AUDITORÍA INFORMATICA A LA ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS EN LA EMPRESA SOCIAL DEL ESTADO HOSPITAL CUMBAL DEL MUNICIPIO DE CUMBAL, DEPARTAMENTO DE NARIÑO

MONICA YAQUELINE CAICEDO ALPALA
HENRY FREDY IRUA TAIMAL

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

AUDITORÍA INFORMATICA A LA ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS EN LA EMPRESA SOCIAL DEL ESTADO HOSPITAL CUMBAL DEL MUNICIPIO DE CUMBAL, DEPARTAMENTO DE NARIÑO

MONICA YAQUELINE CAICEDO ALPALA
HENRY FREDY IRUA TAIMAL

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

Asesor
Ingeniero Msc. MANUEL BOLAÑOS GONZÁLEZ

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

NOTA DE RESPONSABILIDAD

“Las ideas y conclusiones aportadas en el presente trabajo son responsabilidad exclusiva de sus autores”.

Artículo 1, Acuerdo No. 324 de octubre 11 de 1966, emanado por el 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”.

Artículo 13, Acuerdo Nro. 005 de 2010 emanado del Honorable Consejo Académico.

NOTA DE ACEPTACION

_____
_____
_____
_____
_____

_____
Jurado

_____
Jurado

San Juan de Pasto, 2016

AGRADECIMIENTOS

A Dios, que nos concedió fortaleza y nos guio durante todo este camino.

A los ingenieros del Programa de Ingeniería de Sistemas de la Universidad de Nariño, especialmente a Manuel Bolaños, Juan Carlos Castillo, Edgar Dulce, Ricardo Timaran y Francisco Solarte quienes amablemente nos compartieron sus conocimientos, y contribuyeron para que culminemos esta etapa de nuestras vidas.

A nuestros padres, por su apoyo incondicional.

A nuestros familiares, que estuvieron pendientes de nuestros logros.

A amigos y compañeros, que nos brindaron sus amistad y con quienes compartimos incontables jornadas de aprendizaje

DEDICATORIA

A DIOS,
Que me concedió la dicha de recorrer este camino, en el cual tuve la fortuna de ingresar a la Universidad de Nariño, y que, a pesar de las adversidades y dificultades, siempre estuvieron presentes las oportunidades, especialmente, cursar y culminar el Programa de Ingeniería de Sistemas, y así crecer personal y profesionalmente.

A mis padres,
MARIA CARMEN y JOSE TOBIAS, quienes me vieron iniciar este proceso, y con humildad y cariño, me brindaron toda su confianza y nunca renunciaron a apoyarme.

A mi esposa,
LUZ ANGELICA, quien me acompañó a recorrer este camino, y por brindarme siempre todo su cariño, paciencia y comprensión.

A mis hijos,
PAOLA ALEJANDRA y DIEGO FELIPE, quienes llegaron a nuestras vidas y se convirtieron en nuestro motor diario, quienes fortalecen mi espíritu y me llenan de felicidad.

Henry Fredy Irua Taimal

A Dios, por concederme la fuerza para
culminar Esta etapa de mi vida.

A mi padres Luz María y Luis Gilberto, por brindarme
su apoyo incondicional para mejorarme cada día
para cumplir mis objetivos.

A mi esposo Rigoberto Tarapues, por
brindarme su compañía y comprensión

A mi querida hija Lucerito Tarapues,
por ser el regalo más preciado
y el motivo de mi felicidad

Mónica Yaqueline Caicedo Alpala

RESUMEN

El presente trabajo consiste en un caso práctico de aplicación de una auditoría Informática, con el fin de evaluar la ESTRUCTURA ORGANIZACIONAL Y LOS PROCESOS del área de sistemas del Hospital Cumbal, en el Municipio de Cumbal, Departamento de Nariño.

Se pretende evaluar si existen políticas, planes y procedimientos definidos e identificar las amenazas y vulnerabilidades existentes, para determinar los riesgos a los cuales está expuesta la empresa y su probabilidad de ocurrencia.

Para el desarrollo de esta auditoría informática, se enfatizó en la utilización del modelo CObIT (Objetivos de Control para las Tecnologías de la Información), del cual se seleccionaron los dominios, procesos y controles que estén directamente relacionados con el objetivo general de la auditoría, definiendo así, el Programa de auditoría a ejecutar.

Finalmente, se presenta el Informe de auditoría, el cual contiene las recomendaciones necesarias para la mejorar y optimizar los procesos que se desarrollan en el área de sistemas del Hospital Cumbal.

ABSTRACT

This project is a case of application of a Computer Audit, with the final purpose to evaluate the ORGANIZATIONAL STRUCTURE AND PROCESSES in the IT department of the Hospital Cumbal, in the municipality of Cumbal, Nariño department.

The intention is to evaluate if there the policies, plans and procedures defined and identify if exists threats and vulnerabilities, to determine the risks to which it is exposed the hospital and probability of occurrence.

For the development of this computer audit, It emphasizes the use of the model CObIT (Control Objectives for Information and related), which they were selected domains, processes and controls which they are directly related with the overall objective of the audit, thus defining the audit program to run.

Finally, the audit report it presents, which the necessary recommendations to improve and optimize processes, which develop in the IT department of the Hospital Cumbal

TABLA DE CONTENIDO

Contenido Pág.

LISTA DE FIGURAS

LISTA DE FORMATOS

LISTA DE CUADROS

LISTA ANEXOS

Los anexos descritos a continuación se encuentran incluidos en el CD adjunto al presente trabajo, así:

Anexo1. Manual-de-funciones-ESE-Hospital-Cumbal.pdf

Anexo 2. Inventario-equipos-de-computo-ESE-Hospital-Cumbal.xlsx

Anexo 3. Formatos-definicion-fuentes-de-conocimiento.pdf

Anexo 4. Formatos-cuestionarios-cuantitativos.pdf

Anexo 6. Formatos-entrevistas.pdf

Anexo7. Taller-configuracion-SO.docx (Desarrollado en el módulo de sistemas operativos, en el Diplomado de auditoría y Seguridad Informática, dictado por el Ing. Edgar Dulce)

INTRODUCCION

Hoy en día es de vital importancia la presencia de las herramientas informáticas para realización de tareas, la optimización de procesos, por esta razón el proveer a cualquier empresa de tecnología es hoy en día una necesidad primordial, puesto que la utilización de las tecnologías de información trae como resultado la mejora del cumplimiento de los objetivos empresariales y es por ello que de la capacidad de adaptación de la empresa a los cambios dependerán no solo los beneficios sino también su existencia como empresa. Pero un punto fundamental que deben tener en cuenta las organizaciones o empresas, es la supervivencia en caso de pérdidas catastróficas provocadas por accidentes, negligencias, falta de profesionalismo o cualquier otro causal de pérdida o efecto dañoso que amenace con interrumpir las operaciones de la organización, para su crecimiento o reducir sus utilidades. La auditoría consiste en apoyar a los miembros de la empresa en el desempeño de sus actividades por tal motivo se hace necesario definir métodos y controles que ayuden a estimar la magnitud del manejo de cada área o de cada proceso que se lleve dentro de la empresa como tal.

IDENTIFICACION DEL PROBLEMA

Título

AUDITORÍA INFORMATICA A LA ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS EN LA EMPRESA SOCIAL DEL ESTADO HOSPITAL CUMBAL EN EL MUNICIPIO DE CUMBAL, DEPARTAMENTO DE NARIÑO.

Tema

Auditoría aplicada a la estructura organizacional y a los procesos del área de sistemas en la E.S.E. Hospital Cumbal.

Línea de investigación

Teniendo en cuenta las líneas de investigación aprobadas por el Programa de Ingeniería de Sistemas de la Universidad de Nariño, según el Acuerdo Nro. 005 de octubre 10 de 2002, emitido por el Consejo de Facultad, el presente trabajo corresponde a la línea de investigación de SISTEMAS COMPUTACIONALES, que tiene como objetivo planificar, diseñar, implantar, administrar y evaluar los

sistemas computacionales y los servicios apoyados en estos, para lo cual es fundamental la auditoría de sistemas.

Alcance y delimitación

El presente proyecto de auditoría informática se limita a la aplicación de las herramientas y técnicas de auditoría y la presentación del informe final de auditoría, y tiene su alcance en la evaluación de la estructura organizacional y a los procesos del área de sistemas de la E.S.E. Hospital Cumbal del Municipio de Cumbal, Departamento de Nariño.

Modalidad

La modalidad corresponde a TRABAJO DE APLICACIÓN, a realizarse en la E.S.E. HOSPITAL CUMBAL, el cual permitirá ampliar el conocimiento y mejora de la estructura organizacional, los procesos y soporte que brinda el área de sistemas, a través de la aplicación de métodos de organización, funcionamiento, y cumplimiento de políticas institucionales, legislación o normatividad vigente y estándares relacionados.

DESCRIPCIÓN DEL PROBLEMA

Planteamiento del problema

Es necesario aplicar una auditoría Informática a la organización y a los procesos del Área de Sistemas del Hospital Cumba, con el fin garantizar una planificación adecuada para lograr las mayores ventajas del uso de la tecnología y verificar si existe una estructura organizacional y los procesos definidos, para lo cual se plantea las siguientes consideraciones:

Se desconoce si existe la definición de los cargos, funciones y procesos que soporten el adecuado desempeño del área de sistemas.

Se desconoce si existe un proceso definido para realizar adecuadamente las copias de seguridad y respaldo de la información del área de sistemas y demás áreas, con la calidad y garantía apropiada.

Se desconoce si existe un proceso o políticas que garanticen la seguridad de la información y del sistema implementado en la institución.

Se desconoce si existe un proceso o políticas de educación y entrenamiento a los usuarios que usan los recursos informáticos para el desempeño de sus funciones.

Se desconoce si existe un proceso o política definida que soporte el proceso de mantenimiento preventivo o correctivo de los recursos de hardware de la institución.

Se desconoce si existe una adecuada atención a los requerimientos por parte de los funcionarios o usuario de la institución, referentes a la utilización de los recursos informáticos (tecnologías existentes).

Se desconoce si existe un comité, proceso o política para adquirir nuevos recursos informáticos, que pueden ser hardware, software o servicios, que requiera la institución.

OBJETIVOS

Objetivo general

Evaluar la estructura organizacional y los procesos internos del área de sistemas, y analizar si existe la necesidad de definir, documentar o mejorarlos, mediante la aplicación de la auditoría Informática, en la E.S.E. Hospital Cumbal.

Objetivos específicos

Reconocer el área a auditar, mediante visitas y solicitud de información relacionada al área de sistemas del Hospital Cumbal y conocer si existe manual de funciones y de procedimientos.

Planear, diseñar los instrumentos recolección de información y pruebas del programa de auditoría a aplicar.

Construir el Programa de auditoría, seleccionando los controles que se van a evaluar y que estén más relacionados con el objetivo general de la auditoría.

Ejecutar la aplicación de los instrumentos diseñados, realizar las pruebas y realizar el proceso de análisis y evaluación de riesgos para su valoración.

Elaborar el informe final para la empresa donde este contemplado los hallazgos y las recomendaciones planteadas.

Elaborar y entregar el informe final que contenga los Riesgos confirmados y controles propuestos.

JUSTIFICACIÓN

Existe una famosa frase que dice: “Quién tiene la información tiene el poder”, sin embargo, esta frase en un mundo globalizado como el de hoy, ya no es tan cierta, pues no basta con tener información, hay que saberla utilizar y ahí está el verdadero “poder”[1].

Actualmente, para todas las empresas, instituciones y/u organizaciones, la información es un recurso valioso, el cual, según su utilización y manejo, puede garantizar el éxito en las actividades de las mismas.

En el campo de la salud, a su vez, existen muchas instituciones que su funcionamiento tiene por objeto la regulación, financiación, administración, prestación, control y vigilancia de los servicios de salud.

En Colombia, al respecto, la principal institución que existe de orden nacional es el Ministerio de la Salud y Protección Social, encargado de dirigir todo el sistema de salud y protección social, así mismo, garantizar el derecho fundamental de la salud de toda la población, de orden departamental y municipal se encuentran las Secretarias Departamentales de Salud y las Direcciones Locales de Salud, respectivamente. Para el caso del Departamento de Nariño se encuentra el Instituto Departamental de Salud (IDSN) de orden departamental y en el municipio de Cumbal, la respectiva Dirección Local de Salud, quienes velan por el acceso oportuno y la prestación con calidad de los servicios de salud.

Por otra parte, se encuentran las instituciones que se encargan del aseguramiento de la población y contratación de la red de prestación de los servicios de salud, conocidas como entidades responsables de pago o Empresas Promotoras de Salud (EPS). Ejemplo de ellas esta Emssanar ESS, Asmet Salud EPS-S, Salud Vida EPS, Cafesalud, Mallamas EPS-I, Comfamiliar de Nariño, La Nueva EPS, las cuales tienen presencia en Nariño, en su orden, según la población afiliada[2].

También están las instituciones que se encargan de la prestación de los servicios de salud a los afiliados de las entidades responsables de pago, denominadas Instituciones Prestadoras de los Servicios de Salud (IPS), las cuales se encuentran en todos los municipios del territorio colombiano y ofrecen los servicios de salud de Promoción y Prevención, Recuperación de la Salud y todos los servicios relacionados.

[1] http://jorgearestrepog.comunidadcoomeva.com/blog/index.php
[2] Piattini, Mario. Auditoría de tecnologías y sistemas de información. Pág. 7

Estas son algunas instituciones que se han creado en el marco de la Ley 100 de 1996 que creó el Sistema de Seguridad Social en Salud (SGSSS) y todas las normas que la modifiquen y complementen, y se relacionan e interactúan entre sí, con un flujo constante de información de todo tipo, especialmente información personal de los afiliados para el caso de las EPS o pacientes para el caso de las IPS, información de contratación, información de Plan Obligatorio de Salud (POS), información financiera, etc.

De lo anterior, la importancia de que exista en las instituciones de salud, un departamento de sistemas o de tecnologías de la información, que brinde asesoría, soporte y servicios a las demás dependencias[3]; dichos servicios puede ser de:

- Programación y aplicaciones
- Administración de la red
- Administración de usuarios
- Respaldo de Información
- Licenciamiento
- Soporte a usuarios.

El área de sistemas debe contar con procesos y procedimientos que garanticen que la información cumpla con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

En el Municipio de Cumbal del Departamento de Nariño, se encuentra la Empresa Social del Estado Hospital Cumbal, donde actualmente el Área de Sistemas, no cuenta con estructura organizacional, ni procesos y procedimientos definidos, los cuales son necesarios para el adecuado uso de las tecnologías de la Información (IT) y recursos tecnológicos existentes en la institución.

Cada una de las dependencias del Hospital Cumbal, cuenta al menos con un equipo de cómputo, para un total de 50 equipos de cómputo (Anexo2. Inventario-equipos-de-computo-ESE-Hospital-Cumbal.xlsx), además de 10 impresoras, donde la mayoría se encuentran conectados en red y la principal información se gestiona en el software de historias clínica sistematizada denominado SaludIPS Versión 4.10.9, además de información de facturación, contabilidad, nomina, almacén, principalmente.

[3] Echenique, José Antonio. Auditoría en informática. Pág. 16

1 MARCO TEORICO

Conceptos de auditoría

Auditoría informática

Es la evaluación y verificación de las políticas, controles, procedimientos y la seguridad en general, correspondiente al uso de los recursos de informática por el personal de la empresa (usuarios, informática, alta dirección), a fin de que se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Según José A. Echenique, la auditoría en informática "es la utilización, revisión y evaluación de los controles a los sistemas, procedimientos de informática; equipos de cómputo, medición de su eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistemas o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles archivos, seguridad y obtención de información. Ello debe incluir los equipos de cómputo como la herramienta que permite obtener la información adecuada y la organización especifica que hará posible su uso"[4].

Según Mario Piattini Velthuis, la auditoría informática es "el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos"[5].

Auditoría de sistemas

Desde el punto de vista administrativo, cuando se habla de auditoría de sistemas se refiere a los SISTEMAS DE INFORMACIÓN utilizados en las empresas públicas o privadas, mas no al computador como tal, que en sí es una herramienta de los sistemas de información. Se debe tener presente que la administración es un sistema abierto y por tanto cambiante en sus conceptos, técnicas y que está influenciada por lo que acontece en su alrededor.

[4] http://jorgearestrepog.comunidadcoomeva.com/blog/index.php
[5] Piattini, Mario. Auditoria de tecnologías y sistemas de información. Pág. 7.

La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes; también se puede decir que es el examen y evaluación de los procesos del área de Procesamiento Electrónico de Datos (PED) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas"[6].

Conceptos aplicables a la auditoría

Control

"Es el conjunto de normas, técnicas, acciones y procedimientos que interrelacionados e interactuando entre sí con los sistemas y subsistemas organizacionales y administrativos, permite evaluar, comparar y corregir aquellas actividades que se desarrollan en las organizaciones, garantizando la ejecución de los objetivos y el logro de las metas institucionales"[7].

Control interno

Se ejerce con el fin de lograr el cumplimiento de los objetivos de la empresa, y es el proceso que se realiza al interior de ellas y es impulsado por las directivas y administradores quien designa para que lo ejerza a una persona que posee la suficiente ética, moral y formación académica que le amerita credibilidad.

Control externo

Es el ejercido por personal externo a la empresa y su propósito es evaluar en qué proporción las metas y objetivos trazados en las políticas, planes, programas por la administración de la misma se están cumpliendo.

Control interno informático

El establecimiento de controles internos en el área informática y los sistemas de información es muy importante y ayuda a la evaluación de la eficiencia y eficacia de la gestión administrativa, dependiendo de los objetivos que se pretenda con

[6] Echenique, José Antonio. Auditoria en informática. Pág.16.
[7] Auditoría de Sistemas – Una visión práctica. Pág.14.

dichos controles. Además, el control interno es indispensable en la protección de los bienes y el buen desarrollo de las actividades y operación de los sistemas.

A través del control interno se pretende la aplicación de los siguientes objetivos específicos:

- Establecer como prioridad la seguridad y protección de los bienes informáticos, la información y los sistemas de información.

- Promover la confiabilidad, oportunidad y veracidad de la captura de datos, su procesamiento y la emisión de reportes en la empresa.

- Implementar los métodos, técnicas y procedimientos necesarios para contribuir al desarrollo eficiente de las funciones, actividades, y tareas de los servicios que presta el área informática para satisfacer las necesidades de la empresa.

- Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.

- Establecer acciones necesarias para el buen desarrollo del software, a fin de que presten un buen servicio en la empresa.

Papeles de trabajo

Son la herramienta y soporte en la planeación, organización y coordinación del examen de auditoría, y a su vez brindan respaldo a la opinión del auditor. Estos se preparan de acuerdo con el criterio, experiencia y preferencia del auditor y se organizan teniendo en cuenta su uso y contenido. José Dagoberto Pinilla[8], define los papeles de trabajo, así: "comprende el conjunto de cédulas preparadas por el auditor y/o personal colaborador, con motivo del desarrollo del programa de auditoría para obtener evidencia comprobatoria suficiente y competente, que sirva como base objetiva para emitir una opinión independiente sobre el objeto auditado".

Los papeles de trabajo son registros que mantiene el auditor de los procedimientos aplicados, pruebas desarrolladas, información obtenida y conclusiones pertinentes a que se llegó en el trabajo. Algunos ejemplos de papeles de trabajo son los programas de auditoría, los análisis, los memorandos, las cartas de confirmación y declaración, resúmenes de documentos de la compañía y cédulas o comentarios preparados u obtenidos por el auditor. Los

[8] Pinilla Forero, José Dagoberto. Auditoría Informática. Un enfoque operacional Pág. 50.

papeles de trabajo también pueden obtener la forma de información almacenada en cintas, películas u otros medios.

Objetivos de los papeles de trabajo

- Proporcionar la información básica y fundamental necesaria para facilitar la planeación, organización y desarrollo de todas las etapas del proceso de auditoría.

- Respaldar la opinión del auditor permitiendo realizar un examen de supervisión y proporcionando los informes suficientes y necesarios que serán incluidos en el informe de auditoría, además, sirve como evidencia en caso de presentarse alguna demanda.

- Permiten demostrar si el trabajo del auditor fue debidamente planeado, determinando su eficiencia y eficacia.

- Permiten establecer un registro histórico disponible permanentemente en caso que se presente algún requerimiento.

- Servir como punto de referencia para posteriores auditorías.

- Servir de puente entre el informe de auditoría y las áreas auditadas.

Tipos de papeles de trabajo

- **Archivo permanente:** la información que aquí se almacena cubre varios períodos de la auditoría y son de utilidad en exámenes posteriores, representando interés para el administrador de la aplicación y fuente de consulta de aspectos como la naturaleza y justificación de la aplicación, reseña de la aplicación, estructura organizacional respecto al manejo de la aplicación, interacción con otras aplicaciones, documentación de entrada y salidas, diccionario de datos, programas, menús, diagramas del sistema, naturaleza y definición de cada proceso.

