eliminar información importante del Sistema de Información Hospitalario (SIHOS) en donde se pueden ver afectados los pacientes, administrativos y empleados del Hospital Civil de Ipiales.

También se realizó algunas pruebas con la herramienta Openvas en kali Linux en la cual se pudo observar otras vulnerabilidades a las que se encuentra expuesto el servidor del Sistema de Información Hospitalario (SIHOS).

Existe una vulnerabilidad con Openssl ya que no se encuentra actualizado lo cual permite a los atacantes explotar esta vulnerabilidad y obtener información sensible y adquirir la capacidad de leer, insertar y modificar datos, información o mensajes que se trasmite a través del servidor del Sistema de Información Hospitalario (SIHOS). Además Openssl no restringe adecuadamente el procesamiento de los mensajes lo que puede provocar a un atacante secuestrar sesiones y obtener información por medio de inyección CSS

El certificado SSL del servidor remoto no se encuentra actualizado ya que caduco el 3 de junio de 2014. Además, existen certificados con cifrados débiles, los cuales son SSLV2,RC4, y cifrados utilizados de 64 bits que se considera que son vulnerables a métodos de la fuerza bruta.

Además, se encontró que no se está utilizando el cifrado SSLV2 por lo tanto se recomienda deshabilitar este servicio y añadir el cifrado SSLV3 ya que el servicio SSLV2 puede comprometer la seguridad de los datos, y utilizar la criptografía conocida para espiar la conexión entre los clientes y el servicio para tener acceso a la información transferida a través de la red del Sistema de Información Hospitalario (SIHOS).

3.4.5 Evaluación en cuanto usabilidad del SIHOS: en esta sección se evalúan aspectos referentes en cuanto a facilidad de uso del sitio, que permiten identificar el nivel de comprensión y facilidad de uso para todo el personal que utiliza el Sistema de Información Hospitalario (SIHOS).
Los aspectos que se evaluaron fueron:

- ✓ Comprensibilidad del sitio.
- ✓ Mecanismos de ayuda y retroalimentación en línea
- ✓ Aspectos de interfaces.
- ✓ Usabilidad de textos.

Al evaluar el Sistema de Información Hospitalario (SIHOS) en cuanto a la usabilidad se encontró que la ventana del módulo de admisiones y urgencias presenta un texto legible y conciso pero no existen opciones de navegabilidad en multi dispositivos, además existen pocos mecanismos de ayuda y retroalimentación del Sistema de Información Hospitalario (SIHOS) y los pocos manuales de los módulos se encuentran desactualizados.

4. INFORMES FINALES DE AUDITORÍA

4.1 INFORME GENERAL DE AUDITORÍA

4.1.1 Objetivo general

Evaluar del Sistema de Información Hospitalaria (SIHOS) al Hospital Civil de Ipiales basado en el estándar COBIT 4.1que permita establecer recomendaciones necesarias para su mejoramiento.

4.1.2 Objetivos específicos

- Identificar el contexto en el manejo del Sistema de Información Hospitalaria (SIHOS) en el Hospital Civil de Ipiales.

- Diseñar técnicas e instrumentos de recolección de información que permitan evaluar el desempeño del Sistema de Información Hospitalaria (SIHOS).

- Evaluar la seguridad del Sistema de Información Hospitalaria (SIHOS).

- Estructurar el informe final del diagnóstico con los hallazgos, evidencias y recomendaciones.

4.1.3 Alcance y delimitación.

La auditoría se realizó al Sistema de Información Hospitalaria (SIHOS) en el Hospital Civil de Ipiales ubicado en el Departamento de Nariño en la frontera con la República del Ecuador, en el área de Auditoría de Sistemas y se enfocó al sistema de información.

Para evaluar el sistema de información hospitalaria (SIHOS) se tuvieron en cuenta las características de calidad del estándar COBIT 4.1 como son

- Funcionalidad
- Usabilidad
- Portabilidad
- Accesibilidad

- Confiabilidad

A continuación se presentan los resultados obtenidos de la auditoria aplicada al Sistema de Información Hospitalario (SIHOS), de acuerdo a los dominios de COBIT 4.1.

4.2 DOMINIO PLANEAR Y ORGANIZAR (PO).

4.2.1 P01 Definir la planeación estratégica.

Hallazgo 1.

El plan operativo anual no se encuentra bien definido, falta implementar algunos procesos para gestionar de manera adecuada las Tecnologías de Información

Recomendaciones.

- El plan estratégico o plan operativo anual debe definir como contribuir a los objetivos estratégicos de los recursos de la información así como metas, costos, riesgos, fuentes de financiamiento, estrategia de adquisición y requerimientos legales, es decir en este plan se define como se cumplirán y medirán los objetivos de una manera adecuada.

- El plan estratégico debe estar lo suficientemente detallado para permitir la definición de planes tácticos de Tecnologías de Información.

- En el plan táctico se debe describir las iniciativas y los recursos requeridos por las Tecnologías de Información así como monitorear y administrar el uso de recursos y el logro de beneficios de una forma activa.

- Tomar decisiones a partir el plan estratégico que permitan implementar acciones correctivas.

- Evaluar el desempeño de los planes existentes en cuanto a contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.

4.2.2 P02. Definir la arquitectura de información.

Hallazgo 1.

No existe un modelo de arquitectura de información por lo tanto la información se encuentra desordenada y dispersa.

Recomendaciones.

- Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI.

- Este modelo incluye
  - Diccionario de datos que incluya reglas de sintaxis
  - Esquema de clasificación de los datos e información.
  - Documentación de planes existentes

- Definir procedimientos para garantizar la integridad de los datos almacenados en bases de datos, archivos de datos, copias de seguridad.

- Actualizar el manual del Sistema de Información Hospitalario (SIHOS).

- Actualizar el diccionario de datos.

- Realizar mantenimiento a los planes, manuales y documentos.

- Asignar roles y permisos para acceder a secciones o partes de las bases de datos que maneja el Sistema de Información Hospitalario (SIHOS).

- Diseñar el modelo relacional de las bases de datos del Sistema de Información Hospitalario (SIHOS).

- Mantener actualizado el modelo relacional de las bases de datos.

