AUDITORIA A LA INFRAESTRUCTURA TECNOLÓGICA DEL SISTEMA DE INFORMACIÓN SALUDIPS DEL CENTRO DE SALUD SAN MIGUEL ARCÁNGEL E.S.E DEL MUNICIPIO DE OSPINA – NARIÑO

JOSE FERNANDO ARGOTY ERAZO
CARLOS BENAVIDES MONTENEGRO

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

AUDITORIA A LA INFRAESTRUCTURA TECNOLÓGICA DEL SISTEMA DE INFORMACIÓN SALUDIPS DEL CENTRO DE SALUD SAN MIGUEL ARCÁNGEL E.S.E DEL MUNICIPIO DE OSPINA – NARIÑO

JOSE FERNANDO ARGOTY ERAZO
CARLOS BENAVIDES MONTENEGRO

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

Director:
Msc. MANUEL ERNESTO BOLAÑOS GONZÁLEZ

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

NOTA DE RESPONSABILIDAD

”Las ideas y las 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 N. 005 de 2010 emanado del Honorable Consejo Académico.

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

San Juan de Pasto, Febrero de 2016

RESUMEN

La auditoría de sistemas ofrece métodos prácticos y eficientes para identificar vulnerabilidades, riesgos y amenazas, permitiendo establecer acciones necesarias para su control, con lo anterior y en procura de brindar a los usuarios de salud agilidad en el acceso y mayor calidad de los servicios enfocados en la recepción y manejo de la información durante las etapas en el proceso de prestación de servicio de salud que requieran del uso de la infraestructura tecnológica, se aplicó la auditoria de sistemas basada en la evaluación de la infraestructura tecnológica del Centro de Salud San Miguel Arcángel E.S.E. en el Municipio de Ospina la cual dentro de sus actividades tiene una variedad de procesos que requieren de la administración de información. En la actualidad no se encuentra ningún referente de evaluación, ni auditorías realizada a este componente el cual soporta el sistema de información SALUDIPS, aplicativo de gran importancia en la administración de la información en la empresa.

Con el único fin de que esta empresa de salud garantice una mejor calidad en la prestación de sus servicios, en acceso y calidad de la información se auditara las diferentes dependencias que manejen el sistema de información SALUDIPS y que incluyan infraestructura tecnológica como hardware y software: servidores, computadores, red de datos, equipos de comunicación, equipos de protección, sistemas operativos, software de sistemas, etc., y con esto se identificaran vulnerabilidades, riesgos y amenazas, estableciendo controles, con lo cual se propondrán planes de mejora que serán evaluados por el gerente y adoptados por la empresa si la entidad lo dispone.

Para el desarrollo de este trabajo de auditoria se tomó como guía el estándar COBIT (Objetivos de Control para Información y Tecnologías Relacionadas) el cual brinda buenas practicas a través de un marco de trabajo de dominios y procesos, permitiendo un análisis conciso y claro en el desarrollo del proceso de auditoría, para proponer soluciones a las eventualidades encontradas, manteniendo sus fortalezas y que la seguridad de la información del Centro de Salud San Miguel Arcángel E.S.E., este garantizada.

ABSTRACT

The systems audit provides methods practical and efficient to identify vulnerabilities, risks and threats, allowing establish necessary actions to its control, with the above and in pursuit to provide to health the users agility in access and higher quality of services focused on the receipt and handling of information during the stages in the process of providing health services requiring the use of the technological infrastructure, was applied systems audit based in the evaluation of the technological infrastructure health center San Miguel Arcangel ESE Ospina of municipality which in its activities has a variety of processes that require information management. Currently there is no reference evaluation or audit conducted in this component which supports the information system SALUDIPS, application of great importance in information management in the company.

With the sole purpose of that health center guarantees better quality in the provision of their services, access and quality of information is independently audit the different dependencies that handle the systems information SALUDIPS, and include technological infrastructure such as hardware and software: servers, computers, data network, communication equipment, protective equipment, operating systems, systems software, etc., and with this are identified vulnerability, risks and threats, establishing controls, which will be proposed improvement plans that will evaluated by the manager and adopted by the company if the company this proposed.

For the development of this audit work I was taken as guide the COBIT standard (Control Objectives for Information and related Technology) which gives us good practice through a framework of domains and processes , which allows a concise and clear in the development of the audit process, to the extent possible propose solutions to eventualities founds , keeping their strengths and that the information security Health Center San Miguel Arcangel E.S.E. , this guaranteed.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Administración: conjunto de técnicas por medio de las cuales se determinan, clasifican y realizan los propósitos y objetivos de un grupo humano particular.

Amenaza: según [iso/iec 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgo: según [iso/iec guía 73:2002]: uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditor: persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoria: proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad de una organización.

Centro de informática: es un área de trabajo cuya función es la de concentrar, almacenar y procesar datos y funciones operativas de una entidad de manera sistematizada.

Cobit: *(control objetives for information and related technology),* objetivos de control para la información y tecnología relacionada; publicados y mantenidos por isaca. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de tecnología de información, aceptados para ser empleados por entidades y auditores.

Confiabilidad: es el grado de estabilidad que presenta un instrumento al obtener el mismo resultado en oportunidades repetidas bajo condiciones idénticas.

Continuidad: capacidad del servicio de realizar actividades debidas en la secuencia apropiada y sin interrupción del proceso de atención al usuario, desde la primera atención hasta la satisfacción de sus necesidades, solicitudes y expectativas de salud

Contraseña: se refiere al conjunto de caracteres ocultos que le permiten el acceso a un usuario a utilizar cierta proporción de un sistema o a una red.

Datos: término general para la información procesada por un computador.

Disponibilidad: cantidad de recursos por unidad de población a atender. Si solo es una lista de recursos, se le denomina inventario.

Efectividad: conseguir mejoras en la salud mejorando el impacto de la morbilidad sobre una población definida. Consiste en la medición del grado en que una forma eficaz de intervención puede aplicarse o ponerse a disposición de todos los miembros de un grupo definido que podría resultar beneficiado.

Eficacia: capacidad de la ciencia y la tecnología para lograr un resultado favorable en casos individuales, con independencia de los recursos o insumos necesarios. Consiste en determinar objetivamente que una forma de intervención, preventiva, diagnóstica, curativa o restaurativa; es más útil y beneficiosa que inútil o perjudicial para alcanzar la finalidad preconizada, o que es más eficaz que el tipo de intervención que reemplazará, o que en realidad es mejor que no hacer nada.

Eficiencia: consiste en la medición del grado en que se puede alcanzar un nivel determinado de efectividad con un costo mínimo de personal, de recursos y fondos. Es la relación costo/beneficio por la que se obtiene la mejor calidad al menor costo posible. Expresa los resultados finales obtenidos en relación con los costos en términos de dinero, recursos y tiempo

Hardware: conjunto de componentes físicos que realizan las tareas de entrada y salida, también se conoce al hardware como la parte dura o física del computador.

Impacto: es el resultado de una causa a largo plazo

Información: está constituida por un grupo de datos organizados, procesados y supervisados; la información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento

Infraestructura tecnológica: es el conjunto de hardware y software sobre el que se asientan los diferentes servicios que una empresa necesita tener en funcionamiento para poder llevar a cabo todas sus actividades.

Isaca: *(information systems audit and control association):* es una asociación de auditoría y control de sistemas de información que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información.

Misión: declaración respecto al compromiso con los objetivos principales de una organización, discutidos y aceptados previamente por todos sus participantes. Por lo general, se espera que todo y cualquier miembro de la

organización, desde el nivel elemental hasta el ejecutivo principal, pueda expresar con sus palabras la misión, la visión y los valores de la misma.

Reportes: documento impreso o digital de una acción realizada por una persona o máquina.

Objetivo: declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

Política de seguridad: intención y dirección general expresada formalmente por la dirección. Documentos que establecen el compromiso de la dirección y el enfoque de la organización en la gestión de seguridad de información.

Proceso: conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados.

Programa: secuencia de instrucciones que obliga al computador a realizar una tarea determinada.

Riesgo: combinación de la probabilidad de un evento y sus consecuencias. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Sistema de salud: conjunto de elementos que interactúan para producir salud.

Servidor: computador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los computadores que se conecten con él para dicho fin.

Sistema general de seguridad social en salud (sgsss): regula el servicio público esencial de salud y crear condiciones de acceso para toda la población residente del país, en todos los niveles de atención.

Software: componentes inmateriales del computador como programas, sistemas operativos, etc.

TI: tecnologías de Información.

Usuarios: personas que hacen uso de los recursos de cómputo e informáticos.

Vulnerabilidad: debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

INTRODUCCIÓN

En la actualidad las empresas se han adaptado al manejo de las nuevas tecnologías en busca de la optimización de procesos y recursos en el desarrollo de sus actividades, en el momento y para su correcto funcionamiento es de esencial importancia encontrar tecnologías que se adecuen de manera correcta y optima a los procesos de administración información, manteniendo las necesidades de la empresa y de sus usuarios.

Es así como el conjunto de todos los elementos tecnológicos forman parte de una infraestructura la cual soporta múltiples procesos de administración de información y datos, permitiendo a la empresa la optimización de sus recursos, además de integridad, veracidad, seguridad y agilidad a las solicitudes de información por parte de sus usuarios.

Una infraestructura tecnológica diseñada e implementada a las necesidades de la empresa permite que los sistemas de información y recursos se administren de manera óptima. Y es mediante la auditoría de sistemas, la cual ofrece múltiples herramientas y guías de apoyo basadas en estándares o normas para su correcta aplicación, que en la práctica y después de ser auditadas ciertas áreas de la entidad, sus recursos y sistemas de información, se logran identificar riesgos y amenazas, que mediante su evaluación y análisis, permitan emitir un informe o dictamen y ofrecer en este planes de mejora y control aprovechando en mejor medida estos recursos o planteando otras alternativas de solución.

En esta auditoría de sistemas se evaluó las condiciones en las que se encuentra la infraestructura tecnológica por cada dependencia que maneja el sistema de información SALUDIPS, en el Centro de Salud San Miguel Arcángel E.S.E. del Municipio de Ospina, con el fin de dar a conocer por medio de hallazgos y un informe detallado, las vulnerabilidades, riesgos y amenazas existentes en la parte auditada y como adoptando una serie de recomendaciones plasmadas en el informe final, el centro de salud puede gradualmente mejorar sus servicios de salud ofreciendo a sus usuarios servicios de mejor acceso y calidad en la información.

IDENTIFICACIÓN DEL PROBLEMA

Título del proyecto:

“AUDITORIA A LA INFRAESTRUCTURA TECNOLÓGICA DEL SISTEMA DE INFORMACIÓN SALUDIPS DEL CENTRO DE SALUD SAN MIGUEL ARCÁNGEL E.S.E DEL MUNICIPIO DE OSPINA – NARIÑO”.

MODALIDAD

Este proyecto corresponde a la modalidad de Trabajo de aplicación, modalidad estipulada por el Acuerdo 043 del 30 de abril de 2002 del Consejo Académico de la Facultad de ingeniería de la Universidad de Nariño.

LÍNEA DE INVESTIGACIÓN

Según las líneas de investigación aprobadas y definidas en el Programa de Ingeniería de Sistemas de la Universidad de Nariño, como acuerdo de facultad 045 de octubre 10 de 2002 dado por el honorable consejo de la facultad, el trabajo corresponde a la línea de investigación de Sistemas Computacionales. Esta línea tiene como objetivo planificar, diseñar, implantar, administrar y evaluar sistemas computacionales y servicios basados en estos sistemas complejos de información, la cual soporta la temática de auditoría de sistemas

DESCRIPCIÓN DEL PROBLEMA

Planteamiento del problema

La empresa social del estado Centro de Salud San Miguel Arcángel E.S.E del Municipio de Ospina, es una entidad dedicada a la prestación de servicios de salud y a cubrir las necesidades de acceso a estos servicios según se requiera por parte de sus usuarios, prevaleciendo la eficiencia, efectividad y calidad del servicio prestado.

Para garantizar la continuidad de los servicios de salud por parte de la entidad a sus usuarios, es muy importante que la información como principal activo de la empresa se administre de la mejor manera y que la infraestructura tecnológica que soporta la mayoría de información, datos y sus procesos esté en condiciones óptimas y sea estable ante posibles factores que afecten su correcto funcionamiento.

Es así como la evaluación de la infraestructura tecnológica que soporta el sistema de información SALUDIPS el cual la utiliza para sus procesos, tendrá resultados favorables en pro de salvaguardar y hacer más eficaz y eficiente la entrega de la información y el procesamiento de datos, que son continuamente manipulados por las tecnologías informáticas existentes en las diferentes dependencias que manejan este sistema.

La auditoría informática da los medios suficientes para aplicar una evaluación más concisa y organizada, generando unos resultados consistentes, con esto identificar vulnerabilidades, riesgos y amenazas y plantear una serie de recomendaciones que los mitiguen.

La aplicación de esta auditoría se llevó a cabo en la infraestructura tecnológica del sistema de información SALUDIPS, actualmente no hay referentes de auditorías realizadas a este componente y gracias a esta auditoria se identificó fallas recurrentes en la efectividad de la entrega de información, caídas del sistema, pérdida, integridad y calidad de la información y fallas en el hardware y software. Estas fallas hacen que los usuarios se sientan inconformes ante el servicio y que la información de la empresa no se administre de manera óptima haciendo que la entidad no cumpla de manera adecuada con el objetivo de brindar y garantiza sus servicios en salud.

OBJETIVOS

Objetivo general

Garantizar continuidad de los servicios con el mejoramiento a lograr a través de planes de mejora obtenidos con el desarrollo de la auditoria a la Infraestructura Tecnológica que soporta al sistema de Información SaludIPS del Centro de Salud San Miguel Arcángel E.S.E. del Municipio de Ospina – Nariño.

Objetivos específicos:

- Conocer la Infraestructura Tecnológica que soporta al sistema de Información SALUDIPS y los procesos que maneja internamente el Centro de Salud San Miguel Arcángel E.S.E.

- Elaborar el Plan de Auditoria y diseñar los Instrumentos para la recolección de información y soporte de hallazgos, que permitan identificar vulnerabilidades, amenazas y riesgos presentes en la Infraestructura Tecnológica que soporta al sistema de Información SALUDIPS del Centro de Salud San Miguel Arcángel E.S.E.

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

- Elaborar y entregar el informe final al Centro de Salud San Miguel Arcángel E.S.E, que contenga los riesgos conformados y controles propuestos.

JUSTIFICACIÓN

El Centro de Salud San Miguel Arcángel E.S.E en su proceso de mejoramiento de calidad a los servicios que presta, tiene como necesidad primordial brindar a sus usuarios además de servicios integrales de atención en salud, agilidad en los procesos de disponibilidad, acceso y calidad de la información que les es entregada a ellos.

Este trabajo de auditoria pretende por medio del estándar COBIT, evaluar y verificar que aspectos relevantes son los que intervienen en el adecuado manejo de la información, que es soportada por su infraestructura tecnológica. Con el estudio de este estándar y los métodos que ofrece se realizaron dictámenes más agiles y concisos que ayudan a la empresa a establecer planes de mejora.

Con lo anterior, se busca mejores beneficios para la empresa y sus usuarios directos, ahorro de recursos, eficiencia y agilidad en los procesos, generando un mayor nivel de confianza en los usuarios hacia la empresa, así como mejorando la prestación de los servicios de salud que requieran del manejo de la información del usuario.

ALCANCE Y DELIMITACION

Para el desarrollo de este trabajo se tomó como estudio la empresa social del estado Centro de Salud San Miguel Arcángel E.S.E. ubicada en el municipio de Ospina – Nariño. Con la presente auditoria se evaluó las condiciones actuales de la infraestructura tecnológica del sistema de información SALUDIPS en las diferentes áreas donde se utiliza este aplicativo, con el fin de encontrar fallas, sus posibles causas y consecuencias para de esta manera desarrollar planes de mejora y control que optimicen tanto el uso por parte de los usuarios, como el funcionamiento del sistema.

De la infraestructura tecnológica del sistema de información SALUDIPS, se evaluó por dependencias lo siguiente:

Del hardware:

- Las condiciones y seguridad de los servidores, equipos de cómputo, red de datos y elementos que la componen, elementos de comunicación (switchs, routers, etc.), elementos de protección (ups, estabilizadores, plantas eléctricas, etc.) y red eléctrica.
- Disponibilidad de inventario.
- Procesos de mantenimiento.
- Existencia de políticas de seguridad.

Del software:

- Sistemas operativos (licenciamientos),
- Software de sistemas.
- Software de seguridad (antivirus, firewalls, etc.).
- Existencia de políticas de seguridad.

Del talento humano:

- Acceso a su lugar y herramienta de trabajo (computador).
- Capacitación.
- Conocimiento de procedimientos en el manejo de la información.
- Conocimiento de su equipo de cómputo y dispositivos.

1. MARCO TEÓRICO

1.1 ANTECEDENTES

Se tomó como referencia dos trabajos de auditoria aplicados con el estándar COBIT y que han sido de mucha utilidad para estudiar y adquirir conocimientos de muchos conceptos acerca de la auditoria y su importancia en pro del mejoramiento en la administración de la información en las empresas donde se sometieron estas evaluaciones.

Título del trabajo: AUDITORIA INFORMÁTICA EN EL ÁREA DE SISTEMAS E INDICADORES DE FUNCIONAMIENTO DEL HARDWARE EN LA EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S DEL DEPARTAMENTO DE NARIÑO, A CARGO DE; LAURA YANETH NOGUERA QUENGUAN Y EDY YANIRA SANCHEZ PERENGUEZ.

Objetivo general: "EVALUAR LA EFICIENCIA Y EFICACIA DEL HARDWARE DE LAS COMUNICACIONES, LOS SERVIDORES E INDICADORES DE FUNCIONAMIENTO EN EL ÁREA DE SISTEMAS DE EMSSANAR E.S.S, OBTENIENDO UN DIAGNOSTICO QUE PERMITA DEFINIR PLANES DE MEJORAMEINTO EN LA EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S".

Se tomó como referencia este trabajo, ya que se contextualiza dentro del desarrollo de aspectos que evalúan procesos dentro de una empresa prestadora de servicios de salud relacionados con su infraestructura tecnológica.

Título del trabajo: "AUDITORÍA INFORMÁTICA Y DE SISTEMAS APLICADA EN LA EMPRESA DISPROPAN S.A.S DEL DEPARTAMENTO DE NARIÑO Y PUTUMAYO; A CARGO DE; JHOANA LORENA HERNÁNDEZ BENAVIDES.

Objetivo general: "REALIZAR UNA AUDITORIA QUE PERMITA EVALUAR LA EFICIENCIA Y EFICACIA DEL HARDWARE DE EQUIPOS DE CÓMPUTO, EQUIPOS MÓVILES, LOS SERVIDORES Y EL FUNCIONAMIENTO DEL SISTEMA SYSCAFE PARA EN LA EMPRESA DISPROPAN S.A.S, APLICANDO LOS PROCESOS DE ANÁLISIS DE RIESGOS Y AUDITORÍA TENIENDO EN CUENTA EL MODELO ESTÁNDAR DE AUDITORÍA Y MEJORES PRÁCTICAS COBIT COMO HERRAMIENTA DE APOYO EN EL PROCESO EVALUACIÓN DE LOS RIESGOS EXISTENTES Y VERIFICACIÓN DE CUMPLIMIENTO DE CONTROLES, CON EL PROPÓSITO DE AYUDAR A DEFINIR Y ESTABLECER UN PLAN DE MEJORAMIENTO E INTEGRACIÓN DE TECNOLOGÍA".

Se tomó como referencia este trabajo, ya que en su desarrollo se aplica métodos y técnicas de auditoria informática que evalúa la eficiencia y eficacia de recursos tecnológicos informáticos detectando riesgos y amenazas y desarrollando planes de mejora en la empresa auditada.

1.2 ASPECTOS GENERALES DE LA AUDITORIA

Definición de auditoria

Es un instrumento de gestión que incluye una evaluación sistemática, documentada y objetiva de la eficacia de las operaciones administrativas, que se realiza con posterioridad a su ejecución en las entidades públicas o privadas y cuyo producto final es un informe conteniendo opinión sobre la información administrativa auditada, así como conclusiones y recomendaciones tendientes a promover la economía, eficiencia y eficacia de la gestión empresarial o gerencial, sin perjuicio de verificar el cumplimiento de las leyes y regulaciones aplicables[1].