- **Archivo corriente:** se almacena la información correspondiente al periodo auditado, constituyéndose en evidencia del trabajo desarrollado por el auditor, mostrando todas sus fases y sirviendo como respaldo para presentar los informes respectivos, como ejemplo se tiene: el programa de trabajo, utilización de datos de prueba, verificación al contenido de archivos, utilización de programas de auditoría, revisión lógica a los programas del área auditada.

Recolección de información para auditoría informática y de sistemas

Observación

Es una de las técnicas más utilizadas para examinar los diferentes aspectos que intervienen en el funcionamiento del área informática y los sistemas software, permite recolectar la información directamente sobre el comportamiento de los sistemas, del área de informática, de las funciones y actividades, los procedimientos y operación de los sistemas, y de cualquier hecho que ocurra en el área. En el caso específico de la auditoría se aplica para observar todo lo relacionado con el área informática y los sistemas de una organización con el propósito de percibir, examinar, o analizar los eventos que se presentan en el desarrollo de las actividades del área o de un sistema que permita evaluar el cumplimiento de las funciones, operaciones y procedimientos.

Entrevistas

Esta técnica es la más utilizada por los auditores ya que a través de esta se obtiene información sobre lo que está auditando, además de tips que permitirán conocer más sobre los puntos a evaluar o analizar. La entrevista en general es un medio directo para la recolección de información para la captura de los datos informados por medio de grabadoras digitales o cualquier otro medio. En la entrevista, el auditor interroga, investiga e informa directamente sobre los aspectos que se está auditando. En su aplicación se utiliza una guía general de la entrevista que contiene una serie de preguntas sobre los temas que se quiere tocar, y que a medida que avanza pueden irse adaptando para profundizar y preguntar sobre el tema.

Cuestionarios

Los cuestionarios son preguntas impresas en formatos o fichas en que el auditado responde de acuerdo con su criterio, de esta manera, el auditor obtiene información que posteriormente puede clasificar e interpretar por medio de la tabulación y análisis, para evaluar lo que se está auditando y emitir una opinión sobre el aspecto evaluado.

Encuestas

Las encuestas son utilizadas frecuentemente para recolectar información sobre aspectos como el servicio, el comportamiento y utilidad del equipo, la actuación del personal y los usuarios, entre otros juicios de la función informática. No existen reglas para el uso de las encuestas, solo los que regulan los aspectos técnicos y estadísticos tales como la elección del universo y la muestra, que se contemplan dentro de la aplicación de métodos probabilísticos y estadísticos para hacer la mejor elección de las muestras y recolección de opiniones.

Inventarios

Consiste en hacer el recuento físico de lo que se está auditando, con el fin de compararla con la que existe en los documentos en la misma fecha. Consiste en comparar las cantidades reales existentes con las que debería haber para comprobar que sean iguales, de lo contrario iniciar la investigación de la diferencia para establecer las causas. Con la aplicación de esta herramienta de la auditoría tradicional, el auditor de sistemas también puede examinar las existencias de los elementos disponibles para el funcionamiento del área informática o del sistema, contabilizando los equipos de cómputo, la información y los datos de la empresa, los programas, periféricos, consumibles, documentos, recursos informáticos, y demás aspectos que se desee conocer, con el fin de comparar la cantidad real con las existencias que se registra en los documentos.

COBIT (Objetivos de Control para la información y Tecnologías relacionadas)

Las mejores prácticas en auditoría recomiendan CObIT como la herramienta estándar para tecnologías de información más utilizada en la ejecución de auditorías. A continuación, se explica detalladamente algunos conceptos manejados por ésta y los dominios, procesos y actividades que lo conforman:

Efectividad. Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
Eficiencia. Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
Confidencialidad. Se refiere a la protección de información sensible contra divulgación no autorizada.
Integridad. Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
Disponibilidad. Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
Cumplimiento. Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.
Confiabilidad de la información. Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.
Datos. Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.
Aplicaciones. Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.

Tecnología. La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
Instalaciones. Recursos para alojar y dar soporte a los sistemas de información.
Personal. Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.
Niveles de CObIT: La estructura del estándar CObIT se divide en dominios que son agrupaciones de procesos que corresponden a una responsabilidad personal, procesos que son una serie de actividades unidas con delimitación o cortes de control y objetivos de control o actividades requeridas para lograr un resultado medible.

Distribución de los dominios y procesos de CObIT

Se definen 34 objetivos de control generales, distribuidos para cada uno de los procesos de las TI, en los correspondientes dominios, así:

DOMINIOS	**PROCESOS**
PLANEACIÓN Y ORGANIZACIÓN (PO)	PO1 Definir un Plan Estratégico de TI. PO2 Definir la Arquitectura de Información. PO3 Determinar la dirección tecnológica. PO4 Definir la Organización y Relaciones de TI. PO5 Manejar la Inversión en TI. PO6 Comunicar las directrices gerenciales. PO7 Administrar Recursos Humanos. PO8 Asegurar el cumplir Requerimientos Externos. PO9 Evaluar Riesgos. PO10 Administrar proyectos. PO11 Administrar Calidad.
ADQUISICIÓN E IMPLEMENTACIÓN (AI)	AI1 Identificar Soluciones. AI2 Adquisición y Mantener Software de Aplicación. AI3 Adquirir y Mantener Arquitectura de TI. AI4 Desarrollar y Mantener Procedimientos relacionados con TI. AI5 Instalar y Acreditar Sistemas. AI6 Administrar Cambios
SERVICIOS Y SOPORTE (DS)	DS1 Definir niveles de servicio. DS2 Administrar Servicios de Terceros. DS3 Administrar Desempeño y Calidad. DS4 Asegurar Servicio Continuo.

	DS5 Garantizar la Seguridad de Sistemas. DS6 Identificar y Asignar Costos. DS7 Capacitar Usuarios. DS8 Asistir a los Clientes de TI. DS9 Administrar la Configuración. DS10 Administrar Problemas e Incidentes. DS11 Administrar Datos. DS12 Administrar Instalaciones. DS13 Administrar Operaciones
MONITOREO (M)	M1 Monitorear los procesos. M2 Evaluar lo adecuado del control Interno. M3 Obtener aseguramiento independiente. M4 Proveer auditoría independiente.

Estos procesos están agrupados en cuatro grandes dominios que se describen a continuación junto con sus procesos y una descripción general de las actividades de cada uno:

Dominio: Planificación y organización

Cubre la estrategia y las tácticas, se refiere a la identificación de la forma en que la tecnología información puede contribuir de la mejor manera al logro de los objetivos de la organización. La consecución de la visión estratégica debe ser planeada, comunicada y administrada desde diferentes perspectivas y debe establecerse una organización y una infraestructura tecnológica apropiadas.

Procesos:

PO1 Definición de un plan estratégico: el objetivo es lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros.

PO2 Definición de la arquitectura de información: el objetivo es satisfacer los requerimientos de la organización, en cuanto al manejo y gestión de los sistemas de información, a través de la creación y mantenimiento de un modelo de información de la organización.

PO3 Determinación de la dirección tecnológica: el objetivo es aprovechar al máximo de la tecnología disponible o tecnología emergente, satisfaciendo los

requerimientos de la organización, a través de la creación y mantenimiento de un plan de infraestructura tecnológica.

PO4 Definición de la organización y de las relaciones de TI: el objetivo es la prestación de servicios de TI, por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas.

PO5 Manejo de la inversión: el objetivo es la satisfacción de los requerimientos de la organización, asegurando el financiamiento y el control de desembolsos de recursos financieros.

PO6 Comunicación de la dirección y aspiraciones de la gerencia: el objetivo es asegurar el conocimiento y comprensión de los usuarios sobre las aspiraciones de la gerencia, a través de políticas establecidas y transmitidas a la comunidad de usuarios, necesitándose para esto estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables.

PO7 Administración de recursos humanos: el objetivo es maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal.

PO8 Asegurar el cumplimiento con los requerimientos externos: el objetivo es cumplir con obligaciones legales, regulatorias y contractuales, para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos.

PO9 Evaluación de riesgos: consiste en asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI, mediante la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos.

PO10 Administración de proyectos: el objetivo es establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión, para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido.

PO11 Administración de calidad: el objetivo es satisfacer los requerimientos del cliente. Mediante una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización.

Dominio: Adquisición e implementación

Para llevar a cabo la estrategia de TI, las soluciones de Ti deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Procesos:

AI1 Identificación de soluciones automatizadas: el objetivo es asegurar el mejor enfoque para cumplir con los requerimientos del usuario, mediante un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios.

AI2 Adquisición y mantenimiento del software aplicativo: el objetivo es proporcionar funciones automatizadas que soporten efectivamente la organización mediante declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros.

AI3 Adquisición y mantenimiento de la infraestructura tecnológica: el objetivo es proporcionar las plataformas apropiadas para soportar aplicaciones de negocios mediante la realización de una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema.

AI4 Desarrollo y mantenimiento de procedimientos: el objetivo es asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas, mediante la realización de un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento.

AI5 Instalación y aceptación de los sistemas: el objetivo es verificar y confirmar que la solución sea adecuada para el propósito deseado mediante la realización de una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas.

AI6 Administración de los cambios: el objetivo es minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores, mediante un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual.

Dominio: Servicios y soporte

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Procesos

DS1 Definición de niveles de servicio: el objetivo es establecer una comprensión común del nivel de servicio requerido, mediante el establecimiento de convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio.

DS2 Administración de servicios prestados por terceros: el objetivo es asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos, mediante el establecimiento de medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización.

DS3 Administración de desempeño y capacidad: el objetivo es asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado, realizando controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos.

DS4 Asegurar el servicio continuo: el objetivo es mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones, mediante un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio.

DS5 Garantizar la seguridad de sistemas: el objetivo es salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida, realizando controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados.

DS6 Educación y entrenamiento de usuarios: el objetivo es asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados realizando un plan completo de entrenamiento y desarrollo.

DS7 Identificación y asignación de costos: el objetivo es asegurar un conocimiento correcto atribuido a los servicios de TI realizando un sistema de contabilidad de costos asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos.

DS8 Apoyo y asistencia a los clientes de TI: el objetivo es asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente realizando una mesa de ayuda que proporcione soporte y asesoría de primera línea.

DS9 Administración de la configuración: el objetivo es dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios realizando controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia.

DS10 Administración de problemas: el objetivo es asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que no vuelvan a suceder implementando un sistema de manejo de problemas que registre y haga seguimiento a todos los incidentes.

DS11 Administración de datos: el objetivo es asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento, a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI.

DS12 Administración de las instalaciones: el objetivo es proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

DS13 Administración de la operación: el objetivo es asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades.

Dominio: monitoreo y evaluación

Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad.

Procesos

M1 Monitoreo del proceso: el objetivo es asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.

M2 Evaluar lo adecuado del control interno: el objetivo es asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.

M3 Obtención de aseguramiento independiente: el objetivo es incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.

M4 Proveer auditoría independiente: el objetivo es incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes desarrolladas a intervalos regulares de tiempo.

2 METODOLOGÍA

Las metodologías son necesarias para desarrollar cualquier tipo de proyecto de forma ordenada y eficaz, razón por la que la metodología utilizada para la realización de la auditoría informática dentro la E.S.E. Hospital Cumbal es de tipo cuantitativo/subjetivo, basados en un modelo matemático numérico, arrojando como resultado, una lista de riesgos obtenidos al auditar cada uno de los procesos teniendo en cuenta su importancia e impacto dentro del área de sistemas de ahí su calificación y recomendaciones realizadas.

La metodología aplicada en la realización de esta auditoría, se ejecutó mediante la formulación del siguiente plan de auditoría, así:

2.1 PLAN DE AUDITORÍA

2.1.1 Etapa 1: Reconocimiento

- Estudio y reconocimiento de la estructura organizacional de la E.S.E. Hospital Cumbal, dirigido al área de sistemas, haciendo un estudio previo de los procesos a auditar, definiendo las herramientas necesarias para una adecuada planeación de la auditoría informática.

- Visita preliminar a las instalaciones de la E.S.E. Hospital Cumbal con el fin de realizar una observación de los diferentes procesos implementados en el área de sistemas de esta institución y realización de entrevista al director o su delegado, para solicitud de información de la empresa.

2.1.2 Etapa 2: Planeación de la auditoría

- Establecer objetivos específicos de la auditoría, definición de la metodología, elaboración del cronograma de actividades y estudio de los recursos necesarios para implementar el plan de auditoría.

- Elaboración del Plan de auditoría y planificación de su realización por etapas, especificando las distintas herramientas de auditoría que garanticen el cumplimiento de los objetivos planteados.

2.1.3 Etapa 3: Ejecución de la auditoría.

- Elaboración del Programa de auditoría, identificando dentro de los dominios del COBIT, los procesos y los objetivos de control que se van a evaluar.

- Elaboración de cuadros de definición de fuentes de conocimiento, análisis, y pruebas de auditoría, para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para ser auditados.

- Elaboración de los cuestionarios cuantitativos o cualitativos para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para ser auditados.
- Aplicación de las herramientas de auditoría.

- Identificación de hallazgos de los procesos evaluados.

- Análisis de riesgos e identificación de las principales vulnerabilidades mediante una matriz de riesgos, elaboración de las tablas de hallazgos, las consecuencias y su respectivo plan correctivo.

2.1.4 Etapa 4: Dictamen final de la auditoría

- Elaboración del informe final de los procesos evaluados y los hallazgos encontrados con sus respectivas recomendaciones que permitan tomar las medidas necesarias para su correcto funcionamiento.

- Presentación y entrega del informe ejecutivo al gerente de la E.S.E. Hospital Cumbal, para que determine si sigue las recomendaciones a los hallazgos encontrados, ejecutando un plan de mejoramiento.

3. DESARROLLO DEL TRABAJO

Para el desarrollo de la auditoría informática, es necesario conocer cierta documentación e información de la empresa, la cual es de vital importancia y se considera necesaria, para comprender las características de las áreas objeto de auditoría.

Dicha documentación e información, se divide en dos grupos: el archivo permanente y el archivo corriente.

3.1 ARCHIVO PERMANENTE

El archivo permanente reúne información de naturaleza histórica y actual de la entidad. Estos archivos proporcionan una fuente conveniente de información válida para una auditoría eficaz y objetiva, estos documentos están conformados por reglamentos, contratos, manuales de funciones, instructivos y normas.

3.1.1 Legislación nacional

- Ley 100 de 1993: el sistema de salud en el país depende del Art. 48 de la Constitución Nacional, está reglamentada en el segundo libro de la Ley 100 de 1993, expedida por el Congreso de Colombia, estableció el Sistema de Seguridad Social en Colombia, definiendo las reglas fundamentales para regir el servicio público de salud, como: la equidad, la obligatoriedad, la protección integral, la libre escogencia, la autonomía de las instituciones, la descentralización administrativa, la participación social, la concertación y la calidad.[9]

- Ley 1122 de 2007: en la cual se establecen un conjunto de políticas que busca garantizar de manera integrada, la salud de la población por medio de acciones dirigidas tanto de manera individual como colectiva ya que sus resultados se constituyen en indicadores de las condiciones de vida, bienestar y desarrollo[10].

- Ley 1438 de 2011: tiene como objeto fortalecer el SGSSS a través de un modelo de prestación del servicio público en salud que en el marco de la

[9] http://es.wikipedia.org/wiki/Sistema_de_salud_en_Colombia
[10] www.minsalud.gov.co/Normatividad/LEY%201122%20DE%202007.pdf

estrategia atención primaria en salud, permita la acción coordinada del estado, IPS, EPS y sociedad para el mejoramiento de la salud y la creación de un ambiente sano y saludable, que brinde servicios de mayor calidad, incluyentes y equitativos, donde el centro y objetivo de todos los esfuerzos, sean los residentes en el país[11].

- Decreto 806 de 1998: por el cual se reglamenta la afiliación al Régimen de Seguridad Social en Salud y la prestación de los beneficios del servicio público esencial de Seguridad Social en Salud y como servicio de interés general, en todo el territorio nacional.

Este decreto tiene por objeto reglamentar la Seguridad Social en Salud, en todo el territorio nacional, tanto como servicio público esencial como servicio de interés público a cargo de particulares o del propio Estado, el tipo de participantes del Sistema, la afiliación al Régimen de Seguridad Social en Salud y los derechos de los afiliados.[12]

3.1.2 Reseña histórica.

La ESE Hospital Cumbal, es una entidad de primer nivel de atención con una categoría especial de entidad pública descentralizada de propiedad del Municipio de Cumbal, con personería jurídica, patrimonio propio y autonomía administrativa.

Su fundación se remonta al año 1971, prestando servicios de salud en el Puesto de Salud donde se contaba con un recurso humano de un médico, un auxiliar de enfermería y un celador, el Puesto de Salud era dependiente del Hospital Civil de Ipiales, en 1990 se convierte en Centro de Salud y se nombra el primer Director para coordinar las actividades, se incrementó el personal a dos médicos, un odontólogo, una enfermera jefe, laboratorio y servicio de traslado asistencial básico, en esta época el Instituto Departamental de Salud de Nariño dona la primera ambulancia Land Rover, en 1993 después de la promulgación de la Ley 100, la Alcaldía Municipal gestiona recursos para construir las áreas de hospitalización, laboratorio, rayos X, servicio farmacéutico y la parte administrativa, auditorio, finanzas y control interno.

En su proceso de transformación, mediante Acuerdo Nro. 027 de agosto 27 de 1996, se creó la Empresa Social del Estado Hospital Cumbal, descentralizada de orden municipal, dotada de personería jurídica, patrimonio propio y autonomía administrativa adscrita a la Dirección de Seguridad Social en cabeza del Alcalde Municipal, quien nombra como primer gerente al Doctor Álvaro Moncayo, el Hospital Civil realiza todos los procesos de entrega de los equipos médicos,

[11] http://www.minsalud.gov.co/Normatividad/LEY%201438%20DE%202011.pdf
[12] http://www.susalud.com.co

insumos y del personal transferido, cuando se creó la empresa contaba con Centros de Salud en los corregimientos de Panan, Chiles y San Juan de Mayasquer y Puestos de Salud en las veredas de Miraflores, San Martín, Cuetial, Tallambi y La Unión. En el año 2006, asume la Gerencia el Doctor Carlos Burbano Ortiz, quien presentó proyecto ante la Embajada de Estados Unidos a través de las Fuerzas Militares para la gestión de recursos y poder ejecutar el proyecto denominado construcción del área de urgencias el cual se lo construyó con las especificaciones técnicas del Ministerio de Salud y Protección Social.

Pese a las dificultades propias del sector salud, presentes en la última década, la ESE Hospital Cumbal nunca interrumpió la prestación de los servicios de salud, amplio su portafolio de servicios y en la actualidad brinda a sus usuarios: promoción y prevención, medicina general, odontología, psicología, servicio farmacéutico, laboratorio, rayos X, fisioterapia terapia respiratoria, terapia ocupacional, hospitalización, urgencias, traslado asistencial básico y de Nivel II se presta los servicios de telemedicina.

3.1.3 Ubicación geográfica[13].

La E.S.E. Hospital Cumbal, se encuentra tiene domicilio en el Municipio de Cumbal, Departamento de Nariño, el cual cuenta con los siguientes límites y coordenadas:

El Municipio de Cumbal, está situado al Sur Occidente del Departamento de Nariño limitando con la República del Ecuador y la altiplanicie de Tuquerres e Ipiales, hace parte de la Cordillera Andina que se considera como una región de piso térmico frío. Todos sus límites son: Norte, con el Municipio de Guachucal y Mallama. Sur, con la Provincia del Carchi y República del Ecuador. Oriente, con el Municipio de Cuaspud Carlosama. Occidente, con el Municipio de Ricaurte.

Cumbal está junto al gran macizo denominado Nudo de los Pastos, y tiene una extensión de 677 m^2.

La cabecera Municipal tiene temperatura promedio de 10 °C, y está localizada a 0° 55” de latitud norte y 77°48” de longitud Oeste del meridiano de Greenwich y a una altura promedio de 3.050 m.s.n.m.
Distancia de referencia: 120 km de la Capital (San Juan de Pasto).