- Registrar las bases de datos a la superintendencia de industria y comercio vía internet.
- Asignar personal que se responsabilice del modelo de arquitectura de información.

- Asignar un comité que proporcione directrices sobre la arquitectura, verifique el cumplimiento y brinde asesoría sobre su aplicación.

Hallazgo 2.

No se ha implementado herramientas de seguridad que permitan minimizar los riesgos a los cuales está expuesto el Sistema de Información Hospitalario (SIHOS) y los datos.

Recomendaciones.

- Proporcionar procedimientos y herramientas que permitan enfrentar responsabilidades de propiedad de los datos y del Sistema de Información Hospitalario (SIHOS).

- Realizar un plan de pruebas de seguridad utilizando distintas herramientas existentes.

- Someter al Sistema de Información Hospitalario (SIHOS) a las pruebas planeadas en el cronograma.

- Tomar decisiones sobre cómo proteger el Sistema y sus datos de acuerdo a los resultados arrojados de las pruebas realizadas.

4.2.3 P04. Definir los procesos, organización y relaciones de TI.

Hallazgo 1.

No se ha definido un marco de trabajo de procesos de Tecnologías de Información para ejecutar el plan estratégico.

No existen planes alternativos para remplazar algún funcionario en caso de ausencia.

No se realiza evaluaciones en cuanto a desempeño de los funcionarios en la dependencia de Sistemas.

Recomendaciones.

- Diseñar un marco de trabajo de TI que incluya medición del desempeño, mejora cumplimiento de metas y planes para alcanzarlas.

- Definir y comunicar roles y responsabilidades para el personal de Tecnologías de Información y establecer rendición de cuentas para alcanzar las metas propuestas.

- Planear actividades o estrategias para remplazar algún funcionario en caso de ausencia, y evitar sobrecarga de actividades a algún funcionario.

- Planear una evaluación de cómo se están ejecutando las actividades y responsabilidades asignadas a cada funcionario y establecer pautas de mejoramiento.

Hallazgo 2.

No se ha establecido una estructura organizacional interna que refleje las necesidades de la dependencia.

Recomendación.

Establecer una estructura organizacional interna que refleje las necesidades de la dependencia e implementar un proceso para revisar la estructura organizacional de forma periódica para ajustar los requerimientos del personal y de estrategias internas.

4.2.4 P08 Administración de la calidad.

Hallazgo 1.

En el Hospital Civil de Ipiales en la dependencia de sistemas cuenta con distintos procedimientos como son:

- Plan de mejoramiento del Sistema de Información Hospitalario (SIHOS).
- Seguimiento a la ejecución de políticas por medio de indicadores trimestrales basados en la norma ISO 90001.
- Plan de gerencia de la información que está en desarrollo.
- Matriz de necesidades de Recursos de Información.

Pero no existen políticas que estén guiadas a la calidad del Sistema de Información Hospitalario (SIHOS).

Recomendación.

- Se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares probados de desarrollo y de adquisición.

- Identificar requerimientos criterios de calidad, procesos claves de Tecnologías de Información y métodos para definir, detectar, corregir y prever las no conformidades.

- Facilitar por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad, requerimientos y políticas claras de calidad.

- Adoptar y mantener estándares para todo desarrollo y adquisición que siga el ciclo de vida hasta el último entregable. Los estándares a considerar son

    - Estándares de codificación de software
    - Estándares de diseño
    - Estándares de adquisición

- Realizar constante monitoreo y comunicación de los resultados a los interesados que permitan tomar decisiones correctiva y preventivas.

- Mantener y comunicar regularmente el plan de calidad que promueva la mejora continua.

4.2.5 P09. Evaluar y administrar los riesgos de TI.

Hallazgo 1.

En la dependencia de sistemas se encuentran identificados los riesgos de acuerdo a cada proceso y a cada dependencia en una matriz de identificación, además se encuentra una tabla de priorización de riesgos, pero no se ha establecido respuesta a los riesgos identificados.

Recomendación.

- Establecer un plan de respuesta a los riegos que se encuentran identificados de acuerdo a cada proceso.

Hallazgo 2.

No se ha establecido respuesta a diferentes riesgos que se encuentran identificados.

Recomendación.

- Se debe implementar en este plan procesos de respuesta a riesgos o amenazas que necesitan de infraestructura tecnológica (equipos, instalaciones, software).

- Incluir dentro del plan de contingencia de Sistemas de Información y comunicaciones los riesgos identificados en la matriz de riesgos por procesos y establecer mecanismos que minimicen o reduzcan el nivel de impacto.

- Realizar periódicamente un reporte de los riegos evaluados del Sistema de Información Hospitalario (SIHOS) y de la dependencia de sistemas.

- Actualizar y mantener los documentos de la administración de riesgos.

Hallazgo 3.

La mayoría de los funcionarios tienen acceso a la base de datos del Sistema de Información Hospitalario (SIHOS).

Recomendación.

- Asignar roles y permisos para los funcionarios que tiene acceso a la base de datos.

- Permitir el acceso a la base de datos a tablas o secciones según necesite cada funcionario.

- Minimizar el ingreso de varias personas a las bases de datos del Sistema de Información Hospitalario (SIHOS).

4.3 DOMINIO ADQUIRIR E IMPLEMENTAR (AI).

4.3.1 AI2 Adquirir y mantener software aplicativo.

Hallazgo 1.

En varias ocasiones el Sistema de Información Hospitalario (SIHOS) no está disponible.

Recomendación.

- Tener plantas eléctricas en caso de que la energía prestada por el proveedor falle.

- Realizar mantenimiento periódico a la infraestructura tecnológica.

- Implementar servidores espejo que permitan que el Sistema de Información Hospitalario siga funcionando de manera adecuada.

- Realizar una documentación en una bitácora de las amenazas riesgos y vulnerabilidades del Sistema de Información Hospitalario (SIHOS).

- Definir medidas de seguridad para que no vuelva a ocurrir.

- Tener en cuenta los factores económicos y el estudio de factibilidad para los cambios en el Sistema de Información Hospitalario (SIHOS).

Hallazgo 2.

Se está trabajando en plan de aseguramiento de la calidad de la información que es el plan de Gerencia de la Información.