Auditor

Es aquella persona profesional, que se dedica a trabajos de auditoria habitualmente, con libre ejercicio de una ocupación técnica, con gran capacidad para opinar, unidad de instrumentos que validen su información, e independencia de criterio[2]. Esto va al lado de la objetividad. El auditor cuenta con una serie de funciones entre estas se tienen:

- Estudiar la normatividad, misión, objetivos, políticas, estrategias, planes y programas de trabajo.
- Desarrollar el programa de trabajo de una auditoria.
- Definir los objetivos, alcance y metodología para instrumentar una auditoria.
- Obtener y revisar estadísticas sobre información del trabajo realizado.
- Diagnosticar sobre métodos de operación y los sistemas de información.
- Respetar las normas de actuación dictadas por los grupo de filiación, corporativos, sectoriales e instancias normativas y en su caso globalizadoras.
- Proponer los sistemas administrativos y/o modificaciones que permitan elevar la efectividad de la organización.
- Analizar la estructura y funcionamiento de la organización en todos su ámbitos y niveles
- Revisar el flujo de datos y de formas.
- Evaluar los registros contables e información financiera.

---

[1] Disponible en internet: http://www.mailxmail.com/curso-elemental-auditoria/concepto-auditoria

[2] Disponible en internet: http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/notas-clase/nota1- auditoria.pdf

- Mantener el nivel de actuación a través de una interacción y revisión continúa de avances.
- Proponer elementos de tecnología de punta requeridos para impulsar el cambio organizacional.
- Diseñar y preparar reportes de avance e informes de una auditoria.

Tipos de auditoria

La auditoría se clasifica por su lugar de aplicación y se refiere a la forma en que se realiza este tipo de trabajos, y también a cómo se establece la relación laboral en las empresas donde se llevará a cabo la auditoría; esto nos da un origen externo si el auditor no tiene relación directa con la empresa, o un origen interno si existe alguna relación de dicho auditor con la propia empresa[3].

a) Auditoría externa

Se caracteriza porque la realizan auditores totalmente ajenos a la empresa, por lo menos en el ámbito profesional y laboral; esto permite que el auditor externo utilice su libre albedrío en la aplicación de los métodos, técnicas y herramientas de auditoría con las cuales hará la evaluación de las actividades y operaciones de la empresa que audita y, por lo tanto, la emisión de resultados será absolutamente independiente.

Ventajas:

- Al no tener ninguna dependencia de la empresa, el trabajo de estos auditores es totalmente independiente y libre de cualquier injerencia por parte de las autoridades de la empresa auditada.
- En su realización, estas auditorías pueden estar apoyadas por una mayor experiencia por parte de los auditores externos, debido a que utilizan técnicas y herramientas que ya fueron probadas en otras empresas con características similares.

Desventajas:

- La principal desventaja es que, como el auditor conoce poco la empresa, su evaluación puede estar limitada a la información que pueda recopilar.
- Dependen en absoluto de la cooperación que el auditor pueda obtener de parte de los auditados.
- Su evaluación, alcances y resultados pueden ser muy limitados.

[3]Muñoz Razo, Carlos. Pearson Educación, 2002. “Auditoría en Sistemas Computacionales, México, Pág. 12.

- Muchas auditorías de este tipo se derivan de imposiciones fiscales y legales que pueden llegar a crear ambientes hostiles para los auditores que las realizan.

b) Auditoría interna

Se caracteriza porque el auditor que lleva a cabo la auditoría labora en la empresa donde se realiza la misma y, por lo tanto, de alguna manera está involucrado en su operación normal; debido a esto, el auditor puede tener algún tipo de dependencia con las autoridades de la institución, lo cual puede llegar a influir en el juicio que emita sobre la evaluación de las áreas de la empresa.

Ventajas

- Debido a que el auditor pertenece a la empresa, casi siempre conoce integralmente sus actividades, operaciones y áreas; por lo tanto, su revisión puede ser más profunda y con un mayor conocimiento de las actividades, funciones y problemas de la institución.
- Por esta razón, el contenido de su informe es mucho más valioso.
- Es de gran utilidad para la buena marcha de la empresa, ya que permite detectar problemas y desviaciones a tiempo.
- Puede llevarse un programa concreto de evaluación en apoyo a las autoridades de la empresa, lo cual ayudará a sus dirigentes en la evaluación y la toma de decisiones.

Desventajas

- Su veracidad, alcance y confiabilidad pueden ser limitados, debido a que puede haber cierta injerencia por parte de las autoridades de la institución como en la forma de evaluar y emitir el informe.
- En ocasiones la opinión del auditor tal vez no sea absoluta, debido a que, al laborar en la misma empresa donde realiza la auditoría, se pueden presentar presiones, compromisos y ciertos intereses al haber realizado la evaluación.
- Se pueden presentar vicios de trabajo del auditor con relativa frecuencia, ya sea en las formas de utilizar las técnicas y herramientas para aplicar la auditoría, como en la forma de evaluar y emitir su informe sobre la misma.

Enfoques de auditoria

Entre los principales enfoques de Auditoría se tiene los siguientes[4]:

[4] Disponible en internet: https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica https://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3

- Auditoria Informática: consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas

- Auditoria de seguridad de sistemas de información: es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores. Las auditorías de seguridad de si permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

1.3 AUDITORIA INFORMÁTICA COMO MÉTODO DE ESTUDIO

La auditoría en informática es la revisión y evaluación de los controles, sistemas, procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan 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 la adecuada toma de decisiones: [5]

1.3.1 Clasificación de la auditoria informática:

Auditoria informática de sistemas: se ocupa de analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas.

Sistemas operativos: proporcionados por el fabricante junto al equipo. Engloba los Subsistemas de Teleproceso, Entrada/Salida, etc. Los Sistemas deben estar actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si éstas se han producido. El análisis de las versiones de los S.O. permite descubrir posibles incompatibilidades entre algunos productos de Software adquiridos por la instalación y determinadas versiones. Deben revisarse los parámetros de las librerías importantes de los Sistemas, especialmente si difieren de los valores aconsejados por el constructor.

---

[5] Disponible en internet: http://members.tripod.com/~Guillermo_Cuellar_M/informatica.html
Moreno Bravo, Freddy Javier, 2012. “Auditoria y Evaluación de Sistemas”. Pág. 8

Software básico: conjunto de productos que, sin pertenecer al Sistema Operativo, configuran completamente los Sistemas Informáticos, haciendo posible la reutilización de funciones básicas no incluidas en aquél. También puede ser desarrollado por el personal informático de la empresa que permiten mejorar la instalación. El auditor debe verificar que el software no agrede, no condiciona al Sistema, debe considerar el esfuerzo realizado en términos de costos, por si hubiera alternativas más económicas.

Tunning: Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los subsistemas y del sistema en su conjunto. El Tunning posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados. Los Tunning pueden realizarse: cuando existe la sospecha de deterioro del comportamiento parcial o general del Sistema. De modo sistemático y periódico, por ejemplo cada seis meses. En este último caso, las acciones de Tunning son repetitivas y están planificadas y organizadas de antemano. El auditor informático deberá conocer el número de Tunning realizados el último año, sus resultados, analizar los modelos de carga utilizados y los niveles e índices de confianza de las observaciones.

Optimización de los sistemas y subsistemas: técnica de Sistemas Actúa igualmente como consecuencia de la realización de Tunnings pre programado o específico. El auditor verificará que las acciones de optimización fueron efectivas y no comprometieron la Operatividad de los Sistemas ni el "plan crítico de producción diaria" de explotación.

Administración de base de datos: es un área que ha adquirido una gran importancia a causa de la proliferación de usuarios y de las descentralizaciones habidas en las informáticas de las empresas, el diseño de las bases de datos, ya sean relacionales o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada, por lo general, desarrollada en el ámbito de Técnica de Sistemas, y de acuerdo con las áreas de desarrollo y los usuarios de la empresa.

Investigación y desarrollo: como empresas que utilizan y necesitan de informáticas desarrolladas, saben que sus propios efectivos están desarrollando aplicaciones y utilidades que, concebidas inicialmente para su uso interno, pueden ser susceptibles de adquisición por otras empresas, haciendo competencia a las Compañías del ramo. La auditoría informática deberá cuidar de que la actividad de Investigación y Desarrollo no interfiera ni dificulte las tareas fundamentales internas.

Auditoria informática de comunicación y redes: la creciente importancia de las comunicaciones ha determinado que se estudien separadamente del ámbito de Técnica de Sistemas. Se ha producido un cambio conceptual muy profundo en el tratamiento de las comunicaciones informáticas y en la construcción de los

modernos Sistemas de Información, basados en Redes de comunicaciones muy sofisticadas. Para el Auditor Informático, el entramado conceptual que constituyen las Redes Nodales, Líneas, Concentradores, Multiplexores, Redes Locales, etc., no son sino el soporte físico-lógico del Tiempo Real. El auditor no debe olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de Redes Locales, diseñadas y cableadas con recursos propios. El auditor de comunicaciones deberá inquirir sobre los índices de utilización delas líneas contratadas, con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la Red de Comunicaciones, actualizada. La des actualización de esta documentación significaría una grave debilidad. La contratación e instalación de líneas va asociada a la instalación de los Puestos de Trabajo correspondientes (Monitores, Servidores de Redes Locales, Ordenadores Personales con tarjetas de Comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y a ser posible, dependientes de una sola organización.

Auditoria de seguridad informática: la seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La Seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc. Igualmente, a este ámbito pertenece la política de Seguros. La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información. La decisión de abordar una Auditoria Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Tal estudio comporta con frecuencia la elaboración de "Matrices de Riesgo" en donde se consideran los factores de las "Amenazas" a las que está sometida una instalación y de los "Impactos" que aquellas pueden causar cuando se presentan. Las matrices de riesgo se presentan en cuadros de doble entrada "Amenazas\Impacto", en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz.

1.4 METODOLOGÍA DE AUDITORIA INFORMATICA

1.4.1 Metodología. Es una secuencia de pasos lógica y ordenada de proceder para llegar a un resultado. Generalmente existen diversas formas de obtener un resultado determinado, y de esto se deriva la existencia de varias metodologías para llevar a cabo una auditoria informática[6].

[6] Disponible en internet: http://www.ub.edu.ar/catedras/ingenieria/auditoria/tpmetodo/tpmetodo2.htm

1.4.2 Etapas de la metodología. El método de trabajo del auditor pasa por las siguientes etapas:

Definición de alcances y objetivos: el alcance de la auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar. A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoría, es decir cuales materias, funciones u organizaciones no van a ser auditadas. Tanto los alcances como las excepciones deben figurar al comienzo del Informe Final.

Estudio inicial: para la realización de dicho estudio ha de examinarse las funciones y actividades generales de la informática. Para el equipo auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para la realización de esto el auditor deberá fijarse en:

- Organigrama: el organigrama expresa la estructura oficial de la organización a auditar. Si se descubriera que existe un organigrama fáctico diferente al oficial, se pondrá de manifiesto tal circunstancia.
- Departamentos: se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.
- Relaciones jerárquicas y funcionales entre órganos de la Organización: El equipo auditor verificará si se cumplen las relaciones funcionales y Jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes. Las de Jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente subordinables.
- Flujos de Información: además de las corrientes verticales intradepartamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extradepartamentales. Los flujos de información entre los grupos de una organización son necesarios para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio organigrama.
- Número de puestos de trabajo: el equipo auditor comprobará que los nombres de los Puestos de Trabajo de la organización corresponden a las funciones reales distintas. Es frecuente que bajo nombres diferentes se realicen funciones idénticas, lo cual indica la existencia de funciones operativas redundantes.
- Número de personas por Puesto de Trabajo: es un parámetro que los auditores informáticos deben considerar. La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

Entorno operacional: el equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse. Este conocimiento previo se logra determinando, fundamentalmente, los siguientes extremos:

a) Situación geográfica de los Sistemas: se determinará la ubicación geográfica de los distintos Centros de Proceso de Datos en la empresa. A continuación, se verificará la existencia de responsables en cada uno de ellos, así como el uso de los mismos estándares de trabajo.
b) Arquitectura y configuración de Hardware y Software: cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de las compañías. Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.
c) Inventario de Hardware y Software: el auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware figurarán las CPUs, unidades de control local y remoto, periféricos de todo tipo, etc. El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.
d) Comunicación y redes de comunicación: en el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones. Igualmente, poseerán información de las Redes Locales de la Empresa.
e) Aplicaciones bases de datos y ficheros: el estudio inicial que han de realizar los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la empresa auditada. Para ello deberán conocer lo siguiente:

- Volumen, antigüedad y complejidad de las aplicaciones.
- Metodología del diseño: se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones. Si se han utilizados varias a lo largo del tiempo se pondrá de manifiesto.
- Documentación: La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes. La documentación de programas disminuye gravemente el mantenimiento de los mismos.
- Cantidad y complejidad de Bases de Datos y Ficheros: el auditor recabará información de tamaño y características de las Bases de Datos, clasificándolas en relación y jerarquías. Hallará un promedio de número de accesos a ellas por hora o días. Esta operación se repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos. Estos datos proporcionan una visión aceptable de las características de la carga informática.

Determinar los recursos de la auditoria informática: mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

- ✓ Recursos humanos
- ✓ Recursos materiales

Recursos materiales: es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente. Las herramientas de software propias del equipo van a utilizarse igualmente en el sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre el auditor y cliente. Los recursos materiales del auditor son de dos tipos:

Recursos materiales software:

- Programas propios de la auditoría: son muy potentes y Flexibles. Habitualmente se añaden a las ejecuciones de los procesos del cliente para verificarlos.
- Monitores: se utilizan en función del grado de desarrollo observado en la actividad de Técnica de Sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

Recursos materiales hardware:

- Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las computadoras del auditado. Para lo cual habrá de convenir el tiempo de máquina, espacio de disco, impresoras ocupadas, etc.

- Recursos Humanos: La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado depende de la materia auditable. Es igualmente señalable que la auditoría en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria.

Elaboración del plan y de los programas de trabajo: una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo. Decidido éste, se procede a la programación del mismo. El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

a) Si la Revisión debe realizarse por áreas generales o áreas específicas. En el primer caso, la elaboración es más compleja y costosa.

b) Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.

- En el Plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos
- En el Plan se establecen los recursos y esfuerzos globales que van a ser necesarios
- En el Plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- El Plan establece disponibilidad futura de los recursos durante la revisión.
- El Plan estructura las tareas a realizar por cada integrante del grupo.
- En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.
- Una vez elaborado el Plan, se procede a la Programación de actividades. Esta ha de ser lo suficientemente como para permitir modificaciones a lo largo de este trabajo.

Actividades de la auditoria informática: la auditoría Informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos. Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad.

Técnicas de trabajo:

- ✓ Análisis de la información recabada del auditado
- ✓ Análisis de la información propia
- ✓ Cruzamiento de las informaciones anteriores
- ✓ Entrevistas
- ✓ Simulación
- ✓ Muestreos

Herramientas:

- ✓ Cuestionario general inicial
- ✓ Cuestionario Checklist
- ✓ Estándares
- ✓ Monitores
- ✓ Simuladores (Generadores de datos)
- ✓ Paquetes de auditoría (Generadores de Programas)
- ✓ Matrices de riesgo

Informe final: la función de la auditoría se materializa exclusivamente por escrito. Por lo tanto, la elaboración final es el exponente de su calidad. Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

Estructura del informe final: el informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente.

a) Definición de objetivos y alcance de la auditoría.
b) Enumeración de temas considerados: Antes de tratarlos con profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría.
c) Cuerpo expositivo: Para cada tema, se seguirá el siguiente orden a saber:

- Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real
- Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
- Puntos débiles y amenazas
- Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.
- Redacción posterior de la Carta de Introducción o Presentación.

Modelo conceptual de la exposición del informe final: el informe debe incluir solamente hechos importantes. La inclusión de hechos poco relevantes o accesorios desvía la atención del lector. El Informe debe consolidar los hechos que se describen en el mismo. El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

- El hecho debe poder ser sometido a cambios.
- Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
- No deben existir alternativas viables que superen al cambio propuesto.
- La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.

Carta de introducción o presentación del informe final: la carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada.

Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargó o contrató la auditoría. Así como pueden existir tantas copias del informe Final como solicite el cliente, la auditoría no hará copias de la citada carta de Introducción. La carta de introducción poseerá los siguientes atributos:

- Tendrá como máximo 4 folios.
- Incluirá fecha, naturaleza, objetivos y alcance.
- Cuantificará la importancia de las áreas analizadas.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.
- En la carta de Introducción no se escribirán nunca recomendaciones.

1.4.3 Herramientas y técnicas para la auditoria informática.[7] Entre estas herramientas se encuentran las siguientes:

- Observación
- Cuestionarios
- Entrevistas
- Checklist
- Trazas y/o Huellas

Observación: permite recolectar la información directamente sobre las funciones, actividades, procedimientos y operación de los sistemas, se aplica para observar todo lo relacionado con 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.

Cuestionarios: las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias. Se suele solicitar la completación de cuestionarios que se envían a las personas concretas que el auditor cree adecuadas. Estos cuestionarios deben ser específicos para cada situación, y muy cuidados en su fondo y su forma. Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos preimpresos hubieran proporcionado.

[7] Disponible en internet: http://www.fceia.unr.edu.ar/asist/intro-aa-t.pdf

Entrevistas: la entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente.[8]

Cheklist: el auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas “normales”, que en realidad servirán para la cumplimentación sistemática de sus Cuestionarios, de sus Checklists. Los cuestionarios o Checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:[9]

a. Checklist de rango

Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo). Ejemplo de Checklist de rango:

Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cómputos. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tienen los siguientes significados:

1: Muy deficiente
2: Deficiente
3: Mejorable
4: Aceptable
5: Correcto

Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan clasificadas previamente. Basta con que el auditor lleve un

---

[8] http://www.uaeh.edu.mx/docencia/P_Presentaciones/tlahuelilpan/sistemas/auditoria_informatica/auditoria_informatica.pdf

[9] http://www.ub.edu.ar/catedras/ingenieria/auditoria/tpmetodo/tpmetodo2.htm

pequeño guion. La cumplimentación del Checklist no debe realizarse en presencia del auditado.

- ¿Existe personal específico de vigilancia externa al edificio?

Rta/ No, solamente un guardia por la noche que atiende además otra instalación adyacente.
<Puntuación: 1>

- Para la vigilancia interna del edificio, ¿Hay al menos un vigilante por turno en los aledaños del Centro de Cómputos?

Rta/ Sí, pero sube a las otras 4 plantas cuando se le necesita.
<Puntuación: 2>

- ¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas?

Rta/ Sí, pero existen cajas apiladas en dicha puerta. Algunas veces las quitan.
<Puntuación: 2>

- El personal de Comunicaciones, ¿Puede entrar directamente en la Sala de Computadoras?

Rta/ No, solo tiene tarjeta el Jefe de Comunicaciones. No se la da a su gente más que por causa muy justificada, y avisando casi siempre al Jefe de Explotación.
<Puntuación: 4>

El resultado sería el promedio de las puntuaciones: (1 + 2 + 2 + 4) /4 = 2,25 Deficiente.

b. Checklist Binario

Es el constituido por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente.

Ejemplo de Checklist Binario:

Se supone que se está realizando una Revisión de los métodos de pruebas de programas en el ámbito de Desarrollo de Proyectos.

- ¿Existe Normativa de que el usuario final compruebe los resultados finales de los programas?

<Puntuación: 1>

- ¿Conoce el personal de Desarrollo la existencia de la anterior normativa?

<Puntuación: 1>

- ¿Se aplica dicha norma en todos los casos?

<Puntuación: 0>

- ¿Existe una norma por la cual las pruebas han de realizarse con juegos de ensayo o copia de Bases de Datos reales?

<Puntuación: 0>

Obsérvese como en este caso están contestadas las siguientes preguntas:

- ¿Se conoce la norma anterior?

<Puntuación: 0>

- ¿Se aplica en todos los casos?

<Puntuación: 0>

Los Checklists de rango son adecuados si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en el checklist binario.

Los Checklists Binarios siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidos, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del <si o no> frente a la mayor riqueza del intervalo.

Trazas y/o huellas: con frecuencia, el auditor informático debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos Software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa. Las trazas se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el Sistema.

1.4.4 Cobit. Es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI) en 1992. Cobit es un marco de referencia para la dirección de IT, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del

negocio. Cobit permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones[10].

- Cobit enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de Cobit.
- El propósito de Cobit es brindar a la Alta Dirección de una compañía confianza en los sistemas de información y en la información que estos produzcan.
- Cobit permite entender como dirigir y gestionar el uso de tales sistemas así como establecer un código de buenas prácticas a ser utilizado por los proveedores de sistemas.
- Cobit suministra las herramientas para supervisar todas las actividades relacionadas con IT.

El marco de referencia Cobit en su versión 4 (a Julio de 2010), incluye lo siguiente:

Marco de referencia: explica como Cobit organiza la Gestión de IT, los objetivos de control y buenas prácticas del negocio por dominios y procesos de IT, relacionándolos directamente con los requerimientos del negocio. Este marco de referencia contiene un total de 34 niveles de objetivos de control, uno por cada proceso de IT, agrupados en cuatro dominios: Planeamiento y Organización, Adquisición e Implementación, Desarrollo y Soporte y Monitoreo y Evaluación.

