AUDITORIA A LA INFRAESTRUCTURA FÍSICA DE LA RED DE DATOS DE LA SEDE PRINCIPAL Y VERIFICACIÓN DEL CUMPLIMIENTO DE LAS NORMAS DE GOBIERNO EN LÍNEA EN LA PÁGINA DE LA ESE CENTRO HOSPITAL DIVINO NIÑO.

LUIS ALBERTO REYNEL ARAUJO

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2013

AUDITORIA A LA INFRAESTRUCTURA FÍSICA DE LA RED DE DATOS DE LA SEDE PRINCIPAL Y VERIFICACIÓN DEL CUMPLIMIENTO DE LAS NORMAS DE GOBIERNO EN LÍNEA EN LA PÁGINA DE LA ESE CENTRO HOSPITAL DIVINO NIÑO.

LUIS ALBERTO REYNEL ARAUJO

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

Director
ING. MANUEL BOLAÑOS GONZALES

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2013

NOTA DE RESPONSABILIDAD

"Las ideas y conclusiones aportadas en la tesis de grado son responsabilidad exclusiva de los autores"

Artículo 1° del Acuerdo n° 324 de octubre 11 de 1966 emanado del Honorable Consejo Directivo de la Universidad de Nariño.

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

Artículo 13, Acuerdo N 005 de 2010 emanado del Honorable Concejo Académico.

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

Firma del Jurado

_____

Firma del Jurado

San Juan de Pasto, Mayo de 2013

AGRADECIMIENTOS

A Dios por ser esa luz que ha guiado mi camino y quien me ha bendecido con fuerza para seguir en los momentos que quise darme por vencido.

A mi familia por todo el apoyo y amor durante toda mi vida, además de ser un soporte en todo sentido durante este proceso universitario.

Al Ingeniero Manuel Bolaños por su compromiso, energía y apoyo brindado para culminar de la mejor manera con este proceso no solo por ser maestro, si no también por ser un gran amigo.

A todos mis maestros quienes fueron las personas quienes me enseñaron y guiaron con todo su empeño además de ser quienes se convirtieron en mi modelo a seguir.

A mis amigos y compañeros por su amistad, apoyo y todo los buenos momentos compartido durante esta etapa.

DEDICATORIA

Este triunfo se lo dedico a Dios, por las bendiciones recibidas,
A mi madre, quien es el pilar fundamental de mi vida y quien
Me enseña día a día que si nos proponemos algo lo podemos lograr,
a mi padre por todos sus conejos que me han ayudado
y enseñado que a pesar de que uno caiga siempre
se debe levantarse con la cabeza en alto;
A mi abuela quien es mi segunda madre y quien le
Agradezco todo lo que ha hecho por mí durante mi vida.

De igual manera a mis amigos y a mi novia Diana Giraldo por estar conmigo
Y brindarme todo su amor, cariño y apoyo al final de este proceso.
.

LUIS ALBERTO REYNEL ARAUJO

RESUMEN

Las auditorias en toda entidad son de gran importancia para analizar y mejorar los procesos, además, por medio de la auditoria se puede medir la eficiencia y eficacia con la que las tareas administrativas se están desempeñando en las entidades.

Aquí se presenta la ejecución de una auditoría realizada a la E.S.E CENTRO HOSPITAL DIVINO NIÑO en la ciudad de Tumaco, esta auditoria se realiza con el objetivo de encontrar vulnerabilidades en la red física de datos de la sede principal en el área asistencial, además se evalúa la página web de la entidad con el fin de verificar el cumplimiento del decreto 1151 de 2008 del programa Gobierno en Línea e identificar posibles fallas y debilidades de esta.

Para desarrollar este proceso se toma como marco de referencia COBIT (Objetivos de Control para la información y Tecnologías relacionadas), de donde se seleccionaron los diferentes procesos y objetivos de control para ser auditados. Terminado el proceso de auditoria se continua la evaluación de la página web y funcionamiento con los lineamientos de la estrategia de Gobierno en línea, culminado todo los procesos de evaluación se formulan las recomendaciones para el mejoramiento de la red física y de la página web de acuerdo al decreto 1151 de 2008 de Gobierno en Línea.

ABSTRACT

Entity-wide audits are important to analyze and improve processes also through audit can measure the efficiency and effectiveness with which they are performing administrative tasks in the entities.

Here is an implementation of an audit to DIVINE CHILD THAT HOSPITAL CENTER in the city of Tumaco, this audit is performed in order to find vulnerabilities in the physical network data headquarters in nursing care, and evaluates the website of the entity in order to verify compliance with the decree 1151 of 2008 Government Online program and identify potential flaws and weaknesses of this.

To develop this process is taken as a framework COBIT (Control Objectives for Information and Related Technologies), from which we selected the different processes and control objectives to be audited.

After the audit process is continued evaluation of the website and working with the guidelines of the Government Online Strategy, completed all the processes of evaluation makes recommendations for the improvement of the physical network and the website according the Decree 1151 of 2008 Government Online.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

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 riesgos: Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Aplicación: Aunque se suele utilizar indistintamente como sinónimo genérico de 'programa' es necesario subrayar que se trata de un tipo de programa específicamente dedicado al proceso de una función concreta dentro de la empresa.

Archivo de datos: Cualquier archivo creado dentro de una aplicación: por ejemplo, un documento creado por un procesador de textos, una hoja de cálculo, una base de datos o un gráfico. También denominado Documento.

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

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

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Bases de Datos: Colección de datos organizada de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacionar es aquella en la que las conexiones entre los distintos elementos que forman la base de datos están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a éstos.

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Cliente: Cliente o 'programa cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

COBIT (Objetivos de Control de las Tecnologías de la Información y Tecnologías Relacionadas) Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

Conexión física: Permiten a las computadoras transmitir y recibir señales directamente. Las conexiones físicas están definidas por el medio empleado (pueden ser cables hasta satélites) para transmitir la señal, por la disposición

geométrica de las computadoras (topología) y por el método usado para compartir información, desde textos, imágenes y hasta videos y sonidos.

Criptografía: Ciencia dedicada al estudio de técnicas capaces de conferir seguridad a los datos. El cifrado es fundamental a la hora de enviar datos a través de las redes de telecomunicaciones con el fin de conservar su privacidad.

Datos: Término general para la información procesada por un ordenador.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

Factibilidad: Es la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señaladas, sirve para recopilar datos relevantes sobre el desarrollo de un proyecto y en base a ello tomar la mejor decisión.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Hardware: Conjunto de dispositivos de los que consiste un sistema. Comprende componentes tales como el teclado, el Mouse, las unidades de disco y el monitor.

Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros ej., pérdida de reputación, implicaciones legales, etc.

Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Internet: Interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISACA: Information Systems Audit and Control Association. Publica COBIT y emite diversas acreditaciones en el ámbito de la seguridad de la información.

LAN (Local Área Network – Red de Área Local): Interconexión de computadoras y periféricos para formar una red dentro de una empresa u hogar, limitada generalmente a un edificio.

Metodología: Conjunto de métodos utilizados en la investigación científica

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

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

Papeles de trabajo: Registra el planeamiento, naturaleza, oportunidad y alcance de los procedimientos de auditoría aplicados por el auditor y los resultados y conclusiones extraídas a la evidencia obtenida. Se utilizan para controlar el progreso del trabajo realizado para respaldar la opinión del auditor. Los papeles de trabajo pueden estar constituidos por datos conservados en papel, película, medios electrónicos u otros medios.

Password: Conocida también como 'clave de acceso'. Palabra o clave privada utilizada para confirmar una identidad en un sistema remoto que se utiliza para que una persona no pueda usurpar la identidad de otra.

Plan de contingencia: Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudara a controlar una situación de emergencia y minimizar sus consecuencias negativas.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

Procedimiento: Método o sistema estructurado para la ejecución de actividades.
En computación, una subrutina o subprograma, como idea general, se presenta como un algoritmo separado del algoritmo principal, el cual permite resolver una tarea específica.

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

Programa: Secuencia de instrucciones que obliga al ordenador a realizar una tarea determinada.

Programa cliente: Programa cliente o simplemente 'cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

Red: Servicio de comunicación de datos entre ordenadores. Conocido también por su denominación inglesa: 'network'. Se dice que una red está débilmente conectada cuando la red no mantiene conexiones permanentes entre los ordenadores que la forman. Esta estructura es propia de redes no profesionales con el fin de abaratar su mantenimiento.

Repositorio: Donde se almacenan los elementos definidos o creados por la herramienta, y cuya gestión se realiza mediante el apoyo de un Sistema de Gestión de Base de Datos (SGBD) o de un sistema de gestión de ficheros

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Router: Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un router (mediante bridges), y que por tanto tienen prefijos de red distintos.

Segregación de tareas: Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

Servidor: Ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con él para dicho fin. Vocablo más conocido bajo su denominación inglesa 'server'.

Sistema de información: Se denomina Sistema de Información al conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

Software: Componentes inmateriales del ordenador: programas, sistemas operativos, etc.

Switch: Dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

TI: Tecnologías de Información

Técnica: La técnica es el procedimiento o el conjunto de procedimientos que tienen como objetivo obtener un resultado determinado, ya sea en el campo de la ciencia, de la tecnología, de las artesanías o en otra actividad

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Valoración de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

INTRODUCCIÓN

Actualmente los sistemas de información y las tecnologías de información han cambiado la forma en que operan las organizaciones. A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y lo más importante su implantación logra ventajas operativas que se traducen en beneficios para las instituciones o empresas.

La seguridad de la información debe ser un proceso integrado. Esto quiere decir que con el uso de controles técnicos, administrativos y físicos, se debe lograr la confianza en los sistemas y garantizar que cumplan con los parámetros de: disponibilidad, integridad, confidencialidad, confiabilidad y desempeño.

Desde el punto de vista de los sistemas de información se presenta un proyecto para evaluar por medio de un trabajo de auditoría de sistemas los controles relacionados con la seguridad física, de la información que maneja diariamente la E.S.E CENTRO HOSPITAL DIVINO NIÑO, para desempeñar a cabalidad sus funciones y brindar un adecuado servicio a la comunidad.

El presente documento se organiza de la siguiente forma: en la primera parte se plantea el problema y su sistematización, se plantean los objetivos que se alcanzaron luego se hablan de los antecedentes directamente relacionados con el proyecto, de la factibilidad y la metodología que se siguieron. En la última parte se especifican los recursos que se utilizaron así como la distribución en tiempo de las tareas que estaban programadas y fueron realizadas.

IDENTIFICACION DEL PROBLEMA

TITULO DEL PROYECTO

AUDITORIA A LA INFRAESTRUCTURA FÍSICA DE LA RED DE DATOS DE LA SEDE PRINCIPAL Y VERIFICACIÓN DEL CUMPLIMIENTO DE LAS NORMAS DE GOBIERNO EN LÍNEA EN LA PÁGINA DE LA ESE CENTRO HOSPITAL DIVINO NIÑO.

LINEA DE INVESTIGACION

Este proyecto corresponde a la línea de investigación Sistemas Computacionales.

DESCRIPCION DEL PROBLEMA

Planteamiento del Problema: La ESE CENTRO HOSPITAL DIVINO NIÑO es una Institución prestadora de Servicios de Salud en el Municipio de San Andrés de Tumaco. Estos servicios son prestados a población de Régimen Subsidiado, Contributivo y Particular, por consiguiente es de vital importancia que la red de datos en su nivel físico se encuentre bien estructurada y cumpla con la funcion de manejar la información para que dicha entidad garantice su veracidad e integridad.

La página web de la entidad fue terminada bajo criterios profesionales mas no se han seguido los estándares que gobierno en línea pide para este tipo de entidades.

Hasta la fecha la ESE CENTRO HOSPITAL DIVINO NIÑO no ha sido sometida a ningún tipo de proceso o estudio para identificar las posibles falencias en la infraestructura física de la red de datos.

Formulación del Problema: ¿La aplicación de la auditoria para evaluar la infraestructura física de la red de datos y en el portal web en la sede principal de la ESE CENTRO HOSPITAL DIVINO NIÑO va a permitir establecer el grado de confiabilidad de la red y el portal además de brindar las recomendaciones necesarias para mejorarlas?

Sistematización del Problema

- ¿La aplicación de una auditoria para evaluar la infraestructura física de la red de datos de la ESE CENTRO HOSPITAL DIVINO NIÑO va a permitir establecer el grado de confiabilidad de esta?

- ¿La definición del grado de confiabilidad de la red de datos va a permitir establecer las recomendaciones necesarias que permitan mejorarla?

- ¿La aplicación de la auditoria para evaluar el cumplimiento de las normas según el decreto 1151 de 2008 de gobierno en línea en el portal web de la ESE CENTRO HOSPITAL DIVINO NIÑO va a permitir establecer el grado de confiabilidad de esta?

- ¿La definición del grado de confiabilidad en el portal web va a permitir establecer las recomendaciones necesarias que permitan mejorarla?

OBJETIVOS

Objetivo General: Aplicar una auditoría de sistemas para evaluar la infraestructura física de la red de datos de la sede principal de la ESE CENTRO HOSPITAL DIVINO NIÑO para evidenciar vulnerabilidades de seguridad fisica a las que se encuentra expuesta la información, y el cumplimiento del Decreto 1151 de Gobierno en Línea.

Objetivos Específicos

- Realizar de una auditoria para evaluar la infraestructura física de la red de datos y establecer el grado de confiabilidad de esta.

- Establecer las recomendaciones necesarias para mejorar la infraestructura de la red.

- Aplicar la auditoria al portal de la ESE CENTRO HOSPITAL DIVINO NIÑO para verificar el cumplimiento del decreto 1151 de Gobierno en línea.

- Realizar las recomendaciones necesarias para ayudar a mejorar el portal web.

JUSTIFICACIÓN

"*La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de los elementos de una organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alterativos se logre una utilización más eficiente de la información que servirá para una eventual toma de decisiones*."[1]

La auditoría de sistemas es de gran importancia para el excelente desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un excelente nivel de seguridad.

Para ayudar a cumplir a cabalidad las funciones de la ESE CENTRO HOSPITAL DIVINO NIÑO, esta se encuentra regida por los estándares de habilitación que exige el Instituto Departamental de Salud de Nariño. Es justificable la aplicación de medidas y estrategias para asegurar el adecuado y transparente manejo de los recursos y la información que está a cargo de dicha entidad.

Con la realización de la auditoria la ESE CENTRO HOSPITAL DIVINO NIÑO, dispondrá de información necesaria para la realización de un plan de mejoramiento de los procesos relacionados con la administración de información, beneficiando a los usuarios directos e indirectos, ya se mejorará la calidad del sistema de información y por ende la prestación del servicio.

ALCANCE Y DELIMITACIÓN

En el desarrollo del proyecto se identificaron diferentes técnicas de auditoría de sistemas, y se utilizó la más adecuada en cada uno de los casos de estudio.

La aplicación de técnicas de auditoría de sistemas se realizó a la infraestructura de la red de datos de la sede principal y la página web de la ESE CENTRO HOSPITAL DIVINO NIÑO en el municipio de San Andrés de Tumaco, con esto se identificó, comprobó y evaluó las vulnerabilidades de seguridad física a la que está expuesta la entidad en su red de datos de la sede principal. Además, se audito el sitio Web de la entidad y se verifico si cumplía con los lineamientos del Decreto 1151 de 2008 de la estrategia de Gobierno en Línea. Finalmente los resultados de este proceso se plasmaron en este informe que servirá para que la entidad, tome medidas preventivas y correctivas que subsanen los problemas detectados.

[1] ECHENIQE GARCIA José A., Auditoría en informática, segunda edición 2a Ed., Mc Graw Hill D. F. 2005.

1. MARCO TEORICO

1.1. ANTECEDENTES

La auditoría de los sistemas de información ha surgido cuando las empresas e instituciones han tomado conciencia de que los datos que adquieren, conservan, procesan y emiten, es vital para su propia supervivencia diaria y proyección de eficiencia. Por tanto, han elevado a la categoría de sistemas críticos prácticamente todos los sistemas internos que manejan información en uno solo, denominado sistema de información. En consecuencia por su naturaleza crítica el enfoque de auditoría debe anotar una perspectiva que se adecue absolutamente a estos sistemas, sea mediante la transformación de métodos, técnicas y procedimientos de la auditoria tradicional, ósea mediante la creación de unos nuevos.

A principios de los años 80's, se empiezan a utilizar técnicas de tratamiento de la información por medio de computadores, como apoyo a la labor de los auditores. El auditor de sistemas de información empieza a ser también experto en el uso de lenguajes informáticos que le sirven para escribir, compilar y ejecutar programas para la consecución de pruebas y obtención de evidencia.

Con la introducción de nuevas tecnologías, pronto se detectaron las limitaciones de los métodos tradicionales para realizar la auditoria de sistemas. En su afán de maximizar la eficiencia de los procesos de auditorías, surgen nuevos modelos que se adecuan a las crecientes necesidades del sector de las tecnologías de la información, entre ellos se tienen:

Directrices gerenciales de COBIT, desarrollado por la *Information Systems Audit Control Associatio*n (ISACA):

Las Directrices Gerenciales son un marco internacional de referencias que abordan las mejores prácticas de auditoría y control de sistemas de información. Permiten que la gerencia incluya, comprenda y controle los riesgos relacionados con la tecnología de información y establezca el enlace entre los procesos de administración, aspectos técnicos, la necesidad de controles y los riesgos asociados.

The Management of the Control of Data Information Technology, desarrollado por el Instituto Canadiense de Contadores Certificados (CICA):

Este modelo está basado en el concepto de errores que establece responsabilidades relacionadas con la seguridad y los controles correspondientes. Dichos roles están clasificados con base en siete grupos: administración general, gerentes de sistemas, dueños, agentes, usuarios de sistemas de información, así como proveedores de servicios, desarrollo y operaciones de servicios y soporte de sistemas. Además, hace distinción entre los conceptos de autoridad, responsabilidad y respecto a control y riesgo previo al establecimiento del control, en términos de objetivos, estándares y técnicas mínimas a considerar.

SysTrust – Principios y criterios de confiabilidad de Sistemas, desarrollados por la Asociación de Contadores Públicos (AICPA) y el CICA:

Este servicio pretende incrementar la confianza de alta gerencia, clientes y socios, con respecto a la confiabilidad en los sistemas por una empresa o actividad en particular. Este modelo incluye elementos como: infraestructura, software de cualquier naturaleza, personal especializado y usuarios, procesos manuales y automatizados, y datos. El modelo persigue determinar si el sistema de información es confiable, (i.e. si un sistema funciona sin errores significativos, o fallas durante un periodo de prueba determinado bajo un ambiente dado).

Modelo de Evaluación de Capacidades de software (CMM), desarrollado por el Instituto de Ingenieros de Software (SEI):

Este modelo hace posible evaluar las capacidades o habilidades para ejecutar, de una organización con respecto al desarrollo y mantenimiento de sistemas de información. Consiste en 18 sectores clave, agrupados alrededor de cinco niveles de madurez. Se puede considerar que CMM es la base de los principios de evaluación recomendados por COBIT, así como para algunos de los procesos de administración de COBIT.

ISO/IEC 27001(*Information Technology – Security Techniques – Information Security Management System – Requirements*) especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Según el conocido “Ciclo de Deming”: PDCA – acrónimo de plan, *Do Check, Act* (Planificar, Hace, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/17799 (Actual ISO ICE 27002) y tiene su origen en la revisión de la norma Británica *British Standard* BS 7799 – 2: 2002.