3.1.4 Datos generales de la empresa

- Razón Social: Empresa Social del Estado Hospital Cumbal

[13] http://www.cumbal-narino.gov.co/informacion_general.shtml

- NIT: 814.001.329-5
- Localización: Municipio de Cumbal, Departamento de Nariño.
- Dirección: Barrio San Antonio Cra 12 # 8 - 00
- Correo Electrónico: esehospitalcumbal@hotmail.com
- Teléfono: 092 7798043
- Fax: 092 7798420
- Logo:

Misión

La Empresa Social del Estado Hospital Cumbal, presta servicios de salud de primer nivel de atención, con óptima calidad, garantizando una atención oportuna, sin discriminación alguna, y cuenta con personal idóneo, capacitado y con sentido humano, con una capacidad instalada apropiada con el fin de promover estilos de vida saludables, prevenir factores de riesgo y mejorar las condiciones de salud de la población.[14]

Visión

El Hospital Cumbal Empresa Social del Estado, se acreditará para el año 2015 a través de un direccionamiento bien definido servicios de salud de primer nivel de atención bajo el cumplimiento de los estándares de calidad de acuerdo a la normatividad vigente, buscando mejorar las condiciones de salud de la población.[15]

Principios corporativos

Respeto: reconocemos el valor inherente y los derechos innatos de los individuos y de la sociedad
Responsabilidad: reaccionamos de modo positivo al analizar, dar razón y asumir las consecuencias de las propias acciones u omisiones en lo referente a la prestación del servicio esencial de salud.
Humanidad: entendida como el trato con simpatía, comprensión del paciente o usuario que acude a nosotros para la solución de un problema de salud o administrativo.
Confidencialidad: la confidencialidad es el código ético y de ley por el que el clínico no puede divulgar las cuestiones privadas reveladas por el paciente en el contexto de la relación entre el médico y el paciente.

[14] http://www.esehospitalcumbal.gov.co/mision-vision/
[15] http://www.esehospitalcumbal.gov.co/mision-vision/

Tolerancia: respetar y tener consideración hacia las maneras de pensar, actuar y sentir de los demás, aunque estas sean diferentes a las nuestras, sin perjuicio de los derechos y deberes que nos asisten.
Seguridad: ausencia de riesgo o confianza en algo o alguien.

3.1.5 Políticas institucionales

Calidad institucional: todas las actividades desarrolladas por la E.S.E estarán enmarcadas dentro de los estándares de calidad definidos para cada servicio. Los resultados insatisfactorios serán sometidos al análisis y ajuste para evitar su reincidencia.

Usuarios y cliente interno satisfechos: lideraremos con entusiasmo, lealtad y responsabilidad un trabajo eficiente, honesto, lleno de calidez y humanidad con nuestros usuarios. Esa será nuestra cultura de servicio. La institución se diferenciará en el medio por poseer un equipo de trabajo calificado y satisfecho que refleje permanentemente armonía familiar, laboral y personal, para poder transmitir y proporcionar satisfacción al usuario.

Gerencia participativa: esta institución no se concibe sin la participativa activa positiva de todos los miembros del equipo de trabajo y de los actores de la comunidad, serán ellos quienes defiendan los valores, principios y permitan el cumplimiento de las políticas institucionales, garantizando su permanencia, desarrollo y posicionamiento.

Equidad: la aplicación de las normas y reglamentos será igual para todos los colaboradores y las que correspondan a los usuarios en igual sentido sin distingos de ningún tipo.

3.1.6 Mapa de procesos de la E.S.E. Hospital Cumbal

De acuerdo con el MECI (Manual estándar de control interno), el Hospital de Cumbal cuenta con unos procesos definidos en tres categorías:

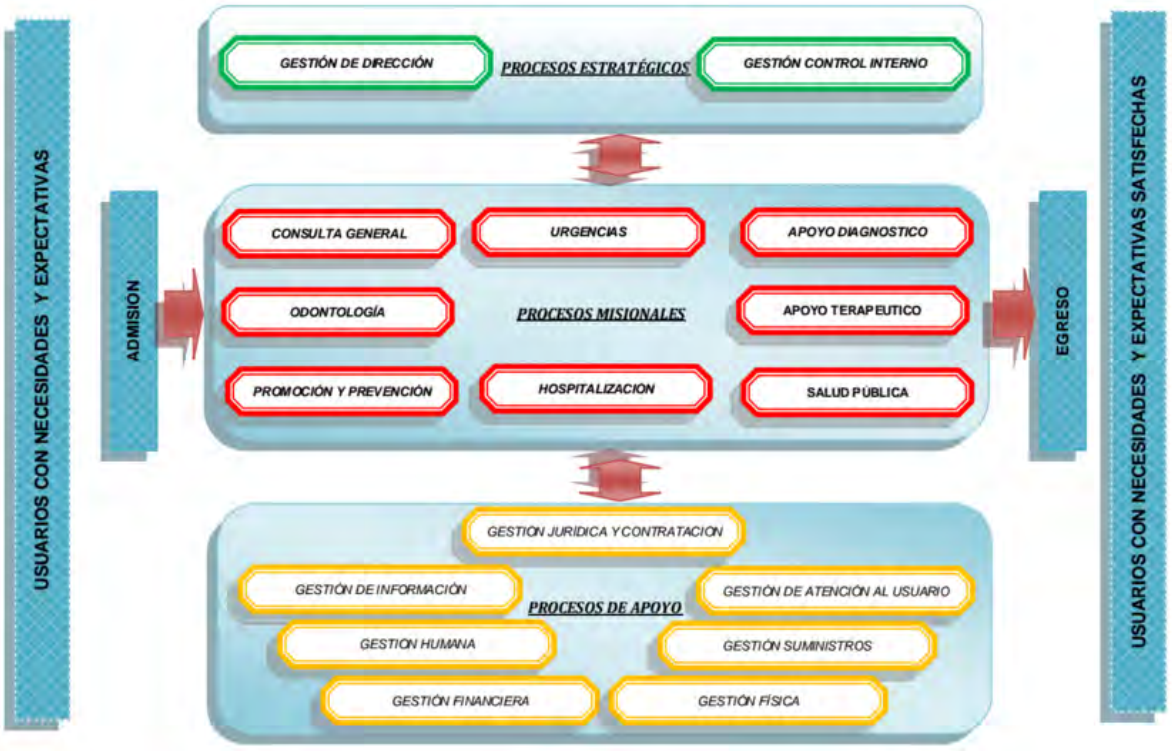
Procesos estratégicos: donde se toman las decisiones importantes para la empresa.

Procesos misionales: los cuales refieren a los servicios de salud que ofrece el Hospital de Cumbal para la población beneficiaria del sistema de salud.

Procesos de apoyo: tienen por objetivo apoyar las actividades que se desarrollan en los procesos misionales y estratégicos.

En la figura a continuación, se muestra el mapa de procesos del Hospital de Cumbal.

Figura 1. Mapa de procesos



Fuente: Sistema de Gestión de la Calidad E.S.E. Hospital Cumbal.

3.1.7 Organigrama

En el Hospital de Cumbal existe una estructura jerárquica, constituida de la siguiente forma:

En primer nivel se encuentra la junta directiva, conformada por el alcalde municipal, el director local de salud, el gerente del hospital y un representante de los trabajadores que pertenezca al área misional.

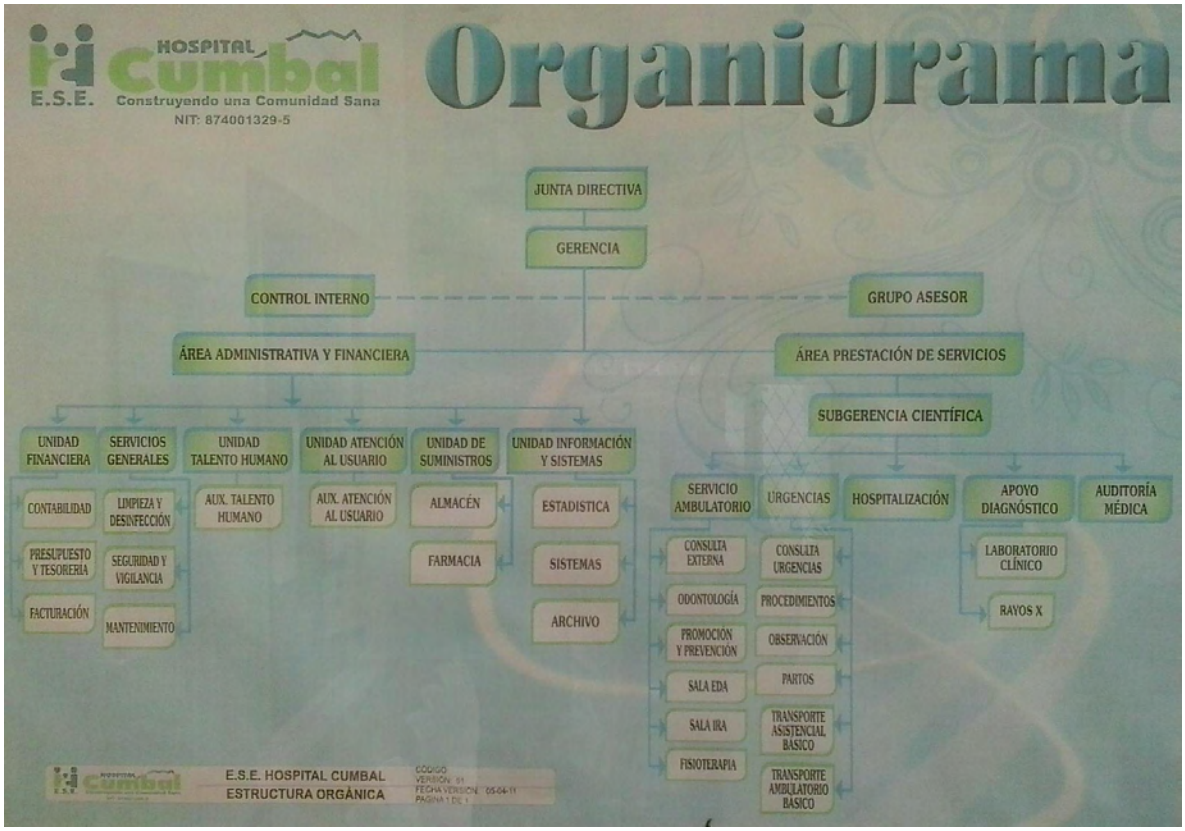
En segundo nivel se encuentra el gerente o representante legal.

En tercer nivel se encuentran el grupo de asesores y el jefe de control interno.

Luego se encuentran definidos los directores del área administrativa y financiera y el área de prestación de servicios.

Posteriormente se encuentran los demás jefes de dependencia y sus respectivos auxiliares como se detalla en la figura siguiente:

Figura 2. Organigrama



Fuente: Sistema de Gestión de la Calidad E.S.E. Hospital Cumbal.

3.1.8 Manual de funciones del área de sistemas

Ver CD/Anexo 1. Manual de funciones ESE Hospital Cumbal.pdf

3.2 ARCHIVO CORRIENTE

Son documentos que soportan la labor y evidencias del proceso de auditoría informática, comprende la evaluación que hizo el auditor a la entidad, tales documentos son informes de pruebas, análisis, hallazgos, cuestionarios, planes y programas de auditoría.

Con el fin de lograr un exitoso desarrollo del proceso de auditoría se realizó una recopilación de información y documentos necesarios para el conocimiento de la entidad y los procesos que allí se desarrollan.

3.2.1 Memorando plan de auditoría

Objetivo general

Evaluar la estructura organizacional y los procesos del área de informática, de la E.S.E. Hospital Cumbal.

Objetivos específicos

- Conocer el área de informática y sus procesos internos, en la E.S.E. Hospital Cumbal.

- Elaborar el Programa de auditoría y diseñar los instrumentos para recolectar la información y pruebas.

- Aplicar los instrumentos diseñados, realizar las pruebas y ejecutar el proceso de análisis y evaluación de riesgos para su valoración.

- Elaborar y entregar el informe final que contenga los riesgos confirmados y controles propuestos.

Alcance

De la estructura organizacional de la E.S.E. Hospital Cumbal, se evaluó lo siguiente:

- Existencia del área de informática, mediante la revisión del organigrama de la E.S.E. Hospital Cumbal.

- Existencia de manuales de funciones y procedimientos del área informática de la E.S.E. Hospital Cumbal.

De los procesos del área de informática de la E.S.E. Hospital Cumbal, se evaluó lo siguiente:

- Existencia de los procesos y procedimientos del área de informática de la E.S.E. Hospital Cumbal.

- Existencia de los procesos y procedimientos documentados del área de informática de la E.S.E. Hospital Cumbal.

- Cumplimiento de los procesos y procedimientos del área de informática de la E.S.E. Hospital Cumbal.

- Existencia y definición del personal responsable del área de informática de la E.S.E. Hospital Cumbal.

De los procesos informáticos y de información, se revisó:

- Existencias de sistemas de control de información de la E.S.E. Hospital Cumbal.

- Existencia de políticas organizacionales, relacionadas con el manejo de información de la E.S.E. Hospital Cumbal.

Metodología

1. Se realizó entrevista al gerente de la E.S.E. Hospital Cumbal, jefe de Control Interno o su delegado, para conocer si existe definido el responsable o encargado el área de informática.

2. Una vez determinado si existe el responsable o encargado del área de informática se procederá a realizó una entrevista para conocer la estructura organizacional y sus respectivos procesos internos.

3. Para elaborar el Programa de auditoría y diseñar los instrumentos para recolectar la información y pruebas, se realizó seleccionando el estándar más acorde con el objetivo de la auditoría informática a la estructura organizacional y a los procesos del área de informática de la E.S.E. Hospital Cumbal.

4. Una vez elaborado el programa de auditoría, se aplica los instrumentos para recolección de información diseñados, al personal elegido de la E.S.E. Hospital Cumbal, se realizó las pruebas y ejecutó el proceso de análisis y evaluación de riesgos para su valoración, según el estándar seleccionado.

5. Para elaborar y entregar el informe final que contenga los riesgos confirmados y controles propuestos, se tuvo en cuenta los resultados del programa de auditoría.

Recursos

- Talento Humano: se conformó el equipo de trabajo, con las personas descritas a continuación:
  Personal auditor
  - Mónica Yakeline Caicedo Alpala
  - Henry Fredy Irua Taimal

  Personal de la institución
  - Administrativo: Gerente, Jefe de Control Interno o su delegado
  - Operativo: Jefes de área.
- Tecnológico
  Hardware: equipo de cómputo, cámara digital, memoria USB, impresora multifuncional.
  Software: sistema operativo Windows 7, paquete ofimático Office 2013, software de base: Adobe Reader, winrar.
- Otros: servicio de internet banda ancha.
- Recursos físicos: instalaciones de la E.S.E. Hospital Cumbal, específicamente área de informática.
- Recursos de papelería: dos resmas de papel tamaño carta, artículos de oficina (grapadora, ganchos grapadora, saca ganchos, perforadora, AZ, lapiceros, lápiz, borrador, CD's.

Presupuesto

No aplica, ya que la presente auditoría informática corresponde a un trabajo académico.

Cronograma de actividades

A continuación se detalla el cronograma de actividades que se estableció para el desarrollo de la auditoria informática:

ACTIVIDAD	Semana 1	Semana 2	Semana 3	Semana 4
Entrevista al gerente, jefe de control Interno o su delegado, para conocer si existe definido en la E.S.E. Hospital Cumbal el responsable o encargado el área de informática				
Si existe responsable o encargado del área de informática, se realizara entrevista para conocer la estructura organizacional del área y sus respectivos procesos internos.				

Elaborar el Programa de auditoría y diseñar los instrumentos para recolectar la información y diseñar pruebas de verificación.				
Aplicar los instrumentos para recolección de información diseñados y pruebas correspondientes.				
Análisis y Evaluación de Riesgos para su valoración				
Elaborar y entregar el informe final que contenga los Riesgos confirmados y controles propuestos				

3.2.2 Programa de auditoría

Para la realización de la auditoría informática a la estructura organizacional y a los procesos del área de sistemas de la E.S.E. Hospital Cumbal, se utilizó la metodología COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas), para lo cual se ha seleccionado los siguientes objetivos de control que se encuentran dentro de los dominios, así:

Dominio: planear y organizar (PO)

Cubre la estrategia y las tácticas, se refiere a la identificación de la forma en que la tecnología información puede contribuir de la mejor manera al logro de los objetivos de la organización. La consecución de la visión estratégica debe ser planeada, comunicada y administrada desde diferentes perspectivas y debe establecerse una organización y una infraestructura tecnológica apropiadas.

- **PO4. Definir los procesos, organización y relaciones de TI.**
  El objetivo es la prestación de servicios de TI, por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas.

  - **PO4.4 Ubicación organizacional de la función de TI:** identificar la ubicación del área de sistemas dentro de la estructura organizacional de la empresa.

  - **PO4.5 Estructura organizacional:** identificar si existe una o más personas en el área de sistemas y verificar si se cuenta con los procesos respectivos.

  - **PO4.6 Establecimiento de roles y responsabilidades: i**dentificar las funciones del personal del área de sistemas y su alcance (nivel jerárquico) y responsabilidad frente a los demás usuarios en la empresa.

- **PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento:** los integrantes del área de sistemas deben considerar el riesgo permanente en la institución para eventuales fallas o incidentes críticos, para lo cual deben .disponer de unas medidas de contingencia para garantizar así la continuidad en la atención y la integridad de la información.

- **PO4.9 Propiedad de datos y sistemas:** se cuenta con procesos y herramientas para acreditar la propiedad de la información y garantice su integridad, además cada jefe de área clasifica la información según su importancia y define como protegerlos.

- **PO4.10 Supervisión:** verifica si se ha implementado prácticas adecuadas de supervisión (autocontrol) dentro del área de sistemas y evaluar si se cuenta con los recursos para ejecutar sus funciones y lleva indicadores de desempeño. Registro de novedades en actividades propias del área; por ejemplo: tareas de mantenimiento.

- **PO4.11 Segregación de funciones:** asigna funciones específicas a cada integrante del área de sistemas, tareas autorizadas y lugar de trabajo

- **PO4.12 Personal de TI:** evaluar que exista el personal necesario en el área de sistemas con el fin de atender de forma suficiente las solicitudes de la empresa relacionadas con TI, y que sea beneficioso para lograr las metas de la empresa.

- **PO7 Administrar los recursos humanos de TI**
  El objetivo es maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal.

- **PO7.1 Reclutamiento y retención del personal:** al contratar personal para el área de sistemas, se debe realizar un adecuado proceso de escogencia y verificación de la idoneidad del personal, acorde los procedimientos generales de la empresa, y brindarle inducción y ambiente positivo de trabajo.

- **PO7.2 Competencias del personal:** verificar de forma periódica que el personal tenga de TI las habilidades para cumplir sus funciones con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando programas de calificación y certificación según sea el caso.

- **PO7.3 Asignación de roles**: definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requerimiento de adherirse a las políticas y procedimientos

administrativos, así como al código de ética y prácticas profesionales. El nivel de supervisión debe estar de acuerdo con la sensibilidad del puesto y el grado de responsabilidades asignadas.

- **PO7.4 Entrenamiento del personal de TI:** proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales.

- **PO7.8 Cambios y terminación de trabajo:** evaluar si la entidad toma medidas respecto a los cambios en los puestos, analizar si realizar la transferencia del conocimiento, reasignación de responsabilidades en especial las terminaciones de contratos, es decir si al personal que sale de la institución se le restringe el acceso al área física y las aplicaciones del área, a fin de minimizar los riesgos.

Dominio: adquirir e implementar (AI)

Para llevar a cabo la estrategia de TI, las soluciones de Ti deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

- **AI4 Facilitar la operación de uso**
  El objetivo es asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas, mediante la realización de un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento.

- **AI4.3 Transferencia de conocimiento a usuarios finales:** verificar la existencia de un plan de entrenamiento que aborden capacitación inicial y continua, así como el desarrollo de habilidades, materiales de entrenamiento, manual de usuario, manual de procedimientos, asistencia a usuarios y evaluación. Que permite que los usuarios finales utilicen con efectividad y eficiencia la(s) aplicación(es).

- **AI4.4 Transferencia de conocimiento al personal de operaciones y soporte:** evaluar la existencia de transferencia de conocimiento que permite que el personal de operaciones y soporte entreguen, apoyen y mantengan la aplicación y la infraestructura funcionando de manera efectiva y eficiente. La transferencia de conocimiento incluye el desarrollo de planes de entrenamiento que aborden capacitación inicial y continua, así como el desarrollo de habilidades, materiales de entrenamiento, manual de usuario, manual de procedimientos, material de uso del sistema en la práctica diaria.

Dominio: entregar y dar soporte (DS)

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

- **DS4 Garantizar continuidad del servicio**
  El objetivo es mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones, mediante un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio.

- **DS4.2 Planes de continuidad de TI:** revisar la existencia de planes de continuidad, diseñados para reducir el impacto de una interrupción mayor de las funciones y los procesos clave de la entidad. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de los servicios TI.

- **DS4.3 Recursos críticos de TI**: 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. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales, requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio

- **DS4.4 Mantenimiento del plan de continuidad de TI**: exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.

- **DS4.6 Entrenamiento del plan de continuidad de TI**: asegurarse de que todas las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.

- **DS4.8 Recuperación y reanudación de los servicios de TI**: planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de los servicios y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio.

- **DS4.9 Almacenamiento de respaldos fuera de las instalaciones**: almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.

- **DS4.10 Revisión post reanudación:** una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

➢ **DS5 Garantizar la seguridad de los sistemas**

El objetivo es salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida, realizando controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados.