Recomendación

- Antes de implementar el plan de aseguramiento de la información se debe terminar todas las estrategias planteadas en este y luego se debe someter a pruebas, e implementar las acciones correctivas que arrojaron las pruebas realizadas.

- Realizar constante mantenimiento y monitoreo.

- Establecer personas responsables de la calidad de la Información que se maneja en el plan de gerencia de la información.

Hallazgo 3.

No existe un plan de pruebas al Sistema de Información Hospitalario (SIHOS).

No existe un plan de mantenimiento al Sistema de Información Hospitalario (SIHOS).

Recomendación.

- Diseñar e implementar un plan de pruebas al Sistema de Información Hospitalario (SIHOS).

- Actualizar y mantener el plan de pruebas al Sistema de Información Hospitalario (SIHOS).

- Diseñar e implementar un plan de mantenimiento al Sistema de Información Hospitalario (SIHOS), que permita medir el desempeño del sistema, el plan debe incluir mantenimiento preventivo, detectivo y correctivo.

Hallazgo 4.

Existen escasas medidas de seguridad del Sistema de Información Hospitalario.

Recomendación.

- Implementar herramientas y configurar los sistemas de tal manera que bloqueen los accesos indebidos al Sistema de Información Hospitalario (SIHOS) por medio de puertos abiertos, acceso indebido a la red, accesos a las bases de datos que se manejan.

- Abordar la seguridad de las aplicaciones y los requerimientos en respuesta a los riesgos identificados y clasificación de datos, la arquitectura de la información, seguridad de la información y la tolerancia a riesgos.

Hallazgo 5.

El Hospital Civil de Ipiales cuenta con una matriz de identificación de necesidades del proceso de recursos de la información, lo cual permite identificar las necesidades del Sistema de Información Hospitalario (SIHOS) y de la dependencia, pero no existe un plan de adquisición de infraestructura tecnológica que garantice un soporte tecnológico continuo par las aplicaciones, además la identificación de necesidades se encuentra desactualizada.

Recomendación.

- Actualizar el proceso de identificación de necesidades de recursos de información con el fin de conocer que necesidades de los años anteriores que ya se han implementado y priorizar las necesidades del año en curso.

- Generar un plan para adquirir, Implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos de los recursos de la información, y que esté de acuerdo con la

dirección tecnológica del Hospital Civil de Ipiales.

- Dentro del plan de adquisición de infraestructura tecnológica se debe incluir la matriz de identificación de necesidades de los recursos de la información por año.

- De acuerdo a las necesidades plasmadas en la matriz el plan de adquisición debe contener costos, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología y viabilidad comercial.

- Implementar medidas de control para seguridad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.

4.3.2 AI3 Adquirir y mantener infraestructura tecnológica.

Hallazgo 1.

- No existen procesos para adquirir e implementar y actualizar la infraestructura tecnológica

Recomendación.

- Generar un plan para adquirir implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos del Hospital Civil de Ipiales.

- Implementar medidas de control para seguridad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.

- Establecer un ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo.

- Dar a conocer a todo el personal involucrado en el proceso de recursos de la información

- Se debe monitorear y evaluar uso de los recursos del plan de adquisición de infraestructura tecnológica.

- Para la implementación de estrategias y metodologías de adquisición se puede tener en cuenta aspectos que se definen el libro PMBOOK.

Hallazgo 2.

No existe un manual de funciones para el personal encargado de realizar mantenimiento prevetivo y correctivo.

Recomendación.

- Diseñar e implementar un manual de funciones que se bebe tener en cuenta a la hora de realizar cualquier tipo de mantenimiento.

- En el manual de funciones se debe contemplar espacios y herramientas para realizar un mantenimiento adecuado y no interrumpir las actividades que se están desarrollando.

- Con la implementación de esta manual permite que disminuir diferentes errores que se presentan cuando no se tiene en cuenta actividades, herramientas y estrategias adecuadas para realizar mantenimiento.

4.3.3 AI4 Facilitar la operación y el uso.

Hallazgo 1.

Falta implementación de planes de entrenamiento a los funcionarios que manejan las tecnologías de información ya que existen errores básicos del manejo de los equipos y del sistema que cada usuario lo puede solucionar de una manera adecuada.

Recomendación

- Trasmitir el conocimiento y habilidades a los usuarios finales utilicen con efectividad y eficiencia las tecnologías de información (sistemas de información, redes de internet, equipos software, hardware).

- La transferencia de conocimiento incluye desarrollo de un plan de entrenamiento continuo, así como desarrollo de habilidades, materiales de entrenamiento, manuales de usuario, ayuda en línea en caso de los sistemas de información y administración de usuarios.

4.3.4 AI6 Administrar cambios.

Hallazgo 1.

No se ha establecido procedimientos formales para los cambios realizados al Sistema de Información Hospitalario (SIHOS).

Recomendación.

- Llevar una documentación en bitácoras del proceso de cambios en el sistema de Información Hospitalaria (SIHOS).

- Evaluar el impacto de los cambios realizados sobre el Sistema de Información Hospitalario (SIHOS).

- Establecer un proceso para definir plantear evaluar y autorizar cambios de emergencia que no sigan el proceso de cambio establecido.

- Establecer un plan de pruebas al Sistema de Información Hospitalario (SIHOS) después de los cambios realizados.

- Mantener actualizado la bitácora de los cambios realizados.

4.4 DOMINIO ENTREGAR Y DAR SOPORTE.

4.4.1 DS4 Garantizar la continuidad del servicio.

Hallazgo 1.

Existe un plan de continuidad de sistemas de información y comunicaciones, pero este plan se está corrigiendo y realizando varios ajustes.

No existe una guía de cómo se debe utilizar el plan de continuidad de sistemas de información y comunicaciones.

Recomendación.

- Dentro del plan de continuidad se bebe describir el riesgo o la amenaza luego establecer paso a paso las acciones que se deben realizar para mitigarlos, de manera que el personal conozca los pasos que debe seguir de manera consecutiva para dar continuidad a los sistemas.

- Dentro del plan de continuidad se debe incluir todos los procesos de los recursos de la información es decir establecer de manera ordenada procesos de continuidad para:

    - El Sistema de Información Hospitalario (SIHOS) (hardware, software, red)
    - La dependencia de sistemas
    - Los recursos humanos

- Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación.