Si se revisan los antecedentes de proyectos relacionados auditoría de sistemas en la universidad de Nariño se encuentran:

Proyecto: DEFINICION DE POLITICAS DE SEGURIDAD INFORMATICA PARA EL CENTRO DE INFORMATICA DE LA UNIVERSIDAD DE NARIÑO.

Realizado por María Constanza Torres B. y Efraín Fajardo Guevara, el trabajo consistió en realizar los procesos de auditoría a la seguridad del centro de informática de la Universidad de Nariño.

Proyecto: TECNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACION Y PAGINAS WEB EN ENTIDADES OFICIALES DEL DEPARTAMENTO DE NARIÑO.

Realizado por Luis Carlos Chaves Yela y Ricardo Alexander Cabrera Solarte, el trabajo consistió en realizar una auditoría al proceso de contratación y evaluar el cumplimiento del decreto 1151 de 2008 concerniente a Gobierno en Línea en el Hospital Universitario Departamental de Nariño E.S.E y el Hospital Civil de Ipiales E.S.E.

Proyecto: TECNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACION Y PAGINAS WEB EN ENTIDADES OFICIALES DEL DEPARTAMENTO DE NARIÑO.

Realizado por Lenin Geovanny Ibarra González y Diego Mauricio Meza García, el trabajo consistió en realizar una auditoría al proceso de contratación y evaluar el cumplimiento del decreto 1151 de 2008 concerniente a Gobierno en Línea en la Alcaldía Municipal de Tangua y Alcaldía Municipal de Yacuanquer

1.2. ASPECTOS GENERALES SOBRE AUDITORIA

La auditoría puede definirse como un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso. [2]

Por otra parte la auditoría constituye una herramienta de control y supervisión que contribuye a la creación de una cultura de la disciplina de la organización y permite descubrir fallas en las estructuras o vulnerabilidades existentes en la organización.

La auditoría como función de control debe ser la herramienta a utilizar para ayudar a los Funcionarios que tienen responsabilidad Administrativa, Técnica y Operacional a que no incurran en falta. Y es por ello que aquí el Control debe ser creativo, inteligente, y constructivo de asesoramiento oportuno a todas las

[2] GESTIOPOLIS, Biblioteca virtual, Auditoria, Disponible en: http://www.gestiopolis.com/recursos/documentos/fulldocs/fin/auditcontxactual.htm,(Citado el 2 de enero de 2013)

direcciones o gerencias a fin de que la toma de decisiones sea acertada, segura y se logren los objetivos, con la máxima eficiencia.

La responsabilidad de un procedimiento de auditoría debe ir más allá de la búsqueda de problemas y de responsables, la visión de la auditoría debe dar la visión de la empresa en su conjunto.

Por lo que saca el máximo provecho de la información real y existente, convirtiéndola en herramienta de reingeniería capaz de retroalimentar procesos o crear nuevos, la auditoria se volvió capaz de identificar necesidades, problemas y soluciones a futuro, con estas facultades el proceso de auditoría se promueve como una función permanente y a largo plazo.

1.2.1. Auditoria Interna. Es una actividad independiente que realiza la empresa y que está encaminada a la revisión de operaciones contables además de la evaluación y medición de la eficacia de otros controles, con la finalidad de prestar un servicio a la dirección. Se aplica mejor en empresas medianas que tienden a aumentar en volumen, extensión geográfica y complejidad y se hace imposible el control directo de las operaciones por parte del director.

El objetivo principal es ayudar a la dirección en el cumplimiento de sus funciones y responsabilidades, proporcionándole un análisis objetivo, evaluaciones y recomendaciones pertinentes sobre las operaciones examinadas.

Otros objetivos que se busca concretar a través de la auditoria interna son: realizar investigaciones especiales solicitadas por la dirección, preparar informes de auditoría acerca de las irregularidades que pudiesen encontrarse como resultado de las investigaciones, expresando igualmente las recomendaciones que se juzguen adecuadas, vigilar el cumplimiento de la recomendaciones contenidas en los informes emitidos con anterioridad.

La auditoría interna posee varias ventajas: facilita una ayuda primordial a la dirección al evaluar de forma relativamente independiente los sistemas de organización y de administración, facilita una evaluación global y objetiva de los problemas de la empresa que generalmente suelen ser interpretados de una manera parcial por los departamentos afectados, pone a disposición de la dirección un profundo conocimiento de las operaciones de la empresa, proporcionado por el trabajo de verificación de los datos contables y financieros, contribuye eficazmente a evitar las actividades rutinarias que generalmente se desarrollan en las grandes empresas, favorece la protección de los intereses y bienes de la empresa frente a terceros.

1.2.2. Auditoria externa. Se puede definir como los métodos empleados por una firma externa de profesionales para averiguar la exactitud del contenido de los estados financieros presentados por una empresa. Se trata de dar carácter público, mediante la revisión, a unos estados financieros que en principio eran privados.

Los objetivos de la auditoría externa son: proporcionar a la dirección y a los propietarios de la empresa unos estados financieros certificados por una autoridad independiente e imparcial, proporcionar asesoramiento a la gerencia y a los responsables de las distintas áreas de la empresa en materia de sistemas contables y financieros, procedimientos de organización y otras numerosas fases de la operatoria de una empresa, suministrar información objetiva que sirva de base a las entidades de información y clasificación crediticia, servir de punto de partida en las negociaciones para la compraventa de las acciones de una empresa, reducir y controlar riesgos accidentales, fraudes y otras actuaciones anormales, liberar implícitamente a la gerencia de sus responsabilidades de gestión.

❖ **Diferencias entre auditoria interna y externa**

- En la Auditoría Interna existe un vínculo laboral entre el auditor y la empresa, mientras que en la Auditoría Externa la relación es de tipo civil.
- En la Auditoría Interna el diagnóstico del auditor, está destinado para la empresa; en el caso de la Auditoría Externa este dictamen se destina generalmente para terceras personas o sea ajena a la empresa.
- La Auditoría Interna está inhabilitada para dar Fe Pública, debido a su vinculación contractual laboral, mientras la Auditoría Externa tiene la facultad legal de dar Fe Pública.

❖ **Principios generales de la auditoria externa**

- **Exposición:** Los estados financieros deben recoger por completo y con claridad todas las transacciones de la empresa.

- **Uniformidad:** la base utilizada en la preparación de los estados financieros de un ejercicio no debe experimentar ninguna variación con respecto al ejercicio precedente.

- **Importancia o** materialidad: Este es el criterio que debe presidir el trabajo del auditor es la importancia económica o materialidad de las partidas.

- **Moderación:** De dos o más posibilidades igualmente validas se debe escoger siempre la que dé los resultados más desfavorables.

❖ **Normas generales de la auditoría externa**

Afectan a las condiciones que debe de reunir el auditor de y a su comportamiento en el desarrollo de la actividad de auditoría.

- Realización por una persona competente.

- Realización por una persona independiente.

- Cuidado profesional en la realización del trabajo y en la confección del informe.

❖ **Normas de trabajo de la auditoría externa**

Hacen referencia a la preparación y ejecución del trabajo a realizar por el auditor, regulan el conjunto de técnicas de investigación e inspección aplicables a los hechos relativos a los documentos contables sujetos a examen, mediante los cuales el auditor fundamenta su opinión responsable e independiente.

- Programación adecuada.

- Supervisión adecuada.

- Análisis del control interno para fijar el alcance de la pruebas.

- Opinión basada en un material y un trabajo razonablemente suficiente.

❖ **Normas del informe de la auditoría externa**

Regulan los principios que han de ser observados en la elaboración y presentación del informe de auditoría estableciendo la extensión y contenido de los diferentes tipos de informes, así como los criterios que fundamenten el modelo de informe a utilizar en cada caso.

- Expresión de si los estados financieros se ajustan a los principios de contabilidad generalmente aceptados.

- Expresión de si se han presentado los estados financieros de manera uniforme con respecto al periodo precedente.

- Exposiciones informativas razonablemente adecuadas a los estados financieros.

- El informe debe contener un dictamen sobre los estados financieros considerados en su conjunto.

❖ **Procedimientos de la auditoría externa**

Son la serie de trabajos que hay que realizar para el adecuado cumplimiento de los principios y las normas, antes de presentar el informe definitivo. Se pueden señalar los siguientes procedimientos:

- Revisión de las actividades en las operaciones.
- Inspecciones físicas y recuentos.
- Obtención de pruebas de evidencia.
- Obtención de pruebas de exactitud.
- Preparación de reconciliaciones.

1.3. EL AUDITOR

El auditor se refiere a la persona que asume la responsabilidad de realizar un trabajo de este tipo, en todo caso el auditor debe poseer ciertas cualidades para afrontar un trabajo como este:

- Deberá dominar las técnicas y metodologías del proceso auditor.
- Debe ser abierto en sus relaciones personales y que sepa dialogar.
- Debe poseer diversas actitudes como la independencia, la objetividad, la creatividad, el espíritu crítico, la diplomacia, etc.
- El auditor debe mantener un cierto grado de independencia en los asuntos que se encuentra evaluando.
- El auditor tiene la obligación de realizar con esmero y cuidado el dictamen o informe para el que fue contratado.
- Debe poseer una actitud positiva frente a la entidad evaluada.
- Debe tener estabilidad emocional frente la entidad.
- Es su obligación la de respetar las ideas de los demás.
- Debe tener capacidad para la negociación.
- Sera discreto y respetuoso con la información de la empresa.
- Su comportamiento debe ceñirse a la ética profesional.

Dadas estas características el auditor responsablemente deberá cumplir con las siguientes funciones:

- 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
- Captar la información necesaria para evaluar la funcionalidad y efectividad de los procesos, funciones y sistemas utilizados.
- Recabar y revisar estadísticas sobre volúmenes y cargas de trabajo.
- Diagnosticar sobre los métodos de operación y los sistemas de información.
- Detectar los hallazgos y evidencias e incorporarlos a los papeles de trabajo.
- Respetar las normas de actuación dictadas por los grupos de filiación, corporativos, sectoriales e instancias normativas y, en su caso, globalizadoras.
- Proponer los sistemas administrativos y/o las modificaciones que permitan elevar la efectividad de la organización.
- Analizar la estructura y funcionamiento de la organización en todos sus ámbitos y niveles.
- Revisar el flujo de datos y formas.
- Considerar las variables ambientales y económicas que inciden en el funcionamiento de la organización.
- Analizar la distribución del espacio y el empleo de equipos de oficina.
- Evaluar los registros contables e información financiera.
- Mantener el nivel de actuación a través de una interacción y revisión continua de avances.
- Proponer los elementos de tecnología de punta requeridos para impulsar el cambio organizacional.
- Diseñar y preparar los reportes de avance e informes de una auditoria.

1.4. TIPOS DE AUDITORIA

Existen algunos tipos de Auditoría entre los que la Auditoría de Sistemas integra un mundo paralelo pero diferente y peculiar resaltando su enfoque a la función informática.

Entre los principales enfoques de Auditoría tenemos los siguientes:

1.4.1. Auditoría fiscal. Es una comprobación científica y sistemática de los estados financieros, libros de cuentas, comprobantes y otros registros financieros y legales de una persona natural, firma o corporación realizado por un auditor con el fin de asegurar si los libros han sido llevados por los principios de contabilidad generalmente aceptados y así brindar confianza y credibilidad a las personas, ya sean naturales o jurídicas que puedan estar interesadas en los estados de la empresa. La persona quien realice la auditoría debe ser un ente ajeno a la empresa, de esta manera se evitan vínculos que puedan verse reflejados en una opinión positiva o parcialización a través de la empresa sin que la misma lo merezca. También es necesario mencionar que si la auditoría esta hecha por una firma con una amplia y reconocida trayectoria esta otorgara una mayor credibilidad

y confianza a las personas interesadas. En conclusión la auditoría fiscal se dedica a observar el cumplimiento de las leyes fiscales.

La auditoría fiscal tiene como principales objetivos:

- Determinar si sus sistemas contables son aceptables.
- Conocer si el catálogo de cuentas es aceptable.
- Verificar si se está al día en el cumplimiento de sus deberes formales.
- Detectar áreas de riesgo y saber exactamente que correctivos aplicar.

1.4.2. Auditoría financiera. Es una revisión de los estados financieros similar a la auditoría externa. Su objetivo es expresar una opinión sobre si las cifras del balance y la cuenta de resultados presentan razonablemente la situación actual de la empresa de acuerdo con los principios de contabilidad generalmente aceptados.

En general la auditoría financiera busca comprobar la veracidad de los estados financieros de la empresa y preparar informes de acuerdo a principios contables

1.4.3. Auditoria operacional. Es una evaluación objetiva, constructiva, sistemática y profesional de las actividades relativas al proceso de gestión de una organización, con el fin de determinar el grado de eficiencia, eficacia, efectividad, economía, equidad, excelencia y valoración de costos ambientales, con que son manejados los recursos; la adecuación y fiabilidad de los sistemas de información y control, de manera que cumpla con las políticas establecidas para alcanzar sus objetivos.

Los informes emergentes de este tipo de auditoría son:

- Auditoría Operativa, relacionada básicamente con los objetivo de eficacia, eficiencia y economía.
- Evaluaciones del Sistema de Control Interno, cuyo propósito es evaluar el diseño y funcionamiento de los Sistemas establecidos.

La auditoría operativa implica:

- El período objeto de examen.
- Examen y verificación de la información relativa al desempeño institucional.
- Revisión y elaboración de informes sobre la administración de recursos.
- Análisis de actividades y procesos clave, evaluación de sistemas de información y control.
- Verificar la utilización de recursos públicos de conformidad a principios de eficiencia, efectividad, economía, eficacia, equidad y excelencia.
- Verificar el cumplimiento de metas y objetivos.

- Evaluar la gestión.

Este tipo de auditoría se aplica generalmente en el Sector Público, Sector Privado, Sector Social.

El objetivo primordial de la auditoria operacional es brindar a todo tipo de organización la información necesaria para utilizar esta poderosa herramienta en forma congruente con sus necesidades y capacidad instalada, a fin de evaluar su comportamiento y derivar las medidas requeridas para mejorar su desempeño. Otras razones por las que se realiza esta auditoria son para establecer el grado en que la entidad y sus servidores han cumplido adecuadamente los deberes y atribuciones que les han sido asignados, determinar el grado en que el organismo y sus funcionarios controlan y evalúan la calidad tanto en los servicios que presta como en los bienes adquiridos y verificar que la entidad auditada cumpla con normas y demás disposiciones.

1.4.4. Auditoria administrativa. Independientemente de ser ella misma parte integrante del sistema total de control superior, es la principal herramienta para la revisión y evaluación de los resultados logrados. Cumple con una doble misión: primero, como parte integrante del control superior; es decir, un medio para obtener y mantener el control; el segundo es; el medio principal para la medición y evaluación de resultados.

Por tanto la dirección superior, propietarios, accionistas, auditores financieros y otros interesados deben confiar en ésta para la prevención de inconvenientes, y para garantizar la adecuada marcha del sistema.

La auditoría administrativa, como función interna, puede verse desde el punto de vista de la organización como:

- Una extensión de la auditoría interna financiera.
- Función independiente de la administración financiera.
- Forma departamental con la auditoría interna.
- Órgano asesor del consejo de administración.

Las funciones de a auditoria administrativa deben quedar enmarcadas dentro de la organización de una empresa en una unidad que, por su situación jerárquica le permita la consecución de sus fines.

El nivel donde deberá quedar la unidad departamental de auditoría administrativa reunirá las siguientes características:

- Jerarquía suficiente para poder inmiscuirse en cualquier unidad administrativa de la empresa.
- Que el tipo de funciones de dicha unidad sea relacionado con la dirección, control y coordinación.
- Que tenga suficiente autoridad sobre los demás departamentos.

Funciones que se van a desarrollar en una auditoria administrativa:

- Investigación constante de planes y objetivos.
- Estudio de las políticas y sus prácticas.
- Revisión constante de la estructura orgánica.
- Estudio constante de las operaciones de la empresa.
- Analizar la eficiencia de la utilización de recursos humanos y materiales.
- Revisión del equilibrio de las cargas de trabajo.
- Revisión constante de los métodos de control.

1.4.5. Auditoría integral. Es el proceso de obtener y evaluar objetivamente, en un período determinado, evidencia relativa a la información financiera, al comportamiento económico y al manejo de una entidad con la finalidad de informar sobre el grado de correspondencia entre aquellos y los criterios o indicadores establecidos o los comportamientos generalizados.

El objetivo de la auditoría integral es evaluar los sistemas de control, implantados por la Gerencia General que le permitan medir el rendimiento económico y los recursos financieros de la empresa.

Además con la auditoría integral se pretende conocer la normativa que regula a la auditoría Integral, analizar el ambiente de aplicación de la auditoría Integral, verificar a través de la utilización de un conjunto estructurado de proceso tomando como objetivo la evaluación sistemática y permanente del ente económico para una aseveración verificable.

La Auditoría Integral implica la ejecución de un trabajo con el trabajo o enfoque, por analogía de las revisiones financieras, de cumplimiento, control interno y de gestión, sistema y medio ambiente con los siguientes objetivos:

- Determinar, si los Estados Financieros se presentan de acuerdo con los Principios de Contabilidad Generalmente Aceptados.

- Determinar, si el ente ha cumplido, en el desarrollo de sus operaciones con las disposiciones legales que le sean aplicables, sus reglamentos, los estatutos y las decisiones de los órganos de dirección y administración.

- Evaluar la estructura del control interno del ente con el alcance necesario para dictaminar sobre el mismo.

- Evaluar el grado de eficiencia en el logro de los objetivos previstos por el ente y el grado de eficiencia y eficacia con que se han manejado los recursos disponibles.

- Evaluar los mecanismos, operaciones, procedimientos, derechos a usuarios, responsabilidad, facultades y aplicaciones específicas de control relacionadas con operaciones en computadora.

- Evaluar el impacto medioambiental producido de manera directa o indirecta por empresas que presentan un perfil ambiental diferente, condicionado por los riesgos aparentes asociados con sus procesos y productos; la edad, historia y estado de una planta, el marco jurídico en el cual opera.

Los principios generales de auditoría integral son: independencia, objetividad, permanencia, certificación, integridad, planeamiento, supervisión, oportunidad, forma, cumplimiento de las Normas de Profesión.

Para que el ejercicio de la Auditoría Integral se desarrolle en un ambiente controlado, es importante conducirla dentro de un concepto de normas que provean una estructura, como la posibilidad de pronosticar los resultados.

La aplicación de normas ayudará a desarrollar una auditoría de alta calidad respondiendo a la necesidad de completar tareas difíciles en forma oportuna, evitando formar juicios prematuros basados en información incompleta por la falta de tiempo, asimismo, establecen orden y disciplina, produciendo auditorías efectivas, garantizando la veracidad de los hallazgos y el soporte adecuado para las recomendaciones, consecuentemente habrá una mayor aceptación por parte de la gerencia.

1.4.6. Auditoria de sistemas. Se ocupa de analizar la actividad que se conoce como técnica de sistemas en todas sus facetas. Hoy, la importancia creciente de las telecomunicaciones ha propiciado que las comunicaciones. Líneas y redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de sistemas.

Su finalidad es el examen y análisis de los procedimientos administrativos y de los sistemas de control interno de la compañía auditada. Al finalizar el trabajo realizado, los auditores exponen en su informe aquellos puntos débiles que hayan podido detectar, así como las recomendaciones sobre los cambios convenientes a introducir, en su opinión, en la organización de la compañía.