- **DS5.2 Plan de seguridad de TI:** verificar si en la entidad se tiene un plan de seguridad de TI según los recursos informáticos en cada dependencia, además de una cultura de seguridad. Asegurar que el plan esta implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.

- **DS5.3 Administración de identidad***:* verificar si todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (Entorno de TI, operación de sistemas, desarrollo y mantenimiento) son identificables de manera única. Confirmar que los permisos de acceso del usuario al sistema y

los datos están en línea con las necesidades del módulo definidas y documentadas y que los requerimientos de trabajo están adjuntos a las identidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central.

- **DS5.4 Administración de cuentas de usuario**: evaluar procedimientos para la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información del módulo deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados.

- **DS5.10 Seguridad de la red**: uso de técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.

- **DS7 Educar y entrenar a los usuarios**
  El objetivo es asegurar un conocimiento correcto atribuido a los servicios de TI realizando un sistema de contabilidad de costos asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos.

- **DS7.1 Identificación de necesidades de entrenamiento y educación**: verificar la existencia de un programa de entrenamiento para cada grupo objetivo de empleados de la entidad, que incluya: implementar procedimientos de capacitación y formación en seguridad de la información, valores sistémicos (valores éticos, cultura de control y seguridad).

- **DS7.2 Impartición de entrenamiento y educación:** evaluar si con base en las necesidades de entrenamiento identificadas, grupos objetivo, mecanismos de impartición eficientes, instructores; organizar el entrenamiento y llevar registros de asistencia y evaluaciones de desempeño.

- **DS7.3 Evaluación del entrenamiento recibido:** evaluar el contenido del entrenamiento respecto a la relevancia, calidad, efectividad, percepción y retención del conocimiento, costo y valor. Los resultados de esta evaluación deben contribuir en la definición futura de los planes de estudio y de las sesiones de entrenamiento.

- **DS9 Administrar la configuración**
  El objetivo es dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios realizando controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia.

  - **DS9.1 Repositorio y línea base de configuración**: monitorear y grabar todos los activos y los cambios a los activos. Mantener una línea base de los elementos de la configuración para todos los sistemas y servicios como punto de comprobación al que volver tras el cambio

  - **DS9.2 Identificación y mantenimiento de elementos de configuración**: establecer procedimientos de configuración para soportar la gestión y rastro de todos los cambios al repositorio de configuración.

  - **DS9.3 Revisión de integridad de la configuración**: revisar periódicamente los datos de configuración para verificar y confirmar la integridad de la configuración actual e histórica. Revisar periódicamente el software instalado contra la política de uso de software para identificar software personal o no licencia de cualquier otra instancia de software en exceso del contrato de licenciamiento actual. Reportar, actuar y corregir errores y desviaciones.

- **DS11 Administración de datos**
  El objetivo es asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento, a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI.

  - **DS11.2 Acuerdos de almacenamiento y conservación**: definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente para conseguir los objetivos de negocio, la política de seguridad de la organización y los requerimientos regulatorios.

  - **DS11.3 Sistema de administración de librerías de medios**: definir e implementar procedimientos para mantener un inventario de medios almacenados y archivados para asegurar su usabilidad integridad.

  - **DS11.4 Eliminación**: definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.

- **DS11.5 Respaldo y restauración:** definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad.

- **DS12 Administración del ambiente físico**
  El objetivo es proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

- **DS.12.2 Medidas de seguridad física:** se requieren implementar medidas de seguridad que incluyan ubicación de equipos, zonas de seguridad y monitoreo de incidentes de seguridad física.

- **DS12.3 Acceso físico:** el acceso al área de sistemas debe justificarse, autorizarse, registrase y monitorearse.

- **DS13 Administración de operaciones**
  El objetivo es asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades.

- **DS13.1 Procedimientos e instrucciones de operación**: definir, implementar y mantener procedimientos estándar para operaciones de TI y garantizar que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos.

- **DS13.2 Programación de tareas:** organizar la programación de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el desempeño y la utilización para cumplir con los requerimientos del negocio. Deben autorizarse los programas iniciales, así como los cambios a estos programas. Los procedimientos deben implementarse para identificar, investigar y aprobar las salidas de los programas estándar agendados.

- **DS13.3 Monitoreo de la infraestructura de TI**: definir e implementar procedimientos para monitorear la infraestructura de TI y los eventos relacionados. Garantizar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que están alrededor de las operaciones.

- **DS13.5 Mantenimiento preventivo del hardware**: evaluar los procedimientos para garantizar el mantenimiento programado y oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.

Dominio: monitorear y evaluar (ME)

Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad.

- **ME1 Monitorear y evaluar el desempeño de TI**
  El objetivo es asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.

- **ME1.4 Evaluación del desempeño**: comparar de forma periódica el desempeño del área de sistemas frente a las metas propuestas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes.

- **ME1.5 Reportes al consejo directivo y a ejecutivos**: proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño. Los reportes de estatus deben incluir el grado en el que se han alcanzado los objetivos planeados, los entregables obtenidos, las metas de desempeño alcanzadas y los riesgos mitigados. Durante la revisión, se debe identificar cualquier desviación respecto al desempeño esperado y se deben iniciar y reportar las medidas de administración adecuadas

- **ME1.6 Acciones correctivas:** identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes. Esto incluye el seguimiento de todo el monitoreo, de los reportes y de las evaluaciones con:• revisión, negociación y establecimiento de respuestas de administración • Asignación de responsabilidades por la corrección • Rastreo de los resultados de las acciones comprometidas

- **ME3 Garantizar el cumplimiento con requerimientos externos:** el objetivo es incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.

- **ME3.1 Identificar los requerimientos de las leyes, regulaciones y cumplimientos contractuales:** identificar, sobre una base continua, leyes locales e internacionales, regulaciones, y otros requerimientos externos que se deben de cumplir para incorporar en las políticas, estándares, procedimientos y metodologías de TI de la organización.

- **ME4 Proporcionar gobierno de TI**
  El objetivo es incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes desarrolladas a intervalos regulares de tiempo.

- **ME4.4 Administración de recursos**: revisar inversión, uso y asignación de los activos de TI por medio de evaluaciones periódicas de las iniciativas y operaciones de TI para asegurar recursos y alineamiento apropiados con los objetivos estratégicos y los imperativos de negocios actuales y futuros.

- **ME4.5 Administración de riesgos:** trabajar con el consejo directivo para definir el nivel de riesgo de TI aceptable por la empresa y obtener garantía razonable que las prácticas de administración de riesgos de TI son apropiadas para asegurar que el riesgo actual de TI no excede el riesgo aceptable de dirección.

3.2.3 Diseño de instrumentos de auditoría

A continuación, se diseña los instrumentos de auditoría que se van a utilizar para la realización de la auditoría informática a la estructura organizacional y a los procesos del área de sistemas de la E.S.E. Hospital Cumbal.

Formato de definición de fuentes de conocimiento: este instrumento sirve para identificar, cuál es la información que se necesita para evaluar un determinado proceso dentro de los dominios del COBIT, también se especifica en el cuales son las pruebas de análisis y de ejecución que se deben realizar.

Fomato1. Formato de definición de fuentes de conocimiento (DFC)

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE DEFINICION DE FUENTES DE CONOCIMIENTO	**REF.** DFC-[proceso]
		Noviembre 2015
		Versión 1.0
		Página 1 de 1
ENTIDAD AUDITADA		
OBJETO DE ESTUDIO		
AREA AUDITADA		
RESPONSABLES		

MATERIAL DE SOPORTE			
DOMINIO		**PROCESO**	
DESCRIPCION DE ACTIVIDAD/PRUEBA			
FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**		
	DE ANALISIS	**DE EJECUCION**	

A continuación, se describen los ítems que se encuentran en este instrumento de auditoría.

- ✓ **REF.** identificación del cuadro de definición.
- ✓ **Entidad auditada**: en este espacio se indica el nombre de la entidad a la cual se le está realizando el proceso de auditoría.
- ✓ **Proceso auditado:** en este espacio se indica el nombre del proceso objeto de la auditoría.
- ✓ **Responsables:** nombre del auditor o auditores.
- ✓ **Descripción de actividad/prueba:** en este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se está revisando.
- ✓ **Material de soporte:** en este espacio se indica el nombre del material que soporta el proceso, para el caso será COBIT.
- ✓ **Dominio**: espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.
- ✓ **Proceso:** espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.
- ✓ **Fuentes de conocimiento**: espacio que permite identificar las herramientas necesarias para obtener la información, puede ser a través de entrevistas, manuales, política, archivos físicos o magnéticos, reportes, contratos, etc.
- ✓ **Repositorio de pruebas**: se divide en dos tipos de pruebas:
    - Repositorio de pruebas de análisis: espacio en el que describe el análisis de cada proceso y de la información obtenida.
    - Repositorio de pruebas de ejecución: se describe las acciones a realizar para la ejecución de la auditoría, como las revisiones, verificaciones, pruebas y obtención de inconsistencias, etc.

Las pruebas de la aplicación de este instrumento de la auditoría corresponden a los formatos de definición de fuentes de conocimiento, que se anexan en medio digital y almacenados en el CD adjunto en la carpeta de */Anexos/Definición-fuentes-de-conocimiento/Anexo2-Formatos-Definicion-fuentes-de-conocimiento.pdf*

Cuestionario cuantitativo: el cuestionario cuantitativo permite dar una calificación numérica a un requerimiento dentro de los procesos que se estén auditando para determinar su vulnerabilidad.

Figura 5. Cuestionario cuantitativo (CC)

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE CUESTIONARIO CUANTITATIVO				**REF.** CC-[proceso] Noviembre 2015 Versión 1.0 Página 1 de 1
ENTIDAD AUDITADA					
PROCESO AUDITADO					
RESPONSABLE(S)					
MATERIAL DE SOPORTE					
DOMINIO		**PROCESO**			
ESCALA DE CALIFICACION. Si su respuesta es SI o NO, califique según la importancia de la pregunta para usted, donde 1 = baja importancia y 5 = Excelente importancia. Si es NA (No Aplica) marque X.					
PREGUNTA			**SI**	**NO**	**NA** / **OBSERVACIONES**
1. ¿?					
2. ¿ ?					
3. ¿?...					
TOTALES					**RIESGO:**
TOTAL CUESTIONARIO					
PORCENTAJE DE RIESGO					
FIRMA ENCUESTADO:		**FIRMA AUDITOR:**			
CARGO ENCUESTADO:		**FECHA APLICACIÓN:**			

A continuación, se describe el cuestionario cuantitativo que está conformado por los siguientes ítems:

- ✓ **REF.** identificación del cuadro de definición.
- ✓ **Entidad auditada**: en este espacio se indica el nombre de la entidad a la cual se le está realizando el proceso de auditoría.

- ✓ **Proceso auditado:** en este espacio se indica el nombre del proceso objeto de la auditoría.
- ✓ **Responsables:** nombre del auditor o auditores.
- ✓ **Descripción de actividad/prueba:** en este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se está revisando.
- ✓ **Material de soporte:** en este espacio se indica el nombre del material que soporta el proceso, para el caso será COBIT.
- ✓ **Dominio**: espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.
- ✓ **Proceso:** espacio reservado para el nombre del proceso específico que se está auditando dentro de los dominios del COBIT.
- ✓ **Pregunta:** planteamiento de la descripción de la información requerida a evaluar.
- ✓ **Si – No – NA:** evalúa si cumple o no con la información requerida. Para el caso del Si o No se debe asignar una calificación de con valores entre 1 y 5, donde 1 significa una calificación de baja importancia y 5 una calificación de Excelente importancia asignada al objetivo de control que se está evaluando. Cuando la respuesta es No Aplica (NA) marcar con una X.
- ✓ **Fuente:** fuente de donde se obtiene la información requerida
- ✓ **Total:** se asigna los valores correspondientes a cada columna la sumatoria de los SI, la sumatoria de los NO y la sumatoria de los NA.
- ✓ **Total cuestionario:** la sumatoria del total de los SI + NO + NA.
- ✓ **Porcentaje de riesgo:** hace referencia a la probabilidad de que el proceso se vea afectado por las acciones de las cuales se está indagando, entre mas alto el porcentaje mayor probabilidad de riesgo tiene el proceso de salir perjudicado.
- ✓ **Firma encuestado:** firma la persona quien responde el cuestionario
- ✓ **Cargo entrevistado:** especifica el cargo de la persona quien responde el cuestionario
- ✓ **Firma auditor:** firma el auditor responsable de aplicar el cuestionario
- ✓ **Fecha aplicación:** fecha de la aplicación del cuestionario

Con la aplicación del cuestionario cuantitativo se obtuvo el porcentaje de riesgo el cual se obtiene aplicando la siguiente fórmula:

$$\%Riesgo = \frac{Sumatoria\ de\ SI * 100}{Total\ Encuesta - Totales\ NA}$$

Luego para hallar el porcentaje de riesgo total se calcula así:

$$\%Riesgo\ Total = \quad 100 - \%Riesgo$$

Para determinar el nivel de riesgo total, se tuvo en cuenta la siguiente categorización:

1% - 30% = Riesgo bajo
31% - 70% = Riesgo medio
71% - 100% = Riesgo alto

Riesgo bajo: las insuficiencias que se exhiben en este nivel no son muy importantes, pero se recomienda considerar soluciones preventivas al largo plazo.

Riesgo medio: las insuficiencias que se exhiben en este nivel son de importancia media ya que se puede controlarlo, lo cual permite solucionarlo en un lapso de tiempo determinado.

Riesgo alto: las insuficiencias que se exhiben en este nivel son de gran importancia y se deben tomar medidas radicales e inmediatas con el objeto de reducir el riesgo, caso contrario este no permitirá alcanzar los objetivos de la entidad.

Para el caso de aplicar este formato de cuestionario cuantitativo a varias personas, el resultado de la probabilidad del riesgo corresponderá a su promedio.

El resultado obtenido, permite formular conclusiones acerca de funcionamiento del proceso evaluado, teniendo en cuenta que éste toma validez con la obtención de presentación de evidencias, que soporte los resultados de la encuesta.

Las pruebas de la aplicación de los formatos de cuestionario cuantitativo, se anexan en medio digital y almacenados en el CD adjunto en la carpeta de */Anexos/Cuestionarios /.*

Entrevistas preguntas abiertas y preguntas cerradas: técnica utilizada para la recolección de información amplia que permita aclarar dudas que dejan los cuestionarios. Los formatos utilizados para hacer las entrevistas están ajustados al personal del área de Sistemas, al personal técnico y en general a todo el personal involucrado en el personal del área de tecnologías de la Información y Comunicación.

Se realizan dos tipos de entrevistas:

Entrevistas con preguntas abiertas: donde la persona entrevistada pueda expresar libremente su respuesta, generando respuesta con detalles, permitiendo hacer más preguntas según vaya respondiendo cada una.

Entrevistas con preguntas cerradas: el entrevistado se limita a contestar Si o No, se recoge información útil para nuestra investigación, permitiendo en este formato adicionar la cantidad de algunos elementos y algunas observaciones.

El formato diseñado es el siguiente:

Formato3. Formato de entrevistas (FE)

<table>
<tr><td rowspan="4">  </td><td rowspan="4">FORMATO DE ENTREVISTAS</td><td colspan="3">REF. FE-[proceso]</td></tr>
<tr><td colspan="3">Noviembre 2015</td></tr>
<tr><td colspan="3">Versión 1.0</td></tr>
<tr><td colspan="3">Página 1 de 1</td></tr>
<tr><td>ENTIDAD AUDITADA</td><td colspan="4">E.S.E. HOSPITAL CUMBAL</td></tr>
<tr><td>PROCESO AUDITADO</td><td colspan="4">ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS</td></tr>
<tr><td>RESPONSABLE(S)</td><td colspan="4">MÓNICA YAQUELINE CAICEDO – HENRY FREDY IRUA TAIMAL</td></tr>
<tr><td>MATERIAL DE SOPORTE</td><td colspan="4">COBIT</td></tr>
<tr><td>DOMINIO</td><td>MONITOREAR Y EVALUAR (ME)</td><td>PROCESO</td><td colspan="2">ME4 Proporcionar Gobierno de TI</td></tr>
<tr><td>ENTREVISTADO</td><td colspan="4"></td></tr>
<tr><td>CARGO</td><td colspan="4"></td></tr>
<tr><td colspan="5">PREGUNTAS
1. ¿?
2. ¿?
3. ¿?...</td></tr>
<tr><td colspan="5">RESPUESTAS
_____
_____
…</td></tr>
<tr><td colspan="3" rowspan="2">FIRMA ENTREVISTADO:</td><td colspan="2">FIRMA AUDITOR:</td></tr>
<tr><td colspan="2">FECHA APLICACIÓN:</td></tr>
</table>

3.2.5 Matriz de probabilidad de ocurrencia e impacto

Fue creada para catalogar un riesgo y saber qué clase de daño puede causar un mal procedimiento en el proceso auditado. Existe la columna de probabilidad de ocurrencia donde se pondrá el valor del porcentaje de riesgo según su resultado, luego se deberá clasificar el impacto según la relevancia del proceso, esta clasificación será hecha por el equipo auditor basándose en el conocimiento de la entidad y del proceso auditado. Una vez hechos estos procedimientos se podrá clasificar el riesgo para su posterior entendimiento.

		IMPACTO		
		BAJO (LEVE)	MEDIO (MODERADO)	ALTO (CATASTROFICO)
PROBABILIDAD	ALTO 61-100%	ZONA DE RIESGO MODERADO	ZONA DE RIESGO IMPORTANTE	ZONA DE RIESGO INACEPTABLE
	MEDIO 31-60%	ZONA DE RIESGO TOLERABLE	ZONA DE RIESGO MODERADO	ZONA DE RIESGO IMPORTANTE
	BAJO 0-30%	ZONA DE RIESGO ACEPTABLE	ZONA DE RIESGO TOLERABLE	ZONA DE RIESGO MODERADO

Análisis y evaluación riesgos preliminares: este formato contiene la siguiente información de los hallazgos:

Formato 4. Descripción del formato de hallazgos.

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS		REF HLLGZ-[Proceso]
			Diciembre 2015
			Versión 1.0
ENTIDAD AUDITADA			
OBJETO DE ESTUDIO			
RESPONSABLES			
MATERIAL DE SOPORTE			
DOMINIO		**PROCESO**	
RIESGOS RELACIONADOS:			
HALLAZGO			
CONSECUENCIAS			
RECOMENDACIONES			

PROBABILIDAD E IMPACTO
EVIDENCIAS

A continuación, se describe los ítems que contiene el formato de hallazgos:

- ✓ **REF.** se refiere al ID del elemento.
- ✓ **Entidad auditada:** en este espacio se indica el nombre de la entidad a la cual se le está realizando el proceso de auditoría.
- ✓ **Proceso auditado:** en este espacio se indica el nombre del proceso objeto de la auditoría.
- ✓ **Responsables:** en este espacio se indican los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.
- ✓ **Material de soporte:** en este espacio se indica el nombre del material que soporta el proceso, para el caso será COBIT.
- ✓ **Dominio:** espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.
- ✓ **Proceso:** espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.
- ✓ **Hallazgo:** aquí se encuentra la descripción de cada hallazgo, así como la referencia al cuestionario cuantitativo que lo soporta.
- ✓ **Consecuencias y riesgos:** en este apartado se encuentra la descripción de las consecuencias del hallazgo, así como la cuantificación del riesgo encontrado.
- ✓ **Evidencias:** aquí encontramos en nombre de la evidencia y el número del anexo donde ésta se encuentra.
- ✓ **Recomendaciones:** en este último apartado se hace una descripción de las recomendaciones que el equipo auditor ha presentado a las entidades auditadas.