- Establecer actividades y estrategias para minimizar los riesgos que se presentan en los sitios más críticos.

- Diseñar una guía que permita identificar como utilizar el plan de continuidad.

- Probar el plan de continuidad de manera periódica.

- Actualizar y realizar mantenimiento al plan de continuidad de sistemas de Información y comunicaciones.

-

Hallazgo 2.

Se realiza copias de seguridad dentro de la dependencia, pero estas copias no son almacenadas en un lugar seguro en donde se restringa el acceso a ellas.

No se realizan copias de seguridad fuera de la dependencia de sistemas es decir en otro lugar, pero dentro del Hospital Civil de Ipiales

No se realizan copias de seguridad fuera de las instalaciones del Hospital Civil de Ipiales

Recomendación.

- Establecer un espacio seguro para guardar las copias de seguridad dentro de la dependencia, donde no todo el personal que ingrese a la dependencia tenga acceso fácil a ellas.

- Realizar las copias de seguridad en un servidor que este ubicado en un cuarto exclusivo para los servidores en donde se restringa el acceso a personal no autorizado.

- Realizar copias de seguridad a través de acuerdos de tecnologías en la nube que permitan ofrecer mayor seguridad de la Información y de los datos almacenados.

- Monitorear y evaluar los procedimientos post reanudación.

Hallazgo 3.

No se lleva una documentación de las interrupciones que se han presentado en el Sistema de Información Hospitalario (SIHOS).

Recomendación

- Llevar una documentación de las dificultades que ha tenido el Sistema de Información Hospitalario (SIHOS), así como las acciones correctivas o

preventivas que se implementó para cada vulnerabilidad o riesgo que se presentó en el sistema.

- Esta documentación permite evaluar y tomar decisiones con respecto al funcionamiento del Sistema de Información Hospitalario (SIHOS) de años anteriores al estado actual.

- Mantener actualizado la documentación de implementaciones que se le ha realizado al Sistema de Información Hospitalario (SIHOS).

4.4.2 DS5 Garantizar la seguridad de los sistemas.

Hallazgo 1.

Se está trabajando en el plan de gerencia de la información en donde se encuentran contemplado la utilización de los recursos de la información de manera adecuada.

Recomendación.

- Dar a conocer el plan de gerencia de la información a todo el personal involucrado.

- Monitorear y realizar seguimiento a los procesos implementados en este plan**.**

Hallazgo 2.

No se ha contemplado estrategias de seguridad para el acceso a los sistemas informáticos ya que el sistema de información Hospitalario maneja la seguridad básica.

No se tiene contempladas medidas de seguridad para personas o intrusos que pueden ingresar al Sistema de Información Hospitalario (SIHOS).

Recomendación.

- Se recomienda planear y ejecutar un plan de pruebas con herramientas como kali Linux back track y demás herramientas existentes para analizar el Sistema de Información Hospitalario (SIHOS) en su totalidad.

- Realizar un análisis a los resultados que arrojaron las pruebas y establecer acciones correctivas que permitan mejorar la seguridad del Sistema de Información Hospitalario (SIHOS).

4.4.3 DS7 Educar y entrenar a los usuarios.

Hallazgo 1.

En la dependencia de sistemas existe una persona encargada de la administración de cuentas de usuarios, pero no existe un documento de la administración de cuentas de usuarios.

Recomendación

- Diseñar un documento de administración de cuentas de usuarios en donde se especifiquen los roles y permisos que tiene cada usuario al Sistema de Información Hospitalario (SIHOS), así como el acceso de los funcionarios a fragmentos o tablas de las bases de datos que conforman el sistema.

- Mantener actualizado y vigilado el documento de administración de cuentas de usuarios.

Hallazgo 2.

Existen escasas capacitaciones dentro y fuera de la dependencia del Hospital Civil de Ipiales por lo que se presentan varios errores en la utilización de tecnologías de información.

Recomendación.

- Capacitar a los usuarios con respecto a las tecnologías de información (planes existentes, sistemas de información, hardware, software) dentro de la dependencia y fuera de la dependencia con el propósito de disminuir errores que presentan los usuarios.

- Al terminar la capacitación evaluar los aspectos expuestos durante la capacitación.

Hallazgo 3.

Cada usuario del sistema de información Hospitalario (SIHOS) tiene asignada su contraseña pero no se exige el cambio periódico de contraseñas.

Recomendación.

- Realizar capacitaciones en donde se divulguen políticas de control de contraseñas que incluyan:

    - Cambio periódico de contraseña
    - Longitud adecuada de contraseña
    - Combinaciones alfanuméricas obligatorias
    - Protección de contraseñas

- Exigir el cambio periódico de contraseñas cada cierto tiempo

4.4.4 DS8 Administrar la mesa de servicio y los incidentes.

Hallazgo 1.

En el Hospital civil de Ipiales existe una permanente comunicación con el usuario para registrar informar atender y analizar incidentes reportados con respecto a las tecnologías de información, para lo cual existe un cronograma para entender incidentes que se reporten durante las 24 horas, este cronograma de atención está a cargo de los funcionarios del área de sistemas.
De manera que haya algún inconveniente en alguna dependencia o en el Sistema de Información Hospitalario (SIHOS) se llama al funcionario de turno, para que solucione de manera adecuada los inconvenientes que se presenten, pero en varias ocasiones los funcionarios llaman al personal de turno por inconvenientes que son muy básicos y que no amerita llamar al personal de sistemas para que los solucione.

Recomendación

- Planear y ejecutar capacitaciones del uso de tecnologías de información en donde se incluya hardware, software, Sistemas de Información, redes de datos, y aspectos básicos que debe conocer cualquier funcionario para hacer uso correcto de las tecnologías.

- Realizar volantes en donde se explique cómo hacer un adecuado de las tecnologías de Información.

4.4.5 DS9 Administrar la configuración.

Hallazgo 1.

El Hospital Civil de Ipiales cuenta con un ambiente de configuración de las tecnologías, ya que existen políticas con respecto a la utilización de software y equipos, además la configuración la realiza únicamente el personal autorizado.