Normalmente, las empresas funcionan con políticas generales, pero hay procedimientos y métodos, que son términos más operativos. Los procedimientos son también sistemas; si están bien hechos, la empresa funcionará mejor. La auditoría de sistemas analiza todos los procedimientos y métodos de la empresa con la intención de mejorar su eficacia.

Existen varios campos de acción en los que la auditoria informática de sistemas puede operar entre ellos se tienen las auditorias más destacadas del tipo:

- **Sistemas Operativos.**

Engloba los Subsistemas de Teleprocesos, Entrada/Salida, etc. Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir la posible incompatibilidad entre otros productos de Software Básicos adquiridos por la instalación y determinadas versiones de aquellas. Deben revisarse los parámetros variables de las librerías más importantes de los Sistemas, por si difieren de los valores habituales aconsejados por el constructor.

- **Software Básico.**

Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al software desarrollado por el personal informático de la empresa, el auditor debe verificar que este no agreda ni condiciona al Sistema Igualmente, debe considerar el esfuerzo en términos de costes, por si hubiera alternativas más económicas.

La auditoría, al igual que cualquier otra actividad, requiere de una buena planeación, que le permita desarrollarse eficientemente y oportunamente.

- **Auditoria Web.**

La auditoría web está diseñada para identificar cuáles son los puntos débiles de la presencia online, para mejorarla y para que en los puntos fuertes se pueda sacar el máximo rendimiento a la internet

Con los diferentes tipos de auditoría web se podrá conocer:

- Las limitaciones técnicas de la página.
- Que le falta a la página para estar optimizada.
- Quién y desde dónde vienen las visitas.

- Cómo se mueven los usuarios de la página.
- Qué productos o servicios visitan más los usuarios.
- Qué sitios enlazan la página.
- Con que palabras clave está mejor posicionada la pagina.

1.5. AUDITORIA DE SISTEMAS COMO OBJETO DE ESTUDIO

Desde que la informática se enfocó hacia el apoyo de la sistematización en las áreas del negocio, se empezaron a implantar aplicaciones administrativas como contabilidad, nómina, etc., lo que originó el proceso conocido como auditoria a sistemas de información.

La auditoría de sistemas es el proceso de 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. También permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes.

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

La auditoría de sistemas permite además verificar que la información desde su entrada, procedimientos, controles, almacenamientos y salidas, sea integra y verificable y por tanto permita el apoyo a la toma de decisiones dentro de una organización.

Dentro de este procedimiento es necesario evaluar los mecanismos de control implantados en una organización, determinando así, si son adecuados y cumplen con los objetivos o estrategias, de esta manera, es posible proponer cambios que se deberían realizar para el mejoramiento de los mismos. Estos mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

1.5.1. Alcance de la auditoria de sistemas. El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría de sistemas, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas. La indefinición de los alcances de la auditoria compromete el éxito o el fracaso de la misma. Así mismo, las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar.

1.5.2. Objetivos de la auditoria de sistemas

- **Objetivo general de la auditoria de sistemas**

El objetivo principal de la auditoria de sistemas es evaluar el uso adecuado de los sistemas para el correcto ingreso de datos, el procesamiento adecuado de la información y la emisión oportuna de los resultados en la organización, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas de información dentro de la empresa.

- **Objetivos específicos de la auditoria de sistemas**

- El control de la función informática.
- El análisis de la eficiencia de los Sistemas Informáticos.
- La verificación del cumplimiento de la Normativa en este ámbito.
- La revisión de la eficaz gestión de los recursos informáticos.

La auditoría de sistemas sirve para mejorar ciertas características en la empresa como:

- Eficiencia.
- Eficacia.
- Rentabilidad
- Seguridad

1.5.3. Principales pruebas y herramientas para efectuar una auditoría de sistemas

- **Pruebas sustantivas:** Verifican el grado de confiabilidad del sistema de información de la organización. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican así mismo la exactitud, integridad y validez de la información.

- **Pruebas de cumplimiento:** Verifican el grado de cumplimiento de aquello extraído el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente

Las principales herramientas de las que dispone un auditor informático son:

- Observación
- Realización de cuestionarios
- Entrevistas a auditados y no auditados
- Muestreo estadístico
- Flujo gramas
- Listas de chequeo
- Mapas conceptuales

1.5.4. Perfiles Profesionales de los auditores informáticos.

Tabla 1. Perfiles Profesionales y Actividades

Profesión	Actividades y conocimientos deseables
Informático Generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costes	Economista con conocimiento de Informática. Gestión de costes.

1.5.5. Pasos a seguir para una auditoria de sistemas en una organización.

Estudio preliminar. Para realizar dicho estudio se examinan las funciones y actividades generales del área o departamento de sistemas, con el fin de tener un contacto inicial con el personal de dicha área, y conocer a grandes rasgos la distribución del sistema, características de equipos, instalaciones y medidas de seguridad visibles.

Para su realización el auditor debe conocer lo siguiente:

- **Organización:** Es de vital importancia conocer dentro del departamento o área de sistemas quien es el jefe, quien diseña y quien ejecuta, para lo cual es necesario conocer:

  - Organigrama: El organigrama permite conocer la estructura oficial dentro de la organización a auditar.

  - Departamentos: Es importante conocer los departamentos que hacen parte de la organización y las funciones que se deben llevar a cabo dentro de cada uno de ellos.

  - Relaciones Jerárquicas y funcionales entre órganos de la Organización: Es necesario verificar si dentro de la organización se cumplen las relaciones funcionales y jerárquicas que se evidencian dentro del organigrama.

- **Corrientes de información:** Los flujos de información entre los diferentes departamentos dentro de una organización son de vital importancia ya que evidencian una gestión eficiente, siempre y cuando estas corrientes no vayan en direcciones no contempladas dentro del organigrama.

En muchas ocasiones es posible que se hayan creado canales de información alternativos, lo cual ocurre cuando existen pequeños o grandes fallos en la estructura de la organización.

Además, la aparición de corrientes de información no planeados pueden obedecer a afinidades personales o desacato a las reglas establecidas. Los cuales pueden producir perturbaciones dentro de la organización.

- **Flujos de información:** Dentro del proceso de auditoría es necesario verificar que los nombres de los cargos dentro de la organización correspondan a las funciones que realiza esa persona.

Puede ocurrir que bajo nombres de cargos diferentes se realicen funciones idénticas, en este caso se estaría realizando tareas redundantes lo cual podría conllevar a deficiencias estructurales.

➢ **Entorno operacional:** Es importante conocer por parte de los auditores de sistemas la referencia del entorno en el cual se va a trabajar, esto se logra determinando:

o Ubicación geográfica del o los centros de procesamiento de información de la empresa. Evaluando además el personal responsable de cada uno de ellos.

o Arquitectura y configuración de Hardware y Software: es fundamental la verificación de la compatibilidad e intercomunicación de los equipos ya que estas, están estrechamente ligadas a los grados de seguridad lógica de las organizaciones.

o Situación geográfica de los Sistemas: el equipo auditor debe estudiar la información que proporcione la organización sobre los elementos físicos y lógicos de las instalaciones.

o Comunicación y Redes de Comunicación: se debe disponer de un inventario, estado y características de las redes de comunicación.

➢ **Aplicaciones bases de datos:** Finalmente para el equipo auditor es necesario tener una idea general de los procesos informáticos realizados dentro de la organización.

Para ello es necesario recolectar la siguiente información:

o Inventario de Hardware y Software

o Volumen, antigüedad y complejidad de las Aplicaciones

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:

o Metodología del diseño: 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.
o Documentación: El auditor recaudara 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.

- **Determinación de recursos de la auditoría de sistemas.** Por medio de los resultados del estudio preliminar es posible determinar los recursos humanos y físicos que son necesarios en el proceso de auditoría.

- **Elaboración del plan y de los programas de trabajo.** El plan de trabajo se realiza de acuerdo a los siguientes criterios:

➢ El proceso de auditoría se llevara a cabo en áreas generales o específicas.

➢ La auditoría se hará de manera global o especifica.

➢ De acuerdo a si se manejaran recursos genéricos o específicos se realizará un cronograma de trabajo.

➢ El Plan establece disponibilidad futura de los recursos durante la revisión.

➢ El Plan estructura las tareas a realizar por cada integrante del grupo auditoria.

➢ 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 flexible como para permitir modificaciones a lo largo del proyecto.

- **Actividades de la auditoría de sistemas.** La auditoría de sistemas 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.** El informe final de la auditoria de sistemas se realiza por escrito, el cual contempla la siguiente estructura:

  - Definición de objetivos y alcance de la auditoría
  - Enumeración de temas objeto de la auditoria
  - Cuerpo de la auditoria: para lo cual se mostrara los siguiente para cada tema:

    - Situación actual
    - Tendencias futuras
    - Puntos débiles y amenazas
    - Recomendaciones y planes de acción
    - Redacción posterior de la Carta de Introducción o Presentación

Algunas Características que deben ser consideradas en los informes son:

Las características de fondo se refieren a que la información sea veraz y oportuna, el uso de la terminología se exacta y objetiva, que exista congruencia con lo observado sin hacer ninguna distorsión de lo encontrado.

Las características de forma: el estilo de redacción concreto conciso, clara, sencilla y amena, que no haya redundancia, redacción impecable en ortografía.

1.6. METODOLOGÍAS DE AUDITORIA DE SISTEMAS

La auditoría de sistemas en el ámbito empresarial, ha sido de gran importancia, puesto que con ella se pretende gestionar la información y sirve como apoyo a la toma de decisiones. Además se busca disponer de un sistema de información que sea eficiente y eficaz para obtener la mayor productividad y calidad posibles, debido a que la información se ha convertido en el activo más importante de las empresas.

En la actualidad, gran parte de las organizaciones consideran que la información y la tecnología representan activos importantes para la misma, sin dejar de lado otros activos indispensables, como los requerimientos de calidad, controles, seguridad e información. Por tal razón los directivos deben establecer un adecuado sistema de control interno, para proporcionar seguridad razonable, respecto a si están lográndose los objetivos como: promover la efectividad y eficiencia de las operaciones, proteger y conservar todos los recursos de la organización, cumplir las leyes y reglamentos internos y externos relacionados con la empresa.

Para esto, se hace necesario aplicar una auditoria de sistemas llevando a cabo una metodología adecuada, que permita evaluar de manera objetiva las vulnerabilidades o falta de controles existentes en la empresa.

Las metodologías desarrolladas y utilizadas en la auditoría y el control informático, se dividen en dos grupos:

- Cuantitativas
- Cualitativas

Las metodologías cuantitativas están basadas en un modelo matemático, diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados unos valores numéricos. Estos valores son datos de probabilidad de ocurrencia de un evento que se debe extraer de un riesgo de incidencias donde el número de incidencias tiende al infinito.

Y las metodologías cualitativas están basadas en el criterio humano capaz de definir un proceso de trabajo. Así mismo, esta metodología establece métodos estadísticos y lógica borrosa, que requiere menos recursos humanos y menos tiempo que las metodologías cuantitativas.

Esta metodología presenta un enfoque amplio y logra un plan de trabajo flexible y reactivo. Sin embargo tiene la desventaja de depender mucho de la experiencia, habilidad y calidad del profesional involucrado. Dicha anomalía nace de la dificultad que tiene un profesional sin experiencia que asume la función auditora y

busca una fórmula fácil que le permita empezar su trabajo rápidamente. Por lo tanto es necesario que el auditor tenga una gran experiencia y una gran formación tanto auditora como informática. Esta formación debe ser adquirida mediante el estudio y la práctica.[3]

Estas últimas hacen parte de los modelos a seguir dentro del control interno y son necesarias para desarrollar cualquier proyecto de manera ordenada y eficaz, por lo que cada una cumple un papel importante y al optar por una de ellas, el auditor debe cumplirlas a cabalidad.

1.6.1. COBIT (Control Objectives for Information and related Technology). La Organización ISACA (Information Systems Audit and Control Association), se formó como una fundación de educación para llevar a cabo los esfuerzos de investigación a gran escala para expandir el conocimiento y el valor de la gobernanza de las Tecnologías de Información (TI) y el campo de control. A través de su Fundación, publicó en 1995 el COBIT, como resultado de cuatro años de intensa investigación.[4]

El COBIT es una metodología utilizada en las empresas para auditar los sistemas de información, donde se evalúa la gestión y el control, enfocado a los administradores de las TI, los usuarios y los auditores encargados del proceso.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos, está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

La estructura del modelo COBIT evalúa los criterios de información, como la seguridad y calidad, así como también se verifican los recursos que comprenden la tecnología de información, como el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos implicados en la organización.

Cuando se implementa el COBIT adecuadamente en una organización, se evalúa de manera ágil y consistente el cumplimiento de los objetivos de control, haciendo que los procesos y recursos de información y tecnología contribuyan al logro de los objetivos de la empresa.

---

[3] PIATTINI, Mario y Emilio del Peso. Auditoría Informática. Un enfoque práctico. Editorial RA-MA.

[4] En la auditoria de sistemas existen varias metodologías como: COBIT (ISACA), COSO, SAC, AICPA (SAS), IFAC (NIA), MARGERIT y EDP[7]. Sin embargo, las metodologías más utilizadas son: COBIT y COSO.

El modelo COBIT, clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro dominios:

- **Dominio: Planificación y organización (PO).**

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Procesos:

- **PO1 Definición de un plan Estratégico**

  - PO1.1 Administración del Valor de TI
  - PO1.2 Alineación de TI con el Negocio
  - PO1.3 Evaluación del Desempeño y la Capacidad Actual
  - PO1.4 Plan Estratégico de TI
  - PO1.5 Planes Tácticos de TI
  - PO1.6 Administración del Portafolio de TI

Objetivo: Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros.

Su realización se concreta a través un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

- La definición de objetivos de negocio y necesidades de TI, la alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.

- El inventario de soluciones tecnológicas e infraestructura actual, se deberá evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.

- Los cambios organizacionales, se deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI.

- Estudios de factibilidad oportunos, para que se puedan obtener resultados efectivos

➢ **PO2 Definición de la Arquitectura de Información**

- PO2.1 Modelo de Arquitectura de Información Empresarial
- PO2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos
- PO2.3 Esquema de Clasificación de Datos
- PO2.4 Administración de Integridad

Objetivo: Satisfacer los requerimientos de negocio, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurándose que se definan los sistemas apropiados para optimizar la utilización de esta información, tomando en consideración:

- La documentación deberá conservar consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.

- El diccionario de datos, el cual incorporara las reglas de sintaxis de datos de la organización y deberá ser continuamente actualizado.

- La propiedad de la información y la clasificación de severidad con el que se establecerá un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información.

➢ **PO3 Determinación de la dirección tecnológica**

- PO3.1 Planeación de la Dirección Tecnológica
- PO3.2 Plan de Infraestructura Tecnológica
- PO3.3 Monitoreo de Tendencias y Regulaciones Futuras
- PO3.4 Estándares Tecnológicos
- PO3.5 Consejo de Arquitectura de TI

Objetivo: Aprovechar al máximo de la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica, tomando en consideración:

- La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.

- El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.

- Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.

- Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

➢ **PO4 Definición de la organización y de las relaciones de TI**

- PO4.1 Marco de Trabajo de Procesos de TI
- PO4.2 Comité Estratégico de TI
- PO4.3 Comité Directivo de TI
- PO4.4 Ubicación Organizacional de la Función de TI
- PO4.5 Estructura Organizacional
- PO4.6 Establecimiento de Roles y Responsabilidades
- PO4.7 Responsabilidad de Aseguramiento de Calidad de TI
- PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento
- PO4.9 Propiedad de Datos y de Sistemas
- PO4.10 Supervisión
- PO4.11 Segregación de Funciones
- PO4.12 Personal de TI
- PO4.13 Personal Clave de TI
- PO4.14 Políticas y Procedimientos para Personal Contratado
- PO4.15 Relaciones

Objetivo: Prestación de servicios de TI

Esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, teniendo en cuenta:

- El comité de dirección el cual se encargara de vigilar la función de servicios de información y sus actividades.

- Propiedad, custodia, la Gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.

- Supervisión, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente

- Segregación de funciones, con la que se evitará la posibilidad de que un solo individuo resuelva un proceso crítico.

- Los roles y responsabilidades, la gerencia deberá asegurarse de que todo el personal deberá conocer y contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas

- La descripción de puestos, deberá delinear claramente tanto la responsabilidad como la autoridad, incluyendo las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.

- Los niveles de asignación de personal, deberán hacerse evaluaciones de requerimientos regularmente para asegurar para asegurar una asignación de personal adecuada en el presente y en el futuro.

- El personal clave, la gerencia deberá definir e identificar al personal clave de tecnología de información.

➢ **PO5 Manejo de la inversión**

- PO5.1 Marco de Trabajo para la Administración Financiera
- PO5.2 Prioridades Dentro del Presupuesto de TI
- PO5.3 Proceso Presupuestal
- PO5.4 Administración de Costos de TI
- PO5.5 Administración de Beneficios

Objetivo: tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando el financiamiento y el control de desembolsos de recursos financieros. Su realización se concreta a través presupuestos periódicos sobre inversiones y operaciones establecidas y aprobados por el negocio, teniendo en cuenta:

- Las alternativas de financiamiento, se deberán investigar diferentes alternativas de financiamiento.

- El control del gasto real, se deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información

- La justificación de costos y beneficios, deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos. Los beneficios derivados de las actividades de TI deberán ser analizados en forma similar.

➢ **PO6 Comunicación de la dirección y aspiraciones de la gerencia**

- PO6.1 Ambiente de Políticas y de Control
- PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI
- PO6.3 Administración de Políticas para TI
- PO6.4 Implantación de Políticas de TI
- PO6.5 Comunicación de los Objetivos y la Dirección de TI

Objetivo: Asegura el conocimiento y comprensión de los usuarios sobre las aspiraciones del alto nivel (gerencia), se concreta a través de políticas establecidas y transmitidas a la comunidad de usuarios, necesitándose para esto estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables. Toma en cuenta:

- Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá ser establecido por la Alta Gerencia y promoverse a través del ejemplo.
- Las directrices tecnológicas

- El cumplimiento, la Gerencia deberá también asegurar y monitorear la duración de la implementación de sus políticas.

- El compromiso con la calidad, la Gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, debiendo ser comprendidos, implementados y mantenidos por todos los niveles de la función de servicios de información.

- Las políticas de seguridad y control interno, la alta gerencia deberá asegurar que esta política de seguridad y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento de estas políticas.

➢ **PO7 Administración de recursos humanos**

- PO7.1 Reclutamiento y Retención del Personal
- PO7.2 Competencias del Personal
- PO7.3 Asignación de Roles
- PO7.4 Entrenamiento del Personal de TI

- PO7.5 Dependencia Sobre los Individuos
- PO7.6 Procedimientos de Investigación del Personal
- PO7.7 Evaluación del Desempeño del Empleado
- PO7.8 Cambios y Terminación de Trabajo

Objetivo: Maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal, tomando en consideración:

- El reclutamiento y promoción, deberá tener como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.

- Los requerimientos de calificaciones, el personal deberá estar calificado, tomando como base una educación, entrenamiento y o experiencia apropiados, según se requiera.

- La capacitación, los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.

- La evaluación objetiva y medible del desempeño, se deberá asegurar que dichas evaluaciones sean llevada a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

- **PO8 Asegurar el cumplimiento con los requerimientos Externos**

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales.Para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos y se toma en consideración:

- Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continúo de los mismos.