Descripción de procesos: incluida para cada uno de los 34 procesos de IT, cubriendo todas las áreas y responsabilidades de IT de principio a fin.

Objetivos de control: suministra objetivos de gestión basados en las mejores prácticas para los procesos de IT.

Directrices de gestión: incluye herramientas para ayudar a asignar responsabilidades y medir desempeños.

Modelos de madurez: proporciona perfiles de los procesos de IT describiendo para cada uno de ellos un estado actual y uno futuro.

[10] Disponible en internet: http://seguridadinformacioncolombia.blogspot.com.co/2010/07/que-es-cobit.html

Dominios del COBIT [11]

- **Dominio: planear y organizar**

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

Procesos:

PO1 Definir un Plan Estratégico de TI
PO2 Definir la Arquitectura de la Información
PO3 Determinar la Dirección Tecnológica
PO4 Definir los Procesos, Organización y Relaciones de TI
PO5 Administrar la Inversión en TI
PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia
PO7 Administrar Recursos Humanos de TI
PO8 Administrar la Calidad
PO9 Evaluar y Administrar los Riesgos de TI
PO10 Administrar Proyectos

- **Dominio: adquirir e implementar**

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos.

Procesos:

AI1 Identificar soluciones automatizadas
AI2 Adquirir y mantener software aplicativo
AI3 Adquirir y mantener infraestructura tecnológica
AI4 Facilitar la operación y el uso
AI5 Adquirir recursos de TI
AI6 Administrar cambios
AI7 Instalar y acreditar soluciones y cambios

[11] auditoriasistemasucb.pbworks.com/f/sis303_pt4_Cobit41.pptx. Marco de referencia Cobit versión 4.1.

- **Dominio: Entregar y dar 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 Definir y administrar los niveles de servicio
DS2 Administrar los servicios de terceros
DS3 Administrar el desempeño y la capacidad
DS4 Garantizar la continuidad del servicio
DS5 Garantizar la seguridad de los sistemas
DS6 Identificar y asignar costos
DS7 Educar y entrenar a los usuarios
DS8 Administrar la mesa de servicio y los incidentes
DS9 Administrar la configuración
DS10 Administrar los problemas
DS11 Administrar los datos
DS12 Administrar el ambiente físico
DS13 Administrar las operaciones

- **Dominio: monitorear y evaluar**

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

Procesos

ME1 Monitorear y evaluar el desempeño de TI
ME2 Monitorear y evaluar el control interno
ME3 Garantizar el cumplimiento regulatorio
ME4 Proporcionar gobierno de TI

Ventajas que ofrece COBIT [12]

Suministra un lenguaje común que permite a los ejecutivos de negocios comunicar sus metas, objetivos y resultados con Auditores, IT y otros profesionales.

Proporciona las mejores prácticas y herramientas para monitorear y gestionar las actividades de IT. El uso de sistemas usualmente requiere de una inversión que necesita ser adecuadamente gestionada.

Ayuda a los ejecutivos a entender y gestionar las inversiones en IT a través de sus ciclo de vida, así como también proporcionándoles métodos para asegurarse que IT entregara los beneficios esperados.

La diferencia entre compañías que gestionan adecuadamente sus recursos IT y las que no es enorme. Cobit permite el desarrollo de políticas claras y buenas prácticas para la gestión de IT. Su marco de referencia permite gestionar los riesgos de IT y asegurar el cumplimiento, la continuidad, seguridad y privacidad.

Al ser Cobit reconocida y aceptada internacionalmente como una herramienta de gestión, su implementación es un indicativo de la seriedad de una organización.
Ayuda a Empresas y profesionales de IT a demostrar su competitividad ante las demás compañías.

[12] Disponible en internet: http://seguridadinformacioncolombia.blogspot.com.co/2010/07/que-es-cobit.html. Marco de referencia **Cobit** versión 4.1. 2007 IT Governance Institute. All rights reserved.

2. DESARROLLO DE LA AUDITORIA

2.1 METODOLOGIA

Al utilizar una metodología de trabajo, estos seguirán una secuencia ordenada de pasos encaminándolos a un desarrollo mucho más ágil y consecuente de los conocimientos adquiridos, es por esto que para la ejecución de este trabajo se plantearon las siguientes etapas:

PRIMERA ETAPA: RECONOCIMIENTO

Se realizó una visita preliminar a las instalaciones del Centro de Salud San Miguel Arcángel E.S.E en el Municipio de Ospina, con el fin de conocer cada área, identificar su infraestructura tecnológica y las dependencias que manejan el sistema de información SALUDIPS.

- Población:

Doce (12) personas se encargan del manejo del sistema SALUDIPS, entre ellas están médico, auxiliares de enfermería, bacteriólogo(a), psicólogo(a), facturador, auxiliar atención al usuario, regente de farmacia, odontólogo(a) y enfermeras jefe.

- Muestra:

Se tomaron ocho (8) personas a las cuales se realizó una encuesta general para obtener información relevante.

Se programaron y realizaron varias visitas para conocer los procesos que maneja la empresa y aplicar entrevistas y cuestionarios a los funcionarios que intervienen en el manejo del sistema de información SALUDIPS.

SEGUNDA ETAPA: PLANEACIÓN DE LA AUDITORIA

En esta etapa se realiza la planificación de todo el proceso de auditoría, desarrollando las siguientes actividades:

- Se identificó el alcance y los objetivos de la auditoría realizada.
- Se realizó un estudio inicial al centro de salud, para identificar la su infraestructura tecnológica y las dependencia que usan el sistema de información SALUDIPS.
- Se determinó los recursos necesarios para la realización de la auditoria.

- Se elaboró un plan de trabajo.

TERCERA ETAPA: EJECUCIÓN DE LA AUDITORIA

En esta etapa se desarrollaron las siguientes actividades para la realización de la auditoría:

- Tomando como guía el modelo COBIT, se realizó un plan de auditoria para así poder identificar los procesos y objetivos de control evaluados.
- Se elaboró cuadros de definición de fuentes de conocimiento para que fueran una fuente clara en la obtención de pruebas.
- Se aplicaron entrevistas que incluyen preguntas abiertas y cerradas para obtener información del manejo y conocimiento de la infraestructura tecnológica y el sistema de información SALUDIPS. También se realizaron cuestionarios de tipo cuantitativo para cada uno de los procesos que se seleccionaron dentro de los dominios del COBIT a auditar.
- Se identificaron los hallazgos presentes en el área auditada.
- Con la identificación de hallazgos, se asignó la probabilidad de ocurrencia e impacto para los riesgos encontrados.
- Se elaboró una matriz de probabilidad e impacto, la cual permitió identificar que riesgos necesitan mitigarse y establecer una serie de controles para tal fin.

CUARTA ETAPA: DICTAMEN FINAL DE LA AUDITORIA

En esta etapa se realizó un informe final en donde se encuentra los procesos evaluados y se dan a conocer todos los hallazgos encontrados con sus respectivas recomendaciones y controles establecidos para así poder solventarlos o reducir su impacto en lo posible.

Este informe se presentó y se entregó al Gerente del CENTRO DE SALUD SAN MIGUEL ARCANGEL E.S.E del Municipio de Ospina, para que se tomen las observaciones y hallazgos evidenciados en los resultados de la auditoria para la ejecución de las respectivas correcciones a implantar mediante un plan de mejoramiento.

2.2 ARCHIVO PERMANENTE

El archivo permanente reúne los documentos de la empresa, tales como: normas, reglamentos, disposiciones, procedimientos, manuales, entre otros, que no son susceptibles de cambio frecuente, que constituyen fuente de consulta en posteriores auditorías. Estos archivos que se usarán continuamente son útiles para la comprobación y también en ejercicios futuros; sus datos se refieren normalmente al pasado, al presente y al futuro. Este archivo debe suministrar al

equipo auditor la información sobre la entidad con el fin de llevar una auditoria eficaz y objetiva.

2.2.1 Leyes y decretos comunes:

- Decreto 4747 de 2008: establece que todas las IPS deben contar con un modelo de atención que garanticen la forma de prestación de servicios de salud de tal manera que garanticen calidad y oportunidad a los usuarios, pertinencia y seguridad a la empresa de tal manera que brinden satisfacción al usuario.[13]

- Ley 715 de 2001, de acuerdo con las responsabilidades adquiridas por la nación y entes departamentales les corresponde según la Ley 715 de 2001 al Ministerio de salud y seguridad social, secretarias departamentales, distritales y municipales de salud, dar asesoramiento, capacitación y asistencia técnica en lo referente al mejoramiento continuo para la prestación de servicios de salud por parte de las E.S.E.[14]

- Ley 1438 de 2011, la E.S.E Centro de Salud San Miguel Arcángel del municipio de Ospina, ampliará y mejorara sus condiciones de habilitación, como cumplimiento para una adecuada prestación de servicios de que le permitan cumplir con los requisitos necesarios para conformar la red integrada de prestadores de servicios de salud que conjuntamente con los municipios de Túquerres, Guaitarilla, Sapuyes, Guachavez, según disposición de la ley 1438 de 2011 se organice la prestación de servicios de salud y la conformación de cooperativas de instituciones hospitalarias para el suministro de medicamentos, e insumos médico quirúrgicos útiles para la prestación de servicios, dotando el Centro de Salud San Miguel Arcángel de elementos, equipos y recurso humano necesario para el desarrollo de actividades asistenciales de primer nivel de atención como odontología, medicina, enfermería y farmacia; que en futuro busquen la permanencia de estos servicios cumpliendo con las políticas nacionales de la prestación de servicios en salud como son accesibilidad, oportunidad y calidad.[15]

- Decreto 139 de 1996, el cual consagra que entre las funciones de los gerentes de las empresas sociales del estado de primer nivel de atención, desarrollar planes, programas y proyectos de salud conforme a la realidad

[13] Tomado del "Modelo de Prestación de Servicios". Centro de Salud San Miguel Arcángel E.S.E. Pág. 3
[14] Ibíd.
[15] Ibíd.

socioeconómica y cultural de la región y planear, organizar y evaluar las actividades de la entidad.[16]

- Ley 100 de 1993 Por medio de la cual se crea el sistema de seguridad social en salud en Colombia.[15]

2.2.2 Reseña histórica: [17]

- El Centro de Salud del municipio de Ospina en cumplimiento de la resolución 1043 del 2006 se inscribe en el registro especial de prestadores de servicios de salud con el código 52-683-006-9001. El único prestador público de servicios de salud en el municipio cuenta actualmente con tres puestos de salud en el corregimiento de San Miguel, San Isidro y Cunchila, contando además con un equipo extramural que se desplaza a través de la unidad médico odontológica hacia los diferentes corregimientos y veredas que conforman el área rural.

- El Centro de Salud San Miguel Arcángel, se encuentra ubicado a 18 minutos de Túquerres, lo que le permitiría conformar la red integrada de entidades prestadoras de servicios de salud públicas, mixtas o privadas, según la ley 1438 de 2011.

- En virtud de la ley 100 de 1993, por la cual se crea el sistema general de seguridad social en salud todas las IPS se deben transformar en EMPRESAS SOCIALES DEL ESTADO, acatando la normatividad el honorable Consejo de Ospina mediante acuerdo No. 035 del 28 de octubre de 1998, por medio del cual se transforma el centro de salud San Miguel Arcángel como empresa social del estado E.S.E. del orden municipal y en este mismo año se da el proceso de descentralización de la Empresa.

2.2.3 Descripción:

- NOMBRE DE LA INSTITUCIÓN: CENTRO DE SALUD SAN MIGUEL ARCANGEL OSPINA EMPRESA SOCIAL DEL ESTADO – ESE
- NIT: 900126676-5 [18]
- LOCALIZACIÓN: MUNICIPIO DE OSPINA, DEPARTAMENTO DE NARIÑO
- CORREO ELECTRÓNICO: censaludospina@hotmail.com [19]

---

[16] Ibíd.

[17] Ibíd.

[18] Ibíd.

[19] Tomado de la página web: www.censaludospina.com

2.2.4 Misión. La Empresa Social del Estado (E.S.E.) CENTRO DE SALUD SAN MIGUEL ARCANGEL es una entidad pública que brinda servicios en salud del primer nivel de atención, con oportunidad, continuidad, accesibilidad y pertinencia, científica, administrativa y tecnológica, contando con talento humano capacitado, comprometido con la Institución y la comunidad, satisfaciendo oportunamente las necesidades y expectativas de nuestros usuarios[20]

2.2.5 Visión. Ser una empresa social del estado que preste servicios de salud en el primer nivel de atención, de preferencia por las aseguradoras y los usuarios, ofertando atención de excelencia, calidad, ética y gestión clínica centrada en el usuario, desarrollando proyectos que busquen el mejoramiento tecnológico, de información, del transporte asistencial y su infraestructura, alcanzando la certificación de sus procesos en la prestación de servicios en salud, que cumplan con las necesidades de la comunidad a marzo 31 de 2016.

2.2.6 Valores. La ESE Centro de Salud San Miguel Arcángel, deberá institucionalizar unos valores humanos básicos que serán el cimiento sobre el cual funcione la empresa y se interioricen en cada uno de los funcionarios para ponerlos en práctica en el desempeño de cada una de sus actividades[21]:

Respeto: con miras a garantizar los derechos universales e irrenunciables de la persona, reflejándose en el mejoramiento de la calidad de vida, el desarrollo individual, social; de conformidad con la dignidad que debe reconocerse a todo ser humano, con la observancia de las diferencias y de la aceptación tal cual como se es y se obtendrá como resultante una sana convivencia.

Responsabilidad: es la obligación de responder de los actos propios o de otro o de indemnizar por un perjuicio, en el cumplimiento de sus funciones o desempeño de las mismas. Ser responsable es acatar las sugerencias y obedecer los mandatos.

Honestidad: consiste en ser Integro, uno de los valores más universales donde acuden todos; es ser equitativo en sus actitudes, obrar con justicia y honradez y en general proceder de manera intachable.

Humanidad: pertenecen a este valor las actitudes de proceder con carácter de humano ante las demás personas, es decir sentir en sí mismo lo que le sucede al otro y a partir de esa premisa servir a los demás.

---

[20] Tomado del “Plan de Gestión”. 2012-2016. Centro de Salud San Miguel Arcángel E.S.E. Pág. 6

[21] Ibíd.

Sociabilidad: poseer una extremada forma de tratar a las personas; ser sociable quiere decir tener una inclinación a convivir en sociedad lo que permite al ser humano mantenerse en armonía y constante dialogo para lograr mejores cosas de servicio general.

2.2.7 Principios. Teniendo en cuenta que un principio es el camino y fundamento sobre los cuales se apoya una actividad, una gestión, una actitud y el don de gentes en los individuos la ESE del municipio de Ospina tendrá como principios fundamentales a nivel de Institución los siguientes[22]:

- Universalidad: atención en salud para todos los habitantes del municipio de Ospina sin ninguna discriminación por creencias, en lo político y en lo social.
- Solidaridad: ampliar la cobertura de sus servicios hacia los lugares de difícil acceso en la zona rural del municipio de Ospina; con el fin de ser justos y equitativos.
- Integralidad: brindar atención continua y oportuna a las familias e individuos dentro de su contexto biopsicosocial.
- Eficiencia: buscar y mejorar la utilización de los recursos humanos, tecnológicos y financieros que optimicen la prestación de los servicios en salud.
- Calidad: brindar servicios agregados al paciente para mantener su fidelidad a la Institución y su satisfacción.
- Equidad: brindar los servicios en salud sin discriminación y dependiendo de la necesidad en salud que presente el usuario.
- Compromiso social: contribuir con el bienestar físico, social y mental de la comunidad del municipio de Ospina.

2.2.8 Políticas:[23]

- Trabajar en valores y principios: será política de la empresa capacitar a sus trabajadores inculcando los principio y valores institucionales para que sean aplicados y desarrollados en el desempeño de sus funciones dirigidas a los usuarios siendo tratados éstos como personas dignas, y por lo tanto, ganarnos los conceptos y las opiniones de la ciudadanía en relación a la prestación de los servicios en salud.
- Funcionamiento de la empresa: garantizar el eficiente funcionamiento de la ESE de acuerdo a la adecuada utilización del presupuesto aprobado anualmente por la Junta Directiva.

[22] Ibíd.

[23] Ibíd.

- Educación al usuario: desplegar una persistente educación y formación con relación a los usuarios de la ESE para el fomento, promoción y la prevención de la enfermedad; utilizando los medios masivos de comunicación existentes en la localidad; para que lleguen con claridad a todos los hogares del municipio de Ospina.
- Contratación o proveedores: la empresa social del estado de manera cuidadosa, justa y honrada contratara a sus proveedores para la presentación de sus propuestas públicamente ya sea por escrito u otros medios de comunicación; con el fin de escoger la alternativa más conveniente para la institución.
- Prestación de servicios: será una política relevante y eficiente la prestación de sus servicios médicos a los afiliados al régimen contributivo, subsidiado y particular, fijándonos la meta de un ciento por ciento a fin de satisfacer las expectativas de esta clase de usuarios.
- Programas de capacitación: de manera urgente implementar proyectos y mecanismos de educación y capacitación al talento humano existente en la empresa; con el fin de formar un equipo de trabajo eficiente, con ética, moral, principios y valores que dejen en alto grado la imagen de la ESE Centro de Salud San Miguel Arcángel del municipio de Ospina.

2.2.9 Red de servicios. La E.S.E Centro de Salud San Miguel Arcángel del municipio de Ospina, ampliará y mejorara sus condiciones de habilitación, como cumplimiento para una adecuada prestación de servicios que le permitan cumplir con los requisitos necesarios para conformar la red integrada de prestadores de servicios de salud que conjuntamente con los municipios de Tuquerres, Guaitarilla, Sapuyes, Guachavez, según disposición de la ley 1438 de 2011 se organice la prestación de servicios de salud y la conformación de cooperativas de instituciones hospitalarias para el suministro de medicamentos, e insumos médico quirúrgicos útiles para la prestación de servicios, dotando el Centro de Salud San Miguel Arcángel de elementos, equipos y recurso humano necesario para el desarrollo de actividades asistenciales de primer nivel de atención como odontología, medicina, enfermería y farmacia; que en futuro busquen la permanencia de estos servicios cumpliendo con las políticas nacionales de la prestación de servicios en salud como son accesibilidad, oportunidad y calidad[24].

2.2.10 Organización de la empresa. La organización de las empresas sociales del estado se establece a partir de las siguientes unidades funcionales para el logro de sus objetivos misionales.

[24] Tomado del “Plan de Gestión”. 2012-2016. Centro de Salud San Miguel Arcángel E.S.E. Pág. 9

Área funcional de dirección: conformada por la junta directiva y el gerente la cual está encargada de procesos destinados a dirigir, orientar y tomar decisiones en la empresa en función del cumplimiento de la misión y objetivos corporativos. El proceso básico de esta área consiste en dirigir y conducir la institución para la toma de decisiones efectivas, tanto estratégicas como tácticas traducidas en acciones orientadas a la prestación de servicios de salud con calidad, eficiencia y efectividad. El área funcional de dirección corporativa será responsable de identificar las necesidades esenciales y las expectativas de los usuarios, determinar los mercados a atender, definir las estrategias del servicio, organizar y asignar recursos adoptando normas de eficiencia y calidad, controlando su aplicación en la gestión institucional dentro del marco jurídico vigente.

Área funcional de atención al usuario: encargada del proceso de producción y prestación del servicio de salud con sus respectivos procedimientos y actividades incluyendo la atención administrativa demandada por el usuario. El área de atención al usuario se encarga de suministrar al cliente los servicios que requiere respondiendo a las necesidades específicas de salud mediante las actividades de recepción, clasificación, pre consulta, prestación de servicios, post consulta, todo ello en condiciones de accesibilidad, oportunidad y pertinencia en la atención al usuario. Su desarrollo debe enfocarse en mejorar la calidad de la atención satisfaciendo las necesidades y expectativas del usuario[24].

El área de atención al usuario incluye las siguientes unidades funcionales.