3.2.6 Valoración de riesgos

A continuación, se procede a listar cada uno de los riesgos identificados mediante la aplicación de los instrumentos de auditoría, donde se obtuvo el porcentaje de probabilidad del riesgo, catalogando cada proceso en Riesgo Bajo, Medio o Alto, y a continuación se valora el impacto que puede generar el riesgo identificado, según criterio del equipo auditor. Esto se realiza de acuerdo a la siguiente nomenclatura:

Probabilidad		**Impacto**	
Alta:	A	Catastrófico:	C
Media:	M	Moderado:	M
Baja:	B	Leve:	L

Cuadro 1. Valoración de los riesgos

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	VALORACIÓN DE LOS RIESGOS	**REF.** VAL-RSG Noviembre 2015 Versión 1.0

N°	**RIESGOS/VALORACIÓN**	**PROBABILIDAD**			**IMPACTO**			**DOMINIO**
		A	**M**	**B**	**L**	**M**	**C**	
R1	No existen procesos definidos ni documentado para el área de sistemas	**X**				**X**		PO4(1)
R2	No existe un manual de funciones para el área de sistemas	**X**				**X**		PO4(2)
R3	No existe un medidas para garantizar la seguridad de los recursos informáticos	**X**					**X**	PO4(3)
R4	No existen bitácoras para registrar las actividades que se desarrollan por el área de sistemas	**X**			**X**			PO4(4)
R5	No existe un perfil requerido para el personal del área de sistemas		**X**		**X**			PO7(1)
R6	No existe un proceso definido ni documentado para seleccionar el personal del área de sistemas		**X**		**X**			PO7(2)
R7	No existen políticas para fomentar capacitaciones para el personal del área de sistemas		**X**		**X**			PO7(3)
R8	No existe un proceso definido ni documentado para la inducción de los usuario finales que utilizan las aplicaciones (programas) de la institución	**X**				**X**		AI4(1)
R9	No existe una persona del área de sistemas encargada de brindar inducción a los usuarios finales para el manejo de las aplicaciones (programas) de la institución	**X**				**X**		AI4(2)
R10	No existe asesoría continua a los usuarios finales para mejorar el manejo de las aplicaciones o	**X**				**X**		AI4(3)

	programas de la institución.							
R11	No existen manuales de usuario para el manejo de las aplicación o programas de la institución	**X**				**X**		AI4(4)
R12	Con el fin de recuperar y dar continuidad al sistema existe únicamente copias del ejecutable del programa SaludIPS, mas no existe un proceso bien definido	**X**					**X**	DS4(1)
R13	Vulnerabilidad en el proceso de respaldo de energía, ya que no existe el proceso automatizado para el cambio de energía oportuno	**X**					**X**	DS4(2)
R14	No existe un plan de recuperación y continuidad de los servicios definidos el cual se pueda actualizar	**X**			**X**			DS4(3)
R15	No existe personal responsable ni entrenado para actuar en caso de un fallo critico	**X**					**X**	DS4(4)
R16	No existe un proceso definido, adecuado y documentado para la restauración y continuidad del servicio	**X**				**X**		DS4(5)
R17	No existe un proceso definido, adecuado y documentado para crear, comprobar y almacenar las copias de seguridad	**X**				**X**		DS4(6)
R18	No existen políticas de almacenamiento de copias de seguridad en sitio o fuera de sitio.	**X**			**X**			DS4(7)
R19	No existe un proceso para evaluar el plan de recuperación y continuidad de los servicios.	**X**				**X**		DS4(8)
R20	No existen políticas de seguridad informática que protejan los recursos informáticos de la empresa	**X**				**X**		DS5(1)
R21	No existe un proceso definido ni documentado para controlar el acceso de personal interno o externo hacia los recursos informáticos	**X**				**X**		DS5(2)

R22	No existe un proceso definido ni documentado para la solicitud, creación, aprobación y desactivación de cuentas de usuario para acceder al programa SaludIPS y otros	**X**				**X**		DS5(3)
R23	El jefe de facturación actualmente es quien crea las cuentas de usuario para ingresar a los módulos de Facturación e Historias Clínicas Sistematizada del aplicativo SaludIPS, de manera Ad-Hoc			**X**	**X**			DS5(4)
R24	No existe políticas para definir los privilegios o permisos dentro de los aplicativos de la institución			**X**	**X**			DS5(5)
R25	No existe un proceso para controlar el acceso no autorizado a la red de datos e identificar infiltraciones o intrusos	**X**					**X**	DS5(6)
R26	Los necesidades de los usuarios para el manejo de los recursos informáticos son atendidos por el jefe de facturación quien tiene conocimientos al respecto pero no le corresponde en sus funciones		**X**		**X**			DS7(1)
R27	No existe un proceso definido ni documentado, ni planificado para capacitación a los usuarios finales acerca del uso de los recursos informáticos		**X**		**X**			DS7(2)
R28	No existe una política para evaluar el desempeño de los usuarios finales frente al uso los recursos informáticos.		**X**			**X**		DS7(3)
R29	No existe un proceso definido ni documentado para la realización y verificación del inventario de activos informáticos	**X**				**X**		DS9(1)
R30	No existe un proceso definido ni documentado para obtener, verificar y almacenar la configuración de los recursos informáticos tales como hojas de	**X**				**X**		DS9(2)

	vida completamente diligenciadas							
R31	No existen políticas ni un proceso definido ni documentado para controlar y verificar la existencia de software personal instalado sin autorización	**X**					**X**	DS9(3)
R32	No existe políticas ni un proceso para definido elegir el formato, la creación, comprobación y eliminación de los medios de almacenamiento de las copias de seguridad de datos y aplicaciones	**X**					**X**	DS11(1)
R33	No existe un monitoreo permanente para verificar el correcto funcionamiento de los recursos informáticos que nos suministre datos históricos e incidentes con mayor frecuencia		**X**			**X**		DS13(1)
R34	No existe un proceso definido ni documentado para autorizar y registrar la salida de recursos informáticos que requieren mantenimiento correctivo externo.	**X**					**X**	DS13(2)
R35	No existen políticas para evaluar el desempeño del área de sistemas frente a las metas propuestas, además no ha sido requeridas por las directivas de la institución		**X**			**X**		ME1(1)
R36	No existen políticas para adoptar medidas correctivas con el fin de mejorar los indicadores con baja calificación	**X**				**X**		ME1(2)
R37	En el manual de funciones del área de sistemas no se contempla la normatividad vigente referente al uso de tecnologías de la información.	**X**			**X**			ME3(1)
R38	No se tiene conocimiento de los todos los informes que hay que presentar a los entes de control, únicamente existe requerimiento para Derechos de autor	**X**					**X**	ME3(2)
R39	No existen políticas para	**X**				**X**		ME4(1

	identificar, evaluar y priorizar las necesidades de recursos tecnológicos que se deban adquirir							)
R40	No existen políticas para evaluar y determinar el nivel de riesgo aceptable para los recursos informáticos, comparado con el nivel de riesgo actual.	**X**				**X**		ME4(2)
R41	No existe un proceso para el control de acceso al área al centro de datos,	**X**					**X**	DS2(1)
R42	No existe un proceso para garantizar la seguridad física de los activos de TI del centro de datos.	**X**					**X**	DS12(2)

3.2.7 Evaluación de matriz de probabilidad de ocurrencia

Una vez valorado el impacto de cada uno de los riesgos, se obtiene la matriz de probabilidad de ocurrencia, con los siguientes resultados:

Cuadro 2. Matriz de probabilidad de ocurrencia de los riesgos

		IMPACTO		
		BAJO (LEVE)	**MEDIO (MODERADO)**	**ALTO (CATASTROFICO)**
PROBABILIDAD	**ALTO 61-100%**	**ZONA DE RIESGO MODERADO** R4(PO4), R14(DS4), R18(DS4), R37(ME3)	**ZONA DE RIESGO IMPORTANTE** R1(PO4), R2(PO4), R8(AI4), R9(AI4), R10(AI4), R11(AI4), R16(DS4), R17(DS4), R19(DS4), R20(DS5), R21(DS5), R22(DS5), R29(DS9), R30(DS9), R36(ME1), R39(ME4), R40(ME4)	**ZONA DE RIESGO INACEPTABLE** R3(PO4), R12(DS4), R13(DS4), R15(DS4), R25(DS5), R31(DS9), R32(DS11), R34(DS13), R41(DS12), R42(DS12)
	MEDIO 31-60%	**ZONA DE RIESGO TOLERABLE** R5(PO5), R6(PO7), R7(PO7), R26(DS7), R27(DS7)	**ZONA DE RIESGO MODERADO** R28(DS7), R33(DS13), R35(ME1)	

	BAJO 0-30%	**ZONA DE RIESGO ACEPTABLE** R23(DS5), R24(DS5)		

3.2.8 Hallazgos

Los procesos evaluados para la identificación de hallazgos, fueron los siguientes:

Dominio: planear y organizar (PO)
- PO4. Definir los Procesos, Organización y Relaciones de TI.
- PO7 Administrar los Recursos Humanos de TI

Dominio: adquirir e implementar (AI)
- AI4 Facilitar la Operación de Uso

Dominio: entregar y dar soporte (DS)
- DS4 Garantizar Continuidad del Servicio
- DS5 Garantizar la Seguridad de los Sistema
- DS7 Educar y Entrenar a los Usuarios
- DS9 Administrar la Configuración
- DS11 Administración de Datos
- DS12 Administración del Ambiente Físico
- DS13 Administración de Operaciones

Dominio: monitorear y evaluar (ME)
- ME1 Monitorear y Evaluar el Desempeño de TI
- ME3 Garantizar el Cumplimiento con Requerimientos Externos
- ME4 Proporcionar Gobierno de TI

Hallazgos identificados en dominio planear y organizar (PO)

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS	**REF. HLLZG-PO4**
		Diciembre 2015
		Versión 1.0
ENTIDAD AUDITADA	E.S.E. HOSPITAL CUMBAL	
PROCESO AUDITADO	ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS	
RESPONSABLE(S)	MÓNICA YAQUELINE CAICEDO – HENRY FREDY IRUA TAIMAL	
MATERIAL DE	COBIT	

SOPORTE			
DOMINIO	PLANEAR Y ORGANIZAR (PO)	**PROCESO**	PO4 Definición de Procesos y Organización y relaciones de TI

RIESGOS RELACIONADOS: R1, R2, R3, R4

HALLAZGOS

1. No existen procesos definidos ni documentado para el área de sistemas
2. No existe un manual de funciones para el área de sistemas
3. No existe un medidas para garantizar la seguridad de los recursos informáticos
4. No existen bitácoras para registrar las actividades que se desarrollan por el área de sistemas

PROBABILIDAD E IMPACTO

Probabilidad de ocurrencia: 66.5%

Impacto según relevancia del proceso: ALTO

EVIDENCIAS

/Evidencias/Cuestionarios/CC-PO4CI.jpg,
/Evidencias/Cuestionarios/CC-PO4IS.jpg,
/Evidencias/Entrevistas/FE-PO4CI.jpg,
/Evidencias/Videos/VIDEO-CIFE-PO4-1.mp4,
/Evidencias/Videos/VIDEO-CIFE-PO4-2.mp4,
/Evidencias/Videos/VIDEO-CIFE-PO4-3.mp4
/Evidencias/Videos/VIDEO-CIFE-PO4-4.mp4
/Anexos/ANEXO1-MANUAL-DE-FUNCIONES.PDF,
/Anexos/ANEXO2-ORGANIGRAMA.PDF

CONSECUENCIAS

- Al no existir los procesos definidos ni documentados, para el área de sistemas, afecta el normal desempeño de la(s) persona(s) que deban realizar funciones propias de esta área, lo cual provoca que su trabajo sea desordenado, desorganizado, baja calidad, y por ende no garantice satisfacción al usuario. Así mismo, por no existir unos procesos definidos para al área, no existe su respectivo Manual de funciones.
- La falta de seguridad de los recursos informáticos, los expone a riesgos que se puedan presentar como robo, daño, perdida, incendios, terremotos, corte de energía, etc.
- La falta de registro de las actividades que se desarrollan por el área de sistemas no permiten evaluar o realizar los seguimientos del desempeño del área, ni conocer o cuantificar lo que se ha realizado en

un periodo de tiempo.
RECOMENDACIONES • Establecer los procesos y documentar los procesos para el área de sistemas, que deben estar bajo la responsabilidad del ingeniero encargado del área, y bajo la supervisión del jefe de control interno, enmarcados en las políticas del MECI. • Una vez definidos los procesos del área de sistemas, el jefe de control interno y coordinador de sistemas debe evaluar las funciones inherentes al proceso y organizarlas dentro de un manual de funciones. • Para evitar la ocurrencia de probables sucesos como robo, daño, perdida, incendios, terremotos, cortes de energía, etc., es necesario establecer políticas de seguridad informática, que contemple medidas de seguridad preventivas. • Se recomienda definir un formato, bitácora, histórico u hoja de vida donde se registre todas las actividades realizadas por el personal del área de sistemas, para medir su desempeño y tener un control de dichas actividades e identificar el estado de los recursos informáticos en algún tiempo determinado.

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS		**REF. HLLZG-PO7** Noviembre 2015 Versión 1.0
ENTIDAD AUDITADA	E.S.E. HOSPITAL CUMBAL		
PROCESO AUDITADO	ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS		
RESPONSABLE(S)	MÓNICA YAQUELINE CAICEDO – HENRY FREDY IRUA TAIMAL		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	PLANEAR Y ORGANIZAR (PO)	**PROCESO**	PO7 Administrarlos Recursos TI
RIESGOS RELACIONADOS: R6, R7			
HALLAZGOS 1. No existe un perfil definido y completo, que contemple varios niveles profesionales para el personal del área de sistemas, ya que solo existe el perfil de ingeniero de sistemas, y para la empresa existe la necesidad de más personal para cumplir con todas tareas solicitadas.			

2. Para elegir el personal del área de sistemas, no se está realizando un proceso de .selección adecuado y transparente para evaluar la mejor opción, sino que se escoge según otros intereses.
3. No existen políticas para fomentar capacitaciones para el personal del área de sistemas.

PROBABILIDAD E IMPACTO

Probabilidad de ocurrencia: 53.5%
Impacto según relevancia del proceso: MEDIO

EVIDENCIAS

/Evidencias/Cuestionarios/CC-PO7IS.JPG
/Evidencias/Cuestionarios/CC-PO7TH.JPG
/Evidencias/Entrevistas/FE-PO7TH.JPG
/Evidencias/Videos/VIDEOTH-FE-PO7.MP4
/Evidencias/Videos/VIDEOTH-FE-PO7-1.MP4

CONSECUENCIAS

- Si no hay un perfil que contemple varios niveles profesionales para el personal de sistemas, impide la posibilidad de vincular técnicos o tecnólogos, quienes podrían desempeñarse adecuadamente en la empresa, además por esta causa no se puede determinar las funciones propias para esta área.
- Al no existir un proceso definido ni documentado para la selección del personal del área de sistemas no se puede contratar al personal competente
- Si no existe políticas para fomentar las capacitaciones al personal de sistemas, no se puede potenciar sus capacidades las cuales podrían estar al beneficio de la empresa.

RECOMENDACIONES

- Elaborar un perfil para el personal de sistemas que sea inclusivo para los diferentes niveles profesionales en esta área, con el fin de contratar personal con capacidades especificas según las necesidades, por ejemplo, personal para el área de mantenimiento, redes, bases de datos, soportes a los demás usuarios.
- El jefe del área de talento humano, con asesoría del jefe de control interno deben definir un proceso debidamente documentado, para Recepcionar las hojas de vida de los aspirantes, y surtir un proceso de selección transparente, que evalué sus conocimientos y capacidades, que garantice la contratación del personal más idóneo.
- Fomentar capacitación al personal del área de sistemas, con el fin de

optimizar tiempo y recursos, para que pueda cumplir sus actividades de forma eficiente.

Hallazgos encontrados en el dominio adquirir e implementar (AI)

E.S.E. HOSPITAL Cumbal Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS		**REF. HLLZG-AI4** Noviembre 2015 Versión 1.0
ENTIDAD AUDITADA	E.S.E. HOSPITAL CUMBAL		
PROCESO AUDITADO	ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS		
RESPONSABLE(S)	MÓNICA YAQUELINE CAICEDO – HENRY FREDY IRUA TAIMAL		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	ADQUIRIR E IMPLEMENTAR (AI)	**PROCESO**	AI4 Facilitar la Operación del Uso
RIESGOS RELACIONADOS: R8, R9, R10, R11			
HALLAZGOS 1. No existe un proceso definido ni documentado para la inducción de los usuarios finales que utilizan las aplicaciones (programas) de la institución. 2. No existe una persona del área de sistemas encargada de brindar inducción a los usuarios finales para el manejo de las aplicaciones (programas) de la institución 3. No existe asesoría continua a los usuarios finales para mejorar el manejo de las aplicaciones o programas de la institución. 4. No existen manuales de usuario para el manejo de la aplicación o programas de la institución.			
PROBABILIDAD E IMPACTO **Probabilidad de ocurrencia:** 92.16% **Impacto según relevancia del proceso:** ALTO			
EVIDENCIAS /Evidencias/Cuestionarios/CC-AI4CM.JPG /Evidencias/Cuestionarios/CC-AI4AU.JPG /Evidencias/Cuestionarios/CC-AI4CA.JPG /Evidencias/Cuestionarios/CC-AI4IS.JPG			

/Evidencias/Cuestionarios/CC-AI4JU.JPG
/Evidencias/Cuestionarios/CC-AI4RF.JPG
/Evidencias/Videos/VIDEOIS-CC-AI4-1.MP4

CONSECUENCIAS

- Si no se cuenta con un proceso de inducción dirigido al nuevo personal quienes serán los usuarios finales de las aplicaciones que se encuentran implementadas en la institución y que para el caso del Hospital de Cumbal son los programas SaludIPS para facturación e historia clínica sistematizada, SisConfi (historial antes de 2011) y Compuconta para información contable y almacén, Sismed para información de medicamentos, entre otros, afectara notoriamente, ya que retrasa los procesos normales de cada área, y la calidad de los resultados estarán en duda, ya que se provocan errores o fallos al registrar información; algunos errores no serán tan graves, pero la probabilidad de que lo sean aumenta por esta causa.
- Si no existe el debido proceso de inducción para el manejo de las aplicaciones, es una razón por la cual no se define una persona que se encargue de esta labor y que lo ideal es sea una personal que haga parte del área de sistemas para quienes se facilita el manejo de los sistemas. Lo anterior, en consecuencia, se convierte en una debilidad para la empresa.
- El manejo de cierto tipo de programas, requiere de un conocimiento básico de sistemas, pero como es común, en la mayoría de empresas no se evalúa al nuevo personal en este aspecto, esto baja la calidad y el rendimiento en las actividades de la empresa.
- También afecta la inexistencia de los manuales de usuario, porque son otra alternativa de asesoría permanente para los usuarios finales, quienes pueden tener inconveniente para el uso de los programas en cualquier momento, en especial cuando sea imposible disponer de una persona directamente, por cuestión de horario o distancia al sitio del trabajador.
- Todo esto afecta para cumplir satisfactoriamente los objetivos de la empresa.

RECOMENDACIONES

- Lo ideal entonces, es que, al contratar el nuevo personal, se verifique y en lo posible se evalué sus conocimientos básicos en sistemas. Que se defina una persona que se responsabilice, levante y documente este proceso y cree el respectivo manual de usuario para que cada vez que se contrate a nuevo personal para las diferentes áreas, quienes serán

los usuarios finales, y según el área asignada tendrán que manejar software, dispongan de este material. Debe considerar que en el Hospital de Cumbal se usan principalmente los siguientes programas: en el área de facturación, SaludIPS módulo de facturación, en el área financiera y de almacén, Compuconta, en el área de farmacia, SaludIPS módulo de Kárdex, y especialmente para el personal asistencial (médicos, enfermeras, auxiliares de enfermería, odontólogos, higienistas) quienes usan SaludIPS el módulo de historias clínicas sistematizada. Facilitar el uso de las TI, es fundamental ya que aumenta el desempeño de la empresa, con el fin de obtener mejores resultados.

Hallazgos encontrados en el dominio entregar y dar soporte (DS).

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS		**REF. HLLZG-DS4**
			Noviembre 2015
			Versión 1.0
ENTIDAD AUDITADA	E.S.E. HOSPITAL CUMBAL		
PROCESO AUDITADO	ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS		
RESPONSABLE(S)	MÓNICA YAQUELINE CAICEDO – HENRY FREDY IRUA TAIMAL		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	ENTREGAR Y DAR SOPORTE (DS).	**PROCESO**	DS4 Garantizar la continuidad del servicio
RIESGOS RELACIONADOS: R12, R13, R14, R15, R16, R17, R18,R19			
HALLAZGOS 1. Con el fin de recuperar y dar continuidad al sistema existe únicamente copias del ejecutable del programa saludIPs, mas no existe un proceso bien definido 2. El Hospital Cumbal cuenta con dos plantas eléctricas de motor diésel, pero el proceso de respaldo de energía no es el recomendado, ya que no existe el proceso automático para el cambio de energía oportuno. 3. No existe un plan de recuperación y continuidad de los servicios definidos el cual se pueda actualizar. 4. No existe personal responsable ni entrenado para actuar en caso de un fallo crítico.			

5. No existe un proceso definido, adecuado y documentado para la restauración y continuidad del servicio.
6. No existe un proceso definido, adecuado y documentado para crear, comprobar y almacenar las copias de seguridad.
7. No existen políticas de almacenamiento de copias de seguridad en sitio o fuera de sitio.
8. No existe un proceso para evaluar el plan de recuperación y continuidad de los servicios.