- Leyes, regulaciones y contratos

- Revisiones regulares en cuanto a cambios

- Búsqueda de asistencia legal y modificaciones

- Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.

- Privacidad

- Propiedad intelectual

- Flujo de datos externos y criptografía

➢ **PO9 Evaluación de riesgos**

- PO9.1 Marco de Trabajo de Administración de Riesgos
- PO9.2 Establecimiento del Contexto del Riesgo
- PO9.3 Identificación de Eventos
- PO9.4 Evaluación de Riesgos de TI
- PO9.5 Respuesta a los Riesgos
- PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos

Objetivo: Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI

Para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos y se toma en consideración:

- Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI (por ej.: tecnológicos, de seguridad, etc.) de manera de que se pueda determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable.

- Definición de alcances, limites de los riesgos y la metodología para las evaluaciones de los riesgos.

- Actualización de evaluación de riesgos.

- Metodología de evaluación de riesgos.

- Medición de riesgos cualitativos y/o cuantitativos

- Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continúa.

- Aceptación de riesgos dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

- **PO10 Administración de proyectos**

  - PO10.1 Marco de Trabajo para la Administración de Programas
  - PO10.2 Marco de Trabajo para la Administración de Proyectos
  - PO10.3 Enfoque de Administración de Proyectos
  - PO10.4 Compromiso de los Interesados
  - PO10.5 Declaración de Alcance del Proyecto
  - PO10.6 Inicio de las Fases del Proyecto
  - PO10.7 Plan Integrado del Proyecto
  - PO10.8 Recursos del Proyecto
  - PO10.9 Administración de Riesgos del Proyecto
  - PO10.10 Plan de Calidad del Proyecto
  - PO10.11 Control de Cambios del Proyecto
  - PO10.12 Planeación del Proyecto y Métodos de Aseguramiento
  - PO10.13 Medición del Desempeño, Reporte y Monitoreo del Proyecto
  - PO10.14 Cierre del Proyecto

Objetivo: Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión.

Para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido y se toma en consideración:

- Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.

- El involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.

- Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.

- Aprobación de fases de proyecto por parte de los usuarios antes de pasar a la siguiente fase.

- Presupuestos de costos y horas hombre

- Planes y metodologías de aseguramiento de calidad que sean revisados y acordados por las partes interesadas.

- Plan de administración de riesgos para eliminar o minimizar los riesgos.

- Planes de prueba, entrenamiento, revisión post-implementación.

➢ **PO11 Administración de calidad**

- PO8.1 Sistema de Administración de Calidad
- PO8.2 Estándares y Prácticas de Calidad
- PO8.3 Estándares de Desarrollo y de Adquisición
- PO8.4 Enfoque en el Cliente de TI
- PO8.5 Mejora Continua
- PO8.6 Medición, Monitoreo y Revisión de la Calidad.

Objetivo: Satisfacer los requerimientos del cliente. Para ello se realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización y se toma en consideración:

- Definición y mantenimiento regular del plan de calidad, el cual deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.

- Responsabilidades de aseguramiento de calidad que determine los tipos de actividades de aseguramiento de calidad tales como revisiones, auditorias, inspecciones, etc. que deben realizarse para alcanzar los objetivos del plan general de calidad.

- Metodologías del ciclo de vida de desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información.

- Documentación de pruebas de sistemas y programas

- Revisiones y reportes de aseguramiento de calidad

- **Dominio: Adquisición e implementación.**

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

Procesos:

- **AI1 Identificación de Soluciones Automatizadas**

  - AI1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio
  - AI1.2 Reporte de Análisis de Riesgos
  - AI1.3 Estudio de Factibilidad y Formulación de Cursos de Acción Alternativos
  - AI1.4 Requerimientos, Decisión de Factibilidad y Aprobación

Objetivo: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario.

Para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios y toma en consideración:

- Definición de requerimientos de información para poder aprobar un proyecto de desarrollo.

- Estudios de factibilidad con la finalidad de satisfacer los requerimientos del negocio establecidos para el desarrollo de un proyecto.

- Arquitectura de información para tener en consideración el modelo de datos al definir soluciones y analizar la factibilidad de las mismas.

- Seguridad con relación de costo-beneficio favorable para controlar que los costos no excedan los beneficios.

- Pistas de auditoría para ello deben existir mecanismos adecuados. Dichos mecanismos deben proporcionar la capacidad de proteger datos sensitivos (ej. Identificación de usuarios contra divulgación o mal uso)

- Contratación de terceros con el objeto de adquirir productos con buena calidad y excelente estado.

- Aceptación de instalaciones y tecnología a través del contrato con el Proveedor donde se acuerda un plan de aceptación para las instalaciones y tecnología específica a ser proporcionada.

- **AI2 Adquisición y mantenimiento del software aplicativo**

  - AI2.1 Diseño de Alto Nivel
  - AI2.2 Diseño Detallado
  - AI2.3 Control y Posibilidad de Auditar las Aplicaciones
  - AI2.4 Seguridad y Disponibilidad de las Aplicaciones

- AI2.5 Configuración e Implantación de Software Aplicativo Adquirido
- AI2.6 Actualizaciones Importantes en Sistemas Existentes
- AI2.7 Desarrollo de Software Aplicativo
- AI2.8 Aseguramiento de la Calidad del Software
- AI2.9 Administración de los Requerimientos de Aplicaciones
- AI2.10 Mantenimiento de Software Aplicativo

Objetivo: Proporciona funciones automatizadas que soporten efectivamente al negocio.

Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros y se toma en consideración:

- Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.

- Requerimientos de archivo, entrada, proceso y salida.

- Interface usuario-maquina asegurando que el software sea fácil de utilizar y que sea capaz de auto documentarse.

- Personalización de paquetes

- Realizar pruebas funcionales (unitarias, de aplicación, de integración y de carga y estrés), de acuerdo con el plan de prueba del proyecto y con los estándares establecidos antes de ser aprobado por los usuarios.

- Controles de aplicación y requerimientos funcionales

- Documentación (materiales de consulta y soporte para usuarios) con el objeto de que los usuarios puedan aprender a utilizar el sistema o puedan sacarse todas aquellas inquietudes que se les puedan presentar.

➢ **AI3 Adquisición y mantenimiento de la infraestructura tecnológica**

- AI3.1 Plan de Adquisición de Infraestructura Tecnológica
- AI3.2 Protección y Disponibilidad del Recurso de Infraestructura
- AI3.3 Mantenimiento de la Infraestructura
- AI3.4 Ambiente de Prueba de Factibilidad

Objetivo: Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios.

Para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema y toma en consideración:

- Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general.

- Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.

- Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

- **AI4 Desarrollo y mantenimiento de procedimientos**

Objetivo: Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas.

Para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:

- Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.

- Manuales de Operaciones y controles, de manera que estén en permanente actualización.

- Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

- **AI5 Instalación y aceptación de los sistemas**

  - AI7.1 Entrenamiento
  - AI7.2 Plan de Prueba
  - AI7.3 Plan de Implantación
  - AI7.4 Ambiente de Prueba
  - AI7.5 Conversión de Sistemas y Datos
  - AI7.6 Pruebas de Cambios
  - AI7.7 Prueba de Aceptación Final.
  - AI7.8 Promoción a Producción
  - AI7.9 Revisión Posterior a la Implantación

Objetivo: Verificar y confirmar que la solución sea adecuada para el propósito deseado

Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas y toma en consideración:

- Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.

- Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.

- Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.

- Acreditación de manera que la Gerencia de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.

- Revisiones post implementación con el objeto de reportar si el sistema proporciono los beneficios esperados de la manera mas económica.

- **AI6 Administración de los cambios**

  - AI6.1 Estándares y Procedimientos para Cambios
  - AI6.2 Evaluación de Impacto, Priorización y Autorización
  - AI6.3 Cambios de Emergencia
  - AI6.4 Seguimiento y Reporte del Estatus de Cambio
  - AI6.5 Cierre y Documentación del Cambio

Objetivo: Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores.

Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual y toma en consideración:

- Identificación de cambios tanto internos como por parte de proveedores

- Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.

- Evaluación del impacto que provocaran los cambios.

- Autorización de cambios

- Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.

- Distribución de software, estableciendo medidas de control especificas para asegurar la distribución de software correcto al lugar correcto, con integridad y de manera oportuna.

- **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 Definición de niveles de servicio**

  - DS1.1 Marco de Trabajo de la Administración de los Niveles de Servicio
  - DS1.2 Definición de Servicios
  - DS1.3 Acuerdos de Niveles de Servicio
  - DS1.4 Acuerdos de Niveles de Operación
  - DS1.5 Monitoreo y Reporte del Cumplimento de los Niveles de Servicio
  - DS1.6 Revisión de los Acuerdos de Niveles de Servicio y de los Contratos

Objetivo: Establecer una comprensión común del nivel de servicio requerido
Para ello se establecen convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio y se toma en consideración:

- Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.

- Definición de las responsabilidades de los usuarios y de la función de servicios de información.

- Procedimientos de desempeño que aseguren que la manera y las responsabilidades sobre las relaciones que rigen el desempeño entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.

- Definición de dependencias asignando un Gerente de nivel de Servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.

- Provisiones para elementos sujetos a cargos en los acuerdos de niveles de servicio para hacer posibles comparaciones y decisiones de niveles de servicios contra su costo.

- Garantías de integridad

- Convenios de confidencialidad

- Implementación de un programa de mejoramiento del servicio.

➢ **DS2 Administración de servicios prestados por terceros**

- DS2.1 Identificación de Todas las Relaciones con Proveedores
- DS2.2 Gestión de Relaciones con Proveedores
- DS2.3 Administración de Riesgos del Proveedor
- DS2.4 Monitoreo del Desempeño del Proveedor

Objetivo: Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos
Para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización y toma en consideración:

- Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.

- Acuerdos de confidencialidad. Además, se deberá calificar a los terceros y el contrato deberá definirse y acordarse para cada relación de servicio con un proveedor.

- Requerimientos legales regulatorios de manera de asegurar que estos concuerde con los acuerdos de seguridad identificados, declarados y acordados

- Monitoreo de la entrega de servicio con el fin de asegurar el cumplimiento de los acuerdos del contrato.

➢ **DS3 Administración de desempeño y capacidad**

- DS3.1 Planeación del Desempeño y la Capacidad
- DS3.2 Capacidad y Desempeño Actual
- DS3.3 Capacidad y Desempeño Futuros
- DS3.4 Disponibilidad de Recursos de TI
- DS3.5 Monitoreo y Reporte

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado.
Para ello se realizan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos y toma en consideración:

- Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información

- Monitoreo y reporte de los recursos de tecnología de información.

- Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.

- Administración de capacidad estableciendo un proceso de planeación para la revisión del desempeño y capacidad de hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar cargas de trabajo con cantidad y calidad de desempeño

- Prevenir que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativos de recursos y de prioridad de tareas.

➢ **DS4 Asegurar el Servicio Continuo**

- DS4.1 Marco de Trabajo de Continuidad de TI
- DS4.2 Planes de Continuidad de TI
- DS4.3 Recursos Críticos de TI
- DS4.4 Mantenimiento del Plan de Continuidad de TI
- DS4.5 Pruebas del Plan de Continuidad de TI
- DS4.6 Entrenamiento del Plan de Continuidad de TI
- DS4.7 Distribución del Plan de Continuidad de TI
- DS4.8 Recuperación y Reanudación de los Servicios de TI
- DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones

- DS4.10 Revisión Post Reanudación

Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones.

Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración:

- Planificación de Severidad
- Plan Documentado
- Procedimientos Alternativos
- Respaldo y Recuperación
- Pruebas y entrenamiento sistemático y singulares

- **DS5 Garantizar la seguridad de sistemas**

- DS5.1 Administración de la Seguridad de TI
- DS5.2 Plan de Seguridad de TI
- DS5.3 Administración de Identidad
- DS5.4 Administración de Cuentas del Usuario
- DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad
- DS5.6 Definición de Incidente de Seguridad
- DS5.7 Protección de la Tecnología de Seguridad
- DS5.8 Administración de Llaves Criptográficas
- DS5.9 Prevención, Detección y Corrección de Software Malicioso
- DS5.10 Seguridad de la Red
- DS5.11 Intercambio de Datos Sensitivos

Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida

Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

- Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso

- Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario

- Administración de llaves criptográficas definiendo implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas

- Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos

- Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.

- Utilización de Firewalls si existe una conexión con Internet u otras redes públicas en la organización

➢ **DS6 Educación y entrenamiento de usuarios**

- DS6.1 Identificación de Necesidades de Entrenamiento y Educación
- DS6.2 Impartición de Entrenamiento y Educación
- DS6.3 Evaluación del Entrenamiento Recibido

Objetivo: Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados.
Para ello se realiza un plan completo de entrenamiento y desarrollo y se toma en consideración:

- Currículo de entrenamiento estableciendo y manteniendo procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información.

- Campañas de concientización, definiendo los grupos objetivos, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento

- Técnicas de concientización proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información

➢ **DS7 Identificación y asignación de costos**

- DS7.1 Definición de Servicios
- DS7.2 Contabilización de TI
- DS7.3 Modelación de Costos y Cargos
- DS7.4 Mantenimiento del Modelo de Costos

Objetivo: Asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI

Para ello se realiza un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y toma en consideración:

- Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios

- Procedimientos y políticas de cargo que fomenten el uso apropiado de los recursos de cómputo y aseguren el trato justo de los departamentos usuarios y sus necesidades

- Tarifas definiendo e implementando procedimientos de costeo de prestar servicios, para ser analizados, monitoreados, evaluados asegurando al mismo tiempo la economía

- **DS8 Apoyo y asistencia a los clientes de TI**

Objetivo: asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente

Para ello se realiza un Buró de ayuda que proporcione soporte y asesoría de primera línea y toma en consideración:

- Consultas de usuarios y respuesta a problemas estableciendo un soporte de una función de buró de ayuda

- Monitoreo de consultas y despacho estableciendo procedimientos que aseguren que las preguntas de los clientes que pueden ser resueltas sean reasignadas al nivel adecuado para atenderlas

- Análisis y reporte de tendencias adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias

- **DS9 Administración de la configuración**

  - DS9.1 Repositorio y Línea Base de Configuración
  - DS9.2 Identificación y Mantenimiento de Elementos de Configuración
  - DS9.3 Revisión de Integridad de la Configuración

Objetivo: Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios

Para ello se realizan controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia y toma en consideración:

- Registro de activos estableciendo procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de adquisición

- Administración de cambios en la configuración asegurando que los registros de configuración reflejen el status real de todos los elementos de la configuración

- Chequeo de software no autorizado revisando periódicamente las computadoras personales de la organización

- Controles de almacenamiento de software definiendo un área de almacenamiento de archivos para todos los elementos de software válidos en las fases del ciclo de vida de desarrollo de sistemas

- **DS10 Administración de Problemas**

  - DS10.1 Identificación y Clasificación de Problemas
  - DS10.2 Rastreo y Resolución de Problemas
  - DS10.3 Cierre de Problemas
  - DS10.4 Integración de las Administraciones de Cambios, Configuración y Problemas

Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder.
Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

- **DS11 Administración de Datos**

  - DS11.1 Requerimientos del Negocio para Administración de Datos
  - DS11.2 Acuerdos de Almacenamiento y Conservación
  - DS11.3 Sistema de Administración de Librerías de Medios
  - DS11.4 Eliminación
  - DS11.5 Respaldo y Restauración
  - DS11.6 Requerimientos de Seguridad para la Administración de Datos

Objetivo: Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento.

Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.

Este proceso deberá controlar los documentos fuentes (de donde se extraen los datos), de manera que estén completos, sean precisos y se registren apropiadamente. Se deberán crear también procedimientos que validen los datos de entrada y corrijan o detecten los datos erróneos, como así también procedimientos de validación para transacciones erróneas, de manera que éstas no sean procesadas. Cabe destacar la importancia de crear procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CDs y cintas magnéticas) de todas las transacciones y datos manejados por la organización, albergados tanto dentro como fuera de la empresa.

La gerencia deberá asegurar también la integridad, autenticidad y confidencialidad de los datos almacenados, definiendo e implementando procedimientos para tal fin.

- **DS12 Administración de las instalaciones**

  - DS12.1 Selección y Diseño del Centro de Datos
  - DS12.2 Medidas de Seguridad Física
  - DS12.3 Acceso Físico
  - DS12.4 Protección Contra Factores Ambientales
  - DS12.5 Administración de Instalaciones Físicas

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

- **DS13 Administración de la operación**

  - DS13.1 Procedimientos e Instrucciones de Operación
  - DS13.2 Programación de Tareas
  - DS13.3 Monitoreo de la Infraestructura de TI
  - DS13.4 Documentos Sensitivos y Dispositivos de Salida
  - DS13.5 Mantenimiento Preventivo del Hardware

Objetivo: Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada.

Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

- **Dominio: Monitorear y Evaluar.**

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

Procesos

- **M1 Monitoreo del Proceso**

  - ME1.1 Enfoque del Monitoreo
  - ME1.2 Definición y Recolección de Datos de Monitoreo
  - ME1.3 Método de Monitoreo
  - ME1.4 Evaluación del Desempeño
  - ME1.5 Reportes al Consejo Directivo y a Ejecutivos
  - ME1.6 Acciones Correctivas

Objetivo: Asegurar el logro de los objetivos establecidos para los procesos de TI.

Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.

Para ello la gerencia podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La gerencia deberá también medir el grado de satisfacción del los clientes con respecto a los servicios de información proporcionados para identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

- **M2 Evaluar lo adecuado del Control Interno**

  - ME2.1 Monitoreo del Marco de Trabajo de Control Interno
  - ME2.2 Revisiones de Auditoría
  - ME2.3 Excepciones de Control
  - ME2.4 Auto Evaluación del Control
  - ME2.5 Aseguramiento del Control Interno
  - ME2.6 Control Interno para Terceros
  - ME2.7 Acciones Correctivas

Objetivo: Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.

Para ello la gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias., evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

- **M3 Obtención de Aseguramiento Independiente**

  - ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales
  - ME3.2 Optimizar la Respuesta a Requerimientos Externos
  - ME3.3 Evaluación del Cumplimiento con Requerimientos Externos
  - ME3.4 Aseguramiento Positivo del Cumplimiento
  - ME3.5 Reportes Integrados

Objetivo: Incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.

Para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios como así también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

- **M4 Proveer Auditoria Independiente**

  - ME4.1 Establecimiento de un Marco de Gobierno de TI
  - ME4.2 Alineamiento Estratégico
  - ME4.3 Entrega de Valor
  - ME4.4 Administración de Recursos
  - ME4.5 Administración de Riesgos
  - ME4.6 Medición del Desempeño
  - ME4.7 Aseguramiento Independiente

Objetivo: Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes desarrolladas a intervalos regulares de tiempo. Para ello la gerencia deberá establecer los estatutos para la función de auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoria. El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa.
Esta auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de auditoría.

La función de auditoría deberá proporcionar un reporte que muestre los objetivos de la auditoria, período de cobertura, naturaleza y trabajo de auditoría realizado, como así también la organización, conclusión y recomendaciones relacionadas con el trabajo de auditoría llevado a cabo.

Los 34 procesos propuestos se concretan en 32 objetivos de control detallados anteriormente.