4.4.6 DS12 Administración del ambiente físico.

Hallazgo 1.

En la dependencia de sistemas no es adecuada para trabajar ya que existen dificultades para movilizase, debido a que en la dependencia existe un cuarto donde se encuentran servidores, y también se realiza mantenimiento a los equipos de cómputo.

Recomendación.

- Definir y seleccionar el centro de datos para soportar la estrategia de tecnología.

- Esta selección y diseño del esquema del centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.

- Establecer procedimientos de seguridad para el acceso a la dependencia.

- Establecer un espacio para realizar mantenimiento a los equipos.

- Reubicar los servidores a un lugar en un cuarto solo para servidores.

- Proporcionar y mantener un ambiente físico adecuado para proteger los activos de Tecnologías Información contra acceso, daño o robo.

Hallazgo 2.

Dentro de la dependencia de sistemas no se encuentran señalizaciones adecuadas para salidas de emergencia.

No se ha prohibido a las personas el consumo de alimentos y debidas dentro de la dependencia.

Recomendación.

- Diseñar señalizaciones de emergencia dentro de la dependencia de sistemas.

- Ubicar carteles en lugares visibles donde se prohíba el consumo de alimentos y bebidas dentro de la dependencia.

Hallazgo 3.

No existen planes alternativos en caso de que los extintores instalados dentro de la dependencia de sistemas fallen.

Recomendación.

- En el plan de contingencia de Sistemas de Información y comunicaciones se debe implementar actividades alternas para dar continuidad a las instalaciones y tecnologías de información.

4.5. DOMINIO MONITOREAR Y EVALUAR (ME).

4.5.1 ME1 Monitorear y evaluar el desempeño de TI.

Hallazgo 1.

No se ha evaluado el desempeño del Sistema de Información Hospitalario (SIHOS) teniendo en cuenta las metas acordadas.

Recomendación.

- Diseñar una evaluación al desempeño del Sistema de Información Hospitalario (SIHOS), en la cual incluya actividades que se han propuesto para el cumplimiento de las metas establecidas, lo cual nos permite identificar las metas atrasadas y dar prioridad de acuerdo a cada meta.

- Establecer un marco de trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para medir la solución y la entrega de servicios de TI.

- Garantizar que el proceso de monitoreo implante un método que brinde un de desempeño adecuado de las Tecnologías de Información.

- Identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes.

4.4.2 ME2 Monitorear y evaluar el control interno.

Hallazgo 1.

No existen políticas o estrategia para monitorear actividades encaminadas a brindar seguridad del Sistema de Información Hospitalario (SIHOS).

Recomendación.

Establecer y direccionar políticas que permitan prevenir ataques al Sistema de Información Hospitalario (SIHOS).

5. HALLAZGOS Y RECOMENDACIONES DE ACUERDO A LA EVALUACIÓN DE LA SEGURIDAD DEL SISTEMA DE INFORMACIÓN HOSPITALARIO (SIHOS).

5.1 Evaluación en cuanto a funcionalidad del SIHOS

Hallazgo 1.

Existen algunos inconvenientes al diligenciar el formato de AIEPI de los niños de 0-2 meses de 2-5 años y de las pacientes embarazadas ya que al diligenciar este formato no permite guardar continuamente los datos ingresados de manera que si se comete algún error en cualquier casilla de los datos que se están diligenciando, el Doctor debe volver a llenar todo el formato lo que implica tiempo de atención de cada paciente.

Recomendación.

- Se debe implementar botones de modificar y guardar que permita ir guardando continuamente los datos que se están ingresando de manera que cuando haya algún error se permita restaurar a una versión anterior o modificar cualquier dato y no se pierdan totalmente los datos diligenciados y se tenga que volver a llenar.

Hallazgo 2.

Existen errores en la prescripción de medicamentos por lo que la lista de medicamentos está incompleta así como el buscador de diagnósticos también está incompleto y en la evolución de imágenes diagnosticas los códigos son erróneos por lo que los Doctores escriben una nota aclaratoria en donde colocan el diagnóstico, los medicamentos que se le debe aplicar, y las imágenes diagnosticas de cada paciente.

Recomendación.

- Realizar modificaciones y actualizaciones en la lista de medicamentos, el buscador de diagnósticos, verificar e implementar los códigos válidos y completos de imágenes diagnósticas para cada paciente.

- Realizar monitoreo continuamente a la prescripción y ordenación de medicamentos e implementar medicamentos actualizados y todos los diagnósticos de los pacientes.

Hallazgo 3.

Existen varios errores al diligenciar la historia clínica de los pacientes por lo tanto cada paciente se ven obligado a acudir a la oficina de sistemas para que puedan cambiar datos y poder continuar con los diferentes tratamientos a cada diagnóstico y a realizar trámites que implican gastos a cada usuario.

Recomendación.

- Realizar evaluación del Sistema de Información junto con los usuarios que manejan el sistema a fin de detectar fallas que se presentan e implementar mejorías a tiempo que permitan disminuir el número de usuarios que se deben atender en la dependencia de sistemas y en muchas ocasiones retrasar trabajo pendiente.

- Realizar reuniones mensuales para verificar el funcionamiento del Sistema de Información Hospitalario (SIHOS) de acuerdo a cada dependencia.

5.2 Evaluación en cuanto a accesibilidad del SIHOS

Hallazgo 1.

Todos los funcionarios de la dependencia acceden a todos los módulos del Sistema de Información, así como a las bases de datos sin existir permisos y restricciones a tablas o partes del sistema y de las bases de datos, lo que implica que se pierda la confidencialidad.

Recomendación.

- Asignar roles y permisos para los funcionarios que tiene acceso a la base de datos.

- Permitir el acceso a la base de datos a tablas o secciones según necesite cada funcionario.

5.3 Evaluación en cuanto a portabilidad del SIHOS

Hallazgo 1.

El sistema no funciona en los sistemas operativos de Linux y las distribuciones ya que solo trabaja en el navegador internet Explorer y en los demás navegadores como mozilla firefox, google chrome, icewesel el Sistema de Información Hospitalario (SIHOS) no funciona.

Recomendación.