- Unidad de consulta externa
- Unidad de urgencias
- Unidad de promoción y prevención
- Unidad de atención al usuario
- Unidad médico-odontológica para servicio extramural

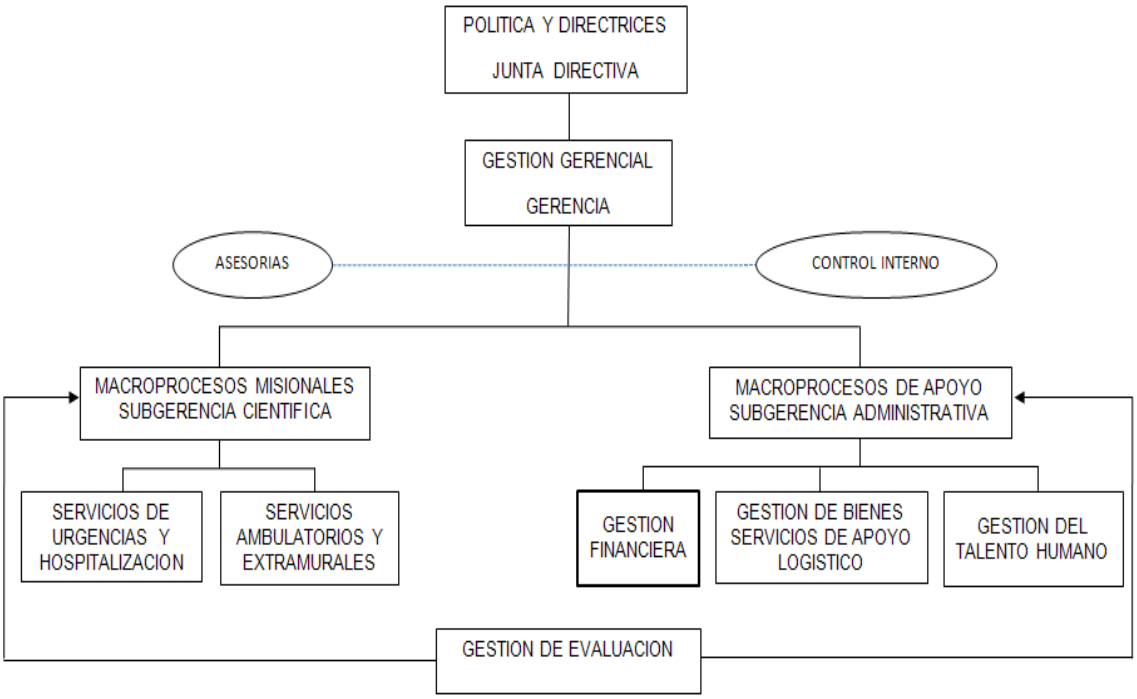
Área funcional de apoyo logístico: encargada de ejecutar en coordinación con las demás aéreas los procesos de planeación, adquisición, manejo, utilización, optimización y control de los recursos humanos, financieros, físicos y de información necesarios para alcanzar y desarrollar los objetivos de la empresa y mantenimiento de la planta física y su dotación. El desarrollo de esta área se orienta a perfeccionar y modernizar la estructura física de la institución de manera que garantice condiciones de seguridad para los clientes internos y externos[25].

- Área de Almacén
- Mantenimiento hospitalario
- Área de farmacia
- Área de servicios generales (Ver figura 1)

[25] Tomado del “Plan de Gestión”. 2012-2016. Centro de Salud San Miguel Arcángel E.S.E. Pág. 11

Organigrama:

Figura 1. Organigrama CSSMA E.S.E Ospina



Fuente: Plan de Gestión. 2012-2016. CSSMA E.S.E. Pág.12

2.3 ARCHIVO CORRIENTE

En este proceso de auditoria se recopila toda la información obtenida durante el desarrollo del trabajo de campo: las pruebas, análisis, gráficos, cuestionarios, entrevistas, documentos de la empresa y los procedimientos utilizados, los cuales en su conjunto constituyen la evidencia del examen de una unidad auditable. Con esta información se puede obtener un conocimiento más amplio de la empresa y abordar una auditoria mejor diseñada y exacta en la entidad.

2.3.1 Memorando de planeación de auditoria:

Objetivo general. Evaluar la infraestructura tecnológica del Centro de Salud San Miguel Arcángel E.S.E que soporta al sistema de información SALUDIPS, con el fin de garantizar efectividad, disponibilidad y calidad de la información y sugerir a la entidad planes de mejora que ofrezcan continuidad en sus servicios de salud.

Alcance. Para el desarrollo de este trabajo se analizó el hardware y software que conforman la infraestructura tecnológica del Centro de Salud San Miguel Arcángel E.S.E la cual soporta el sistema de información SALUDIPS, tomando como guía el estándar COBIT su metodología y procedimientos se evaluó todos sus elementos comprobando su correcto funcionamiento.

Los componentes que se evaluaron fueron:

- Hardware: servidores, equipos de cómputo, red estructurada de datos, elementos de comunicación, elementos de protección y red eléctrica.
- Software: sistemas operativos, software de sistemas y software de seguridad.

De los componentes anteriormente mencionados se evaluaron las condiciones, funcionamiento, disponibilidad, confiabilidad, seguridad, existencia de planos, licencias y planes de contingencia.

Además se evaluó el manejo adecuado por parte de los usuarios de la infraestructura tecnológica.

Metodología:

Para la recopilación de la información se utilizaron diferentes métodos:

Visitas:

- Instalaciones físicas al Centro de Salud San Miguel Arcángel E.S.E.
- Diferentes dependencias o áreas de trabajo que manejan el sistema de información SALUDIPS.

Entrevistas:

- Funcionarios Encargados de manejo del sistema de información SALUDIPS (psicóloga, regente de farmacia, auxiliar atención al usuario, auxiliar de enfermería).
- Encargado del mantenimiento técnico preventivo y correctivo de equipos de cómputo del centro de salud: José Fernando Argoty Erazo.

Encuestas:

- Encuesta general a funcionarios encargados del manejo del sistema de información SALUDIPS. (facturación, psicología, laboratorio, farmacia, atención al usuario, consultorio médico, urgencias y enfermería)

Formularios:

- Cuadros de definición aplicados a la auditoria
- Cuestionarios Cuantitativos
- Cuestionarios Cualitativos
- Evaluación Infraestructura Tecnológica
- Valoración de Riesgos
- Matriz de Probabilidad e Impacto
- Tabla de Hallazgos

2.3.2 Programa de auditoria. Para la realización del proceso de auditoría a la Infraestructura Tecnológica del sistema de información SALUDIPS del Centro de Salud San Miguel Arcángel E.S.E. se utilizó la metodología COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas), y se evaluó algunos objetivos de control que se encuentran dentro de los dominios de esta metodología de la siguiente manera:

Dominio: planeación y organización (Po). Encargado de definir las estrategias y tácticas de las Tecnologías de la Información que permitan contribuir al logro y cumplimiento de los objetivos empresariales, a través del uso óptimo y conocimiento de los recursos de TI, apropiados para las necesidades de la empresa. En el desarrollo de esta auditoria se aplican los siguientes procesos:

PO3 Determinar la dirección tecnológica. Contar con recursos y capacidades que satisfagan requerimientos de negocio actuales y futuros enfocándose en la definición e implantación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas.

PO3.1 Planeación de la dirección tecnológica. Se analiza las tecnologías existentes en la empresa y se planea que dirección tecnológica es apropiada para tomar. La planeación debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.

PO3.2 Plan de infraestructura tecnológica. Verificar la existencia de un plan de infraestructura tecnológica. Evaluar planes de contingencia, evaluar procesos de adquisición y la evolución de los recursos tecnológicos.

PO3.3 Monitoreo de tendencias y regulaciones futuras. Establecer un proceso para monitorear las tendencias ambientales de la empresa, tecnológicas, de infraestructura, legales y regulatorias. Incluir las consecuencias de estas tendencias en el desarrollo del plan de infraestructura tecnológica de TI.

PO3.4 Estándares tecnológicos. Evaluar si existen asesorías sobre funcionamiento de la infraestructura. Verificar si existen guías para la selección de la infraestructura, medir el cumplimiento de estándares y directrices.

PO5 Administrar la inversión en TI. Mejorar de forma continua y demostrable la rentabilidad de TI y su contribución a la rentabilidad del negocio con servicios integrados y estandarizados que satisfagan las expectativas del usuario enfocándose en decisiones de portafolio e inversión en TI efectivas y eficientes, y por medio del establecimiento y seguimiento del presupuestos de TI de acuerdo a la estrategia de TI y a las decisiones de inversión.

PO5.1 Marco de trabajo para la administración financiera. Establecer y mantener un marco de trabajo financiero para administrar las inversiones y el costo de los activos y servicios de TI a través de los portafolios de inversiones habilitadas por TI, casos de negocio y presupuestos de TI.

PO5.2 Prioridades dentro del presupuesto de TI. Implementar un proceso de toma de decisiones para dar prioridades a la asignación de recursos a TI para operaciones, proyectos y mantenimiento, para maximizar la contribución de TI a optimizar el retorno del portafolio empresarial de programas de inversión en TI y otros servicios y activos de TI.

PO5.3 Proceso presupuestal. Establecer un proceso para elaborar y administrar un presupuesto que refleje las prioridades establecidas en el portafolio empresarial de programas de inversión en TI, incluyendo los costos recurrentes de operar y mantener la infraestructura actual.

P09. Evaluar y administrar los riesgos de T.I. Analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de negocio enfocándose en la elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales.

PO9.1 Marco de trabajo de administración de riesgos. Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.

PO9.2 Establecimiento del contexto del riesgo. Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.

PO9.3 Identificación de eventos. Identificar eventos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto

potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto y mantener esta información. Registrar y mantener los riesgos relevantes en un registro de riesgos.

PO9.4 Evaluación de riesgos de TI. Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

PO9.5 Respuesta a los riesgos. Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que controles efectivos en costo mitigan la exposición en forma continua. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.

PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos. Priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

2.3.2.2 Dominio: adquirir e implementar (AI): Identificar estrategias, desarrollarlas o adquirirlas con el fin de proporcionar soluciones y controles apropiados garantizar el cumplimiento de los objetivos de la entidad. De este dominio se aplicaran las siguientes actividades:

AI3 Adquirir y mantener infraestructura tecnológica. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y la configuración en sí de acuerdo a los estándares. Esto permite a las organizaciones apoyar la operatividad del negocio de forma apropiada con las aplicaciones automatizadas correctas.

AI3.1 Plan de adquisición de infraestructura tecnológica. Generar un plan para adquirir, Implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología.

AI3.2 Protección y disponibilidad del recurso de infraestructura. Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para

proteger los recursos y garantizar su disponibilidad e integridad. Se debe monitorear y evaluar su uso.

AI3.3 Mantenimiento de la infraestructura. Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

AI5 Adquirir recursos de TI. Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí.

AI5.1 Control de adquisición. Desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición para adquirir infraestructura relacionada con TI, instalaciones, hardware, software y servicios necesarios por el negocio.

AI5.2 Administración de contratos con proveedores. Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores. El procedimiento debe cubrir, como mínimo, responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad, de propiedad intelectual y responsabilidades de conclusión, así como obligaciones (que incluyan cláusulas de penalización). Todos los contratos y las modificaciones a contratos las deben revisar asesores legales.

AI5.3 Selección de proveedores. Seleccionar proveedores de acuerdo a una práctica justa y formal para garantizar la mejor viable y encajable según los requerimientos especificados. Los requerimientos deben estar optimizados con las entradas de los proveedores potenciales.

AI5.4 Adquisición de recursos de TI. Proteger y hacer cumplir los intereses de la organización en todo los contratos de adquisiciones, incluyendo los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de software, recursos de desarrollo, infraestructura y servicios.

2.3.2.3 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.

DS5 Garantizar la seguridad de los sistemas. Evaluar procesos de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.

DS5.2 Plan de seguridad de TI. Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la 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. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única. Permitir que el usuario se identifique a través de mecanismos de autenticación. Confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio 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 del usuario. Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. 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.

DS5.9 Prevención, detección y corrección de software malicioso. Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correo basura).

DS12 Administración del ambiente físico. La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico.

DS12.1 Selección y diseño del centro de datos. Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.

DS12.2 Medidas de seguridad física. Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.

DS12.3 Acceso físico. Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.

DS12.4 Protección contra factores ambientales. Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente.

DS12.5 Administración de instalaciones físicas. Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud.

DS13 Administración de operaciones. Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI.

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. Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.

2.3.2.4 Dominio: monitorear y evaluar (Me). Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

ME2 Monitorear y evaluar el control interno. Establecer un programa de control interno efectivo para TI requiere un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.

ME2.1 Monitoreo del marco de trabajo de control interno. Monitorear de forma continua, comparar y mejorar el ambiente de control de TI y el marco de trabajo de control de TI para satisfacer los objetivos organizacionales.

ME2.6 Control interno para terceros. Evaluar el estado de los controles internos de los proveedores de servicios externos. Confirmar que los proveedores de servicios externos cumplen con los requerimientos legales y regulatorios y obligaciones contractuales.

ME2.7 Acciones correctivas. Identificar, iniciar, rastrear e implementar acciones correctivas derivadas de los controles de evaluación y los informes.

2.3.3 Proceso de recolección de información y planteamiento de actividades:

Para el desarrollo de este trabajo de auditoria a la Infraestructura Tecnológica del sistema de información SALUDIPS en el centro de salud San Miguel Arcángel E.S.E del Municipio de Ospina, se realizaron visitas al sitio y se utilizó el método

de observación directa para analizar y poder evaluar la infraestructura tecnológica que posee la empresa. Además, se realizaron entrevistas al encargado del mantenimiento preventivo y correctivo de los equipos de cómputo, entrevistas y encuestas a encargados del manejo del SALUDIPS y análisis de documentos e información solicitada a la entidad. Esto con el fin de obtener un dictamen sobre posibles factores que afecten a la integridad, disponibilidad y calidad de la información y proponer recomendaciones que mitiguen los riesgos existentes.

Para el proceso de recolección de la información se utilizaron los siguientes formatos:

Los cuadros de definición: contienen el logo de la Entidad auditada y los ítems relacionados como son:

REF: identificación del cuadro de Definición.

ENTIDAD AUDITADA: nombre de la entidad a la cual se le está realizando el proceso de auditoría.

OBJETO DE ESTUDIO: identificación de la parte a evaluar

RESPONSABLES: nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

MATERIAL DE SOPORTE: nombre del modelo tomado en la aplicación de la auditoria, en este caso COBIT.

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

PROCESO: nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: se describe el objetivo del proceso del dominio del COBIT a aplicar.

FUENTES DE CONOCIMIENTO: en este espacio se deberá consignar todas las fuentes de donde se extrajo la información para el proceso de auditoria lo que servirá como respaldo del proceso.

REPOSITORIO DE PRUEBAS: se divide en dos tipos de pruebas:

DE ANÁLISIS: describir las pruebas de análisis que se van a realizar para evaluar el proceso especifico que se encuentre en estudio. (Ver tabla 1)

DE EJECUCIÓN: describir las acciones a realizar para la ejecución de la auditoria, como las revisiones, verificaciones, pruebas y obtención de inconsistencias, etc.

Tabla 1. Formato cuadro de definición de fuentes de conocimiento

	CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS Y PRUEBAS DE AUDITORIA			**REF**	
				PLAN	
ENTIDAD AUDITADA				**PÁGINA**	
					DE
OBJETO DE ESTUDIO					
RESPONSABLES					
MATERIAL DE SOPORTE					
DOMINIO		**PROCESO**			
DESCRIPCION DE ACTIVIDAD/PRUEBA					
FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**				
	DE ANALISIS		**DE EJECUCION**		

Cuestionario cuantitativo: permite definir preguntas tomando como base el cuadro de definición de fuente de conocimiento. El cuestionario presenta tres opciones de respuesta (SI, NO, NA (No Aplica)), permitiendo así calificar el proceso entre 1 a 5, donde 1 es un nivel insignificante y 5 un nivel crítico, teniendo en cuenta el nivel de importancia de la pregunta, bajo criterio de los auditores, la sumatoria del puntaje de las preguntas da el total de la encuesta, se califica las columnas del SI, las del NO y las NA, sumando el puntaje de las preguntas. La fuente permite identificar los responsables bien sea una determinada persona o cualquier medio del cual se tomó la información para calificar.

Los ítems que se encuentran en este formato, son:

REF: identificación del cuadro de Definición.

ENTIDAD AUDITADA: nombre de la entidad a la cual se le está realizando el proceso de auditoría.

OBJETO DE ESTUDIO: identificación de la parte a evaluar

RESPONSABLES: nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

MATERIAL DE SOPORTE: nombre del modelo tomado en la aplicación de la auditoria, en este caso COBIT.

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

PROCESO: nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

PREGUNTA: listado de preguntas que serán evaluadas.

SI, NO Y NA: posibilidades de respuestas, Cumple, No cumple o No Aplica para la entidad.

FUENTE: de donde se obtiene la información

TOTAL: se asigna los valores correspondientes a cada columna, la sumatoria de los SI, de los NO y NA.

TOTAL CUESTIONARIO: la suma de los campos de las opciones.

PORCENTAJE DE RIESGO: determina el nivel de riesgo total (Riesgo Bajo, Medio o Alto)

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:

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

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.

El resultado obtenido, permitió formular conclusiones acerca de funcionamiento del proceso evaluado, teniendo en cuenta que este toma validez con la obtención de pruebas, que verifique los resultados de la encuesta. Para ello se utilizó el siguiente formato: (Ver tabla 1)

Tabla 2. Formato de cuestionario cuantitativo

	CUESTIONARIO CUANTITATIVO				**REF**
Entidad Auditada	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina				**PÁGINA** **DE**
Objeto de Estudio					
Responsables					
Material de Soporte					
Dominio		**Proceso**			
Pregunta		**SI**	**NO**	**NA**	**OBSERVACIÓN**
Total					
Total Cuestionario					

Entrevistas preguntas abiertas y preguntas cerradas: es una técnica utilizada para recolectar información amplia que permita aclarar dudas que dejan los cuestionarios. Los formatos utilizados para la realización estas entrevistas están ajustados al personal de las dependencias que manejan el sistema de información SALUDIPS y al personal técnico encargado del mantenimiento preventivo y correctivo de equipos de cómputo.

Para la recolección de la información realizaron dos tipos de entrevistas:

Entrevistas con preguntas abiertas: donde la persona entrevistada puede expresar libremente su respuesta y de forma detallada permitiendo hacer preguntas adicionales según vaya respondiendo cada una.

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

Formatos presentados en las dos siguientes páginas, (tabla 3 y 4):

Tabla 3. Formato entrevista I

Tipo de Registro: Entrevista I			
Entidad Auditada	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		N° Guía
Responsables		**Objeto de estudio**	Infraestructura tecnológica
Objetivo			
Respondido por		**Cargo**	
R/PT			
Fecha			
N°	**Pregunta**		

2.3.4 Cuadros de definición de fuentes de conocimiento. De acuerdo con el análisis del COBIT se aplican los procesos y de acuerdo con el tipo de auditoría que se está aplicando la infraestructura tecnológica del sistema de información SALUDIPS, se describen los cuadros de definición de la siguiente manera (tabla 4-13):

Tabla 4. Cuadro de definición de fuentes de conocimiento PO3-1

	CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS Y PRUEBAS DE AUDITORIA			**REF** PLAN PO3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina			**PÁGINA 1 DE 2**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS			
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro			
MATERIAL DE SOPORTE	COBIT 4.1			
DOMINIO	Planeación y organización (PO)	**PROCESO**	Determinar la dirección tecnológica (PO3)	
DESCRIPCION DE ACTIVIDAD/PRUEBA	Analizar y evaluar aspectos tales como dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias, con el fin de que la entidad aproveche al máximo sus recursos tecnológicos.			
FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**			
	DE ANALISIS		**DE EJECUCION**	
• Entrevista al encargado del mantenimiento preventivo y correctivo de equipos de cómputo. • Manual de mantenimiento preventivo y correctivo.	• Analizar entrevista del encargado del mantenimiento preventivo y correctivo de equipos de cómputo. • Analizar manual de mantenimiento preventivo y correctivo.		• Revisión detallada de los manuales de mantenimiento y procedimientos. • Revisión detallada de la arquitectura de red de políticas y aplicación de normas.	

Tabla 5. Cuadro de definición de fuentes de conocimiento PO3-2

	CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS Y PRUEBAS DE AUDITORIA			**REF**	
				PLAN PO3	
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina			**PÁGINA**	
				2	**DE** **2**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS				
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro				
MATERIAL DE SOPORTE	COBIT 4.1				
DOMINIO	Planeación y organización (PO)	**PROCESO**	Determinar la dirección tecnológica (PO3)		
DESCRIPCION DE ACTIVIDAD/PRUEBA	Conocer y evaluar aspectos tales como dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias, con el fin de que la entidad aproveche al máximo sus recursos tecnológicos.				
FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**				
	DE ANALISIS		**DE EJECUCION**		
• Manual de procesos y procedimientos. • Plan de infraestructura tecnológica. • Arquitectura de red. • Soluciones tecnológicas. • Instructivo planes de contingencia hardware y software.	• Analizar el manual de procesos y procedimientos de gestión de la información. • Analizar el plan de infraestructura tecnológica. • Analizar arquitectura de red (diagramas, infraestructura, tipos de red, tipología de red). • Analizar soluciones tecnológicas existentes en la empresa.		• Revisión detallada de planes de contingencia para hardware y software y el conocimiento de estos por parte del personal. • Revisión detallada del plan de infraestructura tecnológica. • Revisar soluciones tecnológicas.		