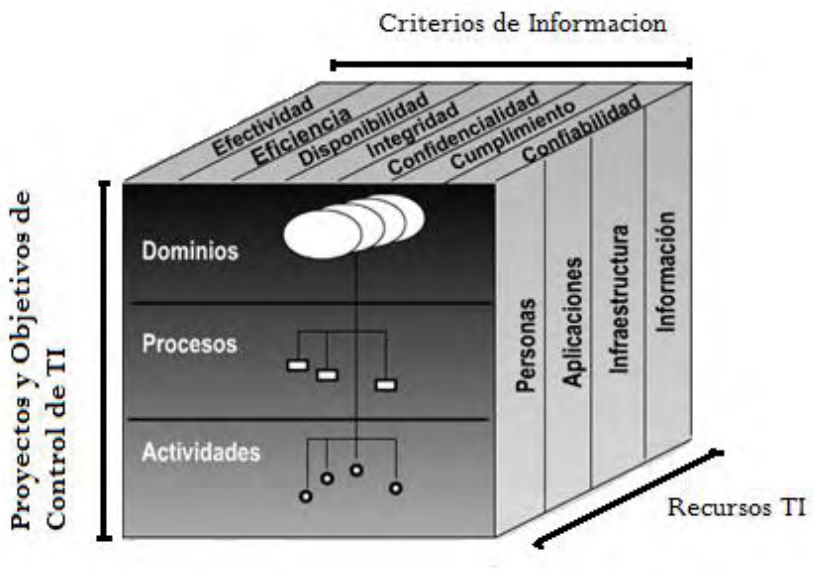
Un Control se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos empresariales se alcanzaran y que los eventos no deseados se preverán o se detectaran, y corregirán"

Un Objetivo de Control se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI".

En resumen, la estructura conceptual se puede enfocar desde tres puntos de vista:

- Los recursos de las TI
- Los criterios empresariales que deben satisfacer la información
- Los procesos de TI

Figura 1. Las tres dimensiones conceptuales de COBIT



Las tres dimensiones conceptuales de COBIT

Estos dominios facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Además, se toma en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano.

Toda organización, necesita desarrollar una tecnología que le permita rediseñar actividades y procesos para lograr un mejor desempeño en las mismas, es así como el COBIT es fundamental en toda empresa, pues esta metodología reduce posibles vulnerabilidades y riesgos de los recursos de las tecnologías de información y así mismo evalúa el resultado de los objetivos de la empresa.

1.6.2. COSO (Sponsoring Organizations of the Treadway Commission). COSO inicio en 1985 recomendando que las organizaciones patrocinadoras de la Comisión trabajen juntas para desarrollar sistemas integrados de orientación sobre el control interno.

El modelo COSO define el control interno como un conjunto de procesos, realizado por los directivos de una organización, y creado para garantizar el logro de los objetivos.

COSO consta de cinco elementos, estos elementos proporcionan un marco eficaz para describir y analizar el sistema de control interno, los cuales son:

- **Entorno de control.** Sirve como base para los demás componentes del control interno, proporcionando disciplina y estructura. Los factores del entorno de control incluyen la integridad, los valores éticos, el estilo de funcionamiento de la administración, la delegación de los sistemas de autoridad, así como los procesos de gestión y desarrollo de las personas en la empresa.

- **Evaluación del riesgo.** Cada empresa se enfrenta a una variedad de riesgos de fuentes externas e internas que deben ser evaluados. Una condición previa para la evaluación de riesgos es el establecimiento de objetivos y por lo tanto la evaluación de riesgos es la caracterización y análisis de los riesgos relevantes para la consecución de los objetivos asignados. La evaluación de riesgos es un requisito previo para establecer cómo los riesgos deberían ser manejados.

- **Las actividades de control.** Las actividades de control son las políticas y procedimientos que ayudan a asegurar la gestión de las directivas se llevan a cabo. También garantizan la toma de medidas necesarias para hacer frente a los riesgos que pueden obstaculizar el logro de los objetivos de la entidad. Las actividades de control se originan en toda la organización, en todos los niveles y en todas las funciones. Estos incluyen una amplia gama de actividades tan diversas como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones de desempeño operativo, la seguridad de los activos y la separación de funciones.

- **Información y comunicación.** Los sistemas de información juegan un papel importante en los sistemas de control interno que producen los informes, incluidos los operativos, financieros y el cumplimiento de información relacionada, que permiten elaborar y controlar la entidad. De manera más amplia, la comunicación eficaz debe garantizar los flujos de información hacia abajo, y hasta a través de la organización.

- **Seguimiento.** Los sistemas de control interno deben ser supervisados, un proceso que evalúa la calidad del desempeño del sistema en el tiempo. Esto se

logra a través de continuas actividades de supervisión o evaluaciones por separado. Las fallas de control interno detectadas a través de estas actividades deberían notificar las medidas de planificación y correctivas garantizando la mejora continua del sistema.

Algunas diferencias entre COSO y COBIT, que son los dos modelos más difundidos actualmente son:

- El modelo COSO está enfocado a toda la empresa, mientras que el COBIT se limita a las tecnologías de la información (TI).

- El COBIT establece como uno de sus objetivos la seguridad de la información, por el contrario COSO, no lo toma en cuenta en su evaluación.

El modelo de control interno que presenta el COSO no es muy completo, a diferencia de la metodología COBIT que contempla políticas, procedimientos y estructuras organizativas, además de procesos para definir el modelo de control interno.

2.7. TÉCNICAS DE AUDITORIA DE SISTEMAS

2.7.1. Selección de áreas de auditoria. Dada la magnitud del universo por auditar, la revisión debe hacerse de manera selectiva, esta técnica es adecuada para empresas con múltiples localizaciones o sucursales, con el fin de dar prioridad a los procesos, se aplican evaluaciones estadísticas a estos en forma periódica, para poder clasificar cuales de estos procesos son claves para el proceso de auditoría.

El uso del computador es indispensable en esta técnica ya que se manejan grandes volúmenes de información y los tamaños de muestra son muy grandes, además esta herramienta mejora la efectividad y eficiencia de los procesos de auditoría, también proporciona pruebas de control efectivas.

Una desventaja de esta técnica es que la construcción de estos modelos es costosa y consume demasiado tiempo y se deben tener conocimientos avanzados y especializados en materia de diseño y construcción.

- **Simulación – Modelaje.** Esta técnica consiste en la creación de modelos conceptuales o físicos bajo ciertas condiciones y simular el comportamiento del sistema computacional, de un programa, o evaluar el sistema financiero en forma periódica(evaluar el incremento o decremento de las cuentas contables o áreas financieras en términos de ingresos, egresos y gastos, para determinar el crecimiento organizacional), estos modelos brindan la posibilidad de realizar

pruebas controladas o realizar comparaciones entre valores proyectados y valores reales en materia financiera, con los resultados obtenidos en la simulación el auditor puede dar una opinión acerca del rendimiento del sistema y también proponer medidas de contingencia al respecto.

- **Sistema de puntajes (Scoring).** A diferencia de las anteriores técnicas la evaluación a los procesos y aplicaciones computarizadas se realiza de forma manual, con el fin de priorizar procesos con base en el análisis de riesgos, con la asignación de valores numéricos a las características claves, el auditor asignara la ponderación que este considere para cada factor, teniendo en cuenta el análisis de riesgo realizado con anterioridad que permita obtener un alto grado de confiabilidad , para llevar a cabo esta técnica se deberá diligenciar un formato de puntajes el que dará por resultado la clasificación para la auditoria.

2.7.2. Técnicas para operacionalizar la función de auditoría

- **Software de auditoria multisitio.** Es una técnica aplicable a grandes empresas que tengan diferentes centros electrónicos de datos (PED, Procesamiento electrónico de datos). Desarrollando un programa o grupo de programas e instalándolos en las regionales para que sean utilizados por los auditores. Se requiere que se guarde uniformidad en el software utilizado en los PED para facilitar el proceso de auditaje, esta técnica es aplicada en ambientes de procesamiento distribuido.

- **Centros de competencia.** Esta técnica funciona a la inversa que la técnica de multisitio, ya que centra toda la información de las regionales en un centro de competencia y después de su análisis, evaluación e informes son enviados a las sucursales para tomar las respectivas decisiones.

2.7.3. Técnicas para probar controles de sistemas en funcionamiento

- **Métodos de datos de prueba.** Las técnicas de datos de prueba se usan durante una auditoría alimentando datos en el sistema de computadora de una entidad y comparando los resultados obtenidos con resultados predeterminados. Un elemento de gran importancia en esta técnica es el diseño de los datos de prueba, lo que en últimas determinara la efectividad de esta técnica. Es recomendable seleccionar datos normales, ilógicos, imposibles, con valores extremos, etc. Un auditor podría usar esta técnica para:

- Poner a prueba los controles específicos en los programas de cómputo, como son la clave de acceso en línea y los controles para el acceso a datos.

- Colocar a prueba transacciones de prueba seleccionadas a partir de transacciones anteriores o creadas por el auditor para verificar las características específicas de procesamiento del sistema de cómputo de una dependencia. En general, estas transacciones se procesan fuera del procesamiento normal que utilice la dependencia.

- Poner a prueba transacciones usadas en un mecanismo integrado de pruebas donde se establece una unidad modelo (por ejemplo, un departamento o empleado ficticio), a la cual se le registran las transacciones durante el ciclo de procesamiento normal.

- Realizar pruebas de cumplimiento de los controles generales, por ejemplo, el uso de datos de prueba para verificar los procedimientos de acceso a las bibliotecas del programa.

- Pruebas de cumplimiento de los controles de aplicación, por ejemplo, el uso de los datos de prueba para verificar el funcionamiento de un procedimiento programado.

Cuando se procesan los datos de prueba con el procesamiento normal de la entidad, el auditor se asegura de que las transacciones de prueba sean eliminadas posteriormente de los registros contables de la entidad.

Se debe tener en cuenta que si se trata de una entidad pequeña y se procesan volúmenes menores de datos, los métodos manuales pueden ser de costo más efectivo.

En los procedimientos de auditoría para controlar las aplicaciones de datos de prueba se deben realizar las siguientes acciones:

- Controlar la secuencia de presentación de datos de prueba cuando se extienda a varios ciclos de procesamiento.

- Realizar corridas de prueba que contengan pequeñas cantidades de datos de prueba antes de presentar los datos de prueba principales de la auditoría.

- Predecir los resultados de los datos de prueba y compararlos con la salida real de datos de pruebas, para las transacciones individuales.

- Confirmar que se usó la versión actual de los programas para procesar los datos de prueba.

o Poner a prueba si los programas usados para procesar los datos de prueba fueron utilizados por la entidad durante el periodo aplicable de auditoría.

En síntesis se puede emplear esta técnica para: evaluación de controles específicos, verificación de validaciones, prueba de perfiles de acceso, prueba a transacciones seleccionadas con las siguientes ventajas y desventajas:

➢ **Ventajas**

o Se empieza por el inicio, tratando de verificar que el aplicativo este en capacidad de validar cualquier tipo de dato introducido en el sistema dejando por supuesto que se ingresen los válidos y advirtiendo del intento de ingreso de datos incorrectos.

o En la mayoría de los casos la información resultado estará protegida y libre de errores cuando el aplicativo permita validar los tipos de datos ingresados al sistema.

➢ **Desventajas**

o Para obtener resultados prestablecidos posiblemente no se los pueda obtener de forma manual puesto que algunos procedimientos de auditoría dependen de un procesamiento mucho más complejo que otros (por ejemplo, análisis estadístico avanzado) o implica cantidades de datos que sobrepasarían cualquier procedimiento manual, implicaría la creación de módulos secuenciales de prueba para obtener dichos resultados.

o Al utilizarlas en sistemas que están en la etapa de producción genera costos por los retazos ocasionados al hacer las respectivas pruebas.

- **Evaluación del sistema en caso base (BCSE).** Cuando la técnica de datos de prueba se mantiene en el tiempo para ser, consistente y cotidianamente, aplicada al sistema en producción, toma el nombre de EVALUACION DEL SISTEMA DEL CASO BASE (ESCB), en tal caso, la prueba es más completa y requiere de un alto grado de cooperación entre usuarios, auditores y personal de sistemas.

Esta técnica se utiliza en auditorias que hacen uso de controles preventivos y detectivos a los sistemas, los cuales manejan aplicativos para sistemas contables, sistema de nómina, sistemas estadísticos, etc., y en fin sistemas que deban validar los campos de datos que se ingresarán al aplicativo, y de forma paralela evaluar los procedimientos internos del sistema.

➢ **Ventajas**

o Alta seguridad en los resultados que se van a obtener, puesto que para crear los datos de prueba se hacen participes los auditores, usuarios y el personal de sistemas que prepararán un material mucho más eficiente para ser objeto de la auditoria.

o Al no abandonarse la prueba en el sistema caso base se puede perfeccionar el sistema ya que cuando se deje de encontrar errores adicionales de lógica o procesamiento se podría decir que se ha creado una versión mejorada de dicha aplicación, para poder desarrollar de mejor manera los cálculos a los datos introducidos a la aplicación y retornar información más confiable.

➢ **Desventajas**

o Se necesitará preparar resultados pre calculados de forma manual para compararlos con los arrojados por el aplicativo.

o El uso de mayor tiempo y de personal.

- **Operación Paralela.** También conocida como pruebas de cumplimiento, se realiza una copia del sistema.

Su uso radica en auditorias donde se haga uso de controles correctivos a los sistemas de información que cuentan con un mecanismo de procesamiento en donde de antemano se sabe que posee algún tipo de error ya sea en su lógica de procesamiento al momento de realizar transacciones o en cálculos matemáticos.

➢ **Ventajas**

o El hecho de llevar de la mano el sistema actual con el nuevo se convierte en una ventaja ya que se va a garantizar que el sistema nuevo funcione de la mejor manera posible, a fin de evitar futuras modificaciones en su lógica o procesamiento.

o Convertir un sistema ya sea manual o computarizado el cual presente algunas falencias, en un sistema mucho más eficiente y con mayor probabilidad de generar cálculos e información mucho más veraz y rápida.

➢ **Desventajas**

o Si el sistema actual falla por lógica de procedimiento o por cálculos, el sistema nuevo también va ha fallar puesto que van de la mano.

- **Facilidad de prueba integrada (Integrated Test Facility).** Su objetivo y uso es similar método de datos de prueba pero su gran diferencia principal radica en que su implementación se realiza sin detener el funcionamiento normal de la instalación, mezclando los datos de prueba con los datos reales, en la misma aplicación.

En esta técnica se realiza un procesamiento simultáneo de datos de prueba que representan operaciones ficticias en un conjunto con datos de operaciones reales, durante un procesamiento real. Esto permite al auditor comparar los resultados de procesamiento de datos de prueba con los resultados previamente determinados. Si los resultados del procesamiento de los datos de prueba resultan conforme a lo esperado, es razonable suponer que el programa de computación procesa los datos reales tal como corresponde.

Esta técnica no se propone revisar la validez de los datos de entrada sino que prueba la validez de los programas de computación que procesan los datos de entrada, a efectos de determinar si operan de conformidad con su diseño previamente aprobado.

Esta técnica se utiliza en auditorias donde exista disposición de los datos reales de la entidad. Es optima cuando se utilizan para auditar los controles defectivos en los sistemas, se utiliza en auditorías externas de sistemas que manejen gran cantidad de tipos de datos en una única transacción, como son sistemas contables, sistema de nómina, sistemas estadísticos, etc., puesto que sus resultados arrojaran un informe intachable.

➢ **Ventajas**

o No requiere una considerable pericia técnica por parte del auditor, sino más bien conocimiento y comprensión sobre el sistema.

o Se utilizan datos reales y por ende se auditará cualquier tipo de transacción de las posibles que soporte el sistema.

o No es necesario solicitar la colaboración del equipo, puesto que las transacciones de prueba se procesan simultáneamente con las reales de la entidad.

o Los resultados e informes obtenidos a través de la entidad ficticia permitirán de forma segura e inmediata analizar la eficiencia del sistema auditado.

➢ **Desventajas**

o Existe la posibilidad de afectar la integridad de la información real.

o Se requiere de un método efectivo que permita eliminar los informes producidos por la entidad ficticia, puesto que se podría borrar información real del sistema.

- **Simulación en paralelo.** Programas independientes creados por la auditoría para procesar datos reales y simular proceso real.

Esta es una técnica en la que el auditor elabora, a través de lenguajes de programación o programas utilitarios avanzados, una aplicación similar a la que va a ser auditada, con el objetivo de ingresar simultáneamente la misma información en ambas aplicaciones para verificar la exactitud del procesamiento de datos de la aplicación en producción.

También denominadas pruebas sustantivas, evaluación de la comparación entre los resultados de dos sistemas diferentes que han recibido los mismos datos de entrada. Simulación total o parcial de componentes del sistema.

Esta técnica se utiliza en auditorias donde se tiene deposición de los datos reales de la entidad, por otra parte se utiliza para verificar controles detectivos en sistemas que manejan aplicativos software como son sistema contable, sistema de nómina, sistemas estadísticos, etc., con el fin de realizar control a la lógica de la aplicación y la precisión de los respectivos cálculos.

➢ **Ventajas**

o Posee mayor disponibilidad de información, puesto que lo que hace es trabajar con los datos reales con los que cuenta la entidad auditada para sus procesos internos. De esta forma no se quedara sin ser evaluada ningún tipo de transacción de las que realiza el aplicativo de forma normal.

o Al trabajar con datos reales se hace más confiables los informes resultado que se esperan obtener.

➢ **Desventajas**

o Se hace necesario preparar módulos computarizados que simulen la aplicación real para poder obtener los resultados con los cuales se comparará los resultados obtenidos en la aplicación real.

2.7.4. Técnicas para seleccionar y monitorear transacciones. Los procedimientos de auditoría son distintos de acuerdo con la filosofía y técnica de cada organización o entidad o de cada departamento. De ahí que se desprendan auditorias de todo tipo entre las que se encuentran las de informática que a su vez se dividen en categorías como las de métodos manuales y las de métodos asistidos por computadoras.

Por lo tanto cuando una auditoria se conduce en un entorno de CIS ("Auditoria en un entorno de sistemas de información por computadora") sus objetivos y su alcance no cambian a través del proceso, pero al aplicar los procedimientos de auditoría, se puede requerir técnicas que usen la computadora como una herramienta para dicha auditoria. A los usos diversos que se le pueden dar a la computadora se los conoce como Técnicas de Auditoria con Ayuda de Computadora (TAACs).

Estas técnicas son relativamente nuevas y son usadas generalmente por altas organizaciones que necesitan analizar información en grandes volúmenes, con las llamadas TAACs la auditoria se centra en el análisis de datos y no en la recolección de los mismos, además inmersas en las TAACs podremos encontrar modelos de auditoría como los siguientes:

- Selección de transacciones de entrada.
- Archivo de revisión de auditoría como control del sistema (SCARF).
- Archivo de revisión de auditoría por muestreo (SARF).
- Registros extendidos.

A partir de este análisis se pueden inferir algunos usos de las TAACs en general y cuando se las debe aplicar; un ejemplo claro es cuando la escases de documentos de entrada o la nula visibilidad del proceso de auditoría puede requerir el uso de las TAACs en la aplicación de procedimientos de cumplimiento, además estos procesos se pueden mejorar en eficiencia y efectividad mediante el uso de esas TAACs.

La necesidad de controlar el procesamiento electrónico de datos en cualquier entidad con el objetivo de garantizar el control permanente de las transacciones y de sus derivados hacen de las siguientes técnicas de auditoría, fundamentales en cualquier entidad, por lo tanto los escenarios de uso de estas técnicas de auditoría son innumerables en áreas que necesiten controlar anomalías que se susciten en sus procesos.