- Se debe implementar o desarrollar para que el Sistema de Información Hospitalario (SIHOS) funcione en distintos sistemas operativos como Linux y sus distribuciones y de esta manera se pueda ejecutar en varios navegadores como icewesel google chrome, Firefox lo que permite que el sistema sea portable y mejore su rendimiento.

5.4 Evaluación en cuanto a confiabilidad del SIHOS

Hallazgo 1.

El sistema no es confiable ya que al sacar algunos reportes de los pacientes no son confiables porque cada día salen diferentes valores que hacen que el usuario no conozca el valor exacto de los distintos tipos de reportes para realizar investigaciones y trabajar en informes.

Recomendación.

- Realizar seguimiento a todo tipo de reporte que se realizan a través del Sistema de Información Hospitalario (SIHOS).

Hallazgo 2.

Existen distintos puertos como son ssh, mysql, squid, samba que se encuentran abiertos y en cualquier momento un atacante puede aprovechar estas

vulnerabilidades e iniciar un ataque a través de cualquier puerto y acceder a la información contenida en algún servicio.

Recomendación.

- Restringir el acceso a los puertos mencionados anteriormente.

Hallazgo 3.

A través del servidor se pudo acceder a algunas copias de seguridad.

Recomendación.

- Restringir el acceso a las copias de seguridad a través de contraseñas de seguridad con una seguridad alta teniendo en cuenta los distintos parámetros para la creación de estas.

- Realizar constante monitoreo a las copias de seguridad y cambiar periódicamente las contraseñas.

5.5 Evaluación en cuanto a usabilidad del SIHOS

Hallazgo 1.

Al evaluar el módulo de admisiones y urgencias presenta un texto legible y conciso pero no existen opciones de navegabilidad en multi dispositivos, además existen pocos mecanismos de ayuda y retroalimentación del Sistema de Información Hospitalario (SIHOS) y los pocos manuales de los módulos se encuentran desactualizados.

Recomendación.

- En el Sistema de Información Hospitalario (SIHOS) se debe implementar mecanismos de ayuda y retroalimentación para lograr una mejor ubicación de los usuarios que manejan el Sistema de Información Hospitalario (SIHOS).

- Actualizar los manuales de Sistema de Información Hospitalario (SIHOS).

6. INFORME GERENCIAL DE AUDITORÍA

San Juan de Pasto 19 de febrero de 2016.

Doctor
Eduardo Efraín Narváez
Gerente Hospital Civil de Ipiales

REF: AUDITORÌA AL SISTEMA DE INFORMACIÓN HOSPITALARIO (SIHOS) DEL HOSPITAL CIVIL DE IPIALES BASADO EN EL ESTANDAR COBIT 4.1

Reciba un atento y cordial saludo.

La presente con el fin de dar a conocer el informe de auditoría al que fue sometido el Sistema de Información Hospitalario (SIHOS) con el objetivo de evaluar los distintos aspectos como son funcionabilidad, usabilidad, portabilidad, accesibilidad, confiabilidad, así como también las entradas, salidas y aspectos de seguridad del Sistema de Información Hospitalario (SIHOS).
Los resultados obtenidos son producto de aplicación de técnicas y Herramientas de auditoría teniendo como base la información suministrada por la entidad auditada.

Los resultados obtenidos en cada uno de los dominios de COBIT, se presentan a continuación:

6.1 DOMINIO PLANEAR Y ORGANIZAR (PO)

De acuerdo a la evaluación y análisis que se realizó al Sistema de Información Hospitalario (SIHOS) al Hospital Civil de Ipiales se encontró que dentro de la dependencia de sistemas existe personal capacitado para manejar las tecnologías de Información y hacer uso adecuado de ellas, y de esta forma brindar un servicio de calidad a los usuarios, de esta manera también se pudo apreciar que el personal se encuentra comprometido con los procesos que se maneja dentro de la dependencia pero de igual forma existen inconvenientes que se han presentado en el sistema y que se pudieron evidenciar al realizar la auditoria al Sistema de Información Hospitalario (SIHOS) entre ellos están:

La mayoría de funcionarios de la dependencia tienen acceso a las bases de datos y al sistema de información sin existir restricciones a partes de las bases de datos y del sistema, lo que puede provocar errores o inconvenientes al modificar información importante que se encuentra almacenada en el Sistema de Información Hospitalario (SIHOS) y de esta manera perder la confidencialidad y seguridad de los datos.

De igual manera en la dependencia de sistemas se están elaborado procedimientos con respecto a la arquitectura de la información como son plan operativo anual, plan de gerencia de la información, plan de contingencia de sistemas de información y comunicaciones, matriz de riesgos por cada proceso, cronograma de desarrollo de requerimientos del Sistema de Información, control y seguimiento a actividades del Sistema de Información Hospitalario (SIHOS), pero todavía hace falta implementar algunos mecanismos con respecto a la arquitectura de la información como son diccionarios de datos del Sistema de Información Hospitalario (SIHOS), esquema de clasificación de la Información, documentación a planes existentes, actualización de planes y manuales del Sistema de Información Hospitalario (SIHOS),diseñar el modelo relacional de las bases de datos del Sistema de Información Hospitalario (SIHOS) evaluar y realizar mantenimiento a los planes existentes.

En cuanto a seguridad no se han implementado herramientas que permitan minimizar los riesgos a los cuales está expuesto el Sistema de Información Hospitalario (SIHOS).

Los procesos de calidad no están guiados al Sistema de Información, para lo cual se debe elaborar y mantener un sistema de administración de calidad el cual incluya procesos y estándares probados de desarrollo y adquisición por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad.

6.2 ADQUIRIR E IMPLEMENTAR (AI)

Al evaluar el Sistema con respecto a este dominio se encontró que el sistema de información Hospitalario (SIHOS), no siempre está disponible por distintos inconvenientes que se pueden presentar como son por fallas eléctricas, por cambio de herramientas o elementos de hardware o por problemas de red. Sin

embargo para estos inconvenientes que se presentan en el equipo de sistemas tiene un plan de contingencia de acuerdo al dificultad es decir si se existen demoras en la recuperación del sistema el equipo de sistemas se encarga de informar a cada dependencia y entregar la documentación pertinente para realizar los procesos y registros de forma manual. Pero existen varios casos en los cuales el sistema se cae por 10 minutos o 20 minutos y en estos casos no se activa el plan de contingencia debido a que es por poco tiempo lo cual retrasa las actividades que se están realizando en cada dependencia y por ende la atención de los pacientes.