Tabla 6. Cuadro de definición de fuentes de conocimiento PO5

	CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS Y PRUEBAS DE AUDITORIA		**REF** PLAN PO5
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		**PÁGINA** **1** **1**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Planeación y organización (PO)	**PROCESO**	Administrar la Inversión en TI. (PO5)
DESCRIPCION DE ACTIVIDAD/PRUEBA	Mantener un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios, prioridades dentro del presupuesto, un proceso presupuestal formal y administración contra ese presupuesto.		

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANALISIS	**DE EJECUCIÓN**
• Entrevista al encargado del mantenimiento preventivo y correctivo de equipos de cómputo. • Manual de procesos y procedimientos. • Plan de inversión de infraestructura tecnológica.	• Analizar programas de inversión en hardware y software. • Analizar prioridades de inversión en TI. • Analizar si existen procesos y procedimientos de inversión en infraestructura tecnológica. • Analizar plan de inversión de infraestructura tecnológica.	• Revisión detallada de planes de inversión. • Revisión de prioridades en el presupuesto de inversiones. • Revisión detallada de procesos y procedimientos para la inversión en TI. • Revisión del plan de inversión tecnológica.

Tabla 7. Cuadro de definición de fuentes de conocimiento PO9

	CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS Y PRUEBAS DE AUDITORIA		**REF** PLAN PO9
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		**PÁGINA** **1** **1**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Planeación y organización (PO)	**PROCESO**	Administrar los recursos humanos de TI (PO9)
DESCRIPCION DE ACTIVIDAD/PRUEBA	Análisis del marco de trabajo de administración de riesgos dirigido a la evaluación de la infraestructura tecnológica del sistema de información SALUDIPS.		
FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**		
	DE ANALISIS		**DE EJECUCIÓN**
• Plan de contingencias del hardware y software. • Documentos de evaluación del riesgo.	• Análisis de los documentos de evaluación del riesgo del hardware y software que componen la infraestructura tecnológica que maneja el sistema de información SALUDIPS.		• Revisión de los planes de contingencia. • Revisar documentación de evaluación del riesgo.

Tabla 8. Cuadro de definición de fuentes de conocimiento AI3

	CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS Y PRUEBAS DE AUDITORIA		**REF** PLAN AI3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		**PÁGINA** **1** **1**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Adquirir e Implementar (AI)	**PROCESO**	Adquirí y Mantener Infraestructura Tecnológica. (AI3)
DESCRIPCION DE ACTIVIDAD/PRUEBA	La empresa debe contar con un plan operativo donde garantice el buen funcionamiento, mantenimiento y cumplimiento de los estándares de la infraestructura tecnológica para dar soporte a los diferentes procesos dentro de la empresa.		

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANALISIS	**DE EJECUCIÓN**
• Entrevista al encargado del mantenimiento preventivo y correctivo de equipos de cómputo. • Plan de adquisición de infraestructura tecnológica. • Roles y responsabilidades del personal encargado de realiza el mantenimiento a la infraestructura tecnológica. • Plan de mantenimiento preventivo y correctivo.	• Analizar políticas y aplicación de normas relacionadas con la adquisición de la infraestructura tecnológica. • Analizar plan de adquisición de infraestructura tecnológica. • Análisis del plan de mantenimiento preventivo y correctivo.	• Verificar existencia de planes de adquisición de infraestructura tecnológica y si la empresa tiene estipulado políticas y normas. • Comparar los roles con los roles asignados en la empresa del personal que realiza los mantenimientos y sus responsabilidades.

Tabla 9. Cuadro de definición de fuentes de conocimiento AI5

	CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS Y PRUEBAS DE AUDITORIA		**REF** PLAN AI5
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		**PÁGINA** **1** **1**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Adquirir e implementar (AI).	**PROCESO**	Adquirir recursos de TI. (AI5)
DESCRIPCION DE ACTIVIDAD/PRUEBA	Suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí.		

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANALISIS	**DE EJECUCIÓN**
• Entrevista al encargado del mantenimiento preventivo y correctivo de equipos de cómputo. • Documentos de políticas y normas para la adquisición de nueva infraestructura tecnológica. • Documentos de selección de proveedores. • Manual de procesos y procedimientos de gestión de la información.	• Analizar que procedimiento se siguen para autorizar adquisición de hardware y software en la empresa. • Analizar las políticas, normas y procedimientos de adquisición de hardware y software. • Analizar cómo se realiza la selección de proveedores.	• Revisión detallada de los procedimientos en la adquisición de nueva infraestructura tecnológica. • Revisión detallada de política y normas en la adquisición de infraestructura tecnológica. • Revisión detallada del procedimiento de selección de proveedores.

Tabla 10. Cuadro de definición de fuentes de conocimiento DS5

	CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS Y PRUEBAS DE AUDITORIA		**REF** PLAN DS5
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		**PÁGINA** **1** **1**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte (DS).	**PROCESO**	Garantizar la seguridad de los sistemas(DS5)
DESCRIPCION DE ACTIVIDAD/PRUEBA	Analizar los procesos de integridad de la información y protección de activos de TI y los procesos de administración de seguridad.		

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANALISIS	**DE EJECUCIÓN**
• Entrevista al encargado del mantenimiento preventivo y correctivo de equipos de cómputo. • Entrevistas y encuestas realizadas a funcionarios encargados del manejo del sistema SALUDIPS. • Manual de procesos y procedimientos de gestión de la información. • Instalaciones físicas por dependencia.	• Verificar políticas de seguridad de la infraestructura tecnológica. • Verificar existencia de cuentas de usuario. • Analizar procedimientos para monitorear incidentes de seguridad reales y potenciales. • Analizar procesos y procedimientos realizados par copias de seguridad de datos. • Analizar procesos de corrección de errores contra virus informáticos.	• Mediante observación directa verificar seguridad de la infraestructura tecnológica. • Mediante observación directa verificar la autenticación de los usuarios. • Revisión detallada del manual de procesos y procedimientos de gestión informática. • Mediante observación directa comprobar nivel de protección contra virus.

Tabla 11. Cuadro de definición de fuentes de conocimiento DS12

	CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS Y PRUEBAS DE AUDITORIA		**REF** PLAN DS12
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		**PÁGINA** **1** **1**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte (DS).	**PROCESO**	Administración del ambiente físico. (DS12)
DESCRIPCION DE ACTIVIDAD/PRUEBA	Se encarga de mantener un ambiente físico adecuado para protección de equipo de cómputo y del personal. Define los requerimientos para acceso físico y protección contra factores ambientales.		

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANALISIS	**DE EJECUCIÓN**
• Entrevista al personal encargado al acceso físico a las instalaciones. • Políticas y procedimientos para controlar el acceso físico a las instalaciones. • Políticas y procedimientos para protección de factores ambientales.	• Verificar existencia de procesos de seguridad a los activos de TI. • Verificar el acceso a áreas donde se encuentran servidores, computadores, red de datos. • Verificar si la infraestructura tecnológica opera según las especificaciones técnicas de la empresa (red eléctrica, red de datos, servidores, computadores, sistemas operativos)	• Mediante observación directa comprobar la efectividad de los procesos de acceso físico a la infraestructura tecnológica. -Acceso físico al edificio. -Red de datos -Servidores -Equipos de comunicación. -Alarmas, cámaras, extintores.

Tabla 12. Cuadro de definición de fuentes de conocimiento DS13

	CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS Y PRUEBAS DE AUDITORIA		**REF** PLAN DS13
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		**PÁGINA** **1** **1**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte (DS).	**PROCESO**	Administración de operaciones(DS13)
DESCRIPCION DE ACTIVIDAD/PRUEBA	Se encarga de evaluar la efectividad en la administración y protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware en la Institución.		

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANALISIS	**DE EJECUCIÓN**
• Entrevista al personal encargado del mantenimiento preventivo y correctivo de equipos de cómputo. • Entrevistas y encuestas personal encargado del manejo del sistema SALUDIPS • Plan de mantenimiento preventivo y correctivo.	• Verificar existencia de procesos de seguridad a los activos de TI. • Verificar el acceso a áreas donde se encuentran servidores, computadores, red de datos. • Verificar si la infraestructura tecnológica opera según las especificaciones técnicas de la empresa (red eléctrica, red de datos, servidores, computadores, sistemas operativos)	• Mediante observación directa comprobar la efectividad de los procesos de acceso físico a la infraestructura tecnológica. -Acceso físico al edificio. -Red de datos -Servidores -Equipos de comunicación. -Alarmas, cámaras, extintores. • Revisión detallada al plan de mantenimiento preventivo y correctivo.

Tabla 13. Cuadro de definición de fuentes de conocimiento ME2

	CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS Y PRUEBAS DE AUDITORIA		**REF** PLAN ME2
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		**PÁGINA** **1** **1**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Monitorear y Evaluar (ME).	**PROCESO**	Monitorear y Evaluar el control interno (ME2)
DESCRIPCION DE ACTIVIDAD/PRUEBA	Se encarga de establecer un programa de control interno efectivo para TI. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables		

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANALISIS	**DE EJECUCIÓN**
• Entrevista al personal encargado de la realizacion el control interno al Centro de Salud San Miguel Arcángel E.S.E. • Políticas y procedimientos relacionados con los procesos de monitoreo que brinden seguridad física de la infraestructura tecnológica.	• Analizar la información relacionada a la infraestructura tecnológica dentro de los procesos de control interno. • Analizar las políticas y procedimientos relacionados con los procesos de monitoreo de la infraestructura tecnológica.	• Revisión detallada de los contenidos en cuanto a infraestructura tecnológica dentro del control interno. • Revisión detallada de las políticas y procedimientos de monitoreo de la infraestructura tecnológica.

2.3.5 Cuestionarios cuantitativos. Permite definir preguntas tomando como base el cuadro de definición de fuente de conocimiento. El cuestionario presenta tres opciones de respuesta (SI, NO, NA (No Aplica)), permitiendo así calificar el proceso entre 1 a 5, donde 1 es un nivel insignificante y 5 un nivel crítico, teniendo en cuenta el nivel de importancia de la pregunta, bajo criterio de los auditores, la sumatoria del puntaje de las preguntas da el total de la encuesta, se califica las columnas del SI, las del NO y las NA, sumando el puntaje de las preguntas. La fuente permite identificar los responsables bien sea una determinada persona o cualquier medio del cual se tomó la información para calificar. Se utilizan los siguientes cuestionarios así: (Ver tabla 14-31)

Tabla 14. Cuestionario cuantitativo PO3_1

	CUESTIONARIO CUANTITATIVO			**REF** PLAN PO3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina			**PÁGINA** **1** **2**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS			
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro			
MATERIAL DE SOPORTE	COBIT 4.1			
DOMINIO	Planeación y organización (PO)	**PROCESO**		Determinar la dirección tecnológica. (PO3)

PREGUNTAS	**SI**	**NO**	**NA**	**OBSERVACIÓN**
1. ¿Existe un plan de infraestructura tecnológica?		**5**		
2. ¿Existen planes de adquisición de infraestructura tecnológica?		**5**		
3. El plan de infraestructura tecnológica contempla:				
• ¿Procesos de adquisición de recursos tecnológicos?		**4**		
• ¿Estrategias de continencias		**5**		
4. ¿Existe un inventario actualizado del hardware?				
• Servidores	**4**			
• Equipos de computo	**5**			
• Red de datos	**4**			
• Equipo de comunicaciones	**3**			
• Equipos de protección(ups, reguladores)	**4**			

Tabla 15. Cuestionario cuantitativo PO3_2

	CUESTIONARIO CUANTITATIVO				REF
					PLAN PO3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina				**PÁGINA** **2** **2**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|				
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro				
MATERIAL DE SOPORTE	COBIT 4.1				
DOMINIO	Planeación y organización (PO)	**PROCESO**			Planeación y organización (PO3)
PREGUNTAS		**SI**	**NO**	**NA**	**OBSERVACIÓN**
5. ¿Existen planes de contingencia de la infraestructura tecnológica instalada?			**4**		
6. ¿Existe planes de contingencia en el caso de que el hardware y software fallen?			**5**		
7. ¿Los planes de contingencia contemplan los pasos y procesos seguir después de una falla?			**5**		
8. ¿Existe inventario actualizado de infraestructura tecnológica?			**3**		
9. ¿Existe partes adicionales en el inventario en caso de fallas?		**5**			
10. ¿Existe hoja de vida de equipos de cómputo?		**4**			
11. ¿Existe hoja de vida de servidores?		**4**			
12. ¿Existe una persona encargada de vigilar el buen funcionamiento del hardware y software?		**4**			
TOTAL		37	36		
TOTAL CUESTIONARIO				73	

Porcentaje de riesgo = (37*100)/(73-0) =50,68%

Porcentaje riesgo total = 100-50,68%=49,32%(Riesgo Medio)

Tabla 16. Cuestionario cuantitativo PO5

	CUESTIONARIO CUANTITATIVO	REF
		PLAN PO5
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina	**PÁGINA** **1** **1**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS	
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro	
MATERIAL DE SOPORTE	COBIT 4.1	
DOMINIO	Planeación y organización (PO)	**PROCESO** Administra la Inversión en TI (PO5)

PREGUNTAS	**SI**	**NO**	**NA**	**OBSERVACIÓN**
1. ¿Existe un plan de inversión en Infraestructura tecnológica?		**5**		
2. ¿Existen prioridades dentro del presupuesto de la entidad para inversión en infraestructura tecnológica?		**4**		
3. ¿Existen proyectos de inversión en el que se contemplen activos como servidores, equipos de cómputo, equipos de comunicación, equipos de protección (reguladores, ups)?	**4**			
4. ¿Existen procesos de inversión los cuales contemplen la operación y mantención de la infraestructura tecnológica?	**4**			
5. ¿Existen personas encargadas que den prioridades en la inversión en infraestructura tecnológica?		**4**		
TOTAL	8	13		
TOTAL CUESTIONARIO			21	

Porcentaje de riesgo = (9*100)/(21-0) =42,85%

Porcentaje riesgo total = 100-42,85%=57,14%(Riesgo Alto)

Tabla 17. Cuestionario cuantitativo PO9

	CUESTIONARIO CUANTITATIVO				**REF**
					PLAN PO9
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina				**PÁGINA** **1** **1**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS				
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro				
MATERIAL DE SOPORTE	COBIT 4.1				
DOMINIO	Planeación y organización (PO)	**PROCESO**			Evaluar y Administrar los Riesgos de TI (PO9)

PREGUNTAS	**SI**	**NO**	**NA**	**OBSERVACIÓN**
1. ¿En el Centro de Salud San Miguel Arcángel existen un plan de control del riesgo aplicados a la infraestructura tecnológica de la institución?		**5**		
2. El plan contempla los siguientes aspectos:				
• ¿Importancia del riesgo?		**5**		
• ¿Riesgos relacionados con infraestructura tecnológica seguridad, disponibilidad e integridad?		**5**		
• ¿Reducción de riesgos?		**5**		
• ¿Proyectos de inversión para mitigar los riesgos?		**5**		
3. ¿Existen políticas de administración del riesgo?		**4**		
4. ¿La gerencia es informada de la importancia y cambios que generan un riesgo en la infraestructura tecnológica?	**5**			
5. ¿Existen procesos y procedimientos en análisis y gestión de riegos que contemplen la infraestructura tecnológica?		**3**		
6. ¿Existen políticas o procedimientos de adquisición de pólizas de seguros para el manejo del riesgo?		**4**		
TOTAL	5	36		
TOTAL CUESTIONARIO			41	

Porcentaje de riesgo = (5*100)/(41-0) =12,19%

Porcentaje riesgo total = 100-12,19%=87,8%(Riesgo Alto)

Tabla 18. Cuestionario cuantitativo AI3_1

	CUESTIONARIO CUANTITATIVO				**REF** PLAN AI3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina				**PÁGINA** **1** **5**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|				
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro				
MATERIAL DE SOPORTE	COBIT 4.1				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**			Adquisición e Implementación (AI)
PREGUNTAS		**SI**	**NO**	**NA**	**OBSERVACIÓN**
1. ¿Existe personal capacitado para el manejo, adquisición y mantenimiento de la infraestructura tecnológica?		**3**			.
2. ¿Existen políticas y procedimientos de adquisición de hardware y software?			**4**		
3. ¿Estas políticas o procedimientos contienen: Solicitud de nuevas adquisiciones de hardware en cuanto a:					
• Servidores			**4**		
• Redes			**4**		
• Equipos de comunicación			**4**		
• Equipos de protección			**4**		
• Software			**4**		
• Sistemas operativos			**4**		
• Antivirus			**4**		
• Software de sistema			**3**		

Tabla 19. Cuestionario cuantitativo AI3_2

	CUESTIONARIO CUANTITATIVO	**REF**
		PLAN AI3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina	**PÁGINA** **2** **5**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|	
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro	
MATERIAL DE SOPORTE	COBIT 4.1	

DOMINIO	Adquisición e Implementación (AI)	**PROCESO**	Adquisición e Implementación (AI3)

PREGUNTAS	**SI**	**NO**	**NA**	**OBSERVACIÓN**
4. ¿El funcionario encargado del mantenimiento, configuración e instalación conoce estas políticas y procedimientos?		**5**		.
5. ¿Existe documentación de la información anterior?		**5**		
6. ¿Existen procesos y procedimientos de adquisición de infraestructura tecnológica que manejen listas y propuestas de proveedores?		**4**		
7. ¿Estos procesos y procedimientos están documentados?		**4**		
8. ¿Existe un plan de mantenimiento de la infraestructura tecnológica?	**4**			
9. El plan de mantenimiento de la infraestructura tecnológica contiene:				
• ¿Mantenimiento preventivo y correctivo de hardware de servidores?		**5**		
• ¿Mantenimiento preventivo y correctivo de hardware de computadores?	**4**			
• ¿Mantenimiento preventivo y correctivo de hardware de comunicaciones?	**4**			
• ¿Instalaciones de software?		**3**		
• ¿Limpieza física (utilizando sopladoras, cremas, productos especializados)?	**4**			
10. En cuanto al mantenimiento preventivo y correctivo se realizan:				

Tabla 20. Cuestionario cuantitativo AI3_3

	CUESTIONARIO CUANTITATIVO				REF
					PLAN AI3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina				**PÁGINA** **3** **5**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|				
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro				
MATERIAL DE SOPORTE	COBIT 4.1				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**			Adquisición e Implementación (AI3)

PREGUNTAS	**SI**	**NO**	**NA**	**OBSERVACIÓN**
• ¿Pruebas de funcionamientos de dispositivos internos y externos (monitores, teclado, memorias, discos duros, fuentes)?	**5**			.
• ¿Pruebas de funcionamiento de dispositivos de red (cables, conectores, dispositivos de comunicaciones)?	**5**			
11. ¿Existe un manual de funciones para el encargado del mantenimiento preventivo y correctivo de equipos de cómputo?	**5**			
12. Existe un manual de funciones para los procesos de mantenimiento preventivo y correctivo de otra infraestructura tecnológica como:				
• ¿Servidores?		**5**		
• ¿Dispositivos de protección (ups, reguladores)?		**5**		
• ¿Equipos de comunicación (switchs, routers, firewalls)?		**5**		
• ¿Dispositivos externos (impresoras, fotocopiadoras, escáner)?		**4**		
• ¿Red estructurada (canaletas, cables, conectores, etc.)?		**5**		
13. ¿Existe en la entidad un inventario detallado de elementos que componen la infraestructura tecnológica?		**4**		

Tabla 21. Cuestionario cuantitativo AI3-4

	CUESTIONARIO CUANTITATIVO	**REF** PLAN AI3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina	**PÁGINA** 4 5
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|	
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro	
MATERIAL DE SOPORTE	COBIT 4.1	
DOMINIO Adquisición e Implementación (AI)	**PROCESO**	Adquirir y Mantener Infraestructura Tecnológica(AI3)

PREGUNTAS	**SI**	**NO**	**NA**	**OBSERVACIÓN**
14. ¿Con que periodicidad se lleva un control de actualización de inventario • Trimestral • Semestral • Anual	**3**			
15. Cuando una dependencia se presentan fallas o caídas hay procedimientos a seguir para la siguiente infraestructura tecnológica: • ¿Servidor? • ¿Computadores? • ¿Red? • ¿Equipos de comunicación? • ¿Equipos de protección? • ¿Software (sistema operativo, software de sistema?	**5** **5** **5** **5** **5** **4**			
16. ¿Estos procedimientos están documentados?		**5**		
17. Estos procedimientos contemplan: • ¿Realización por parte del funcionario responsable una solicitud por escrito? • ¿Entrega (mediante constancia) por parte del funcionario del equipo al personal de mantenimiento? • ¿Revisión y solución de acuerdo a procedimientos y políticas establecidas para tal fin?		**5** **5** **5**		
18. ¿Los procesos y procedimientos se dan a conocer a los usuarios de la infraestructura tecnológica y al encargado de solucionar los problemas?		**4**		