PROBABILIDAD E IMPACTO

Probabilidad de ocurrencia: 75%

Impacto según relevancia del proceso: ALTO

EVIDENCIAS

/Evidencias/Cuestionarios/CC-DS4IS.JPG

CONSECUENCIAS

Considerando que el Hospital de Cumbal, no está exento de todo tipo de Riesgo, como daño, robo, incendios, sismo o terremoto, inundación, relámpagos, etc., y que la probabilidad de ocurrencia es latente, no contar con un proceso definido ni mucho menos documentado para recuperar y dar continuidad a los procesos de la empresa que estén basados en TI, es una situación crítica ya que los servicios del Hospital de Cumbal, actualmente se apoyan de las tecnologías de la información, convirtiéndose casi en imprescindible, ya que todo el registro de las historias clínicas de los pacientes están almacenados en el servidor principal de la empresa, donde se encuentra la base de datos y la aplicación SaludIPS que la gestiona.

Almacenar algunas copias del ejecutable del programa o de la base de datos o archivos de Excel, Word o Acces, y no disponer de un proceso definido pone en riesgo a la empresa, porque ante un fallo critico o evento catastrófico puede suceder que no funcionen o que no se puedan reinstalar, o que la base de datos haya perdido su integridad por un apagón, todo esto impide la continuidad en la prestación de los servicios médicos.

En el municipio de Cumbal los cortes de energía son constantes, lo cual pone en riesgo todos los dispositivos electrónicos, incluidos los recursos informáticos, al no contar con un sistema de respaldo de energía automático, aumenta la probabilidad de afectaciones como fuentes, boards o discos duros quemados, o hasta incluso daño o perdida la información almacenada.

En consecuencia, al no contar con un plan de recuperación y continuidad que

este actualizado, ni se define una o varias personas debidamente entrenadas para el proceso de creación, comprobación y almacenamiento de las copias de seguridad del sistema (que puede ser en sitio o fuera de sitio) o que deban poner en funcionamiento un sistema de restablecimiento de energía, o poner el funcionamiento todo el sistema de la empresa, bien sea, continuidad del servicio del talento humano o tecnológico como los sistemas o programas, incrementa la probabilidad de fallar al tratar de recuperar el sistema y darle continuidad, después de un eventual fallo critico o catástrofe.
RECOMENDACIONES Darle mayor importancia a los riesgos a los que está expuesto el Hospital de Cumbal como daño de software o hardware por mal manejo o cortes de energía, robo, incendios, sismo o terremoto, inundación, etc., ya que la probabilidad de ocurrencia es latente y se debe tomar las medidas necesarias para prevenir que se afecte su normal funcionamiento, o que sea interrumpido por tiempo prolongado, para lo cual es pertinente, de suma importancia y prontitud, definir el proceso, y la o las personas que deban responsabilizarse de esta situación, quienes actuaran inmediatamente frente a una fallo o incidente critico o catastrófico. El proceso debe ser documentado y debe contar con un Manual o Plan de Recuperación y Continuidad, que contemple como crear, comprobar y almacenar las copias de seguridad, respaldos o instaladores de las aplicaciones que existen en la institución, con las versiones más recientes de los programas SaludIPS, Compuconta, SisConfi con sus respectivas instrucciones de instalación. Para el manejo de las dos plantas eléctricas (provistas por motores diésel cada una) que dispone el Hospital Cumbal, se recomienda definir su manual de operaciones e implementar un sistema autónomo para el cambio de energía. También se recomienda definir un registro de los fallos críticos o incidentes presentados, con el fin de obtener estadísticas de los eventos más frecuentes y fortalecer medidas para prevenirlos. Finalmente, después de cada incidente o fallo crítico, se debe evaluar las acciones realizadas con el fin de identificar debilidades y mejorar este proceso.

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS	**REF. HLLZG-DS5**
		Noviembre 2015
		Versión 1.0
ENTIDAD AUDITADA	E.S.E. HOSPITAL CUMBAL	
PROCESO AUDITADO	ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS	
RESPONSABLE(S)	MÓNICA YAQUELINE CAICEDO – HENRY FREDY	

	IRUA TAIMAL		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	ENTREGAR Y DAR SOPORTE (DS)	**PROCESO**	DS5 Garantizar la seguridad de los sistemas
RIESGOS RELACIONADOS: R20, R21, R22, R23, R24, R25			
HALLAZGOS 1. No existen políticas de seguridad informática que protejan los recursos informáticos de la empresa. 2. No existe un proceso definido ni documentado para controlar el acceso de personal interno o externo hacia los recursos informáticos. 3. No existe un proceso definido ni documentado para la solicitud, creación, aprobación y desactivación de cuentas de usuario para acceder al programa SaludIPS y otros. 4. El jefe de facturación actualmente es quien crea las cuentas de usuario para ingresar a los módulos de Facturación e Historias Clínicas Sistematizada del aplicativo SaludIPS, de manera Ad-Hoc. 5. No existe políticas para definir los privilegios o permisos dentro de los aplicativos de la institución. 6. No existe un proceso para controlar el acceso no autorizado a la red de datos e identificar infiltraciones o intrusos.			
PROBABILIDAD E IMPACTO **Probabilidad de ocurrencia:** 60.6% **Impacto según relevancia del proceso:** ALTO			
EVIDENCIAS /Evidencias/Cuestionarios/CC-DS5-ATENCION-AL-USUARIO.JPG /Evidencias/Cuestionarios/CC-DS5-CONTROL-INTERNO.JPG /Evidencias/Cuestionarios/CC-DS5-COORDINADORA-CALIDAD.JPG /Evidencias/Cuestionarios/CC-DS5-COORDINADOR-ALMACEN.JPG /Evidencias/Cuestionarios/CC-DS5-COORDINADORA-MEDICA.JPG /Evidencias/Cuestionarios/CC-DS5-JEFE-URGENCIAS.JPG /Evidencias/Cuestionarios/CC-DS5-PAGADORA.JPG /Evidencias/Cuestionarios/CC-DS5-REGENTE-FARMACIA.JPG /Evidencias/Entrevistas/FE-DS5-ATENCION-AL-USUARIO.JPG /Evidencias/Entrevistas/FE-DS5-CONTROL-INTERNO.JPG /Evidencias/Entrevistas/FE-DS5-COORDINADORA-CALIDAD.JPG /Evidencias/Entrevistas/FE-DS5-COORDINADORA-MEDICA.JPG /Evidencias/Entrevistas/FE-DS5-INGENIERA-SISTEMAS.JPG			

/Evidencias/Entrevistas/FE-DS5-JEFE-URGENCIAS.JPG
/Evidencias/Entrevistas/FE-DS5-PAGADORA.JPG
/Evidencias/Entrevistas/FE-DS5-REGENTE-FARMACIA.JPG
/Evidencias/Videos/VIDEOAU-FE-DS5.mp4
/Evidencias/Videos/VIDEOAU-FE-DS51.mp4
/Evidencias/Videos/VIDEOAU-FE-DS52.mp4
/Evidencias/Videos/VIDEOCC-FE-DS51.mp4
/Evidencias/Videos/VIDEOCC-FE-DS52.mp4
/Evidencias/Videos/VIDEOCF-FE-DS51.mp4
/Evidencias/Videos/VIDEOCF-FE-DS52.mp4
/Evidencias/Videos/VIDEOCI-FE-DS52.mp4
/Evidencias/Videos/VIDEOCM-CC-DS5.mp4
/Evidencias/Videos/VIDEOCM-CC-DS51.mp4
/Evidencias/Videos/VIDEOCM-CC-DS52.mp4
/Evidencias/Videos/VIDEOCM-FE-DS51.mp4
/Evidencias/Videos/VIDEOCM-FE-DS52.mp4
/Evidencias/Videos/VIDEOCM-FE-DS52.mp4
/Evidencias/Videos/VIDEOIS-FE-DS5.mp4
/Evidencias/Videos/VIDEOIS-FE-DS51.mp4
/Evidencias/Videos/VIDEOIS-FE-DS52.mp4
/Evidencias/Videos/VIDEOIS-FE-DS53.mp4
/Evidencias/Videos/VIDEOIS-FE-DS54.mp4
/Evidencias/Videos/VIDEOIS-FE-DS55.mp4
/Evidencias/Videos/VIDEOIS-FE-DS56.mp4
/Evidencias/Videos/VIDEOJU-FE-DS51.mp4
/Evidencias/Videos/VIDEOJU-FE-DS52.mp4
/Evidencias/Videos/VIDEOJU-FE-DS53.mp4
/Evidencias/Videos/VIDEOP-FE-DS51.mp4
/Evidencias/Videos/VIDEOP-FE-DS52.mp4
/Evidencias/Fotografias/camara1-consulta externa.jpg
/Evidencias/Fotografias/camara2-urgencias.jpg

CONSECUENCIAS

Al no existir políticas de seguridad que protejan los recursos informáticos de la empresa, estos recursos son vulnerables a pérdidas o daños, mucho más, si no se controla el acceso del personal interno o externo. Además, la ausencia de técnicas de control de acceso, como cámaras de seguridad o registro de entrada y salida de la institución, después de un daño o robo, hace imposible la identificación y seguimiento de los responsables del hecho. No controlar las cuentas de usuario, de los programas del Hospital Cumbal, como SaludIPS,

Compuconta, SisConfi o Sismed principalmente, puede ser muy riesgoso, porque quedan expuestos a posibles casos suplantación de identidad o acceso no autorizado, por ejemplo, personal que ya fue despedido de la institución y aún está activa su cuenta de usuario, puede acceder al sistema y alterar datos. Que el jefe de facturación actualmente sea quien cree las cuentas de usuario para ingresar a los módulos de Facturación e Historias Clínicas Sistematizada del aplicativo SaludIPS, lo cual no es lo recomendable, ya que al presentarse algún inconveniente grave puede ser responsabilizado injustamente ya que no son funciones propias de su cargo

Si no existe políticas para definir los privilegios o permisos de los usuarios para el manejo de los aplicativos de la institución, permite que se pueda ingresar voluntaria o involuntariamente a módulos no autorizados o que no son los pertinentes según el cargo de la persona, y registrar información equívocamente.

Si no hay control de acceso a la red, se pueden fácilmente presentar infiltraciones al sistema, o intrusos que pueden consultar, modificar o eliminar información, sin ninguna autorización, como también saturar la red y volver lento el sistema.

RECOMENDACIONES

Se recomienda al gerente del Hospital de Cumbal, adoptar políticas de seguridad informática, que eviten o minimicen el riesgo de posibles daños o robos de recursos informáticos, consulta, modificación, copia o eliminación de información propia y reservada de la empresa, las cuales deben contemplar medidas de seguridad física, como es controlar y vigilar el ingreso a la institución de usuarios internos y externos, mediante la implementación de un sistema de televisión cerrada, que cuente con las suficientes cámaras para cubrir toda las áreas, y que sean de apoyo al personal de seguridad (celadores). Que todas las oficinas cuenten con cerraduras apropiadas para proteger los equipos de cómputo de posibles daños o robos, y en lo posible asegurados todas sus partes al escritorio y que cada CPU tenga un candado que impida abrirla. El acceso al centro de datos debe ser restringido y únicamente se debe permitir al personal autorizado, porque allí se encuentra el servidor principal, UPS, rack y switches que concentran el cableado de la red de datos.

En cuanto a cuentas de usuario y privilegios se debe definir y documentar un proceso, y asignar una persona que se responsabilice de administrar todas las cuentas de usuario, que atienda las solicitudes para la creación de nuevas cuentas, modifique privilegios y desactive cuando sea necesario. Los privilegios de las cuentas de usuario deben asignarse acorde a las funciones

de cada usuario., para lo cual debe asesorarse de los jefes de área. Dentro de este proceso debe llevar un registro de todas las cuentas existentes y las novedades de cada una, con el fin de conocer cuántas y cuales están activas o inactivas. Con respecto a la red de datos, se recomienda evaluar si cumple con la norma y los estándares, específicamente EIA/TIA 568A o EIA/TIA 568B, definir su clasificación según el área de cobertura y la tecnología que usa, verificar si cuenta con el respectivo diseño y subneting adecuado. Además, se debe examinar periódicamente el tráfico de información que circula en la red, utilizando técnicas o herramientas como *WIRESHARK* o *ADVANCED IP SCANNER* para detectar equipos conectados a red, entre otros. De esta manera se previene de posibles ataques por la red. También, verificar se maneje un buen sistema de cifrado y descifrado en la clave de red wifi, que no existan claves con estándar WEP (Wired Equivalent Privacy – Protocolo de Equivalencia con red cableada) que ya no son seguras, y que se maneje un estándar con un buen nivel de encriptación, por ejemplo, WPA2 (WIFI Protec Acces).

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS		**REF. HLLZG-DS7**
			Noviembre 2015
			Versión 1.0
ENTIDAD AUDITADA	E.S.E. HOSPITAL CUMBAL		
PROCESO AUDITADO	ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS		
RESPONSABLE(S)	MÓNICA YAQUELINE CAICEDO – HENRY FREDY IRUA TAIMAL		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	ENTREGAR Y DAR SOPORTE (DS)	**PROCESO**	DS7 Educar y Entrenar a los Usuarios
RIESGOS RELACIONADOS: R26, R27, R28			
HALLAZGOS 1. Las necesidades de los usuarios para el manejo de los recursos informáticos son atendidos por el jefe de facturación quien tiene conocimientos al respecto pero no le corresponde en sus funciones. 2. No existe un proceso definido ni documentado, ni planificado para capacitación a los usuarios finales acerca del uso de los recursos informáticos. 3. No existe una política para evaluar el desempeño de los usuarios finales			

frente al uso los recursos informáticos.

PROBABILIDAD E IMPACTO

Probabilidad de ocurrencia: 84,5%

Impacto según relevancia del proceso: ALTO

EVIDENCIAS

/Evidencias/Cuestionarios/CC-DS7-ATENCION-AL-USUARIO.jpg
/Evidencias/Cuestionarios/CC-DS7-COORDINADORA-MEDICA.jpg
/Evidencias/Cuestionarios/CC-DS7-INGENIERA-SISTEMAS.jpg
/Evidencias/Cuestionarios/CC-DS7-PAGADORA.jpg

CONSECUENCIAS

No contar con una política definida ni documentada para educar, capacitar y evaluar a los usuarios afecta directamente al Hospital Cumbal, sobre todo, porque su principal actividad es la prestación de servicios de salud los cuales están enfocados hacia los pacientes, quienes requieren atención oportuna, humana y eficiente, por tal motivo, si un trabajador no está suficientemente preparado y actualizado para el uso de los recursos tecnológicos por lo general trabajadores de mayor edad, no podrán afrontar o solventar situaciones que puedan ser solucionadas mediante el uso de las tecnologías de la información, por ejemplo, uso del teclado, manejo de un correo electrónico, escaneo de un documento, configuración de una impresora, encendido de un computador, registro de datos equivocadamente, etc., lo cual retarda y baja la calidad de la prestación del servicio. Que las necesidades de los usuarios para el manejo de los recursos informáticos sean atendidas por el jefe de facturación quien tiene conocimientos al respecto, afecta a la institución porque le demanda tiempo que debe dedicarlos a funciones propias de su cargo, retardando la presentación de las cuentas de cobro a las EPS.

RECOMENDACIONES

Teniendo en cuenta que la tecnología avanza con rapidez, implica que todo el personal que deba usarla, debe estar al actualizado, para lo cual el Hospital Cumbal puede apoyar brindando educación y capacitación al respecto. Entonces se recomienda definir y documentar políticas y proceso de Educación y Capacitación para el uso de tecnologías de la información. Debe definir una persona encargada de esta función, quien socializara y ejecutara un cronograma de capacitación. Esta persona debe ser recomendablemente del área de sistemas.

Los temas que se deben tratar son: Manejo y seguridad de Internet, adecuado uso de redes sociales, conceptos básicos de spyware, malware, scareware; importancia y manejo de antivirus, definición de contraseñas seguras las

cuales deben ser "***fáciles de recordar, y difíciles de adivinar",*** que garanticen confidencialidad y reserva de información (especialmente de historia clínica sistematizada), uso adecuado de cuentas de correo electrónico, cursos virtuales, configuración básica de impresoras, seguridad en Windows.

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS		**REF. HLLZG-DS9**
			Noviembre 2015
			Versión 1.0
ENTIDAD AUDITADA	E.S.E. HOSPITAL CUMBAL		
PROCESO AUDITADO	ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS		
RESPONSABLE(S)	MÓNICA YAQUELINE CAICEDO – HENRY FREDY IRUA TAIMAL		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	ENTREGAR Y DAR SOPORTE (DS)	**PROCESO**	DS9 Administrar la configuración
RIESGOS RELACIONADOS: R29, R30, R31			
HALLAZGOS No existe un proceso definido ni documentado para la realización y verificación del inventario de activos informáticos correctamente. No existe un proceso definido ni documentado para obtener, verificar y almacenar la configuración de los recursos informáticos tales como hojas de vida completamente diligenciadas. No existen políticas ni un proceso definido ni documentado para controlar y verificar la existencia de software personal instalado sin autorización.			
PROBABILIDAD E IMPACTO **Probabilidad de ocurrencia:** 72% **Impacto según relevancia del proceso:** ALTO			
EVIDENCIAS /Evidencias/Cuestionarios/CC-DS9-INGENIERA-SISTEMAS.jpg /Anexo 2. INVENTARIO-EQUIPOS-DE-COMPUTO.xlsx			
CONSECUENCIAS			

La deficiencia en el manejo del inventario de los activos informáticos, afecta económicamente al Hospital de Cumbal, porque puede propiciar o facilitar la pérdida de recursos informáticos, ya que no hay registros actualizados de los equipos de cómputo que constan de pantallas, teclados, mouse, CPU y sus componentes internos, impresoras, servidores, rack, switches, etc. No tener un inventario de activos informáticos actualizado también impide determinar la persona responsable de su uso. Así mismo, impide verificar y comprobar la configuración según la hoja de vida de cada recurso tecnológico. No se puede obtener información histórica de adquisición de equipos de cómputo, ni el desempeño durante su vida útil. No se puede determinar cuáles son los daños más frecuentes y los repuestos más requeridos.

Si no existe políticas ni un proceso definido ni documentado para controlar y verificar periódicamente la existencia de software personal instalado sin autorización, aumenta el riesgo de saturar el computador de aplicaciones innecesarias, disminuyendo el rendimiento para las funciones para el cual está destinado, se puede instalar software de dudosa reputación que contengan virus peligrosos para el sistema.

RECOMENDACIONES

Uno de los primeros pasos que se debe realizar es un inventario de los activos para reconocerlos e identificarlos dentro de la organización. En este inventario hay que clasificar y obtener toda la información posible como, por ejemplo, tipo de activo (equipo de cómputo, impresora, dispositivo de red, servidor, teléfono VoIP) valor, factura de venta, garantía acta de entrega, proveedor, localización dentro de la empresa, responsable a quien se asigna, configuración y drivers instalados.

Se recomienda tener en cuenta el SGSI (Sistema General de Seguridad de la Información) de ISO-27001, que propone que para cada activo, se debe establecer un propietario que defina el grado de seguridad que hay que aplicarle al mismo, aunque no necesariamente será la persona que gestione el día a día del mismo. [16]

El inventario de activos informáticos debe estar en conocimiento, dirección y supervisión del jefe del área de sistemas.

Para controlar la instalación de software, control de acceso al sistema operativo (SO) y mejorar las políticas de seguridad lógica se recomienda implementar el servicio de DIRECTORIO ACTIVO, SERVICIOS DE DNS en el servidor, bajo el sistema operativo de Windows Server 2012 (instalado actualmente), donde se configure un Dominio (bosque) denominado HOSPITALCUMBAL, en el cual se crea UNIDADES ORGANIZATIVAS por

cada área, con sus respectivos USUARIOS. Además configurar servicios de SERVIDOR DHCP, donde se define los ámbitos de trabajo de cada unidad organizativa, donde se configura la subneting adecuada que se diseñe.

Anexo3. Tutorial de configuración desarrollado en el módulo de Sistema Operativos, Diplomado de auditoría y Seguridad Informática, dictado por el Ing. Edgar Dulce.

[16] https://www.isotools.orgdel /2014/08/19/iso-27001-activos-informacion-empresa-3/

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS		**REF. HLLZG-DS11**
			Noviembre 2015
			Versión 1.0
ENTIDAD AUDITADA	E.S.E. HOSPITAL CUMBAL		
PROCESO AUDITADO	ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS		
RESPONSABLE(S)	MÓNICA YAQUELINE CAICEDO – HENRY FREDY IRUA TAIMAL		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	ENTREGAR Y DAR SOPORTE (DS)	**PROCESO**	DS11 Administración de datos.
RIESGOS RELACIONADOS: R32			
HALLAZGOS No existe políticas ni un proceso definido para elegir el formato, creación, comprobación y eliminación de los medios de almacenamiento de las copias de seguridad de datos y aplicaciones.			
PROBABILIDAD E IMPACTO **Probabilidad de ocurrencia:** 100% **Impacto según relevancia del proceso:** ALTO			
EVIDENCIAS /Evidencias/Cuestionarios/CC-DS11-INGENIERA-SISTEMAS.jpg			
CONSECUENCIAS No disponer de copias de seguridad que cumplan con los criterios disponibilidad e integridad, puede aumentar el riesgo de que no funcionen correctamente y que frente a eventualidad que requiera restaurar una copia de			

seguridad, ésta no funcione y no se pueda disponer de la información requerida.
RECOMENDACIONES Definir y documentar el proceso de Respaldo o copias de seguridad de los datos (backups), que garantice la disponibilidad e integridad de la información, para lo cual se debe implementar un proceso que en lo posible genere automáticamente lo archivos de backups en las frecuencia, fecha y hora más conveniente, y que exista una persona responsable de comprobar si funcionan correctamente, luego rotula con los siguientes datos: contenido, fecha y hora de creación, responsable y resultado de la comprobación, se define su formato o medio de almacenamiento como disco duro interno, disco duro externo, USB, CD, DVD y finalmente se transfiere a su lugar de almacenamiento, el cual debe garantizar su seguridad y conservación, bien sea en sitio o fuera de sitio acorde a las políticas de seguridad informática adoptadas. Además se debe definir la frecuencia y criterios para eliminar algunos medios que ya no sean necesarios.