Por otra parte existen escasas medidas de seguridad del Sistema de Información Hospitalario (SIHOS), por lo tanto se hace necesario implementar herramientas de seguridad y configurar el sistema de tal manera que bloqueen los accesos indebidos o ataques que se intenten realizar a través de los puestos abiertos.

En la dependencia de sistemas se realizan capacitaciones y reuniones programadas, sin embargo hace falta implementación de planes de entrenamiento a los funcionarios que manejan las tecnologías de información ya que existen errores básicos del manejo de los equipos y del sistema que cada usuario lo puede solucionar de una manera adecuada.

6.3 ENTREGAR Y DAR SOPORTE (DS)

En la dependencia de sistemas se está trabajando en el plan de continuidad de sistemas de información y comunicaciones por lo tanto es necesario terminal el documento probar y evaluar de tal manera que pueda prevenir detectar y atender riesgos y vulnerabilidades que se presentan en el sistema y si es necesario se realizan correcciones con el fin de mejorar la calidad del Sistema de Información Hospitalario (SIHOS)

El Sistema de Información Hospitalario (SIHOS) maneja todos los usuarios que utilizan el sistema de Información y cada usuario de acuerdo al cargo que desempeña tiene asignado sus permisos, pero no existe un documento de la administración de cuentas de usuarios del sistema, además no se exige el cambio de contraseñas y la utilización de técnicas de creación de contraseñas con una seguridad alta.

El Hospital Civil de Ipiales cuenta con un ambiente de configuración de las tecnologías, ya que existen políticas con respecto a la utilización de software y equipos, además la configuración la realiza únicamente el personal autorizado, pero se han presentado inconvenientes al realizar mantenimiento a los equipos debido a que el personal no se percata de la información que contienen dichos equipos, por lo tanto se recomienda realizar mantenimiento a los equipos siguiendo los pasos estipulados en el plan de mantenimiento.

De igual manera no existe un espacio adecuado para guardar las herramientas con las cuales se realiza mantenimiento por lo que los funcionarios de la dependencia realizan mantenimiento en la oficina de sistemas y guardan las herramientas en el cuarto donde se encuentran algunos servidores, por estas razones y las restricciones de espacio en la oficina de sistemas impiden que se puedan desarrollar las diferentes actividades asignadas a cada funcionario.

Además no existen restricciones para ingresar a la dependencia de sistemas y a l cuarto de servidores, por lo cual es un riesgo para la oficina de sistemas ya que se pueden acceder a información relevante de la dependencia y del Sistema de Información Hospitalario así como a las copias de seguridad.

Se realizan copias de seguridad del Sistema de Información Hospitalario (SIHOS), pero no se encuentran almacenadas en un lugar seguro, y de esta manera no se ha contemplado realizar copias de seguridad fuera de la dependencia de sistemas, y de la ciudad.

Al realizar la evaluación al servidor del Sistema de Información Hospitalario (SIHOS) se pudo acceder a algunas copias de seguridad almacenadas en el servidor, este es un debilidad latente en el sistema que puede afectar directamente a todo los usuarios y personal involucrado debido a que cualquier persona puede leer modificar o eliminar las copias de seguridad almacenadas en el servidor.

6.4 MONITOREAR Y EVALUAR (ME)

A través de la información recolectada y al evaluación al sistema se observó que en la dependencia de sistemas se realiza seguimiento a las políticas por medio de indicadores trimestrales basados en la norma ISO 90001 con el fin de brindar

oportunidades de mejoramiento para los pacientes y sus familias, de igual manera es necesario que se evalúe el desempeño del sistema de Información Hospitalario (SIHOS) teniendo en cuenta las metas acordadas y con base en el plan operativo anual.

También es necesario evaluar el recurso humano de la dependencia de sistemas de acuerdo a sus funciones que realizan.

De la misma manera se debe monitorear de forma periódica los cambios que se le han realizado al Sistema de Información Hospitalario (SIHOS) de manera que permitan implementar planes de mejoramiento que conlleven a la toma de decisiones acertadas del sistema.

Finalmente esperamos que este informe aporte al mejoramiento del Sistema de Información del Hospital.

Atentamente,

Leidy Doraly Santander Chamorro
Auditora.

Msc José Javier Villalba Romero
Director del proyecto de auditoría

Msc Francisco Nicolas Solarte Solarte
Co- Director del Proyecto de Auditoría

7. ASPECTOS QUE SE DEBEN RESALTAR DEL INFORME

En este informe se detallan todos los hallazgos que se encontraron al realizar la evaluación al Sistema de Información Hospitalario (SIHOS) de acuerdo a los dominios de Cobit 4.1 así como los resultados de las pruebas que se realizaron al Sistema.

De este informe se resaltan algunos hallazgos que son perdida de información, suspensión del Sistema de Información Hospitalario (SIHOS), no se cuenta con un modelo de arquitectura de información, se tiene acceso a las bases de datos por varios usuarios de la dependencia, en la oficina de sistemas se encuentran ubicados varios servidores y herramientas para realizar mantenimiento, almacenamiento de copias de seguridad en lugares no seguros, acceso a algunas copias de seguridad del servidor del Sistema de Información Hospitalario (SIHOS).

Igualmente se pudo detectar existe mucha vulnerabilidad en el Sistema de Información Hospitalario (SIHOS) por lo que no hay conciencia del manejo de la información y de los datos ya que no se han planeado evaluaciones al sistema desde sus entradas procedimientos y salidas así como el entorno físico y humano que soportan el Sistema de Información Hospitalario (SIHOS).

Además existe mucha inestabilidad del Sistema de Información Hospitalario (SIHOS), ya sea por cambio de tecnología, herramientas, fallas eléctricas u otros imprevistos que hacen que el sistema no se encuentre disponible y se retrasen muchas actividades en las que se ven involucrados los usuarios debido a que no existe un plan de mantenimiento al Sistema de Información Hospitalario (SIHOS)

Este informe sirve para implementar controles y recomendaciones que faciliten la mejora continua del Hospital Civil de Ipiales del área de sistemas y del Sistema de Información Hospitalario (SIHOS).