Tabla 22. Cuestionario cuantitativo AI3_5

	CUESTIONARIO CUANTITATIVO				**REF** PLAN AI3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina				**PÁGINA** **5** **5**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|				
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro				
MATERIAL DE SOPORTE	COBIT 4.1				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**			Adquirir y Mantener Infraestructura Tecnológica(AI3)
PREGUNTAS		**SI**	**NO**	**NA**	**OBSERVACIÓN**
19. ¿Existen planos de la red estructurada de datos?			**5**		
TOTAL		66	117		
TOTAL CUESTIONARIO			183		

Porcentaje de riesgo = (66*100)/(183-0) =36%

Porcentaje riesgo total = 100-36%=64%(Riesgo Medio)

Tabla 23. Cuestionario cuantitativo AI5_1

	CUESTIONARIO CUANTITATIVO	**REF**
		PLAN AI5
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina	**PÁGINA** **1** **2**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|	
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro	
MATERIAL DE SOPORTE	COBIT 4.1	
DOMINIO	Adquisición e Implementación (AI)	**PROCESO** Adquirir Recursos de TI (AI5)

PREGUNTAS	**SI**	**NO**	**NA**	**OBSERVACIÓN**
1. ¿Existen políticas o procedimientos relacionados con la adquisición de recursos en cuanto a infraestructura tecnológica se refiere (hardware y software)?		**5**		.
2. Las política o procedimientos contienen:				
• ¿Políticas de adquisición de recursos en infraestructura tecnológica?		**4**		
• ¿Políticas de selección de nuevos proveedores?		**4**		
• ¿Estándares de nueva infraestructura adquirida?		**4**		
3. Existe un procedimiento para la adquisición de infraestructura tecnológica en cuanto a:				
• Documentación de nuevas adquisiciones		**5**		
• Normas de instalación física de hardware y software(servidores, equipos de cómputo, redes, sistemas operativos)		**5**		
4. ¿Se evalúan los contratos con los proveedores en cuanto a la adquisición de infraestructura tecnológica?	**4**			

Tabla 24. Cuestionario cuantitativo AI5_2

	CUESTIONARIO CUANTITATIVO				**REF** PLAN AI5
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina				**PÁGINA** 2 2
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|				
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro				
MATERIAL DE SOPORTE	COBIT 4.1				
DOMINIO	Adquisición e Implementación (AI)	**PROCESO**		Adquirir Recursos de TI(AI5)	
PREGUNTAS		**SI**	**NO**	**NA**	**OBSERVACIÓN**
5. Para la adquisición de infraestructura tecnológica con proveedores se tiene en cuenta lo siguiente: • ¿Listado de proveedores acreditados? • ¿Se ajusta a los requerimientos de la entidad? • ¿Impacto ambiental? • ¿Tiempo de garantía de la infraestructura a adquirí?			**5** **5** **5** **5**		
TOTAL		4	47		
TOTAL CUESTIONARIO				51	

Porcentaje de riesgo = (4*100)/(51-0) =7,8%

Porcentaje riesgo total = 100-7,8%=92,1%(Riesgo Alto)

Tabla 25. Cuestionario cuantitativo DS5_1

	CUESTIONARIO CUANTITATIVO	**REF**
		PLAN DS5
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina	**PÁGINA** **1** **2**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|	
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro	
MATERIAL DE SOPORTE	COBIT 4.1	
DOMINIO	Entregar y Dar Soporte (DS)	**PROCESO** Garantizar la seguridad de los Sistemas (DS5)

PREGUNTAS	**SI**	**NO**	**NA**	**OBSERVACIÓN**
1. ¿Existen procedimientos documentados de acceso a las diferentes dependencias de la institución?		**5**		.
2. ¿Existe una persona responsable de la seguridad?	**5**			
3. ¿Existen cuentas de usuario con sus respectivas contraseñas?	**5**			
4. ¿Existe un plan de seguridad que garantice la protección de los dispositivos y recursos de las dependencias?		**4**		
5. ¿Existen pólizas para asegurar el servidor?		**5**		
6. ¿Existen procedimientos para copias de seguridad?	**5**			
7. ¿Estos procedimientos están documentados?	**5**			
8. ¿Los funcionarios tienen conocimiento de estos procedimientos?		**5**		
9. ¿Se controla el trabajo fuera del horario?		**3**		
10. ¿Se identifica a la persona que ingresa?	**3**			

Tabla 26. Cuestionario cuantitativo DS5_2

	CUESTIONARIO CUANTITATIVO				**REF** PLAN DS5
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina				**PÁGINA** **2** **2**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|				
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro				
MATERIAL DE SOPORTE	COBIT 4.1				
DOMINIO	Entregar y Dar Soporte (DS)	**PROCESO**			Garantizar la seguridad de los Sistemas (DS5)
PREGUNTAS		**SI**	**NO**	**NA**	**OBSERVACIÓN**
11. ¿Existen controles de correo electrónico?			**3**		
12. ¿Existen antivirus que controlen la intrusión de software malicioso?		**5**			
13. ¿Existen bitácoras donde se guarde los procesos realizados por los usuarios de red?			**3**		
14. ¿Se informa a los usuarios sobre las políticas de seguridad de acceso a las instalaciones?			**4**		
15. ¿Existen puntos de red habilitados?			**5**		
TOTAL		28	34		
TOTAL CUESTIONARIO				62	

Porcentaje de riesgo = (28*100)/(62-0) =45,1%

Porcentaje riesgo total = 100-45,1%=54,8%(Riesgo Medio)

Tabla 27. Cuestionario cuantitativo DS12_1

	CUESTIONARIO CUANTITATIVO				**REF** PLAN DS12
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina				**PÁGINA** 1 2
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|				
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro				
MATERIAL DE SOPORTE	COBIT 4.1				
DOMINIO	Entregar y Dar Soporte (DS)	**PROCESO**			Administración del Ambiente Físico (DS12)

PREGUNTAS	**SI**	**NO**	**NA**	**OBSERVACIÓN**
1. ¿Existe un área habilitada dentro de la empresa para el encargado del mantenimiento de la infraestructura tecnológica?		**5**		.
2. ¿Existe un cuarto de equipos independiente dentro de la empresa en donde estén el gabinete de comunicaciones y el servidor?		**5**		
3. ¿Las dependencias que manejan infraestructura tecnológica cumplen con las siguientes características:				
• ¿Movilidad adecuada (facilidad de movilidad de los equipos y las personas)?		**5**		
• ¿Espacios adecuados de acuerdo a la cantidad de equipos que maneja cada dependencia?		**5**		
• ¿Ventilación?		**5**		
• ¿Iluminación?		**5**		
• ¿Control contra incendios?		**5**		
• ¿Suministro eléctrico adecuado?		**5**		
• ¿Tablero eléctrico independiente?		**5**		
• ¿Polos a tierra?	**4**			
• ¿Existen extintores cercanos?	**3**			
4. En la entidad se maneja sistemas de seguridad como:				
• ¿Cámaras?		**4**		
• ¿Extintores?	**5**			
• ¿Detectores de humo?		**4**		
• ¿Polos a tierra?	**5**			

Tabla 28. Cuestionario cuantitativo DS12_2

	CUESTIONARIO CUANTITATIVO				**REF** PLAN DS12
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina				**PÁGINA** **2** **2**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|				
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro				
MATERIAL DE SOPORTE	COBIT 4.1				
DOMINIO	Entregar y Dar Soporte (DS)	**PROCESO**			Administración del Ambiente Físico (DS12)
PREGUNTAS		**SI**	**NO**	**NA**	**OBSERVACIÓN**
5. ¿Existe planta eléctrica que garantice continuidad de los servicios		**5**			
6. ¿Existen Ups de tiempo prolongado para servidores y estaciones de trabajo?			**5**		
7. ¿Existe señalizaciones de evacuación?		**3**			
8. ¿Se han realizado simulacro de evacuación en la entidad?			**5**		
TOTAL		25	63		
TOTAL CUESTIONARIO				88	

Porcentaje de riesgo = (25*100)/(88-0) =28,4%

Porcentaje riesgo total = 100-28,4%=71,6%(Riesgo Alto)

Tabla 29. Cuestionario cuantitativo DS13

	CUESTIONARIO CUANTITATIVO				**REF** PLAN DS13
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina				**PÁGINA** 1 1
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|				
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro				
MATERIAL DE SOPORTE	COBIT 4.1				
DOMINIO	Entregar y Dar Soporte (DS)	**PROCESO**			Administración de Operaciones(DS13)
PREGUNTAS		**SI**	**NO**	**NA**	**OBSERVACIÓN**
1. ¿El encargado del mantenimiento preventivo y correctivo da soporte en el tiempo que los usuarios lo determinan?		**5**			
2. ¿Se realizan mantenimientos en los equipos de cómputo y servidores?		**5**			
3. ¿Existen políticas de seguridad por parte del encargado del soporte para evitar fallas futuras?			**4**		
4. ¿Se realiza mantenimientos continuos?			**4**		
5. ¿Existen resguardos adecuados para administrar el inventario de infraestructura tecnológica?			**4**		
TOTAL		10	12		
TOTAL CUESTIONARIO				22	

Porcentaje de riesgo = (10*100)/(22-0) =45,45%

Porcentaje riesgo total = 100-32.69%=54,54%(Riesgo Medio)

Tabla 30. Cuestionario cuantitativo ME2

	CUESTIONARIO CUANTITATIVO				**REF** PLAN ME2
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina				**PÁGINA** **1** **1**
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS|				
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro				
MATERIAL DE SOPORTE	COBIT 4.1				
DOMINIO	Entregar y Dar Soporte (DS)	**PROCESO**			Monitorear y Evaluar Control Interno(ME2)

PREGUNTAS	**SI**	**NO**	**NA**	**OBSERVACIÓN**
1. ¿Existen procedimientos para garantizar la seguridad del hardware y software en la institución?		**5**		
2. ¿Existen procedimientos para garantizar la seguridad física (servidores, equipos de cómputo, redes, equipos de comunicación, equipos de protección)?		**5**		
3. Existe una evaluación continua enfocada a mejorar el ambiente de control en cuanto a:				
• ¿Instalaciones?		**4**		
• ¿Servidores?		**4**		
• ¿Equipos de cómputo?		**4**		
• ¿Redes?		**4**		
• ¿Software?		**4**		
4. ¿Está definido quién es el responsable de la realización del monitoreo de evaluación?	**5**			
5. ¿Se toman acciones correctivas de acuerdo al resultado de la evaluación del monitoreo?	**3**			
6. ¿Existe un registro o documentación que soporte el proceso de evaluación del monitoreo realizado?		**5**		
TOTAL	8	35		
TOTAL CUESTIONARIO			43	

Porcentaje de riesgo = (8*100)/(43-0) =18,6%
Porcentaje riesgo total = 100-18,6%=81.4%(Riesgo Alto)

Tabla 31. Valoración de riesgos

	VALORACIÓN DE RIESGOS	REF
		VLRN_1

N°	RIESGOS/VALORACIÓN	PROBABILIDAD			IMPACTO			DOMINIO
		A	M	B	L	M	C	
R1	No existe un plan de infraestructura tecnológica.		X			X		PO3(1)
R2	No existen planes de contingencia de la infraestructura tecnológica (hardware y software) que contemple procesos y procedimientos a seguir.	X					X	PO3(2)
R3	No existe un plan de inversión en Infraestructura Tecnológica.		X			X		PO5(1)
R4	No existen personas encargadas que prioricen la inversión en infraestructura tecnológica.			X		X		PO5(2)
R5	No existen políticas y procedimiento para análisis y gestión del riesgo que evalúen la infraestructura tecnológica de la institución.		X				X	PO9(1)
R6	No existen políticas y procedimientos de adquisición de infraestructura tecnológica.		X			X		PO9(2)
R7	No existen políticas y procedimientos para propuestas y lista de proveedores de adquisición de hardware y software.		X			X		PO9(3)
R8	Los planes de mantenimiento de hardware y software no están debidamente documentados y se encuentran incompletos.	X				X		AI3(1)
R9	Los procesos y procedimientos de atención a fallas en la infraestructura tecnológica no están documentados.	X				X		AI3(2)
R10	No existen planos de cableado estructurado de datos en la institución.	X				X		AI3(3)

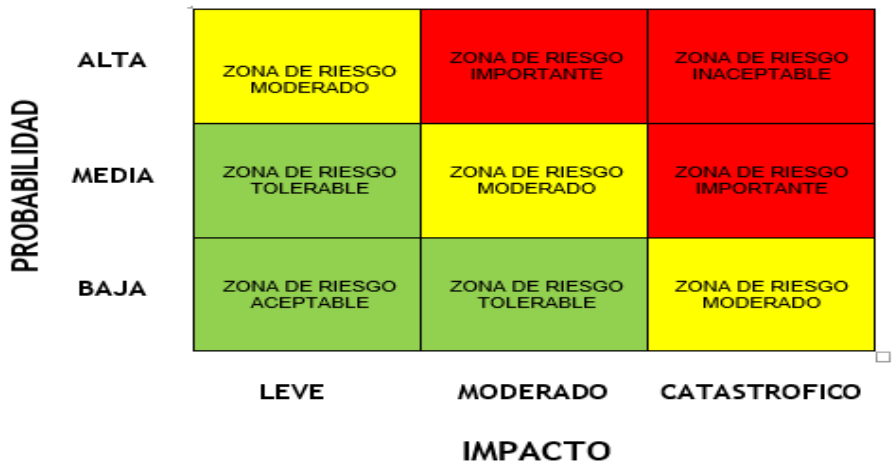
R11	No existe un inventario detallado de los elementos que componen la infraestructura tecnológica.		**X**			**X**		AI3(4)
R12	No existen políticas y procedimientos relacionados con la adquisición de (hardware y software)		**X**			**X**		AI5
R13	No existen procedimientos documentados de acceso a las diferentes dependencias de la institución.	**X**				**X**		DS5
R14	No existen planes de seguridad que garanticen la protección de los recursos y dispositivos en las diferentes dependencias de la institución.	**X**					**X**	DS12(1)
R15	No existen pólizas de seguridad del servidor principal.	**X**				**X**		DS12(2)
R16	Los funcionarios no tienen conocimiento de los procesos y procedimientos de gestión de la información.	**X**				**X**		DS12(3)
R17	No hay conocimiento de los usuarios sobre las políticas de seguridad sobre acceso a las instalaciones.		**X**			**X**		DS12(4)
R18	No existe un área habilitada para el encargado del mantenimiento de la infraestructura tecnológica.	**X**				**X**		DS12(5)
R19	No existe un cuarto de equipos independiente de funcionamiento del servidor y el gabinete de comunicaciones.	**X**				**X**		DS12(6)
R20	Las instalaciones físicas se encuentran muy limitadas en cuanto espacio, movilidad, iluminación, ventilación, suministro eléctrico.	**X**				**X**		DS12(7)
R21	El cableado estructurado de datos no cumple con las normas adecuadas.	**X**					**X**	DS12(8)
R22	El cableado eléctrico y sistemas eléctricos no cumplen con las normas adecuadas.	**X**					**X**	DS12(9)
R23	En muchas dependencias no existen sistemas de protección (ups, reguladores)	**X**				**X**		DS12(10)

R24	No existen sistemas de seguridad como cámaras, detectores de humo.	**X**					**X**	DS12(11)
R25	No se realizan mantenimientos continuos a la infraestructura tecnológica.	**X**				**X**		DS13
R26	No existen procesos y procedimientos de monitoreo para evaluación de la infraestructura tecnológica en la institución por parte del encargado de control interno.	**X**				**X**		ME2

2.3.6 Matriz de probabilidad e impacto. Los riesgos encontrados durante la aplicación de la auditoria a través de visitas, cuestionarios y entrevistas, se clasifican dentro de la matriz de probabilidad e impacto, que es un instrumento que nos permite establecer si un riesgo se califica bajo, intermedio o elevado a través de la mezcla de las dos dimensiones de un riesgo: su posibilidad de que suceda y su impacto en los objetivos, si el riesgo llegase a ocurrir. (Ver figura 2)

La probabilidad de ocurrencia va en el eje y, en el eje x va el impacto así:

Figura 2. Matriz de probabilidad e impacto



Riesgos que necesitan MONITORIZACIÓN: planes de actuación detectivos.

Riesgos que necesiten INVESTIGACIÓN: planes de actuación preventivos.

Riesgos que necesitan MITIGACIÓN: planes de actuación correctivos.

Hallazgos Infraestructura Tecnológica del sistema de información SALUDIPS del Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina

Formato de Hallazgos:

Teniendo en cuenta la aplicación de los instrumentos para recolección de información, los objetivos planteados con anterioridad y los riesgos definidos en la Matriz se obtiene la siguiente tabla de hallazgos que está definida así:

REF: identificación de la tabla de hallazgos.

ENTIDAD AUDITADA: nombre de la entidad a la cual se le está realizando el proceso

ÁREA AUDITADA: nombre del área a la cual se aplica la auditoria

OBJETO DE ESTUDIO: identificación de la parte a evaluar.

RESPONSABLES: nombre del equipo auditor que está llevando a cabo el proceso de auditoría.

MATERIA DE SOPORTE: nombre del modelo tomado en la aplicación de la auditoria, en este caso COBIT 4.1.

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

PROCESO: nombre del proceso en específico que se está auditando dentro de los dominios del COBIT

HALLAZGO: aquí se encontrara la descripción de cada hallazgo encontrado en los diferentes dominios

CONSECUENCIA: en este apartado se encuentra la descripción del efecto actual o futuro que tendrá las dependencias de no tomar las precauciones oportunas.

RECOMENDACIONES: se hace referencia a las descripciones correctivas de carácter preventivo que el equipo auditor ha presentado a las dependencias.

PROBABILIDAD E IMPACTO: hace referencia a la posibilidad de ocurrencia del riesgo y las consecuencias que puede ocasionar la materialización del riesgo

EVIDENCIAS: hace referencia de la descripción de los archivos que dan credibilidad al hallazgo. (Ver tabla 32)

Tabla 32. Descripción del formato de hallazgos.

	HALLAZGOS		**REF** **H1-(P03)**
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO		**PROCESO**	
HALLAZGO			
CONSECUENCIAS			
RECOMENDACIONES			
PROBABILIDAD E IMPACTO			
EVIDENCIAS			

Hallazgos:

A continuación se describe las posibles amenazas encontradas en las condiciones, funcionamiento, adquisición, selección y evaluación de la Infraestructura Tecnológica del sistema de información SALUDIPS del Centro de Salud San Miguel Arcángel E.S.E del Municipio de Ospina.

Dominios y procedimientos auditados infraestructura tecnológica del sistema de información SALUDIPS.

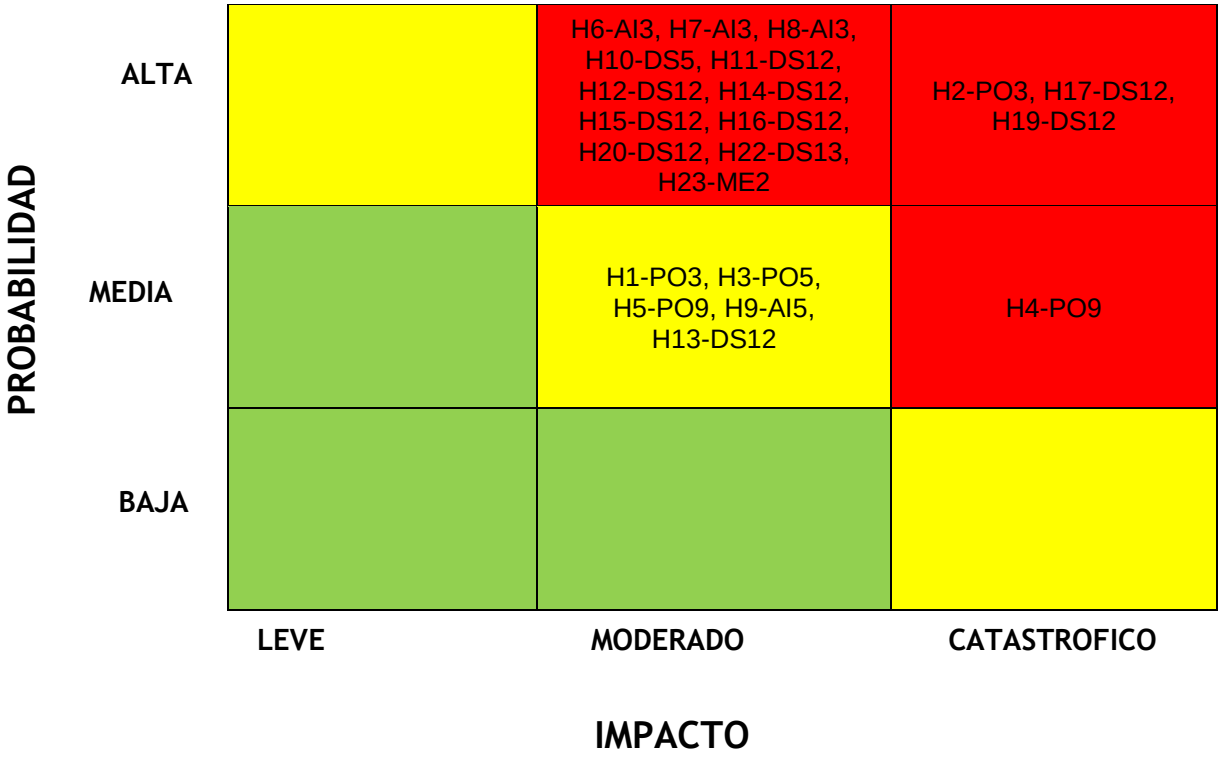
DOMINIO: PLANEACIÓN Y ORGANIZACIÓN (PO).
PO3 Determinar la Dirección Tecnológica.
PO5 Administrar la Inversión en TI.
PO9. Evaluar y Administrar los Riesgos de TI.