- **Selección de Transacciones de Entrada.** Esta técnica es ejecutada por un software de auditoría el cual es independiente a todos los sistemas, consiste en seleccionar y separar datos de entrada que son parte de las aplicaciones. Y se las hace en base al criterio del auditor.

Entre las ventajas más significativas de este método es la seguridad del método ya que no cabe espacio para el fraude o el error, ya que el riesgo de alteración de los datos del sistema es evidentemente bajo.

Se utiliza en auditorias para verificar los controles detectivos utilizados en sistemas de información computarizados que hayan sido modificados con el fin de verificar el buen funcionamiento de la lógica y los cálculos matemáticos.

➢ **Ventajas**

o Esta técnica es relativamente fácil de aplicar.

o No necesita modificar el código fuente de la aplicación.

o No se presentan riesgos de alteración de la información generada por el sistema.

➢ **Desventajas**

o Se requiere de un aplicativo que permita seleccionar los datos de entrada y las transacciones dependiendo de los parámetros que crea pertinente el auditor.

- **Archivo de Revisión de auditoría como control del sistema (SCARF).** Este tipo de técnica consiste en incorporar aplicaciones de auditoria dentro del sistema para que ejecute rutinas de supervisión y monitoreo en forma permanente. La aplicación de este tipo de software se conoce como subrutina, a partir de esta subrutina se seleccionaran muestreos previamente definidos.

Esta técnica se utiliza en sistemas que manejan aplicativos software como son sistema contable, sistema de nomina, sistemas estadísticos, etc., los cuales manejan una gran numero de diversos tipos de transacciones con el fin de realizar control a la lógica de la aplicación y la precisión de los respectivos cálculos.

➢ **Ventajas**

o Con esta técnica no solo se obtiene resultados para ser comparados sino que permite, supervisar, obtener muestreos y reportes de excepciones al momento de desarrollarse una transacción en el aplicativo.

- Este tipo de técnica permiten auditar de forma más continua las transacciones producidas por un aplicativo, puesto que se incrustan módulos que permiten controlar de forma permanente el desarrollo de las transacciones.

- Permite abrir una ventana en la caja negra, para observar y controlar el proceso de la transacción.

➢ **Desventajas**

- Trabaja con un gran número de transacciones, dependiendo del peso de trabajo que tenga el aplicativo de la entidad.

- Se hace necesario preparar e implantar las rutinas de auditoría a la medida para las aplicaciones software de la entidad auditada, lo que requiere tiempo y costos.

- Se requiere pericia técnica por parte del auditor.

- Necesidad de intervención activa del auditor durante las diversas etapas de su desarrollo y aplicación.

• **Archivo de revisión de auditoría por muestreo (SARF).** Esta técnica es muy parecida a SCARF, la diferencia radica en que la selección de las transacciones ya no se hacen en forma automática predefiniéndolas sino que por el contrario se realizan al azar, esto con el fin de capturar archivos representativos para analizarlos con el apoyo de la estadística.

Se requiere un analista de sistema o programador para que preparen los módulos a decisión del auditor.

Esta técnica se utiliza para auditar sistemas que tengan gran carga de trabajo en cuanto a variedad de transacciones se refiere como son sistemas que manejan aplicativos contable en bancos, aerolíneas, etc.

➢ **Ventajas**

- Posibilita el monitoreo permanente de la ejecución de una transacción particular del sistema.

- Permite abrir una ventana en la caja negra, para observar y controlar el proceso de la transacción reduciendo la posibilidad de fraude de la información.

- No trabaja con un gran número de transacciones, puesto que las selecciona al azar ya que se apoya en muestreos estadísticos.

➢ **Desventajas**

o Se hace necesario preparar e implantar los módulos de auditoría a la medida para las aplicaciones software de la entidad auditada, lo que requiere tiempo y costos.

o Se requiere pericia técnica por parte del auditor.

o Necesidad de intervención activa del auditor durante las diversas etapas de su desarrollo y aplicación.

• **Registros Extendidos.** Con la aplicación de pequeñas rutinas se recogen datos que han afectado el funcionamiento del sistema, todo este tipo de rutina se conocen como pistas de auditoría, los cuales dejan un historial de todas las actividades secuencias y/o fallos del sistema.

Esta técnica se utiliza en auditorias para verificar los controles detectivos y correctivos en sistemas que manejan aplicativos software como son sistema contable de bancos, sistema de nómina, sistemas estadísticos, etc. con el fin de obtener una pista de toda la información clave de las diferentes transacciones.

➢ **Ventajas**

o Se incluye en algún tipo de registro información significativa sobre las transacciones o el sistema, que luego pude ser consultada por el auditor.
o Al igual que en SCARF este tipo de registros permiten auditar de forma más continua las transacciones producidas por los aplicativos software.

o Al guardar en un solo registro cualquier tipo de modificación que se hagan a las transacciones, será más fácil encontrar la causa de que se produzca algún tipo de información errónea o no valida.

➢ **Desventajas**

o Se hace necesario preparar e implantar las rutinas de auditoría a la medida para las aplicaciones software de la entidad auditada, lo que requiere tiempo y costo de desarrollo.

o Se requiere pericia técnica por parte del auditor.

o Necesidad de intervención activa del auditor durante las diversas etapas de su desarrollo y aplicación.

1.7.5 Técnicas para la auditoria de información almacenada. El fin de un proceso auditor es asistir a la gerencia o al departamento auditado para brindar apoyo en la identificación de los diversos hallazgos y posibles riesgos, y formular soluciones que sirvan para el control que eviten estos errores y minimicen los riesgos, generalmente algunas tareas del proceso auditor toman demasiado tiempo como por ejemplo el planteamiento, desarrollo y documentación; la automatización de algunas tareas puede resultar muy productivo para el equipo auditor, especialmente en el caso de auditoría de sistemas donde algunos procesos se prestan para ser automatizados.

Estos procesos toman cada vez más fuerza a nivel mundial después de lo acontecido con los desfalcos que llevaron a la quiebra a grandes empresas como Parmalat (italiana) y Enron (norteamericana) los cual replantea el proceso de auditoría tanto interna, como externa y la utilización de herramientas informáticas tanto de nivel general como herramientas especializadas.

La automatización como se menciona anteriormente, se facilita para algunos procesos en la auditoria de sistemas, lo cual brinda algunos beneficios como la clara reducción en el tiempo y posiblemente de recursos en el desarrollo del proceso automatizado, la estandarización en los procesos y a su vez una mayor flexibilidad ante los cambios lo cual se puede ver reflejado en una mejora en la calidad, provee mecanismos de monitoreo y retroalimentación, además la posibilidad de realizar análisis con diversos criterios, tales como recalculo de operaciones, búsqueda avanzada de información, seguimiento de transacciones, etc., convirtiéndose así en un poderoso aliado del equipo auditor permitiéndoles enfocarse en otros campos y obtener así un mejor y más profundo resultado.

El avance tecnológico que se ha vivido en los últimos años en el mundo ha generado la importancia para las personas y empresas de mantenerse actualizado e informado, pero esta información debe cumplir con ciertas características importantes como la veracidad, confiabilidad y oportunidad de la misma. Con el fin de obtener y gestionar esta información han surgido las NTIC (Nuevas Tecnologías de la Información y la comunicación); gracias a esto la información que se ha convertido en uno de los más valiosos recursos en las empresas, puede ser obtenida, tratada y almacenada para una mejor toma de decisiones.

Al introducir una herramienta tan poderosa como el computador en el proceso de auditoría esto conlleva a la utilización de herramientas informáticas para analizar la información que en su gran mayoría se encuentra en medios de almacenamiento magnético (discos duros, cd, dvd), con esto se busca evaluar la consistencia que presentan los sistemas de información, análisis de datos de una muestra de transacciones para verificar la integridad, consistencia y confiabilidad de la información presentada a través de los sistemas de información, el auditor

debe desarrollar procedimientos en el que se consideren la herramientas informáticas como apoyo para la realización de la auditoria.

- **Aplicaciones estandarizadas para grandes volúmenes de información.** Es indispensable que las empresas realicen auditorias rigurosas frecuentemente, especialmente a las áreas más sensibles del negocio, realizar un manual del comportamiento de la empresa con las normas y procedimientos internos.

➢ **Ventajas**

o Controlar el riesgo de fraudes en las empresas, para que se disminuyan las constantes quiebras empresariales que causaron fuertes impactos económicos negativos a nivel mundial, las cuales manejaban grandes volúmenes de información y que necesitaban de un ajuste en sus auditorías internas y externas.

o Las herramientas utilizadas en esta técnica son superiores a las técnicas manuales puesto que evalúan gran cantidad de información en menor tiempo y reducen costos.

o Amplían el alcance de la investigación y permiten realizar pruebas que no pueden efectuarse manualmente, en algunos casos los paquetes permiten la lectura de varios archivos simultáneamente.

o "Esta técnica utiliza herramientas que pueden ser usadas para seleccionar una muestra, analizar las características de una archivo, identificar tendencias en los datos y evaluar la integridad de los mismos".[5]

o Estas herramientas de auditoría generalizadas pueden analizar los datos procesados por muchas aplicaciones, además de elevar la calidad y fiabilidad de las verificaciones realizadas, categorizar y muestrear datos de grandes volúmenes de información para realizar un análisis y ayudar a la toma de decisiones.

➢ **Desventajas**

o Para tener en cuenta uno de los retos a afrontar por las aplicaciones estandarizadas para grandes volúmenes de información se da debido a la gran diversidad de ambientes de procesamiento de información ya que las características de los sistemas varían debido a los diferentes entornos de software y hardware, diferentes estructuras de datos, formatos de registros y funciones de procesamiento, poseen limitantes a la hora de verificar la lógica de procesamiento, para este tipo de aplicaciones es todavía complicado adaptarse a los cambios en

[5] ORACLE, Biblioteca virtual, Database, Disponible en: http://www.oracle.com/global/lad/database/audit-vault.html, (Citado el 5 de enero de 2013)

los objetivos de la aplicación y otro inconveniente es capacitar a los auditores en el uso del software.

o En caso donde el volumen de información no sea muy amplio los métodos manuales son más efectivos y menos costosos, además algunos tipos de aplicaciones son costosas de desarrollar, implementar y operar.

- **Programas utilitarios y usos generales.** El auditor emplea esta técnica cuando en el proceso de auditoría requiere utilizar diferentes programas los cuales servirán para proteger y salvaguardar la información existente en la empresa.

➢ **Ventajas**

o Es de gran ventaja utilizar esta técnica cuando se trata de manipular una gran cantidad de información y la empresa no cuenta con software especializado para dichas tareas.

o Los programas utilitarios son un aliado efectivo del software operacional, para posibilitar la optimización general de los recursos de informática.

o El auditor dispone de gran variedad de software general para la realización de tareas básicas de la auditoria tales como la documentación, creación de actas o presentación de informes o resultados.

Estas herramientas no proveen una aplicación especializada en el proceso de la auditoría, aún así, considerando el proceso total de auditoría, estas herramientas son igualmente útiles. Entre muchas herramientas se encuentran paquetes de ofimática como Microsoft Office, hojas de cálculo como Excel, lotus 1-2-3, diseñadores de gráficos como Visio, Smart Draw o administradores de correo electrónico como Outlook; con estas herramientas se facilita la creación y administración de documentos, cálculos matemáticos y financieros, creación de diagramas de proceso, organigramas, presentación de gráficos estadísticos etc.

➢ **Desventajas**

o Implica mucha complejidad técnica, puesto que el auditor requiere de mucho conocimiento para poder realizar una evaluación interna de la aplicación.

o Los programas utilitarios podrían fácilmente dañar el sistema, por lo tanto el auditor debe tomar ciertas medidas para evitar pérdida accidental de información y daño en los programas utilizados en la organización.

o Las herramientas utilizadas en esta técnica son muy limitadas en su funcionamiento y alcance con respecto al software hecho a la medida y el software especializado.

- **Software hecho a la medida.** Motivados por alcanzar los estándares de calidad internacional las empresas realizan auditorías internas con el fin de cumplir con los requerimientos exigidos, pero la contratación de un asesor o grupo de asesores conlleva a destinar grande presupuestos para cumplir con las auditorias en las empresas, por tal motivo se han visto en la tareas de realizar software especializados, específicos, hechos a la mediada o software de auditoría con sistemas expertos, permitiendo evaluar la gestión inicial en el tema de calidad, lo cual se refleja en la preparación que presentan a la hora de la realización de la auditoria.

Permite examinar a las empresas en áreas sistematizadas, en donde se pueden crear o desarrollar programas especiales para la empresa, en este caso el auditor haría las veces de usuario y el área de sistemas la respuesta y la solución a los requerimientos del usuario.

Existen herramientas de mucha productividad para la auditoria, una de ellas es Groupware "una herramienta especializada que permite a equipos de negocios trabajar más rápido, compartir más información, comunicarse mas efectivamente, y hacer un mejor trabajo de completamiento de tareas.

Groupware es una forma natural de automatizar el proceso de auditoría. Que usa características de base de datos y procesamiento de flujo de trabajo que pueden ser usados para almacenar e integrar información recolectada y empleada en el proceso de auditoría.

Así como también toman un rol muy importante dentro de la auditoria las herramientas asistidas por computadora CAATs "usadas para evaluar la integridad de una aplicación, determinar la conformidad con procedimientos y monitorear los resultados de procesamientos.

- **Ventajas**

o Actualmente existen diversas técnicas de auditoría, algunas de las cuales permiten un seguimiento y rastreo continuo de las aplicaciones mediante las llamadas rutinas embebidas. Su nombre se debe a que estas son rutinas que se incluyen en el desarrollo de las aplicaciones con el fin de realizar durante el funcionamiento de la aplicación auditada un monitoreo de las diversas transacciones y también se suele incluir un módulo anexo para obtener estadísticas e informes de dichas transacciones. Dado la naturaleza de estas técnicas la información se provee de primera mano, lo cual es una clara ventaja a la hora de realizar los análisis de las transacciones de la aplicación.

o Garantiza el cumplimiento de las normas legislativas y de la organización y en cualquier momento es posible ingresar, modificar, eliminar criterios de evaluación de las diferentes modalidades de auditoría existentes, ubicando errores y posibles

fraudes, disminuyendo considerablemente el riesgo de no-detección de los problemas.

- Leer y comparar los datos de la empresa permitiendo que estos permanezcan intactos para preservar la calidad e integridad, ubicar errores y posibles fraudes, limpiar y normalizar los datos para garantizar la coherencia y los resultados.

- Restringe el acceso a la información de la auditoria ya que define usuarios con permisos de ejecución, consulta según su cargo para acceder al sistema.

- Satisfacen requerimientos específicos de la auditoria como por ejemplo una rutina de muestreo para la selección de transacciones.

- Ayudan a la administración de la empresa en forma permanente al crear rutinas que realicen tareas de actualización de datos, manejo de base de datos de grandes volúmenes de información.

- No presenta limitaciones relacionales con el lenguaje de consulta que emplea, diseño de procedimientos específicos al sistema informático empleado para el registro de operaciones.

- Permite la verificación de controles de aplicación, tales como: secuencia, integridad, rango, validez fecha.

- Permite organizar datos, consolidarlos y totalizarlos en función de los objetivos perseguidos por el auditor.

- Se puede simular en paralelo los procedimientos a partir de los mismos datos de entrada, para comparar los resultados obtenidos con los ficheros de salida de la aplicación auditada, en la práctica esta herramientas son de gran importancia a la hora de mejorar la evaluación de las áreas examinadas ya que estas permiten realizar pruebas de cumplimiento y pruebas sustantivas, poseen herramientas y gráficos estadísticos, retroalimentan sus bases de conocimiento y presentan informes flexibles y dinámicos.

- **Desventajas**

- Conocimiento amplio en lenguajes de programación.

- El desarrollo de rutinas embebidas implica mayor tiempo y costos en el desarrollo de las aplicaciones.

- El hecho de ser software a la medida este no se puede aplicar a otros sistemas ni a otras empresas.

- Dependen en gran medida del sistema actual en uso en la entidad auditada y además necesitan un mantenimiento continuo del sistema para lograr una adaptación a las posibles actualizaciones y cambios del mismo.

- Estos programas y su documentación, deben ser antes revisados por el auditor, para pasar por un proceso de prueba y ensayo en donde se determinara si el software cumple con todas las normas y requerimientos de la empresa.

- **Backup o vaciado de archivos.** La técnica Backup o vaciado de archivos le permite al auditor examinar el contenido de los archivos que se encuentran en el computador, esto se hará mediante una copia o vaciado de archivos en un medio de almacenamiento cualquiera.

➢ **Ventajas**

- Al hacer una Backup de los archivos, el auditor observará detalladamente cada uno de estos, realizando a su vez transacciones, que más adelante se comparan con los archivos originales, permitiendo así, obtener un resultado veraz y efectivo de los datos evaluados.

- Esta técnica es de muy útil para hacer copias de los archivos y como soporte de los centros de PED (Procesamiento electrónico de los datos), evitando una posible destrucción parcial o total de los mismos.

➢ **Desventaja**

- No sería ventajoso emplear esta técnica cuando exista demasiada información, pues aumentaría tiempo y por lo tanto habría retraso en la evaluación.

1.7.6 Técnicas para examinar programas aplicativos

- **Snapshot: Auditoría Operativa y de Sistemas de Información, herramientas de diagnóstico en tiempo record. (Imagen Instantánea).** Es una técnica que permite tomar una copia o una fotografía de la memoria de un proceso para llegar a la toma de decisiones en el momento de su actividad. Esta técnica tiene en cuenta los datos de entrada.

➢ **Ventajas**

- Manejar grandes volúmenes de información al permitir tomar una copia de la memoria de un proceso.

- Maneja instrucciones para reconocer y registrar el flujo de transacciones.

- Se sigue todo un proceso entre el auditor y los analistas o desarrolladores para llegar al producto final en el cual el auditor recibe toda la documentación de los procesos para finalmente realizar el análisis de los objetivos predefinidos en la auditoria.

- Manejo de una clave especial para el manejo de la información (datos de entrada).

- Los snapshots son mucho más rápidos que los backups anteriores ya que solo necesitan trabajar con porciones de datos alteradas.

- Se pueden crear varios snapshots ya que el tamaño en disco es menor a la base de datos original.

- Es más fácil trabajar con snapshots y mucho más rápido para realizar copias de seguridad y restauraciones al sistema.

- Se pueden recuperar datos, eliminados por la snapshot para reparar la base de datos principal.

- Tiene la capacidad de restaurar la base de datos utilizando esta herramienta.

- Facilita al auditor comprender los pasos de procesamiento, verificando el flujo lógico del programa.

➢ **Desventaja**

- La indexación de texto completo no se admite en la Snapshot

- Si los datos de la snapshot cambian en periodos cortos no se lograra una diferencia con los backups tradicionales.

- No se puede deshabilitar la base de datos primaria ya que los snapshot están atados a esta.

- Requiere bastante conocimiento de PED y de programación de computador, consume bastante tiempo.

• **Mapping.** Es una técnica que utiliza una herramienta la cual permite evaluar cada una de las instrucciones de un programa, presentando reportes, tanto del número de veces que es ejecutada una instrucción como el tiempo que duró el procesador en ejecutarlas.

- **Ventajas**

o Permite deshabilitar instrucciones ilegales.

o Identifica instrucciones que no son utilizadas, pues es una técnica segura que sirve como soporte al control de calidad de sistemas para medir eficiencia.

o Ejecuta procedimiento de depuración de software.