8. CONCLUSIONES

Durante el proceso de auditoría realizado al Sistema de Información Hospitalario (SIHOS) del Hospital Civil de Ipiales se evaluó los procesos de entrada y salida de datos, cumplimiento de requerimientos, funcionamiento de la seguridad lógica y física y los demás recursos involucrados dentro del Sistema de tal manera se pudieron establecer controles y recomendaciones necesarias que se deben implementar con el fin de garantizar la seguridad e integridad para el continuo mejoramiento del Sistema de Información Hospitalario (SIHOS) del Hospital Civil de Ipiales.

Se puede concluir que durante la evaluación de los procesos de entrada y salida de datos que presenta el Sistema de Información Hospitalario (SIHOS) es necesario realizar algunas revisiones en la parte de los reportes debido a que se han presentado inconvenientes en los resultados obtenidos.

En cuanto a la seguridad del Sistema de Información Hospitalario (SIHOS) se observaron algunas debilidades ya que hace falta implementar políticas que estén guiadas a la administración y gestión de la seguridad e implementación de herramientas, procedimientos y controles que permitan minimizar el impacto de los riesgos y poner en peligro la integridad del Sistema de Información Hospitalario (SIHOS).

De la misma manera se puede concluir que las instalaciones de la dependencia de sistemas no son las óptimas debido a que existen restricciones de movilidad que impiden que el personal que labora en esta oficina no pueda realizar su trabajo de una manera adecuada.

Los datos e información son uno de los activos más importantes en cualquier empresa, y más en el sector de la salud, es por eso que se deben realizar supervisiones continuas a los sistemas informáticos para generar seguridad y confianza a los usuarios.

La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyan al logro de los objetivos de cualquier empresa.

Todas las entidades deben prestar mayor atención al área de sistemas ya que esta es el soporte de cualquier entidad que preste servicios de información y atención a usuarios.

9. RECOMENDACIONES

Realizar seguimiento a los datos que se tiene dentro del Sistema de Información Hospitalario (SIHOS) implementando un diccionario de datos y un esquema de clasificación que se encuentren dentro de un modelo de arquitectura de Información.

Realizar planes de mejoramiento que ayuden a optimizar los procesos, con el fin de mitigar los riesgos encontrados mediante el establecimiento de medidas preventivas y correctivas.

Mantener actualizados todos los documentos como son planes de contingencia, planes estratégicos, planes de Gerencia, inventarios, documentos de identificación de necesidades, manuales del Sistema de Información Hospitalario (SIHOS), documentos de identificación de riesgos, entre otros.

Implementar un plan de pruebas al Sistema de Información Hospitalario (SIHOS) que permita disminuir y prevenir los riesgos asociados al sistema.

Fortalecer apoyo y concientización de la Gerencia del Hospital Civil de Ipiales para que se puedan implementar medidas de seguridad, que conlleven al mejoramiento continuo del Sistema de Información Hospitalario (SIHOS).

Planificar a tiempo las etapas o fases de la auditoria y seguirlas de manera consecutiva.

Tener muy en cuenta los objetivos específicos para abordar con el objetivo general que se planteó, es decir se debe comenzar con el primer objetivo específico hasta el último.

Planear diseñar y aplicar a tiempo los instrumentos de recolección de información de manera ordenada es decir de acuerdo a cada dominio y objetivos de control del COBIT para posteriormente realizar un buen análisis de la información recolectada

BIBLIOGRAFIA

CONSEJO MEXICANO PARA LA INVESTIGACIÓN Y EL DESARROLLO DE NORMAS DE INFORMACIÓN FINANCIERA (CINIF) E INSTITUTO MEXICANO DE CONTADORES PÚBLICOS (IMCP). (2009).Normas de información financiera. (28ª ed.) México: CNINIF /IMCP.

CORLETTI ESTRADA, Alejandro. Seguridad por Niveles, Ediciones primera.

DESONGLES CORRALE, Juan Ayudante Técnico en Informática de la Junta de Andalucía. Editorial MAD, S.L, 2005. ISBN: 84-665-201-39N.

ECHENIQUE GARCIA, José Antonio, Auditoría Informática, segunda Ed., Mc GRAW-HILL, México D.F., 2001.

ESTEBARANZ GARCÍA, Araceli. Didáctica e Innovación curricular. Universidad de Sevilla, Primera edición 1994.

ESTEBAN GARCÍA, J.; Vicens Gómez, J. (1990). Información Clínica y Gestión hospitalaria. (1990). (Araceli)

GARCÍA RUBIO, Fernando. Las Nuevas Tecnologías ante el Derecho y la Organización Administrativa.2003.

HERNÁNDEZ SAMPERI, Roberto. Metodología de la Investigación: Mc Graw-Hill de México, S.A de C.V., 2007.

HEREDIA VIVEROS, Nora Ligia. Gerencia de Compras la Nueva Estrategia Competitiva Ediciones primera edición Bogotá D.C.2003.

KAPLAN B. (1988). Development and Acceptance of Medical Information Systems: an historical overview. J. Health Hum. Resour. Adm. 1988.

LUPPI, Heddy. Control Interno Hoy. [En línea] <http://controlinternohoy.blogspot.com/2010/10/el-informe-coso.html> [Consulado 8 marzo de 2015]

MUÑOZ RAZO, Carlos Auditoría en Sistemas Computacionales. México: Pearson Education, 2002.

PIATTINI, Mario G. Auditoría Informática. Un Enfoque Práctico, México, Alfamega-RA-MMA, 2001.

ROGER S, Pressman. Ingeniería de software un Enfoque Práctico. Mc Graw-Hill/Inter Americana de España, S.A.U, 1998

RIVAS Gonzalo, Alonso, Auditoría Informática Ediciones Díaz de Santos., México D.F., 2005.

SITIO OFICIAL DEL HOSPITAL CIVIL DE IPIALES NARIÑO, COLOMBIA. Documentos del Hospital [En Linea] <http://www.hospitalcivilese.gov.co/site/> [Citado 03 de junio de 2015].