DOMINIO: ADQUIRIR E IMPLEMENTAR (AI).
AI3 Adquirir y Mantener la Infraestructura Tecnológica.
AI5 Adquirir Recursos de TI.

DOMINIO: ENTREGAR Y DAR SOPORTE (DS).
DS5 Garantizar la Seguridad de los Sistemas
DS12 Administración del Ambiente Físico
DS13 Administración de Operaciones.

DOMINIO: MONITOREAR Y EVALUAR (ME
ME2 Monitorear y Evaluar el Control Interno (Ver tabla 33)

Tabla 33. Clasificación de hallazgos matriz de probabilidad e impacto.



En seguida se detalla en tablas los hallazgos encontrados organizados por dominios, explicando sus consecuencias y las recomendaciones que el grupo auditor considera pertinentes. (Ver tabla 34-53)

Tabla 34. Hallazgo H1–PO3

	HALLAZGOS		**REF** H1-PO3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Planeación y Organización	**PROCESO**	Determinar la dirección Tecnológica
HALLAZGO			
No existe un plan de infraestructura tecnológica.			
CONSECUENCIAS			
La no existencia de planeación de la infraestructura tecnológica genera: • Incertidumbre en los procesos de obtención, mantenimiento y renovación de recursos tecnológicos existentes en la empresa. • Mala organización de los recursos tecnológicos en la institución. • Procesos de administración de inventario deficientes. • Mala distribución en los presupuesto de inversión en tecnología. • Desaprovechamiento de los recursos tecnológicos. • Inseguridad en los procesos de adquisición de nueva infraestructura tecnológica.			
RECOMENDACIONES			
Conformar un mesa de trabajo en donde se reúnan el Gerente de la entidad, el jefe de presupuesto, el jefe de control interno y el responsable de TI para analizar y evaluar la posibilidad de implementar un plan de infraestructura tecnológica en la entidad que contemplen principalmente: • Administración de los recursos tecnológicos (adquisición, instalación y mantenimiento) • Estrategias de contingencia de hardware y software. • Integración de los recursos físicos, informáticos, tecnológicos y humanos. Con esto se ratifica que los procesos y procedimientos de administración de la infraestructura tecnológica estén garantizados.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Media Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3		

Tabla 35. Hallazgo H2–PO3

	HALLAZGOS		**REF** H2-PO3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Planeación y Organización	**PROCESO**	Determinar la dirección Tecnológica
HALLAZGO			
No existen planes de contingencia de la infraestructura tecnológica que contemplen planes y procedimientos a seguir.			
CONSECUENCIAS			
Ante el riesgo de una falla o daño en la infraestructura tecnológica y en ausencia de un plan de contingencia se incurriría en tomar decisiones equivocadas en la solución del problema, por parte de quienes estén involucrados en el manejo de la infraestructura tecnológica, dando a lugar a incrementar la problemática, incrementando costos de operación.			
RECOMENDACIONES			
Generar documentación que contenga los procedimientos a seguir ante una eventualidad, permitiendo tomar decisiones adecuadas frente a una problemática, obteniendo tiempos de respuesta adecuados ante estas situaciones así como minimizar costos de reparación.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alta Impacto: Critico			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3		

Tabla 36. Hallazgo H3–PO5

	**HALLAZGOS**		**REF** H3-PO5
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Planeación y Organización	**PROCESO**	Administrar la Inversión en TI
HALLAZGO			
No existe un plan de inversión en infraestructura tecnológica.			
CONSECUENCIAS			
Al momento de presentarse una necesidad de relevancia o mejoramiento que necesite de solución inmediata se deberá tomar opciones que pueden incurrir en mayores costos debido a que no fueron planeadas con anterioridad			
RECOMENDACIONES			
Generar documentación donde se plantee posibilidades de mejora y expansión a la infraestructura tecnológica, con toda la información necesaria que permita la mejor toma de decisiones ante la necesidad tanto corto, mediano y largo plazo			
PROBABILIDAD DE IMPACTO			
Probabilidad: Media Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3		

Tabla 37. Hallazgo H4–PO9

	HALLAZGOS		**REF** H4-PO9
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Planeación y Organización	**PROCESO**	Evaluar y administrar los riesgos de TI
HALLAZGO			
No existen políticas y procedimientos para el análisis y gestión del riesgo que evalúen la infraestructura tecnológica de la institución			
CONSECUENCIAS			
Ante una situación de riesgo se tomaran decisiones que pueden ser equivocadas o no las mejores, incurriendo en mayores costos en su solución así como incrementar el tiempo de la misma.			
RECOMENDACIONES			
Generar documentación donde se tomen a consideración los riesgos a los que se ve la infraestructura tecnológica además del respectivo procedimiento a desarrollar ante los riesgos mencionados.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Media Impacto: Catastrófico			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3		

Tabla 38. Hallazgo H5–PO9

	HALLAZGOS		**REF** H5-PO9
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Planeación y Organización	**PROCESO**	Evaluar y administrar los riesgos de TI
HALLAZGO			
No existen políticas y procedimientos para propuestas y lista de proveedores de adquisición de hardware y software.			
CONSECUENCIAS			
Incremento en los costos frente a la necesidad de reemplazar parte de la infraestructura tecnológica antes una necesidad de solución inmediata que impida realizar un sondeo de los mejores proveedores teniendo en cuenta calidad y costos debido al tiempo de respuesta necesitado			
RECOMENDACIONES			
Generar documentación con listado de proveedores o posibles proveedores frente a las necesidades que pueden ocurrir al momento de reemplazar la infraestructura tecnológica, así como el debido proceso ante la necesidad de reemplazar dicho componente sea hardware o software			
PROBABILIDAD DE IMPACTO			
Probabilidad: Media Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3		

Tabla 39. Hallazgo H6-AI3

	HALLAZGOS		**REF** H6-AI3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Adquirir e Implementar	**PROCESO**	Adquirir y Mantener Infraestructura Tecnológica
HALLAZGO			
Los planes de mantenimiento de hardware y software no están debidamente documentados y se encuentran incompletos.			
CONSECUENCIAS			
Ante un daño o falla del hardware o software no será posible determinar la fecha precisa, si existe, de la última revisión de mantenimiento, para de esta manera dar una idea de lo realizado en esa última revisión así como las observaciones de quien lo realizo, que fue reemplazado y que fue revisado, para de ser necesario aplicar políticas de garantía ante la revisión realizada o determinar si los mantenimientos son los adecuados para la infraestructura que se maneja			
RECOMENDACIONES			
Solicitar a la persona que realiza los mantenimientos la descripción completa de lo realizado en los en estos, de ser necesario generar nuevos formatos de mantenimiento que contengan toda la información necesaria para el debido seguimiento ante una eventualidad.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alto Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENC-MATENIMIENTO.MP3 REF: /EVIDENCIAS/DOCUMENTOSESE/MANTENIMIENTO1.DOCX REF: /EVIDENCIAS/DOCUMENTOSESE/MANTENIMIENTO2.DOCX		

Tabla 40. Hallazgo H7-AI3

	HALLAZGOS		**REF** H7-AI3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Adquirir e Implementar	**PROCESO**	Adquirir y Mantener Infraestructura Tecnológica
HALLAZGO			
Los procesos y procedimientos de atención a fallas en la infraestructura tecnológica no están documentados.			
CONSECUENCIAS			
No será posible realizar seguimiento a lo realizado ante las fallas presentadas en la infraestructura tecnológica, lo cual permite tomar decisiones frente a la parte afectada como puede ser reemplazo o implementar un nuevo mantenimiento, dando a lugar a incrementar el riesgo de un daño mucho mayor que pudo ser prevenido			
RECOMENDACIONES			
Generar documentación que contenga la información necesaria ante una falla de la infraestructura tecnológica para de esta manera tomar las decisiones pertinentes frente a la parte afectada que eviten incrementar un mayor riesgo en mediano y largo plazo			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alto Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-AUXENFERMERIA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-REGFARMACIA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-PSICOLOGA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-ATUSUARIO.MP3		

Tabla 41. Hallazgo H8-AI3

	HALLAZGOS		**REF** H8-AI3
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Adquirir e Implementar	**PROCESO**	Adquirir y Mantener Infraestructura Tecnológica
HALLAZGO			
No existen planos de cableado estructurado de datos en la institución.			
CONSECUENCIAS			
Ante la necesidad de una reparación o expansión del cableado estructurado se dificultara la ubicación de los puntos necesarios a modificar o reparar, incurriendo en mayores costos debido al levantamiento de información necesaria para la realización de esta actividad por parte de quien la ejecuta.			
RECOMENDACIONES			
Realizar un levantamiento de información del cableado y mantenerlo actualizado de ser necesario, para evitar incrementar los costos ante una necesidad de expansión o reparación de corto plazo o que requiriera de una solución inmediata.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alto Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3		

Tabla 42. Hallazgo H9-AI5

	HALLAZGOS		**REF** H9-AI5
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Adquirir e Implementar	**PROCESO**	Adquirir y Mantener Infraestructura Tecnológica
HALLAZGO			
No existen políticas y procedimientos relacionados con la adquisición de nuevo hardware y software.			
CONSECUENCIAS			
Ante la necesidad de adquirir nuevo hardware o software se tomara decisiones equivocadas debido a que no puede ser necesario, sino más bien una actualización parcial, incurriendo en incremento en los costos de adquisición así como desaprovechamiento de los recursos ya existentes.			
RECOMENDACIONES			
Generar la documentación necesaria que de los pasos a tomar frente a una necesidad de adquisición de hardware o software, la cual debe traer a lugar la documentación de la infraestructura tecnológica para de esta manera tomar la decisión adecuada frente a adquisición o actualización y necesidades de la entidad.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Medio Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3		

Tabla 43. Hallazgo H10-DS5

	HALLAZGOS		**REF** H10-DS5
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Garantizar la seguridad de los sistemas
HALLAZGO			
No existen procedimientos documentados de acceso a las diferentes dependencias de la institución.			
CONSECUENCIAS			
Se pueden realizar accesos no autorizados a la infraestructura tecnológica por puntos no tomados en cuenta lo que incurriría en daños no solo a la infraestructura tecnológica sino a los datos.			
RECOMENDACIONES			
Documentar los puntos de acceso a las diferentes dependencias para ser tomados en cuenta en la toma de decisiones de la seguridad de la entidad.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alta Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-AUXENFERMERIA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-REGFARMACIA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-PSICOLOGA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-ATUSUARIO.MP3		

Tabla 43. Hallazgo H11-DS12

	HALLAZGOS		**REF** H11-DS12
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración del Ambiente Físico
HALLAZGO			
No existen planes de seguridad que garanticen la protección de los recursos y dispositivos en las diferentes dependencias de la institución.			
CONSECUENCIAS			
Al no existir planes de seguridad frente a la infraestructura tecnológica existe riesgo de pérdida y/o daños a la infraestructura tecnológica, ya sea por terceros no autorizados como la acción del ambiente y la no protección frente al mismo de los diferentes dispositivos.			
RECOMENDACIONES			
Generar la documentación necesaria que informe a quienes interactúen con la infraestructura tecnológica de los planes de seguridad de los recursos y dispositivos, para de esta manera minimizar los daños o perdidas de estos, como pueden ser actas de salida de los dispositivos, así como políticas de protección.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alta Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-AUXENFERMERIA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-REGFARMACIA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-PSICOLOGA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-ATUSUARIO.MP3		

Tabla 44. Hallazgo H12-DS12

	HALLAZGOS		**REF** H12-DS12
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración del Ambiente Físico
HALLAZGO			
No existen pólizas de seguridad del servidor principal.			
CONSECUENCIAS			
Siendo los datos un recurso indispensable para la entidad y debido a que todos convergen en el servidor, ante un daño el costo por reparación sería demasiado alto en comparación a mantener una póliza de seguridad ante daños que pueden presentarse.			
RECOMENDACIONES			
Adquirir una póliza que garantice no solo la reparación sino la agilidad en la solución de cualquier eventualidad de daño al servidor, teniendo en cuenta que es indispensable para el funcionamiento de la entidad.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alta Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3		

Tabla 45. Hallazgo H13-DS12

	HALLAZGOS		**REF** H13-DS12
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración del Ambiente Físico
HALLAZGO			
No hay conocimiento de los usuarios sobre las políticas de seguridad sobre acceso a las instalaciones.			
CONSECUENCIAS			
Las políticas de seguridad o normas de ingreso las instalaciones físicas de la entidad, tienen que conocerse por todo el personal de la empresa, el desconocimiento de estas normas, hacen que los funcionarios no tengan definidas sus responsabilidades ante posibles violaciones de seguridad o robos. Lo anterior genera muchos riesgos asociados con la seguridad de la información y elementos de la empresa, ya que son susceptibles a la disposición de los funcionarios.			
RECOMENDACIONES			
Comunicar por parte del gerente al nuevo personal que ingresa a la institución, las normas y políticas de seguridad existentes de acceso a las instalaciones físicas al edificio y a las diferentes áreas y dependencias.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Media Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-AUXENFERMERIA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-REGFARMACIA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-PSICOLOGA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-ATUSUARIO.MP3		

Tabla 46. Hallazgo H14-DS12

	HALLAZGOS		**REF** H14-DS12
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración del Ambiente Físico
HALLAZGO			
No existe un área habilitada para el encargado del mantenimiento de la infraestructura tecnológica.			
CONSECUENCIAS			
La falta de espacios adecuados para realizar el mantenimiento de la infraestructura tecnológica de la institución del hardware y software, genera interrupciones en las áreas de trabajo. Además los espacios no son aptos para realizar dichos mantenimientos o hay que realizarlos en horarios o jornadas no laborales.			
RECOMENDACIONES			
Analizar y evaluar la creación de un espacio apto para el personal de mantenimiento de la infraestructura tecnológica que contemple la norma ANSI/TIA/EIA-569-A (norma de recorridos y espacios de telecomunicaciones en edificios comerciales). Con la creación de este espacio, el desempeño laboral del encargado de la mantención de la infraestructura tecnológica seria el adecuado.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alto Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3		

Tabla 47. Hallazgo H15-DS12

	HALLAZGOS		**REF** H15-DS12
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración del Ambiente Físico
HALLAZGO			
No existe un cuarto de equipos independiente de funcionamiento del servidor y el gabinete de comunicaciones.			
CONSECUENCIAS			
• Manipulación de los equipos por personal no autorizado ante respuesta a fallas. • Riesgos de seguridad ante posibles daños por personal ajeno y no capacitado en la manipulación de estos recursos tecnológicos. • Se pueden generar robos, daños y pérdidas de dispositivos internos y externos. • Respuesta a fallas inadecuadas, al haber muchos recursos tecnológicos físicos (computadores, ups, reguladores, cables, impresoras, etc) en el área donde operan estos elementos, haciendo más difícil identificar el problema.			
RECOMENDACIONES			
Analizar y evaluar la habilitación de un espacio o cuarto de equipos independiente que almacene el servidor y el gabinete de comunicaciones que disponga de un buen ambiente físico basado de acuerdo a la norma ANSI/TIA/EIA-569-A (norma de recorridos y espacios de telecomunicaciones en edificios comerciales).			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alto Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3		

Tabla 48. Hallazgo H16-DS12

	HALLAZGOS		**REF** H16-DS12
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración del Ambiente Físico
HALLAZGO			
Las instalaciones físicas se encuentran muy limitadas en cuanto espacio, movilidad, iluminación, ventilación, suministro eléctrico.			
CONSECUENCIAS			
Existen espacios muy limitados físicamente en cuanto a espacio y movilidad, además existen problemas en el suministro eléctrico, la iluminación de los espacios y la ventilación. Esto genera desempeños laborales deficientes, riesgo de daños al hardware por golpes o caídas, perdida de información y datos físicos,			
RECOMENDACIONES			
Disponer los espacios de acuerdo a la norma ANSI/TIA/EIA-569-A (norma de recorridos y espacios de telecomunicaciones en edificios comerciales), para garantizar la seguridad de la infraestructura tecnológica y el talento humano dentro de la empresa.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alto Impacto: Moderado			

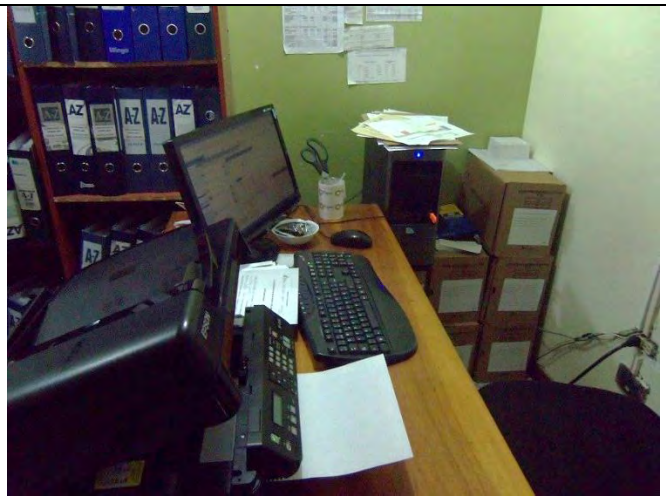
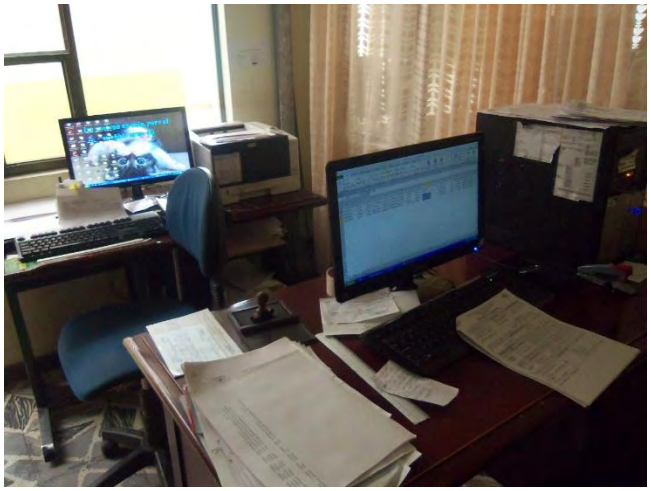
EVIDENCIAS	 REF: /EVIDENCIAS/FOTOS/IMG1-AFISICO.JPG  REF: /EVIDENCIAS/FOTOS/IMG2-AFISICO.JPG

Tabla 48. Hallazgo H17-DS12

	HALLAZGOS		**REF** H17-DS12
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración del Ambiente Físico
HALLAZGO			
El cableado estructurado de datos no cumple con las normas adecuadas.			
CONSECUENCIAS			
La solución a problemas en la red de datos está expuesta a ser inadecuada por parte del personal especializado y encargado de atención a estas fallas. Existe la posibilidad que la falla se solucione por un tiempo determinado y vuelva a ocurrir. La mala distribución y seguridad del cableado estructurado permite deterioro de este elemento en el tiempo y mala administración de este recurso. Los cables a la vista generan mala imagen de la institución ante usuarios internos externos.			
RECOMENDACIONES			
Analizar y evaluar la posibilidad de acogerse a la norma EIA/TIA 568-A que especifica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. Se hacen recomendaciones para: • Las topología • La distancia máxima de los cables • El rendimiento de los componentes • Las tomas y los conectores de telecomunicaciones			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alto Impacto: Catastrófico			