- **Desventajas**

o La desventaja es que se requiere de conocimientos avanzados en programación para su desarrollo, consume demasiado tiempo y es costosa.

- **Tracing y Flujograma de control.** El Tracing es una técnica muy importante en cuanto a los lenguajes de programación, puesto que identifica y muestra las instrucciones que fueron ejecutadas y en que secuencia aparecen.

El flujograma de control es una técnica muy valiosa puesto que permite evaluar los sistemas de una forma integral, tanto en el aspecto funcional como en el de control.

- **Ventajas**

o Periódicamente deben ser evaluados ciertos factores o elementos que de una u otra manera brinden confiabilidad al sistema informático, ya que los equipos pueden fallar y producir accidentes informáticos, los errores humanos y los actos intencionales siendo estos los más perjudiciales e importantes.

o Con el fin de evitar en gran parte se presente este tipo de problemas el sistema debe contar con un componente de identificación de usuarios, asignado roles y permisos de acceso y atribuciones, aquí es donde tracing actúa, verificando a posteriori quienes han ingresado al sistema a qué tipo de información han tenido acceso, que tipo de modificaciones realizaron (fecha, hora, si elimino o modifico información), una gran ventaja a la hora de auditar las entradas al sistema por parte de los usuarios.

o Tracing obtiene un listado de las transacciones utilizadas, permitiéndole al auditor identificar fácilmente el cumplimiento de los objetivos.

o Los flujogramas Facilitan la tarea de comparar el funcionamiento manual con el sistema total, verificando que este funcionando de la forma en como están en la documentación.

o Además los flujogramas de control son excelentes para el entrenamiento de nuevos auditores.

o El flujograma de control, detecta las deficiencias en materia de control y en el tipo operacional.

- **Comparación de código y control de cambio.** La técnica de comparación de códigos se la utiliza para comparar códigos de una misma versión con el fin de comprobar que estos estén funcionando de una manera correcta.

Esta técnica debe ser aplicada cuando ya existe un control de cambio, de otra forma se debe buscar alternativas que permitan la búsqueda de la evidencia.
La técnica de control de cambio es la que verifica el número de bytes de los programas.
Estas dos técnicas básicamente Impiden que personas infructuosas se sometan a la alteración o cambio de programas, afectando de esta manera a la empresa.

➢ **Ventajas**

o En el control de cambio, evita el aumento de instrucciones perjudiciales para la empresa. Además esta técnica es muy confiable en cuanto a integridad de los programas y respaldando así el contenido de archivos.

o Una ventaja en cuanto a comparación de código es la de ofrecer mayor seguridad en el cambio de programas y librerías de programas.

o Se puede obtener una clara identificación del origen de un hallazgo en el código fuente, en qué versión se originó, inclusive, quién estuvo a cargo de dicho cambio.

➢ **Desventajas**

o La técnica de comparación de código no proporciona evidencia sobre confiabilidad de los archivos de datos ni sobre eficiencia de los programas.

o La desventaja de la técnica de control de cambio es que exige un riguroso sistema de control interno.
o No es recomendable aplicarla en empresas pequeñas o desarrollos simples, por lo que puede dificultar notablemente la aplicación de dicha técnica, el esfuerzo y recursos necesarios pueden ser excesivos para al final no obtener resultados significativos.
o Debe existir un historial de versiones. De otra forma no es posible aplicar esta herramienta, ya sea que se lleve control sobre las versiones o comparación de código.

- **Análisis de la lógica del programa.** Esta técnica consiste en evaluar la lógica del programa y el contenido de su documentación de forma descriptiva.

➢ **Ventajas**

- Es la técnica que mejor controla todas las particularidades de un programa.
- Describe detalladamente un programa.

➢ **Desventajas**

- Seguridad de que la información es una representación exacta de los programas utilizados. Que la documentación no este desactualizada.

- El auditor debe tener el conocimiento del lenguaje de programación utilizado, para cumplir rápidamente con los objetivos de la auditoria. Que los auditores y revisores fiscales tengan el conocimiento básico en lenguajes de programación para que tengan una buena comunicación con el ingeniero de sistemas o con el experto en el tema.

- El auditor debe conocer ampliamente todos los sistemas a evaluar para estar al tanto de la forma de la relación entre módulos y programas para tener una mejor comprensión del sistema total.

Utilizado únicamente para la evaluación de módulos, porque resulta dificultoso en programas extensos y sofisticados.

2. METODOLOGÍA

Para realizar esta auditoría de sistemas como trabajo de grado, se limitó al estudio de la infraestructura de la red física de la sede principal y a la página web de la E.S.E. Centro Hospital Divino Niño, se utilizó una metodología tipo de investigación cuantitativa, ya que permite examinar los datos de manera científica, o de manera más específicamente en forma numérica, generalmente con ayuda de herramientas del campo de la estadística al no contar con la suficiente experiencia para utilizar la metodología cualitativa.

Es responsabilidad de la administración el contenido de la información suministrada por la institución y analizada por Luis Alberto Reynel Araujo, estudiante de la Universidad de Nariño.

Para alcanzar los objetivos propuestos, se utilizó la metodología de tipo empírico, porque se realiza recolección y análisis de datos, además se toma como fuente primaria de información la observación directa por parte del auditor, también, se estudian y aplican conceptos y esquemas teóricos, también cabe mencionar que esta metodología clasifica dentro del tipo de investigación aplicada, ya que todas las recomendaciones finales deberán ser aplicadas para tener un funcionamiento de calidad.

De conformidad con lo anterior, se planeó y ejecutó el trabajo de manera que el examen y el resultado de las pruebas proporcionaran una base razonable para fundamentar la opinión y los conceptos expresados en el Informe

La auditoría realizada por el auditor fue dividida en varias etapas así:

Etapa I. Familiarización con el Entorno.

En esta etapa se realiza el estudio previo al inicio de la Auditoria con el propósito de conocer en detalle la entidad auditada y en si la infraestructura física de la red de datos de la sede principal, además se evalúa el portal web de la entidad, bajo dos diferentes estrategias incluyendo la proporcionada por la estrategia Gobierno en Línea bajo el decreto 1151 de abril de 2008.

Los resultados de la exploración permiten, además, hacer la selección de las técnicas y metodologías de auditoría a utilizar. Se realizaron visitas a la entidad donde se tuvo un contacto directo tanto con personal de la oficina de sistemas como con la documentación solicitada por el auditor y la observación directa de los equipos de cómputo, redes de datos, servidores entre otros.

Etapa II. Planeación de la auditoría de sistemas.

En esta etapa se realizó la planificación de todo el proceso que se requiere para la realización de la auditoría.

- Identificar el alcance y los objetivos de la Auditoría a realizar.

- Realizar el estudio inicial en la entidad a auditar para recolectar datos sobre la infraestructura física de la red de datos y el cumplimiento del decreto 1151 de 2008 de Gobierno en Línea.

- Determinar los recursos necesarios para realizar la auditoría.

- Elaboración del plan de trabajo.

Etapa III. Realización de las Actividades de la Auditoría.

En esta etapa se hicieron efectivos todos los planteamientos de la etapa anterior, con la aplicación de las metodologías y técnicas seleccionadas que garantizaron el cumplimiento de los objetivos planeados.

Las actividades que se realizaron dentro de esta etapa fueron:

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

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

- Realización de pruebas sobre los procesos seleccionados y sobre la infraestructura de la red..

- Elaboración de los cuestionarios cuantitativos para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para ser auditados.

- Identificación de hallazgos dentro del proceso evaluado.

- Asignación de la probabilidad de ocurrencia e impacto para los riesgos detectados mediante la aplicación del formato de hallazgos.

- Análisis del cumplimiento del decreto 1151 de 2008 de Gobierno en Línea

Etapa IV. Presentación del Informe Final.

Se realizó un informe final dirigido a la E.S.E. Centro Hospital Divino Niño, donde se describen los hallazgos encontrados, junto a las recomendaciones necesarias para subsanar los hallazgos encontrados, Además se hace un análisis profundo de los desaciertos del portal web de la entidad.

3. DESARROLLO DEL TRABAJO

3.1. ARCHIVO PERMANENTE

El archivo permanente contiene información tanto constante como variable en el tiempo. Esta información es de vital importancia y se considera necesaria para comprender en forma exacta, rápida y sencilla las características de las áreas objeto de auditoría.

3.1.1. Leyes y decretos comunes. En este apartado se citaran las leyes y decretos que regularon el proceso de auditoría en las dos entidades.

- **Decretos.** El decreto que rige los estatutos de conformación de la página web s el siguiente.

➢ Decreto 1151 de abril de 2008.

3.1.2. Centro Hospital Divino Niño

3.1.2.1. Misión. Somos una Empresa Social del Estado de primer nivel de atención que prestaservicios integrales de salud, con enfoque familiar y comunitario, con profesionales altamente calificados, tecnología de punta, con calidad y eficiencia; garantizando rentabilidad social y financiera.

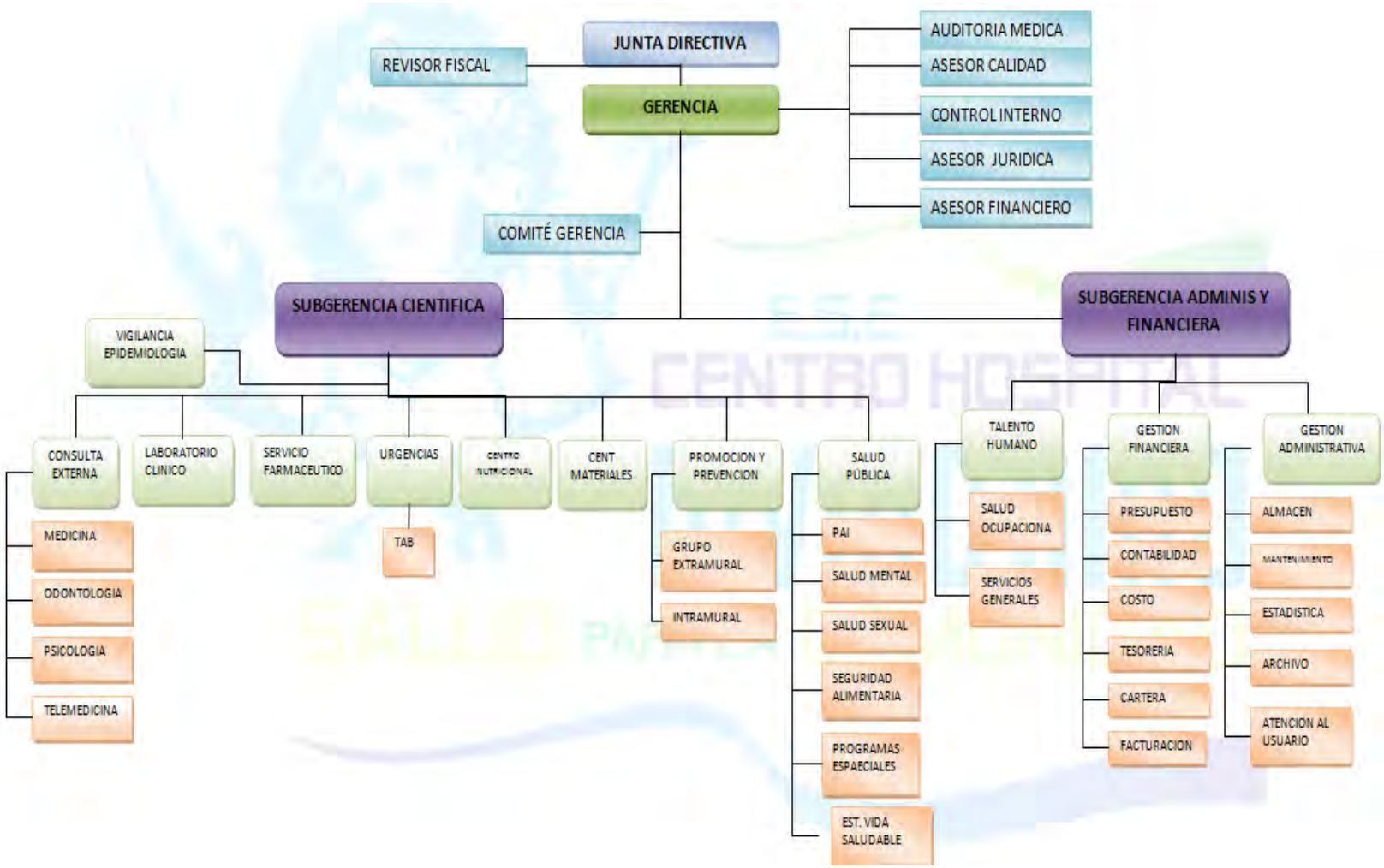
3.1.2.2. Visión. Ser para el 2014 una ESE de primer nivel certificada en su red de servicios urbana y rural. Reconocida por la calidad, competitividad y modernización de sus servicios; en camino a la acreditación.

3.1.2.3. Objetivos Estratégicos. Garantizar el desarrollo estratégico, Gerencial del Centro Hospital Divino Niño ESE en aspectos como:

- Promover y desarrollar el trabajo en equipo.
- Lograr el crecimiento y mantenimiento de la participación en el mercado.
- Lograr el Equilibrio operacional.

- Implementar el sistema de información enfocado a los procesos y resultados empresariales.
- Desarrollar el sistema de control interno.
- Identificar, prevenir y disminuir la ocurrencia de riesgos tanto al usuario como a la Empresa.

3.1.2.4. Organigrama Centro Hospital Divino Niño



3.2. ARCHIVO CORRIENTE

Para llevar a cabo el proceso de auditoría se hará una recopilación de documentos que tendrán que ver directamente con este desarrollo.

3.2.1. Programa de auditoria. Para la realización del proceso de auditoría al Funcionamiento del aspecto físico de la red de datos, se utilizará la metodología COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas), se evaluaran algunos objetivos de control que se encuentran dentro de los dominios del COBIT así:

3.2.1.1. Objetivos de control para el Centro Hospital Divino Niño.

- **DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)**

➢ **Definir un Plan Estratégico de TI (PO1)**. La definición clara y con óptima proyección de un plan estratégico sobre el buen funcionamiento de la red física de datos hace parte fundamental para el cumplimiento de los objetivos empresariales, ya que los procesos que aquí se involucran son directamente relacionados con elementos tecnológicos.

- **PO1.3 Evaluación del Desempeño y la Capacidad Actual:** El departamento de sistemas debe diseñar e implementar una metodología de evaluación de desempeño de los planes que se encuentran en ejecución en la entidad los cuales servirán para cumplir las metas propuestas.

- **PO1.4 Plan Estratégico de TI:** El Centro Hospital Divino Niño debe realizar planes de evaluación y adquisición de nuevas opciones tecnologías de acuerdo a las necesidades operativas.

➢ **Determinar la dirección tecnológica (PO3).** Es importante para la empresa tener un soporte tecnológico basado en políticas directas que busquen mejorar el desempeño en las actividades tras ejecutar modelos adecuados que direccionen objetivos claros con herramientas calificadas.

- **PO3.1 Planeación de la Dirección Tecnológica:** Se debe realizar análisis periódicos sobre el actual estado tecnológico en el que se encuentra la red de datos.

➢ **Definición de la Organización y de las Relaciones de TI (PO4).** Para lograr óptimo funcionamiento en los procesos es de gran importancia la asignación de

roles a funcionarios que ejecuten procesos en el campo funcional de la red física de datos para obtener un buen desempeño organizacional.

- **PO4.6 Establecimiento de Roles y Responsabilidades:** El área de sistemas debe definir y dar a conocer a la institución el personal que deberá encargarse del desempeño y funcionamiento de la red de datos. Además sus funciones deberán de quedar guardadas en el manual de funciones interno del área y de la institución.

- **PO4.13 Personal Clave de TI:** El área de sistemas deberá identificar la persona clave de TI para la administración de la red de datos y disminuir la dependencia en una sola persona para realizar funciones críticas.

➢ **Administrar la Inversión en TI (PO5).** Los recursos de inversión para implementación de elementos tecnológicos que se utilizan para el buen funcionamiento de la red física de datos necesitan de controles y proyecciones óptimas buscando el beneficio de la entidad.

- **PO5.1 Marco de Trabajo para la Administración Financiera:** Se deberá designar un equipo de trabajo para encargarse de la administración de la inversión y costos del funcionamiento de la red de datos.

- **PO5.2 Prioridades Dentro del Presupuesto de TI:** Si la entidad quiere que sus recursos que se inviertan en la infraestructura de la red de datos retorne la contribución al portafolio empresarial y sus objetivos, se debe de priorizar los proyectos, mantenimientos y compras de nueva tecnología en el presupuesto.

➢ **Evaluación y Análisis de Riesgos (PO9).** Tanto los procesos de información como los elementos propios de la red de datos necesitan del estudio y análisis de riesgos que planifiquen toma de decisiones en caso de eventos negativos para la red de datos.

- **PO9.1 Marco de Trabajo de Administración de Riesgos:** El área de sistemas debe de iniciar un plan de administración de riesgos que afecte la red de datos de la entidad.

- **PO9.3 Identificación de Eventos:** se debe de realizar autoevaluaciones de manera periódica para identificar los principales elementos de la red de datos que se encuentran predispuestos a todo tipo de riesgo, amenazas, vulnerabilidades de cualquier evento que afecte el funcionamiento de la red de datos, además de determinar su naturaleza.

- **PO9.4 Evaluación de Riesgos de TI:** Se evaluaran los riegos de forma sistemática de manera cuantitativa y cualitativa, su probabilidad de impacto y sus efectos sobre el funcionamiento de la red de datos.

- **PO9.5 Respuesta a los Riesgos:** Teniendo identificados los riesgos se debe de diseñar un plan de procesos en el cual se pueda 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:** El plan de riesgos debe de ser apoyado desde la alta dirección para que pueda ser ejecutado en el momento de ser necesario y ser monitoreado con el fin de dar respuestas en cualquier momento ante algún riesgo.

- **DOMINIO - ADQUISICION E IMPLEMENTACION (AI)**

➢ **Adquirir y Mantener Software Aplicativo (AI2).** Es importante contar con software que se utilice para monitorear la red de datos y además darle mantenimiento al software para que el proceso de monitoreo sea correcto y oportuno.

- **AI2.5 Configuración e Implantación de Software Aplicativo Adquirido:** Se debe de tener un software que sea configurado e implementado a las necesidades de la red de datos para ayudar en su monitoreo y buen funcionamiento.

- **AI2.10 Mantenimiento de Software Aplicativo:** El software debe de tener un plan de mantenimiento como una guía de actualizaciones que ayuden a mejorar su rendimiento.

➢ **Adquirir y Mantener la infraestructura Tecnológica (AI3).** Debido al costo y a la importancia de los elementos que constituyen la red física de datos es prioritario tanto la adquisición como el mantenimiento de estos elementos fundamentales para el proceso tecnológico de la entidad.

- **AI3.1 Plan de Adquisición de Infraestructura Tecnológica:** El área de sistemas debe de tener claro cuáles son las necesidades a nivel de infraestructura que necesita la red de datos para así poder diseñar un plan de adquisición, implementación y mantenimiento, además de tener en cuenta futuras ampliaciones en la capacidad de funcionamiento de la red de datos.

- **AI3.3 Mantenimiento de la Infraestructura:** Se analizara si la infraestructura de la red de datos cuenta con lo necesario para responder a los procesos ejecutados por la entidad a través de ella además de diseñar un plan de mantenimiento de los elementos que la conforman.