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS		**REF. HLLZG-DS12**
			Noviembre 2015
			Versión 1.0
ENTIDAD AUDITADA	E.S.E. HOSPITAL CUMBAL		
PROCESO AUDITADO	ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS		
RESPONSABLE(S)	MÓNICA YAQUELINE CAICEDO – HENRY FREDY IRUA TAIMAL		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	ENTREGAR Y DAR SOPORTE (DS)	**PROCESO**	DS12 Administración del Ambiente Físico
RIESGOS ASOCIADOS:			
HALLAZGOS 1. No existe un proceso para el control de acceso al área al centro de datos, 2. No existe un proceso para garantizar la seguridad física de los activos de TI.			
PROBABILIDAD E IMPACTO **Probabilidad de ocurrencia:** 100%			

Impacto según relevancia del proceso: ALTO
EVIDENCIAS /Evidencias/Cuestionarios/CC-DS12-INGENIERA-SISTEMAS.JPG /Evidencias/Fotografias/centro-de-datos-servidor1.JPG /Evidencias/Fotografias/centro-de-datos-servidor2.JPG /Evidencias/Fotografias/centro-de-datos-UPS.JPG /Evidencias/Fotografias/centro-de-datos-switch-D-LINK.JPG /Evidencias/Fotografias/centro-de-datos-switch-HP.JPG /Evidencias/Fotografias/centro-de-datos-switch-CISCO.JPG /Evidencias/Fotografias/centro-de-datos-rack.JPG /Evidencias/Fotografias/centro-de-datos-techo.JPG
CONSECUENCIAS Si no existe un proceso definido para el control de acceso al área del centro de datos, no se garantiza la seguridad física de sus activos de TI, que los proteja contra daño mal intencionado o robo. Es importante considerar que allí se concentra todo el cableado de la red de datos, en un rack, que cuenta con 3 switchs, así, uno de marca D-LINK, otro HP y otro CISCO, cada uno de 24 puertos, se encuentra un servidor LENOVO Think Pad, un servidor HP ML-220, una UPS de 3000 Kw, que se consideran como los recursos informáticos más costosos y de más alto valor para la empresa, ya que contienen la base de datos principal de historia clínica sistematizada, Kárdex de farmacia, facturación, Res, 4505, Contabilidad, con sus respectivas aplicaciones de administración.
RECOMENDACIONES Se recomienda que el director del área de sistemas evalué las condiciones físicas del centro de datos y si cumple con los requerimientos mínimos según el estándar TIA942 de 2005, ya que, al diseñar los centros de datos conforme a la norma, se obtienen ventajas fundamentales, como son: Nomenclatura estándar, Funcionamiento a prueba de fallos, Aumento de la protección frente a agentes externos, y Fiabilidad a largo plazo, mayores capacidades de expansión y escalabilidad.[17] Se recomienda usar cámaras de seguridad, cerraduras de acceso y permiso de ingreso restringido. _____ [17] http://www.c3comunicaciones.es/data-center-el-estandar-tia-942/

E.S.E. HOSPITAL Cumbal Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS		**REF. HLLZG-DS13**
			Noviembre 2015
			Versión 1.0
ENTIDAD AUDITADA	E.S.E. HOSPITAL CUMBAL		
PROCESO AUDITADO	ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS		
RESPONSABLE(S)	MÓNICA YAQUELINE CAICEDO – HENRY FREDY IRUA TAIMAL		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	ENTREGAR Y DAR SOPORTE (DS)	**PROCESO**	DS13 Administración de operaciones.
RIESGOS RELACIONADOS: R33, R34			

HALLAZGOS

1. No existe un monitoreo permanente (mantenimiento) para verificar el correcto funcionamiento de los recursos informáticos que nos suministre datos históricos e incidentes con mayor frecuencia. Tampoco existe el lugar apropiado para realizar esta labor.

2. No existe un proceso definido ni documentado para autorizar y registrar la salida de recursos informáticos que requieren mantenimiento correctivo externo.

PROBABILIDAD E IMPACTO

Probabilidad de ocurrencia: 50%

Impacto según relevancia del proceso: MEDIO

EVIDENCIAS

/Evidencias/Cuestionarios/CC-DS13-INGENIERA-DE-SISTEMAS.jpg

CONSECUENCIAS

Si no existe un monitoreo permanente para verificar el correcto funcionamiento de los recursos informáticos, se puede presentar un desconocimiento de la situación actual de la empresa en cuanto al estado de los recursos informáticos, y los daños o fallas se vuelven comunes, porque no se previó su ocurrencia, derivando en gastos adiciones para el Hospital Cumbal. También provoca el retraso en las funciones de la persona que tiene a cargo el recurso informático averiado, siendo más grave si implica la atención de usuarios externos, considerando como críticos las áreas de atención al usuario, manejo de historia clínica sistematizada por

parte del personal asistencial, farmacia y pagaduría.

Si no se controla la salida de los recursos informáticos, cuando requieren controles correctivos, puede causar la demora o pérdida, sin que alguien se responsabilice.

RECOMENDACIONES

Se recomienda definir y documentar un proceso que contemple las actividades de mantenimiento de los recursos informáticos, con el fin de prever y evitar posibles fallos. El mantenimiento debe ser de tipo preventivo, el cual nos puede evitar que tengamos que realizar el mantenimiento correctivo muchas veces. La frecuencia que se recomienda es trimestral. Se debe especificar la persona del área de sistemas que se responsabilice de esta función y el lugar adecuado, y debe realizar la programación (cronograma) para atender a todas las dependencias, el cual debe ser socializado previamente para notificar a las personas que tienen a su cargo recursos informáticos y coordinar la fecha y hora para este proceso. Es recomendable que el área de sistemas disponga de las herramientas adecuadas, básicamente un juego de destornilladores, pulsera antiestática, brocha suave, sopladora, trozos de tela secos y limpios, alcohol isopropílico, silicona, grasa disipadora de calor para el procesador y lubricante para ventiladores (coolers). El mantenimiento preventivo debe enfocarse en dos aspectos, hardware y software. Para el hardware, suspender el suministro de energía y realizar limpieza del *CASE* externa e internamente para retirar todo el polvo que se acumula, limpiar los ventiladores para evitar que se bloquee la ventilación y prevenir un fallo grave en el procesador por sobrecalentamiento, por ultimo revisar todo se encuentre bien conectado. Para el software se debe realizar las siguientes tareas: desfragmentar el disco duro, hacer respaldo de los datos almacenados, instalar actualización de seguridad del SO, mantener las aplicaciones actualizadas, verificar si existe instalado software de dudosa procedencia, escanear el sistema y eliminar datos de navegación, archivos temporales, y los que sean innecesarios, vaciar la papelera de reciclaje, verificar el consumo de recursos y evaluar que aplicaciones deben iniciar con el sistema y remover los que no se necesiten.[18]

El mantenimiento correctivo se realiza cuando algo falla, si el fallo es de software, comúnmente se utiliza antivirus para solucionarlo, se verifica los drivers, se libera espacio, se realiza actualizaciones de los programas. Si el fallo es de hardware se presentan señales como pantallazos azules, mensajes de pánico del núcleo (kernel panic), bloqueos repentinos o continuos, sonidos extraños, el ordenador se apaga solo o ya no prende. En el peor de los casos, se tiene que formatear el disco duro y reinstalar el SO, si falla algún componente se puede corregir al reemplazarlo, pero en

algunos casos se puede echar a perder el equipo. Lo recomendable para el mantenimiento correctivo es buscar ayuda con personal especializado, el cual generalmente es externo. Finalmente, el área de sistemas debe definir los formularios necesarios para registrar todas las actividades que se realicen con los recursos informáticos, para lo cual debe elaborar una carpeta por cada uno. Los formatos relacionados son los siguientes: hoja de vida, acta de entrega al funcionario responsable, formato de mantenimiento preventivo, formato de mantenimiento correctivo, reporte de servicio externo para mantenimiento correctivo, dictamen técnico para baja de recurso informático.

Por lo anterior, se debe fortalecer la cultura de cuidar los recursos informáticos a los usuarios internos del hospital Cumbal, especialmente los que están a su cargo, y así garantizar que los ordenadores se mantengan más tiempo funcionando satisfactoriamente (vida útil).

_____

[18] http://hipertextual.com/archivo/2014/02/mantenimiento-preventivo-correctivo-pc/

Hallazgos encontrados en el dominio monitorear y evaluar

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS		**REF. HLLZG-ME1**
			Noviembre 2015
			Versión 1.0
ENTIDAD AUDITADA	E.S.E. HOSPITAL CUMBAL		
PROCESO AUDITADO	ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS		
RESPONSABLE(S)	MÓNICA YAQUELINE CAICEDO – HENRY FREDY IRUA TAIMAL		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	MONITOREAR Y EVALUAR (ME)	**PROCESO**	ME1 Monitorear y Evaluar Desempeño de TI
RIESGOS ASOCIADOS: R35, R36			
HALLAZGOS 1. No existen políticas para evaluar el desempeño del área de sistemas frente a las metas propuestas, además no ha sido requeridas por las directivas de			

la institución 2. No existen políticas para adoptar medidas correctivas con el fin de mejorar los indicadores con baja calificación
PROBABILIDAD E IMPACTO **Probabilidad de ocurrencia:** 100% **Impacto según relevancia del proceso:** ALTO
EVIDENCIAS /Evidencias/Cuestionarios/CC-ME1-CONTROL-INTERNO.jpg /Evidencias/Cuestionarios/CC-ME1-INGENIERA-SISTEMAS.jpg /Evidencias/Videos/VIDEOCI-FE-ME11.jpg /Evidencias/Videos/VIDEOCI-FE-ME12.jpg /Evidencias/Videos/VIDEOCI-FE-ME13.jpg /Evidencias/Entrevista/FE-ME1-CONTROL-INTERNO.jpg
CONSECUENCIAS Si no existe políticas para evaluar el desempeño del área de sistemas, no se puede determinar si su desempeño está influyendo positiva o negativamente en el Hospital Cumbal, desconociendo información que puede ser vital para la toma de decisiones estratégicas de la dirección. No se puede saber si el personal del área de sistemas está cumpliendo a cabalidad con sus funciones y metas propuestas.
RECOMENDACIONES Con el fin de conocer el impacto del área de sistemas en el Hospital Cumbal, se recomienda que se determinen unos indicadores que apliquen para esta área, y se pueda medir el desempeño global como área e individual por integrante. Esto favorece a la empresa, ya que si se conoce las debilidades, se puede aprovechar las fortalezas existentes y mitigar con mayor eficiencia las vulnerabilidades, amenazas y riesgos informáticos.

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS	**REF. HLLZG-ME3**
		Noviembre 2015
		Versión 1.0
ENTIDAD AUDITADA	E.S.E. HOSPITAL CUMBAL	
PROCESO AUDITADO	ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS	
RESPONSABLE(S)	MÓNICA YAQUELINE CAICEDO – HENRY FREDY IRUA TAIMAL	
MATERIAL DE	COBIT	

SOPORTE			
DOMINIO	MONITOREAR Y EVALUAR (ME)	**PROCESO**	ME3 Garantizar el Cumplimiento de los Requerimientos Externos

RIESGOS RELACIONADOS: R37

HALLAZGOS

1. No existe el manual de funciones del área de sistemas, por tanto, no se contempla la normatividad vigente referente al uso de tecnologías de la información.
2. No se tiene conocimiento de los todos los informes que hay que presentar a los entes de control, únicamente existe requerimiento para Derechos de autor

PROBABILIDAD E IMPACTO

Probabilidad de ocurrencia: 86%

Impacto según relevancia del proceso: ALTO

EVIDENCIAS

/Evidencias/Cuestionarios/CC-ME3-CONTROL-INTERNO.jpg
/Evidencias/Cuestionarios/CC-ME3-INGENIERA-SISTEMAS.jpg
/Evidencias/Entrevistas/FE-ME3-CONTROL-INTERNO.jpg

CONSECUENCIAS

No existir el manual de funciones del área de sistemas, además de desconocer las funciones del personal del área de sistemas, acarrea como consecuencia el desconocimiento de la normatividad, siendo perjudicial para la empresa, ya que se puede incurrir en acciones indebidas con el manejo de información que puede ser reservada de la empresa, o privada de los pacientes. Otra consecuencia de desconocer la norma, es que se pase por alto la adquisición de licencias para los sistemas operativos instalados, paquetes ofimáticos, servidor, considerando que en los computadores del Hospital de Cumbal se tiene instalado en su mayoría S.O. Windows7 y versiones de Office 2010 y 2013, y el servidor tiene instalado Windows Server 2012.

RECOMENDACIONES

Definir políticas para el conocimiento de la normatividad informática, la cual debe estar obligatoriamente contemplada en los procesos propios del área de sistemas. En Colombia se encuentra en vigente la Ley 1273 de 2009 LEY DE DELITOS INFORMATICOS, que modifica el código penal y crea un nuevo bien jurídico tutelado, denominado “DE LA PROTECCION DE LA INFORMACION Y DE LOS DATOS”, que tiene relación integral con los sistemas que utilicen

tecnologías de la información y las comunicaciones. Trata de evitar posibles atentados contra la confidencialidad, la integridad y la disponibilidad de los datos de los sistemas informáticos, de los siguientes amenazas: Acceso abusivo a un sistema informático, obstaculización ilegitima de sistema informático o red de telecomunicaciones, interceptación de datos informáticos, daños informáticos, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales, además de establecer la circunstancias de agravación punitiva.[19]

A partir del año 2011 se encuentra en discusión el proyecto de Ley 241 de 2011, conocida como LEY LLERAS, por la cual se regula la responsabilidad por las infracciones de derecho de autor y los derechos conexos a internet.

De orden internacional se adelanta desde el año 2013 la propuesta legislativa de ARMONIZACION DEL DERECHO INFORMATICO EN AMERICA LATINA, propuesta por el Dr. Manuel José Cárdenas.

Existe también el proyecto de Ley H.R.3261 de 2011, planteado en E.E.U.U. ACTO DE CESE DE PIRATERIA EN LINEA, que busca aumentar las capacidades de la ley estadounidense prevenir el tráfico de contenidos con derecho de autor, pero que a la vez tiene un gran número de opositores por considerarla contraproducente contra el derecho a la libertad de expresión. [20]

En Colombia, la Unidad Administrativa Especial del Ministerio de Interior, a través de su oficina de Dirección Nacional de Derecho de Autor, tiene por objetivo de contribuir a los fines del Estado Colombiano mediante el diseño, dirección, administración y ejecución de políticas gubernamentales en materia de derechos de autor y derechos conexos, funciones asignadas mediante el Decreto 2041 de 1991. [21]

Existen también, el Decreto 1747 de 11 de septiembre de 2000, Resolución 36904 de 2001, las cuales regulan en materia de certificados y firmas digitales, que es otro aspecto que también tiene que ver con el Hospital de Cumbal, para el reporte de información a entes de control que exigen la autenticidad e integridad de la información. [22]

_____

[19] Ley 1273, Ministerio de Interior y Justicia de la Republica de Colombia. 2009.
[20] http://www.colombiadigital.net/opinion/columnistas/cultura-mas/item/1580-legislaci%C3%B3n-inform%C3%A1tica-en-colombia-ley-lleras-y-tlc.html
[21] http://derechodeautor.gov.co/objetivos-y-funciones
[22] http://datateca.unad.edu.co/contenidos/233005/contenido%20en%20linea%20PELSI_I_2013/leccin_30_legislacin_en_seguridad_informtica_en_colombia.html

HOSPITAL Cumbal E.S.E. Construyendo una Comunidad Sana	FORMATO DE HALLAZGOS		**REF. HLLZG-ME4**
			Noviembre 2015
			Versión 1.0
ENTIDAD AUDITADA	E.S.E. HOSPITAL CUMBAL		
PROCESO AUDITADO	ESTRUCTURA ORGANIZACIONAL Y A LOS PROCESOS DEL AREA DE SISTEMAS		
RESPONSABLE(S)	MÓNICA YAQUELINE CAICEDO – HENRY FREDY IRUA TAIMAL		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	MONITOREAR Y EVALUAR (ME)	**PROCESO**	ME4 Proporcionar Gobierno de TI

RIESGOS RELACIONADOS: R39, R40

HALLAZGOS

1. No existen políticas para identificar, evaluar y priorizar las necesidades de recursos tecnológicos que se deban adquirir.
2. No existen políticas para evaluar y determinar el nivel de riesgo aceptable para los recursos informáticos, comparado con el nivel de riesgo actual.

PROBABILIDAD E IMPACTO

Probabilidad de ocurrencia: 100%

Impacto según relevancia del proceso: ALTO

EVIDENCIAS

/Evidencias/Cuestionarios/CC-ME4-INGENIERA-SISTEMAS.jpg
/Evidencias/Entrevistas/FE-ME4-COORDINADOR-ALMACEN.jpg
/Evidencias/Entrevistas/VIDEOCA-FE-ME4.mp4

CONSECUENCIAS

Si no existen políticas para determinar el nivel de riesgo aceptable para los recursos informáticos en el Hospital Cumbal, no se podrá evaluar ni priorizar las necesidades de estos recursos, ya que no existe un marco de referencia para determinar, si la empresa asume la responsabilidad de continuar su operación, con las falencias o debilidades de TI existentes. Esto puede acarrear consecuencias como adquirir recursos informáticos o repuestos por urgencia y necesidad forzosa, sin estudio previo de factibilidad, incumplimiento en reporte de informes, retraso en la prestación del servicio, lentitud en el rendimiento del sistema, etc.

RECOMENDACIONES

Definir una política gerencial, conjuntamente con la dirección del área de sistemas evalué la necesidad de nuevos recursos informáticos, acordes al avance de las nuevas tecnologías, lo cual permite optimizar procesos, y mejorar la calidad en las operaciones de la empresa, además debe establecer los criterios técnicos, financieros o humanos para evaluar el riesgo aceptable que la empresa está dispuesta a asumir por la ausencia o vulnerabilidad de los recursos informáticos, por ejemplo: no contar con UPS en cada computador, no adquirir licencias, comprar más computadores, más impresoras, fotocopiadora, instalar una red WIFI, etc.

Todo lo anterior debe enmarcarse dentro del Plan Anual de Adquisiciones del Hospital Cumbal, para garantizar su cumplimiento, y además debe reportarse al Sistema Electrónico de Contabilidad Pública de la Republica de Colombia. [23].

_____
[23] https://www.contratos.gov.co/consultas/consultarArchivosPAA2015.do

3.2.9 Informe de auditoría

El informe ejecutivo de auditoría va dirigido o al gerente y jefe sistemas de la E.S.E. Hospital Cumbal.

Cumbal, 25 de Febrero de 2016

Doctora.
ROCIO DEL PILAR JUELPAZ TATICUAN
Gerente E.S.E. Hospital Cumbal
Cumbal – Nariño

Ref. Informe de auditoría informática a la estructura organizacional y a los procesos del área de sistemas en la E.S.E. Hospital Cumbal.

Afectuoso saludo,

Respetuosamente, no dirigimos a usted con el fin de presentar el informe de la auditoría Informática aplicada al área de sistemas de la E.S.E. Hospital Cumbal, para evaluar la Estructura organizacional y a los procesos.

Entre los aspectos evaluados, cabe resaltar los favorables, como:

La institución cuenta con una estructura organizacional adecuada, de acorde a sus objetivos institucionales y misionales, tiene muy bien definido su Mapa de Procesos, donde especifica los Estratégicos, Misionales y de Apoyo. En este último se define el proceso de Información, en el cual se enmarca el área de sistemas. Así mismo, el Hospital Cumbal, tiene como fortaleza que cuenta con una red de datos implementada prácticamente nueva, la cual garantiza la conectividad entre todos los equipos del hospital, ya que fue realizada en el año 2015.

Existe disponibilidad y aceptación por parte de sus directivas, para apoyar al equipo auditor, fundamental para el desarrollo de la presente auditoría informática.