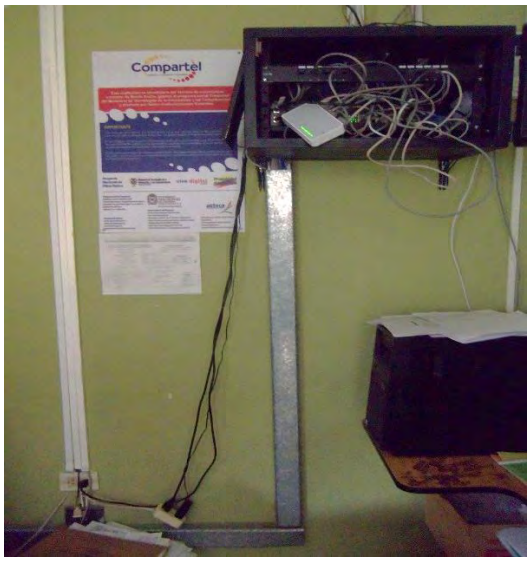
EVIDENCIAS	 REF/EVIDENCIAS/FOTOS/IMG1-REDDATOS.JPG  REF: /EVIDENCIAS/FOTOS/IMG2-REDDATOS.JPG  REF: /EVIDENCIAS/FOTOS/IMG3-REDDATOS.JPG

Tabla 49. Hallazgo H19-DS12

	HALLAZGOS		**REF** H19-DS12
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración del Ambiente Físico
HALLAZGO			
El cableado eléctrico y sistemas eléctricos no cumplen con las normas adecuadas.			
CONSECUENCIAS			
La mala administración del suministro de corriente puede generar choque eléctricos y las temperaturas excesivas; capaces de provocar quemaduras, incendios, explosiones u otros efectos peligrosos • Riesgos de cortos e incendios provocados por chispas, ya que los cables están sin canaletas y no siguen una norma. • Electroestática en el sitio o dependencia de trabajo. • Riesgos laborales y accidentes por manipulación de cables por personas no especializadas para tal fin.			
RECOMENDACIONES			
Acogerse a las normas o reglamento Técnico de Instalaciones Eléctricas – RETIE, cuyo objeto es establecer las medidas que garanticen la seguridad de las personas, la vida animal y vegetal, y la preservación del medio ambiente, previniendo, minimizando o eliminando los riesgos de origen eléctrico.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alta Impacto: Catastrófico			

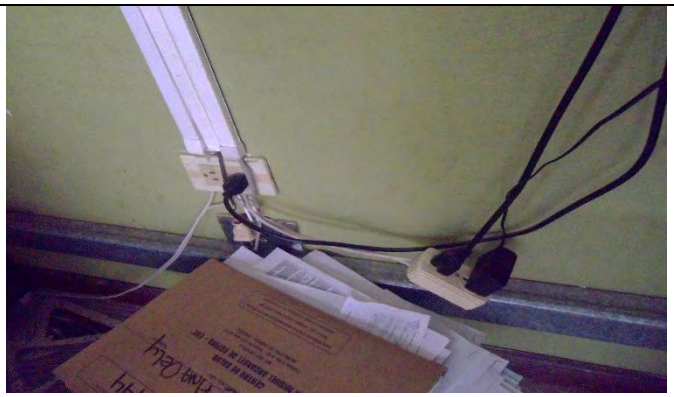
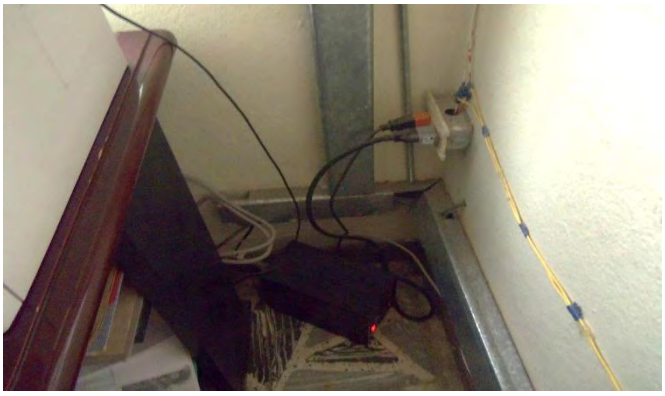
EVIDENCIAS	 REF: /EVIDENCIAS/FOTOS/IMG1-REDELECTRICA.JPG  REF: /EVIDENCIAS/FOTOS/IMG2-REDELECTRICA.JPG

Tabla 50. Hallazgo H20-DS12

	HALLAZGOS		**REF** H20-DS12
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración del Ambiente Físico
HALLAZGO			
En muchas dependencias no existen sistemas de protección (ups, reguladores)			
CONSECUENCIAS			
La no utilización de sistemas de protección como reguladores de voltaje y ups puede generar inestabilidad en el suministro de voltaje a los recursos tecnológicos ya que comúnmente la electricidad llega con variaciones que provocan desgaste de los elementos electrónicos a largo plazo en las fuentes de alimentación de las computadoras, servidores. Además genera fallas en los elementos electrónicos de todos los dispositivos conectados.			
RECOMENDACIONES			
Dotar a las dependencias que no tiene sistemas de protección tales como reguladores los cuales protegen los aparatos eléctricos y electrónicos contra altos y bajos voltajes, y además, protege contra picos de voltaje. Dotar a las dependencias que no tiene sistemas de protección tales como UPS que son dispositivo que provee y mantiene energía eléctrica de respaldo en caso de interrupciones eléctricas o eventualidades en la línea o acometida.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alto Impacto: Moderado			

EVIDENCIAS	 REF: /EVIDENCIAS/FOTOS/IMG1-SISPROTECCION.JPG  REF: /EVIDENCIAS/FOTOS/IMG2-SISPROTECCION.JPG

Tabla 51. Hallazgo H21-DS12

	HALLAZGOS		**REF** H21-DS12
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración del Ambiente Físico
HALLAZGO			
No existen sistemas de seguridad como cámaras y detectores de humo.			
CONSECUENCIAS			
Ante el riesgo de un robo no se podría detectar a tiempo o permitir una búsqueda estableciendo horas de acceso y uso de la infraestructura, mediante el uso de cámaras. Siendo la infraestructura tecnológica tales como computadores, cableado, y dispositivos entre otros, vulnerables al daño por posibles incendios, el no tener detectores se incrementa el tiempo de exposición ante esta vulnerabilidad, aumentando de manera considerable los daños.			
RECOMENDACIONES			
Establecer un sistema de monitoreo por cámaras en los puntos principales de acceso, así como detectores de humo en los lugares con mayor vulnerabilidad a incendios.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alto Impacto: Catastrófico			
EVIDENCIAS	REF: OBSERVACION DIRECTA		

Tabla 52. Hallazgo H22-DS13

	HALLAZGOS		**REF** H22-DS13
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Entregar y Dar Soporte	**PROCESO**	Administración de Operaciones
HALLAZGO			
No se realizan mantenimientos continuos a la infraestructura tecnológica.			
CONSECUENCIAS			
Se podría incurrir en mayores costes de reparación en comparación a los costos de mantenimiento, así como la detección y seguimiento de daños que pudieron ser detectados durante un mantenimiento			
RECOMENDACIONES			
Establecer la documentación que guíe al proceso de mantenimientos a la infraestructura tecnológica			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alto Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-AUXENFERMERIA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-REGFARMACIA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-PSICOLOGA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-ATUSUARIO.MP3 REF: /EVIDENCIAS/DOCUMENTOSESE/MANTENIMIENTO1.DOCX REF: /EVIDENCIAS/DOCUMENTOSESE/MANTENIMIENTO2.DOCX		

Tabla 53. Hallazgo H23-ME2

	HALLAZGOS		**REF** H23-ME2
ENTIDAD AUDITADA	Centro de Salud San Miguel Arcángel E.S.E Municipio de Ospina		
OBJETO DE ESTUDIO	Infraestructura tecnológica del sistema de información SALUDIPS		
RESPONSABLES	José Fernando Argoty Erazo y Carlos J. Benavides Montenegro		
MATERIAL DE SOPORTE	COBIT 4.1		
DOMINIO	Monitorear y Evaluar	**PROCESO**	Monitorear y Evaluar el Control Interno
HALLAZGO			
No existen procesos y procedimientos de monitoreo para evaluación de la infraestructura tecnológica en la institución por parte del encargado de control interno.			
CONSECUENCIAS			
Se incurre en la no detección temprana de fallas o daños a la infraestructura, lo cual provocaría mayores costos de reparación que pudieron ser solventados durante la programación de un mantenimiento.			
RECOMENDACIONES			
Generar la documentación necesaria que permita establecer, procedimientos de monitoreo a la infraestructura tecnológica por parte del encargado de control interno.			
PROBABILIDAD DE IMPACTO			
Probabilidad: Alto Impacto: Moderado			
EVIDENCIAS	REF: /EVIDENCIAS/ENTREVISTAS/ENT-ENCMATENIMIENTO.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-AUXENFERMERIA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-REGFARMACIA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-PSICOLOGA.MP3 REF: /EVIDENCIAS/ENTREVISTAS/ENT-ATUSUARIO.MP3		

2.3.7 Informe ejecutivo de auditoria:

San Juan de Pasto, 1 Febrero de 2016

Doctor:
OSCAR LENIN CALDERON MORILLO
Gerente

REF: AUDITORIA A LA INFRAESTRUCTURA TECNOLÓGICA DEL SISTEMA DE INFORMACIÓN SALUDIPS DEL CENTRO DE SALUD SAN MIGUEL ARCÁNGEL E.S.E DEL MUNICIPIO DE OSPINA – NARIÑO.

Cordial Saludo.

En el presente informe de auditoría a la cual fue sometida la Infraestructura Tecnológica del sistema de información SALUDIPS del Centro de Salud se evaluaron por parte de los auditores elementos de hardware y software y los diferentes procesos que intervienen en su funcionamiento dentro de la empresa.

El desarrollo de este trabajo de auditoria fue soportada por información y documentación que nos suministró la entidad auditada y por técnicas y herramientas que nos brindaron los estándares.

A continuación se hace un énfasis en general en los hallazgos encontrados y aspectos positivos que se resaltan en la entidad; los resultados obtenidos fueron los siguientes:

Se encontraron deficiencias en los procesos de adquisición y mantenimiento de la infraestructura tecnológica (hardware y software), no existen los procedimientos adecuados para la administración de las tecnologías existente en las diferentes dependencias, esto genera una mala organización, desaprovechamiento y mala administración de los recursos tecnológicos, por otra parte no se asignan rubros importantes en la inversión en TI y no existe documentación sobre políticas y procedimientos para el análisis y gestión del riesgo que evalúen la infraestructura tecnológica esto hace que las decisiones no sean las más adecuadas o se tomen malas decisiones.

Recomendaciones:

Analizar, estudiar y generar un plan de infraestructura tecnológica y un plan de análisis y gestión del riesgo en donde se evalué los procesos de administración de recursos tecnológicos informáticos y administración de la información,

desarrollando procedimientos sistemáticos que ayuden a mejorar la toma de decisiones.

Invertir en TI y asignar rubros importantes; con esto se garantiza renovación en recursos tecnológicos y mejor soporte en los procesos, garantizando la eficiencia, disponibilidad y calidad de la información.

En cuanto a los planes de mantenimiento de la infraestructura tecnológica, existen pero no se documentan adecuadamente, en los documentos no se observan formatos ni procesos a seguir, se manejan mantenimientos al hardware de los equipos de cómputo y no a toda la infraestructura tecnológica como el software, las redes, los elementos de protección, los elementos de comunicación y demás dispositivos tecnológicos. Además cuando los elementos que componen la infraestructura tecnológica fallan se brinda el soporte pero no se documenta, ni se tiene un historial de los procedimientos a seguir en la solución del problema por parte del encargado de brindar estos soportes, esto hace que no haya un seguimiento constate de las posibles fallas o factores que hayan provocado los daños.

Recomendaciones:

Realizar mantenimientos periódicos y generar por parte del encargado una documentación completa y actualizada que incluya procesos y procedimientos de mantenimiento al hardware y software en su totalidad especificado en formatos.

Generar por parte del encargado de atención a fallas de la infraestructura tecnológica documentación necesaria que incluya procedimientos en la solicitud por parte del jefe de dependencia y procedimientos de solución por parte del encargado del soporte.

En cuanto a la red estructurada de datos y red eléctrica se encuentran muchas debilidades, siendo estas un elemento importante en la administración de la información y datos que es entregada por el sistema de información SALUDIPS. Por una parte no existen planos o diagramas de red, esto ocasiona que ante posibles fallas no se identifique de manera eficiente el problema y el encargado de la atención a la falla solucione el problema en un tiempo mayor al estimado o en el peor de los casos no lo solucione. Por otra parte el cableado no sigue normas de instalación y se encuentra a la vista de los usuarios generando deterioro de los cables, mala imagen ante los usuarios internos y externos y posibles caídas del sistema por cortes del cable o manipulación indebida por personal no especializado. Además en la parte eléctrica genera riesgos laborales al estar los cables expuestos y posibles sobrecargas de energía e incendios al conectar muchos dispositivos en un solo toma.

Recomendaciones:

Analizar, estudiar y generar planos de la red estructurada de datos y red eléctrica.

Acogerse a la norma EIA/TIA 568-A que especifica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. En cuanto a: las topologías, La distancia máxima de los cables, El rendimiento de los componentes, las tomas y los conectores de telecomunicaciones.

Acogerse a las normas o reglamento Técnico de Instalaciones Eléctricas – RETIE, cuyo objeto es establecer las medidas que garanticen la seguridad de las personas y la preservación del medio ambiente, previniendo, minimizando o eliminando los riesgos de origen eléctrico.

En cuanto a la administración de los espacios físicos y seguridad en ellos, en el centro de salud, no se cuenta con espacios físicos adecuados. No existe un espacio habilitado para brindar soporte a la infraestructura tecnológica por parte del encargado de estos procesos, haciendo más difícil su labor. Por otra parte no se cuenta con un espacio físico independiente que contenga al servidor y el equipo de comunicaciones, todos estos elementos y dos (2) terminales mas, se encuentran en un espacio físico reducido, sin ventilación, se administran muchos dispositivos en él, esto genera que los procesos de soporte ante una falla no se identifiquen en un tiempo prudencial y se interrumpa las actividades de los funcionarios.

La seguridad también se ve muy afectada ya que hay acceso al espacio donde se encuentra el servidor de personal no autorizado lo que provoca posibles daños por caídas, manipulación indebida y robos de los equipos y dispositivos internos o externos.

Recomendaciones:

Analizar, estudiar y habilitar espacios aptos para el personal de mantenimiento y cuarto de equipos independiente que contemple la norma ANSI/TIA/EIA-569-A (norma de recorridos y espacios de telecomunicaciones en edificios comerciales).

Implementar políticas de seguridad de acceso a las zonas donde se encuentre el servidor y el armario de comunicaciones.

En cuanto a los planes de contingencia, no existe documentación ni procesos de planes de contingencia en la entidad que contemplen la infraestructura tecnológica debido a esto la capacidad de respuesta ante fallas puede ser nula y su recuperación se extienda en el tiempo o genere parálisis total en la continuidad de los servicios que presta la entidad.

Recomendaciones:

Crear documentos donde se contemplen procedimientos que indiquen acciones a seguir ante determinados riesgo en la infraestructura tecnológica evidenciando las etapas de evaluación, planificación, pruebas de viabilidad, ejecución y recuperación.

Fortalezas

- Existe un manual de procesos y procedimientos en Gestión de la Información esto hace que los procesos automatizados de los sistemas de información la administren de manera eficiente y segura. Los usuarios que manejan el sistema de información SALUDIPS generan de manera adecuada y satisfactoria sus copias de seguridad y la gestionan de manera oportuna en caso de caídas o fallas en sus sistemas.

- Existe personal idóneo para identificar y solventar problemas a nivel de fallas que se presenten en la infraestructura tecnológica, estableciendo controles adecuados y tiempos de respuesta eficientes.

- La gerencia adopta de manera pertinente las solicitudes del encargado del mantenimiento de la infraestructura tecnológica en cuanto a adquisición de elementos y/o componentes que relacionan el correcto funcionamiento de los recursos informáticos y tecnológicos, para oportunas respuestas ante posibles fallas.

Plan de mejoramiento:

Con la realización de la auditoria se espera que el Gerente adopte un plan estratégico en donde relacione los procesos y procedimientos de administración de la infraestructura tecnológica (hardware y software) con esto se pretende que mediante vulnerabilidades encontradas se diseñe un plan de mejoramiento que permita mitigar riesgos y amenazas presentes en este componente.

La adopción de este plan permite un mejor aprovechamiento y distribución de los recursos tecnológicos, mejor gestión ante riesgos, mejores estrategias ante posibles factores que afecten el buen funcionamiento de los recursos tanto internos como externos, mejora y distribución en el espacio físico, documentación de procedimientos en la atención a fallas, controles de acceso y seguridad a los espacios físicos, documentación de planos de red eléctrica y de datos, creación y documentación de planes de contingencia ante posibles eventualidades catastróficas.

Atentamente,

_____.
José Fernando Argoty Erazo
Auditor

_____.
Carlos Benavides Montenegro
Auditor

3. CONCLUSIONES

La infraestructura tecnológica en las empresas es la base donde se afirman la mayoría de procesos en la administración de la información y datos; controlar, mantener y mejorar este componente permite que estos procesos se realicen de manera segura y eficiente, esto se puede lograr con una evaluación continua y con la creación de planes que permitan su correcta gestión.

La auditoría informática ofrece métodos veraces y confiables que permiten la revisión y evaluación de los controles, sistemas y procedimientos presentes en el área a auditar, con esto se logra una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Los procesos de auditoria aplicados a la infraestructura tecnológica del centro de salud San Miguel Arcángel E.S.E de Municipio de Ospina, lograron detectar riesgos y amenazas presentes en este componente esto evidencia que tan vulnerable se encuentra el hardware y software ante múltiples factores que afectan su correcto funcionamiento.

Por medio del estándar COBIT se logró mejores prácticas en la aplicación de la auditoria y fue una guía de alto nivel para la definición y evaluación de los procesos de la empresa, además permite un marco de trabajo más específico en el desarrollo de las actividades de auditoria y establece métodos eficaces que evalúan la confidencialidad, seguridad, integridad y disponibilidad de la información.

Se logró en la práctica aplicar los conocimientos teóricos obtenidos en el Diplomado de Auditoria y Seguridad Informática, el cual fue un referente importante y nos brindó herramientas suficientes por medio del estudio de diferentes conceptos y la elección del mejor estándar para realizar procesos de auditoria sólidos y consecuentes.

4. RECOMENDACIONES

Realizar auditorías que evalúen todos los procesos que intervienen en la administración de la información en la entidad, con el fin de garantizar en todas las áreas de la empresa mejor calidad en los servicios y un mejoramiento constante en la disponibilidad y entrega de la información a los usuarios finales.

Aplicar herramientas de recolección de datos como: entrevistas, cuestionarios cuantitativos, listas de chequeo, observación directa, para asegurar una correcta y verídica obtención de la información en las fases iniciales de la auditoria informática.

Implementar planes que contengan pasos sistemáticos y contemplen procedimientos en el análisis y evaluación de riesgos, adquisición y mantenimiento de infraestructura tecnológica y administración de la información y recursos tecnológicos para lograr mitigar riesgos y amenazas presentes en la infraestructura tecnológica.

Documentar de manera adecuada los procesos y procedimientos de mantenimiento y asistencia a fallas de la infraestructura tecnológica del sistema de información SALUDIPS.

Acoger a las normas y estándares de instalación y distribución de red estructurada de datos, red eléctrica y acondicionamiento y distribución de los espacios físicos en las diferentes dependencias que manejan el sistema de información SALUDIPS.

Implementar políticas de seguridad y control de acceso a las instalaciones físicas donde se encuentra el servidor, el cuarto de comunicaciones y demás dispositivos tecnológicos para evitar posibles pérdidas y daños ocasionales por personal no autorizado.

Implementar y documentar planes de contingencia por medio de definición de procedimientos en la recuperación a fallos referentes a la infraestructura tecnológica, para que la información y datos estén protegidos y se garantice la continuidad de los servicios.

Mantener un monitoreo continuo por parte del encargado del control interno en los procesos de obtención, mantenimiento y mejoramiento de infraestructura tecnológica.

BIBLIOGRAFÍA

ECHENIQUE GARCÍA, José Antonio. Auditoría en Informática. México, Mc. GrawHill, 2001

MARCO DE REFERENCIA COBIT VERSIÓN 4.1. 2007 IT Governance Institute. All rights reserved.

MORENO BRAVO, Freddy Javier. Auditoria y Evaluación de Sistemas. 2012

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

NETGRAFÍA

INGENIERO FRANCISCO NICOLAS SOLARTE SOLARTE. (Septiembre de 2010) Auditoria Informática y de Sistemas. Retrieved from http://auditordesistemas.blogspot.com/

http://www.mailxmail.com/curso-elemental-auditoria/concepto-auditoria

http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/notas-clase/nota1-auditoria.pdf

http://www.ub.edu.ar/catedras/ingenieria/auditoria/tpmetodo/tpmetodo2.htm

http://www.fceia.unr.edu.ar/asist/intro-aa-t.pdf

http://es.slideshare.net/j_moreno/auditoria-informatica-y-de-sistemas-de-informacion