La aplicación de esta auditoría tuvo lugar entre los días 11 y 20 de enero del 2016, utilizando la metodología COBIT (Objetivos de Control para la información y Tecnologías relacionadas), y mediante entrevistas, cuestionarios, y observación directa, se evaluaron los siguientes aspectos:

Dominio. Planear y organizar

Hallazgos	Recomendaciones
PO4: Definición de procesos y organización y relaciones de TI	
1. No existen procesos definidos ni documentado para el área de sistemas 2. No existe un manual de funciones para el área de sistemas 3. No existe un medidas para garantizar la seguridad de los recursos informáticos 4. No existen bitácoras para registrar las actividades que se desarrollan por el área de sistemas	Establecer, definir y documentar los procesos para el área de sistemas, que deben estar bajo la responsabilidad del ingeniero encargado del área, y bajo la supervisión del jefe de control interno, enmarcados en las políticas del MECI. Establecer las funciones inherentes al proceso y organizarlas dentro de un manual de funciones. Establecer políticas de seguridad informática, que contemple medidas de seguridad preventivas, como: Definir un formato, bitácora, histórico u hoja de vida donde se registre todas las actividades realizadas por el personal del área de sistemas.
PO7 Administrarlos recursos TI	
1. No existe un perfil definido y completo, que contemple varios niveles profesionales para el personal del área de sistemas, ya que solo existe el perfil de ingeniero de sistemas, y para la empresa existe la necesidad de	Elaborar un perfil para el personal de sistemas que sea incluya los diferentes niveles profesionales en esta área con técnicos y tecnólogos en sistemas, con el fin de contratar personal con capacidades específicas según las necesidades.

más personal para cumplir con todas tareas solicitadas. 2. Para elegir el personal del área de sistemas, no se está realizando un proceso de .selección adecuado y transparente para evaluar la mejor opción, sino que se escoge según otros intereses. 3. No existen políticas para fomentar capacitaciones para el personal del área de sistemas.	Definir un proceso debidamente documentado, para Recepcionar las hojas de vida de los aspirantes, y surtir un proceso de selección transparente. Fomentar capacitación al personal del área de sistemas, con el fin de optimizar tiempo y recursos, para que pueda cumplir sus actividades de forma eficiente.

Dominio. Adquirir e implementar

Hallazgos	Recomendaciones
AI4 Facilitar la operación del uso	
1. No existe un proceso definido ni documentado para la inducción de los usuarios finales que utilizan las aplicaciones (programas) de la institución. 2. No existe una persona del área de sistemas encargada de brindar inducción a los usuarios finales para el manejo de las aplicaciones (programas) de la institución 3. No existe asesoría continua a los usuarios finales para mejorar el manejo de las aplicaciones o programas de la institución. 4. No existen manuales de usuario para el manejo de la aplicación o programas de la institución.	Al contratar el nuevo personal, se verifique y evalué sus conocimientos básicos en sistemas. Definir una persona que se responsabilice, levante y documente este proceso Crear el respectivo manual de usuario para nuevo personal de las diferentes áreas, quienes serán los usuarios finales de los programas: en el área de facturación, SaludIPS, en el área financiera y de almacén, Compuconta, en el área de farmacia, SaludIPS, y especialmente para el personal asistencial (médicos, enfermeras, auxiliares de enfermería, odontólogos, higienistas) quienes usan SaludIPS el módulo de historias clínicas sistematizada. Facilitar el uso de las TI, es fundamental ya que aumenta el desempeño de la empresa, con el fin de obtener mejores resultados.

Dominio. Entregar y dar soporte

Hallazgos	Recomendaciones
DS4 Garantizar la continuidad del servicio	
1. Con el fin de recuperar y dar continuidad al sistema existe	Dar mayor importancia a los riesgos a los que está expuesto el Hospital de Cumbal

únicamente copias del ejecutable del programa SaludIPS, mas no existe un proceso bien definido 2. El Hospital Cumbal cuenta con dos plantas eléctricas de motor diésel, pero el proceso de respaldo de energía no es el recomendado, ya que no existe el proceso automático para el cambio de energía oportuno. 3. No existe un plan de recuperación y continuidad de los servicios definidos el cual se pueda actualizar. 4. No existe personal responsable ni entrenado para actuar en caso de un fallo crítico. 5. No existe un proceso definido, adecuado y documentado para la restauración y continuidad del servicio. 6. No existe un proceso definido, adecuado y documentado para crear, comprobar y almacenar las copias de seguridad. 7. No existen políticas de almacenamiento de copias de seguridad en sitio o fuera de sitio. 8. No existe un proceso para evaluar el plan de recuperación y continuidad de los servicios.	como daño de software o hardware por mal manejo o cortes de energía, robo, incendios, sismo o terremoto, inundación, etc., ya que la probabilidad de ocurrencia es latente y se debe tomar las medidas necesarias para prevenir que afecten el normal funcionamiento incluso por tiempo prolongado. Definir el proceso, y la o las personas que deban responsabilizarse de esta situación, donde contemple su entrenamiento. Crear un Manual o Plan de Recuperación y Continuidad. Definir un registro de los fallos críticos o incidentes presentados, con el fin de obtener estadísticas de los eventos más frecuentes y fortalecer medidas para prevenirlos. Finalmente, después de cada incidente o fallo crítico, se debe evaluar las acciones realizadas con el fin de identificar debilidades y mejorar este proceso.
DS5 Garantizar la seguridad de los sistemas	
1. No existen políticas de seguridad informática que protejan los recursos informáticos de la empresa. 2. No existe un proceso definido ni documentado para controlar el acceso de personal interno o externo hacia los recursos informáticos. 3. No existe un proceso definido ni documentado para la solicitud, creación, aprobación y desactivación de cuentas de usuario para acceder al programa SaludIPS y otros. 4. El jefe de facturación actualmente es quien crea las cuentas de usuario para ingresar a los módulos de Facturación e Historias Clínicas Sistematizada del aplicativo SaludIPS,	Adoptar políticas de seguridad informática, las cuales deben contemplar medidas de seguridad física, como controlar y vigilar el ingreso a la institución de usuarios internos y externos, mediante la implementación de un sistema de televisión cerrada, que cuente con las suficientes cámaras para cubrir toda las áreas. Apoyo al personal de seguridad (celadores). Que todas las oficinas cuenten con cerraduras Proteger los equipos de cómputo asegurándolos al escritorio y que cada CPU tenga un candado que impida abrirla.

de manera Ad-Hoc. 5. No existe políticas para definir los privilegios o permisos dentro de los aplicativos de la institución. 6. No existe un proceso para controlar el acceso no autorizado a la red de datos e identificar infiltraciones o intrusos.	El acceso al centro de datos debe ser restringido y únicamente se debe permitir al personal autorizado. En cuanto a cuentas de usuario y privilegios se debe definir y documentar un proceso, y asignar una persona que se responsabilice de administrar todas las cuentas de usuario Los privilegios de las cuentas de usuario deben asignarse acorde a las funciones de cada usuario. Con respecto a la red de datos, se recomienda evaluar si cumple con la norma y los estándares, específicamente EIA/TIA 568A o EIA/TIA 568B Además, se debe examinar periódicamente el tráfico de información que circula en la red, utilizando técnicas o herramientas como *WIRESHARK* o *ADVANCED IP SCANNER* para detectar equipos conectados a red, entre otros. Verificar se maneje un buen sistema de cifrado y descifrado en la clave de red wifi, que no existan claves con estándar WEP (Wired Equivalent Privacy – Protocolo de Equivalencia con red cableada) que ya no son seguras, y que se maneje un estándar con un buen nivel de encriptación, por ejemplo, WPA2 (WIFI Protec Acces).
DS7 Educar y entrenar a los usuarios	
1. Las necesidades de los usuarios para el manejo de los recursos informáticos son atendidos por el jefe de facturación quien tiene conocimientos al respecto pero no le corresponde en sus funciones. 2. No existe un proceso definido ni documentado, ni planificado para capacitación a los usuarios finales acerca del uso de los recursos informáticos. 3. No existe una política para evaluar el desempeño de los usuarios finales frente al uso los recursos	Apoyar al personal brindando educación y capacitación en cuanto a TI. Se recomienda definir y documentar políticas y proceso de Educación y Capacitación para el uso de tecnologías de la información. Debe definir una persona del área de sistemas encargada de esta función, quien socializara y ejecutara un cronograma de capacitación. Hacer énfasis en temas como: Manejo y seguridad de Internet, redes sociales, conceptos básicos de spyware, malware, scareware; importancia y manejo de

informáticos.	antivirus, definición de contraseñas seguras las cuales deben ser "***fáciles de recordar, y difíciles de adivinar",*** que garanticen confidencialidad y reserva de información, uso adecuado de cuentas de correo electrónico, cursos virtuales, configuración básica de impresoras, seguridad en Windows.
DS9 Administrar la configuración	
1. No existe un proceso definido ni documentado para la realización y verificación del inventario de activos informáticos correctamente. 2. No existe un proceso definido ni documentado para obtener, verificar y almacenar la configuración de los recursos informáticos tales como hojas de vida completamente diligenciadas. 3. No existen políticas ni un proceso definido ni documentado para controlar y verificar la existencia de software personal instalado sin autorización.	Realizar es un inventario de los activos informáticos dentro de la organización. Obtener toda la información posible como, por ejemplo, tipo de activo (equipo de cómputo, impresora, dispositivo de red, servidor, teléfono VoIP) valor, factura de venta, garantía acta de entrega, proveedor, localización dentro de la empresa, responsable a quien se asigna, configuración y drivers instalados. El inventario de activos informáticos debe estar en conocimiento, dirección y supervisión del jefe del área de sistemas. Para controlar la instalación de software, control de acceso al sistema operativo (SO) y mejorar las políticas de seguridad lógica se recomienda implementar el servicio de DIRECTORIO ACTIVO, SERVICIOS DE DNS en el servidor, bajo el sistema operativo de Windows Server 2012 (instalado actualmente).
DS11 Administración de datos.	
1. No existe políticas ni un proceso definido para elegir el formato, creación, comprobación y eliminación de los medios de almacenamiento de las copias de seguridad de datos y aplicaciones.	Definir y documentar el proceso de Respaldo o copias de seguridad de los datos (backups), que garantice la disponibilidad e integridad de la información Que exista una persona responsable de comprobar si funcionan correctamente, luego rotula y finalmente se transfiere a su lugar de almacenamiento, el cual debe garantizar su seguridad y conservación, bien sea en sitio o fuera de sitio acorde a las políticas de seguridad informática adoptadas.

	Además se debe definir la frecuencia y criterios para eliminar algunos medios que ya no sean necesarios.
DS12 Administración del Ambiente Físico	
1. No existe un proceso para el control de acceso al área al centro de datos. 2. No existe un proceso para garantizar la seguridad física de los activos de TI.	Evalué las condiciones físicas del centro de datos y si cumple con los requerimientos mínimos según el estándar TIA942 de 2005, ya que, al diseñar los centros de datos conforme a la norma, se obtienen ventajas fundamentales, como son: Nomenclatura estándar, Funcionamiento a prueba de fallos, Aumento de la protección frente a agentes externos, y Fiabilidad a largo plazo, mayores capacidades de expansión y escalabilidad. Se recomienda usar cámaras de seguridad, cerraduras de acceso y permiso de ingreso restringido.
DS13 Administración de operaciones.	
1. No existe un monitoreo permanente (mantenimiento) para verificar el correcto funcionamiento de los recursos informáticos que nos suministre datos históricos e incidentes con mayor frecuencia. Tampoco existe el lugar apropiado para realizar esta labor. 2. No existe un proceso definido ni documentado para autorizar y registrar la salida de recursos informáticos que requieren mantenimiento correctivo externo.	Definir y documentar un proceso que contemple las actividades de mantenimiento de los recursos informáticos, con el fin de prever y evitar posibles fallos. El mantenimiento debe ser de tipo preventivo, el cual nos puede evitar que tengamos que realizar el mantenimiento correctivo muchas veces. Debe ser al hardware y al software. La frecuencia que se recomienda es trimestral. Se debe especificar la persona del área de sistemas que se responsabilice de esta función y asignarle un lugar adecuado Realizar la programación (cronograma) para atender a todas las dependencias El mantenimiento correctivo se realiza cuando algo falla, puede ser software o hardware. Recomendable para el mantenimiento correctivo es buscar ayuda con personal especializado, el cual generalmente es

	externo. Finalmente, el área de sistemas debe definir los formularios necesarios para registrar todas las actividades que se realicen debe elaborar una carpeta por cada recurso informáticos. Los formatos relacionados son los siguientes: hoja de vida, acta de entrega al funcionario responsable, formato de mantenimiento preventivo, formato de mantenimiento correctivo, reporte de servicio externo para mantenimiento correctivo, dictamen técnico para baja de recurso informático. Fortalecer la cultura de cuidar los recursos informáticos de parte de los usuarios internos, y así garantizar que los ordenadores se mantengan más tiempo funcionando satisfactoriamente (vida útil).

Dominio. Monitorear y evaluar

Hallazgos	Recomendaciones
ME1 Monitorear y evaluar desempeño de TI	
1. No existen políticas para evaluar el desempeño del área de sistemas frente a las metas propuestas, además no ha sido requeridas por las directivas de la institución 2. No existen políticas para adoptar medidas correctivas con el fin de mejorar los indicadores con baja calificación	Determinar indicadores que apliquen para el área de sistemas, y se pueda medir el desempeño global como área e individual por integrante. Esto favorece a la empresa, ya que si se conoce las debilidades, se puede aprovechar las fortalezas existentes y mitigar con mayor eficiencia las vulnerabilidades, amenazas y riesgos informáticos.
ME3 Garantizar el cumplimiento de los requerimientos externos	
1. No existe el manual de funciones del área de sistemas, por tanto, no se contempla la normatividad vigente referente al uso de tecnologías de la información. 2. No se tiene conocimiento de los todos los informes que hay que presentar a los entes de control,	Definir políticas para el conocimiento de la normatividad informática, la cual debe estar obligatoriamente contemplada en los procesos propios del área de sistemas. Conocer la Ley 1273 de 2009 LEY DE DELITOS INFORMATICOS, la cual trata de evitar posibles atentados contra la confidencialidad, la

únicamente existe requerimiento para Derechos de autor	integridad y la disponibilidad de los datos de los sistemas informáticos, de los siguientes amenazas: Acceso abusivo a un sistema informático, obstaculización ilegitima de sistema informático o red de telecomunicaciones, interceptación de datos informáticos, daños informáticos, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales.
ME4 Proporcionar gobierno de TI	
1. No existen políticas para identificar, evaluar y priorizar las necesidades de recursos tecnológicos que se deban adquirir. 2. No existen políticas para evaluar y determinar el nivel de riesgo aceptable para los recursos informáticos, comparado con el nivel de riesgo actual.	Definir una política gerencial, conjuntamente con la dirección del área de sistemas para evaluar la necesidad de nuevos recursos informáticos Enmarcar dentro del Plan Anual de Adquisiciones del Hospital Cumbal, para garantizar su cumplimiento, y además debe reportarse al SECOP.

Lo anterior corresponde a los procesos fundamentales que debe desempeñar el área de sistemas para una adecuada asistencia al Hospital de Cumbal, y se recomienda que la ingeniera de sistemas Amanda Concha, quien actualmente se encuentra al frente de dicha área, acate las recomendaciones propuestas para mejorar y contribuir al progreso continuo de las operaciones de la empresa.

Sin otro particular,

Atentamente,

MONICA CAICEDO **HENRY IRUA**
Auditores

CONCLUSIONES

La auditoría informática es susceptible de aplicar en cualquier tipo de empresa, sin depender de la actividad a la cual se dedica, o del tamaño. El Hospital Cumbal, empresa de salud, clasificada como mediana empresa, califica perfectamente para la realización de la auditoría informática, que permita encontrar debilidades, amenazas y vulnerabilidades, y de esta manera mitigar o eliminar su probabilidad de ocurrencia.

En la empresa social del estado se está subutilizando las capacidades del ingeniero de sistemas encargado quien debe definir, documentar, seguimiento y evaluar los procesos referentes al área de sistemas, debido a que únicamente se lo contrata para el mantenimiento preventivo y correctivo de los recursos informáticos. Además no se valora como debe ser las capacidades de un ingeniero de sistemas, lo cual se ve reflejado en la contratación por OPS que se maneja.

Para el presente análisis, se concluye que la auditoría informática aplica muy bien para evaluar desde aspectos básicos como la estructura organizacional, hasta aspecto complejos como seguridad de la información.

El diseño de las herramientas de la auditoría informática, como entrevistas, o encuestas son de vital importancia, y es fundamental, razonar muy bien para determinar lo que se desea conocer, y esta manera realizar la adecuada formulación de preguntas, ya que de estas depende el éxito de la auditoría.

No es difícil establecer un Plan de auditoría, lo cual debe ser un motivo para fomentar el desarrollo de las auditorías informáticas a las empresas, se debe hacer énfasis en el programa de auditoría con el fin de cumplir y evaluar correctamente según el objetivo de general de la auditoría.

RECOMEDACIONES

Previo a realizar una auditoría informática se aconseja analizar detalladamente el contexto dentro del cual se desenvuelve la empresa, con el fin de identificar y definir claramente el entorno organizacional, la actividad principal, las metas y objetivos que la empresa pretende alcanzar, con el fin de planificar correctamente la auditoría.

Para una adecuada aplicación de auditoría informática a cualquier empresa, es conveniente plantear las preguntas de las herramientas de auditoría, como cuestionario o entrevistas, con la mayor precisión y claridad posible, lo cual garantizará resultados coherentes, e identificación correcta de riegos.

La observación directa a la empresa, mediante visitas autorizadas y programadas contribuye considerablemente para soportar los hallazgos que se encuentren en la ejecución de la auditoría.

Mediante la aplicación de auditorías informáticas en las empresas, contribuye al optimizar el aprovechamiento de sus activos tecnológicos y nuevas tecnologías de la información existentes, con lo cual mejora el desempeño de la misma.

Las empresas deben ampliar su concepto del área de sistemas, y comprender que al definir su estructura organizacional y sus procesos, de forma adecuada, obtendrá grandiosos beneficios que se pueden reflejar en tiempo de respuesta, mejora en la atención y prestación de servicios, e inclusive en el ahorro de recursos económicos.

BIBLIOGRAFIA

ACOSTA, Diego. QUETAMA, Heider. Auditoría informática a la parte física y lógica de la red de datos en la Empresa Solidaria de Salud Emssanar E.S.S. sedes corporativa Pasto y sedes Alto Putumayo. 2015**.**

Acuerdo de Facultad Nro. 005, Consejo de Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Universidad de Nariño. Octubre 10 de 2010.

BENAVIDES, Jhoana. Auditoría Informática a nivel de los Sistemas e Indicadores de Funcionamiento del Hardware y Software en la Empresa DISPROPAN S.A.S del Departamento de Nariño y Putumayo. 2014.

Echenique, José Antonio. Auditoría en informática. Pág. 16

Ley 1273, Ministerio de Interior y Justicia de la Republica de Colombia. 2009.

NOGUERA, Laura. SANCHEZ, Edy. Auditoría Informática en al área de Sistemas e Indicadores de Funcionamiento del Hardware en la Empresa Solidaria de Salud EMSSANAR E.S.S. del Departamento de Nariño. Universidad de Nariño. 2010.

OVIEDO, Melany. AZA, Oscar. Auditoría de sistemas aplicada a los módulos de facturación, consultas e historia clínica del software INFO-SALUD en la IPS Indígena Guaitara del Municipio de Ipiales. 2015**.**

Piattini, Mario. Auditoría de tecnologías y sistemas de información. Pág. 7

BIBLIOWEB

http://jorgearestrepog.comunidadcoomeva.com/blog/index.php

http://es.wikipedia.org/wiki/Sistema_de_salud_en_Colombia

www.minsalud.gov.co/Normatividad/LEY%201122%20DE%202007.pdf

http://www.minsalud.gov.co/Normatividad/LEY%201438%20DE%202011.pdf

http://www.susalud.com.co

http://www.cumbal-narino.gov.co/informacion_general.shtml

http://www.esehospitalcumbal.gov.co/mision-vision/

https://www.isotools.orgdel /2014/08/19/iso-27001-activos-informacion-empresa-3/

http://www.c3comunicaciones.es/data-center-el-estandar-tia-942/

http://hipertextual.com/archivo/2014/02/mantenimiento-preventivo-correctivo-pc/

http://www.colombiadigital.net/opinion/columnistas/cultura-mas/item/1580-legislaci%C3%B3n-inform%C3%A1tica-en-colombia-ley-lleras-y-tlc.html

http://derechodeautor.gov.co/objetivos-y-funciones

http://datateca.unad.edu.co/contenidos/233005/contenido%20en%20linea%20PELSI_I_2013/leccin_30_legislacin_en_seguridad_informtica_en_colombia.html

https://www.contratos.gov.co/consultas/consultarArchivosPAA2015.do

http://auditordesistemas.blogspot.com.co/2011/11/conceptos.html