- **DOMINIO - ENTREGAR Y DAR SOPORTE (DS)**

➢ **Administración de instalaciones (DS12).** Debido a la importancia de información que se maneja en terminales o servidores y la importancia de cada uno de los elementos de la red de datos es de vital importancia darle control y manejo adecuado a cada una de las instalaciones.

o **DS12.1 Selección y Diseño del Centro de Datos:** En la E.S.E Centro Hospital Divino Niño se debe de diseñar e implementar el centro de datos como considera las leyes y regulaciones correspondientes, para que así la comunicación a través de la red de datos sea optima y cumpla con las necesidades del servicio.

o **DS12.2 Medidas de Seguridad Física:** Al no encontrarse ninguna medida de seguridad física la red se encuentra vulnerable a múltiples amenazas tanto de origen ambiental como de origen humano. Se debe de tener claro la persona encargada de aplicar los correctivos y ejecutar las medidas diseñadas para solucionar cualquier riesgo.

o **DS12.3 Acceso Físico:** Se debe tener claro los roles del personal de sistemas y demás áreas de la entidad, ninguna persona sin autorización o el rol adecuado puede estar en área de los equipos de comunicación de la red de datos.

o **DS12.5 Administración de Instalaciones Físicas:** Las instalaciones físicas de los equipos que conforman la red de datos deben de ser administrados de tal manera que cumplan con los lineamientos de seguridad, leyes, reglamentos y requerimientos por el cual están en funcionamiento.

- **DOMINIO - MONITOREAR Y EVALUAR (ME)**

➢ **Evaluar lo adecuado del control interno (ME2).** Es fundamental llevar control con actividades ejecutadas según el control interno de la entidad para así analizar si los procesos donde esté relacionada la red física de datos se ejecuten de la mejor manera y buscando el óptimo desempeño.

o **ME2.1 Monitoreo del Marco de Trabajo de Control Interno:** El área de sistemas debe de implementar un marco de trabajo de monitorización de la red de datos para que se garantice los procesos en los cuales se ve involucrada y sirva para cumplir las metas de la entidad.

o **ME2.7 Acciones Correctivas:** De acuerdo a los controles que se ejecuten sobre la red de datos, el área de sistemas diseñara y ejecutara planes de acciones correctivas.

3.2.2. Diseño de los elementos de auditoría: Para la realización del proceso de auditoría a la E.S.E. Centro Hospital Divino Niño, se utilizaron diferentes instrumentos de recolección de información, a continuación se describe cada uno de ellos:

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

Los ítems relacionados a continuación son los que describirán el elemento de auditoría.

REF: Se refiere al ID del elemento.

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

PROCESO AUDITADO: En este espacio se indicara el nombre del proceso objeto de la auditoria, para el caso será Contratación TI.

RESPONSABLES: En este espacio se indicaran los nombres del equipo auditor que esta llevando a cabo el proceso de auditoría.

DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: En este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se está revisando.

MATERIAL DE SOPORTE: En este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.

DOMINIO: Espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.

PROCESO: Espacio reservado para el nombre del proceso en especifico que se está auditando dentro de los dominios del COBIT.

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: Este espacio está destinado para describir las pruebas de análisis que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

DE EJECUCIÓN: Este espacio está destinado para describir las pruebas de ejecución que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

Tabla 2. Definición de fuentes de conocimiento, pruebas de análisis de auditoria

TABLA DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS DE AUDITORIA	REF	

ENTIDAD AUDITADA	E.S.E. Centro Hospital Divino niño	**PAGINA**		
		1	DE	1
PROCESO AUDITADO	Funcionamiento del aspecto físico de la red de datos			
RESPONSABLE	Luis Alberto Reynel Araujo			
MATERIAL DE SOPORTE	COBIT			
DOMINIO				
PROCESO				

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANALISIS	**DE EJECUCION**

AUDITOR RESPONSABLE:
Luis Alberto Reynel Araujo.

- El Desarrollo de los cuadros de definición de fuentes de conocimiento, pruebas de análisis de auditoria se encuentran en la carpeta de anexos FUENTE _DE_CONOCIMIENTO_CHDN

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

Este cuestionario cuantitativo esta conformado por los siguientes items:

REF: Se refiere al ID del elemento.

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

PROCESO AUDITADO: En este espacio se indicara el nombre del proceso objeto de la auditoria, para el caso será Contratación TI.

RESPONSABLES: En este espacio se indicaran los nombres del equipo auditor que esta llevando a cabo el proceso de auditoría.

DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: En este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se está revisando.

MATERIAL DE SOPORTE: En este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.

DOMINIO: Espacio reservado para colocar el nombre del dominio de COBIT que se esta evaluando.

PROCESO: Espacio reservado para el nombre del proceso en especifico que se está auditando dentro de los dominios del COBIT.

PREGUNTA: Espacio donde se indicara la descripción de la consulta de la cual se indagara.

SI – NO: Posibilidades de respuesta, cumple, no cumple, o no aplica para la entidad.

REF: referencia a la evidencia o el hallazgo que se obtuvo después de indagar.

PORCENTAJE DE RIESGO: Hace referencia a la probabilidad de que el proceso se vea afectado por las acciones de las cuales se está indagando, entre mas alto el porcentaje mayor probabilidad de riesgo tiene el proceso de salir perjudicado.

El cálculo de este porcentaje se hace de la siguiente forma:

Porcentaje de riesgo parcial = (Total SI * 100) / Total

Porcentaje de riesgo = 100 - Porcentaje de riesgo parcial

Las equivalencias utilizadas para la puntuación serán de uno a cinco, siendo uno el valor mínimo considerado de poca importancia y cinco el máximo considerado de mucha importancia.

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

1% - 30% = Riesgo Bajo
31% - 70% = Riesgo Medio
71% - 100% = Riesgo Alto

Tabla 3. Cuestionario cuantitativo.

	CUESTIONARIO CUANTITATIVO	REF

ENTIDAD AUDITADA	E.S.E. Centro Hospital Divino niño	**PAGINA**		
		1	DE	1
PROCESO AUDITADO	Funcionamiento del aspecto físico de la red de datos			
RESPONSABLE	Luis Alberto Reynel Araujo			
MATERIAL DE SOPORTE	COBIT			
DOMINIO		**PROCESO**		

PREGUNTA	SI	NO	NA	REF	FUENTE
1. ¿ ?					
2. ¿ ?					

TOTALES			
TOTAL CUESTIONARIO			

PORCENTAJE DE RIESGO

AUDITOR RESPONSABLE
Luis Alberto Reynel Araujo

- El Desarrollo de los cuestionarios cuantitativos se encuentran en la carpeta de anexos CUESTIONARIOS_CHDN

- **Matriz de Probabilidad de ocurrencia e Impacto según relevancia del proceso**

Esta matriz fue creada para catalogar un riesgo y saber qué clase de daño puede causar un mal procedimiento en el proceso auditado.

En la matriz existe la columna de probabilidad de ocurrencia donde se pondrá el valor del porcentaje de riesgo según su resultado.

Luego se deberá clasificar el impacto según la relevancia del proceso, esta clasificación será hecha por el equipo auditor basándose en el conocimiento de la entidad y del proceso auditado.

Una vez hechos estos procedimientos se podrá clasificar el riesgo para su posterior entendimiento.

MATRIZ DE PROBABILIDAD DE IMPACTO

Tabla 4. Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso

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

- **Manual de navegación de hallazgos.** En este manual se describe las inconsistencias encontradas.

Esta información será desglosada de la siguiente manera:

REF: Se refiere al ID del elemento.

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

PROCESO AUDITADO: En este espacio se indicara el nombre del proceso objeto de la auditoria, para el caso será Contratación TI.

RESPONSABLES: En este espacio se indicaran los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

MATERIAL DE SOPORTE: En este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.

DOMINIO: Espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.

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

HALLAZGO: Aquí se encontrara la descripción de cada hallazgo, así como la referencia al cuestionario cuantitativo que lo soporta.

CONSECUENCIAS Y RIESGOS: En este apartado se encuentra la descripción de las consecuencias del hallazgo así como la cuantificación del riesgo encontrado.

EVIDENCIAS: Aquí encontramos en nombre de la evidencia y el número del anexo donde ésta se encuentra.

RECOMENDACIONES: En este último apartado se hace una descripción de las recomendaciones que el equipo auditor ha presentado a las entidades auditadas.

Tabla 5. Hallazgos

	HALLAZGO HOSPITAL DIVINO NIÑO	**REF**

PROCESO AUDITADO	Funcionamiento del aspecto físico de la red de datos	**PÁGINA**		
		1	DE	1
RESPONSABLE	LUIS ALBERTO REYNEL ARAUJO			
MATERIAL DE SOPORTE	COBIT			
DOMINIO		**PROCESO**		

DESCRIPCIÓN:

REF_PT:

CONSECUENCIAS:

RIESGO:

RECOMENDACIONES:

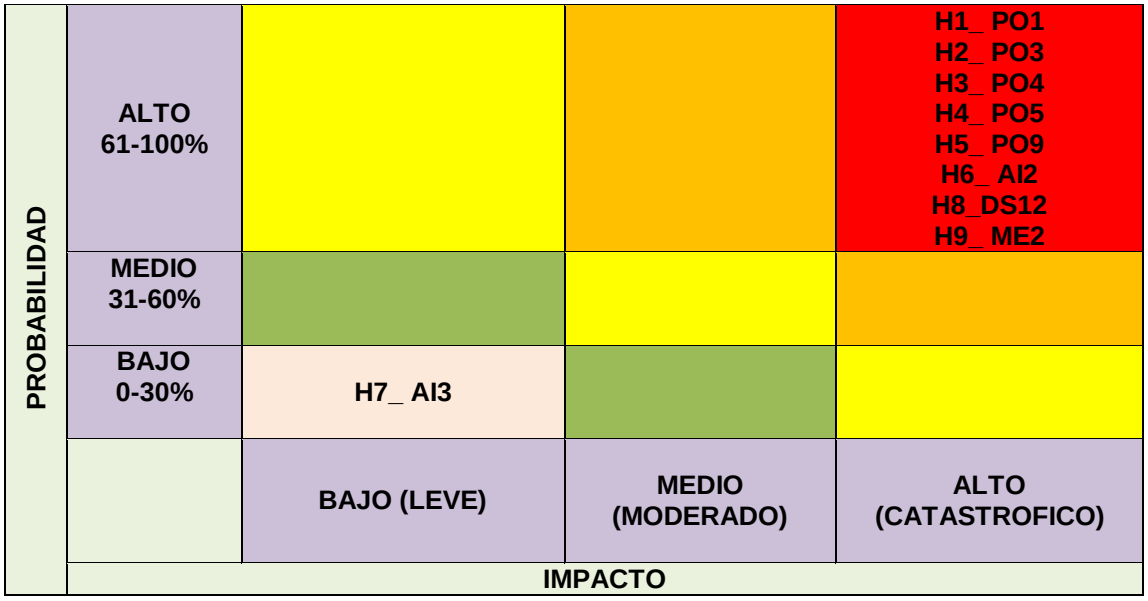
- **Resultado Matriz de probabilidad**

3.2.3. Hallazgos. A continuación se describirán los hallazgos encontrados en la E.S.E. Centro Hospital Divino Niño.

3.2.3.1. Dominios y Procesos Auditados en la E.S.E. Centro Hospital Divino Niño. Los hallazgos encontrados en la E.S.E. Centro Hospital Divino Niño se presentaran en el orden de los dominios y procesos auditados los cuales fueron:

- **DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)**

➢ Definir un Plan Estratégico de TI (PO1).
➢ Determinar la dirección tecnológica (PO3).
➢ Definición de la Organización y de las Relaciones de TI (PO4).
➢ Administrar la Inversión en TI (PO5).
➢ Evaluación y Análisis de Riesgos (PO9).



- **DOMINIO - ADQUISICION E IMPLEMENTACION (AI)**

➢ Adquirir y Mantener Software Aplicativo (AI2).
➢ Adquirir y Mantener la infraestructura Tecnológica (AI3)

- **DOMINIO - ENTREGAR Y DAR SOPORTE (DS)**

➢ Administración de instalaciones (DS12).

- **DOMINIO - MONITOREAR Y EVALUAR (ME)**

➢ Evaluar lo adecuado del control interno (ME2).

3.2.3.2. Hallazgos Centro Hospital Divino Niño

Tabla 6. Hallazgo 1 CHDN

	HALLAZGO CENTRO HOSPITAL DIVINO NIÑO			REF
				HHDN_O1
PROCESO AUDITADO	Funcionamiento del aspecto físico de la red de datos			**PÁGINA** 1 DE 1
RESPONSABLE	LUIS ALBERTO REYNEL ARAUJO			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planear y Organizar (PO)	**PROCESO**	Definir un plan estratégico de TI (PO1)	

DESCRIPCIÓN:

- No existe un grupo encargado de evaluar y estudiar el desempeño de la red de datos en su aspecto físico.
- No existen políticas ni procedimientos relacionados con la conformación adecuada de la arquitectura y del aspecto físico de la red de datos.

Esto es debido a la falta del manual de funciones donde se especifique el personal a cargo de la red de datos ni los procedimientos que se realizaran por parte de los funcionarios.

REF_PT:
CUESTIONARIOS_CHDN**/PLAN_PO1**(ANEXO 1)
E_AUDIO**/A_CHDN_01**

CONSECUENCIAS:
- Al no existir un grupo encargado de evaluar y estudiar el desempeño del aspecto físico de la red de datos se pierde la claridad para tomar decisiones pertinentes en caso de un desempeño no aceptado de la red de datos.
- Al no existir políticas ni procedimientos relacionados con la conformación de la arquitectura y del aspecto físico de la red de datos se pierde la opción de ajustar a las condiciones adecuadas que necesita la entidad los servicios de red de datos.

RIESGO:
- **Probabilidad de ocurrencia:** $= 100\%$
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:
- Conformar un grupo determinado de funcionarios que evalúen y estudien el desempeño de la red física de datos para con ello tomen decisiones oportunas y adecuadas en la eventualidad de no cumplir objetivos planteados.
- Elaborar e implementar políticas y procedimientos relacionados con la conformación de la arquitectura y del aspecto físico de la red de datos para ajustar los servicios de red a las necesidades propias que necesite la entidad.

Tabla 7. Hallazgo 2 CHDN

	HALLAZGO CENTRO HOSPITAL DIVINO NIÑO	**REF**
		HHDN_O2

PROCESO AUDITADO	Funcionamiento del aspecto físico de la red de datos	**PÁGINA**		
		1	DE	1
RESPONSABLE	LUIS ALBERTO REYNEL ARAUJO			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planear y Organizar (PO)	**PROCESO**	Determinar la dirección tecnológica (PO3)	

DESCRIPCIÓN:

- No existen políticas ni procedimientos relacionados con el estudio o análisis de nuevas tecnologías y elementos que sean implementados para el mejoramiento de la red de datos.
- No se lleva un registro documentado de los estudios de nuevas tecnologías y elementos que pueden ser incorporados al sistema de la red de datos.

A falta de un grupo o personal que deben evaluar el estado y desempeño de la red de datos, no se puede pensar en adquirir nuevas tecnologías.

REF_PT:

CUESTIONARIOS_CHDN**/PLAN_PO3** (ANEXO 2).
E_AUDIO**/A_CHDN_02.**

CONSECUENCIAS:

- Al no existir políticas de estudio o análisis de nuevas tecnologías y elementos que puedan mejorar el desempeño del sistema de red de datos se deja de lado la implementación de estas herramientas que permitan la optimización de los procesos de la red de datos.
- Al no documentar los estudios de nuevas tecnologías y elementos que puedan mejorar el desempeño de la red de datos aumentara en alto grado la dificultad de una implementación de estas en el futuro.

RIESGO:

- **Probabilidad de ocurrencia:** 71,43%
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Crear políticas que estén relacionadas con la búsqueda de nuevas tecnologías y elementos que mejoren el desempeño del sistema de red de datos.
- Documentar los estudios que se realicen de nuevas tecnologías y elementos que mejoren el desempeño de la red de datos para lograr implementarlas en el futuro con mayor facilidad.

Tabla 8. Hallazgo 3 CHDN

<table>
<tr><td></td><td colspan="3">HALLAZGO CENTRO HOSPITAL DIVINO NIÑO</td><td colspan="3">REF
HHDN_O3</td></tr>
<tr><td>PROCESO AUDITADO</td><td colspan="2">Funcionamiento del aspecto físico de la red de datos</td><td colspan="3">PÁGINA
1 DE 1</td></tr>
<tr><td>RESPONSABLE</td><td colspan="5">LUIS ALBERTO REYNEL ARAUJO</td></tr>
<tr><td>MATERIAL DE SOPORTE</td><td colspan="5">COBIT</td></tr>
<tr><td>DOMINIO</td><td>Planear y Organizar (PO)</td><td>PROCESO</td><td colspan="3">Definición de la Organización y de las Relaciones de TI (PO4)</td></tr>
<tr><td colspan="6">DESCRIPCIÓN:

• No existe manual de funciones o procedimientos especifico para los trabajadores encargados de la administración y mantenimiento del aspecto físico de la red de datos
• No existe dentro del manual de funciones la definición o descripción de los cargos relacionados con el manejo del aspecto físico del sistema de red de datos.
• No existen dentro del manual de funciones especificaciones de requisitos mínimos que deban cumplir las personas para ocupar los cargos relacionados con el manejo del aspecto físico de la red de datos.
• No existe un plan de contingencia que se ejecute cuando se presente ausencia de los funcionarios encargados de manejar el aspecto físico de la red de datos.

La alta gerencia ni el área de Talento Humano no se preocupa por el área de sistemas no existe un manual de funciones ni el personal suficiente para empezar a desarrollarlo

REF_PT:
CUESTIONARIOS_CHDN/PLAN_PO4 (ANEXO 3).
E_AUDIO/A_CHDN_03.
CONSECUENCIAS:

• Al no existir un manual de funciones o procedimientos especifico para el personal encargado del manejo y administración del aspecto físico de la red de datos se atenta contra el optimo funcionamiento y desempeño de tareas ya que no existen objetivos claros de orientación para subsanar requerimientos en este campo que a su vez afecta el normal desempeño de otras dependencias de la entidad.
• Al no existir la descripción o definición de los cargos relacionados con el manejo del aspecto físico de la red de datos se pierde ejecución de tareas específicas ya que las funciones pertinentes a este campo no tendrán la guía a seguir por parte de los funcionarios.
• Al no existir las especificaciones de los requisitos mínimos que se deben cumplir para ocupar los cargos relacionados con el manejo del aspecto físico de la red de datos se presenta ausencia de exigencia de perfiles que afectara la normatividad que debe llevar la entidad para el optimo funcionamiento de actividades.
• Al no existir un plan de contingencia que subsane la ausencia del personal encargado del manejo del aspecto físico de la red de datos se truncan los procesos ya que no existirá la guía para que el personal adecuado tome la responsabilidad de ejecutar las diferentes tareas y se opere con normalidad.

RIESGO:
• Probabilidad de ocurrencia: 100%
• Impacto según relevancia del proceso: Alto

RECOMENDACIONES:

• Elaborar el manual de funciones o procedimientos especifico para los trabajadores encargados del manejo y administración del aspecto físico de la red de datos y con esto se oriente al personal para un óptimo funcionamiento y desempeño de las tareas que se deben realizar en este campo.
• Implementar dentro del manual de funciones o procedimientos para los trabajadores encargados del manejo y administración del aspecto físico de la red de datos las descripciones o definiciones adecuadas, para no perder una guía concreta para la ejecución de tareas fundamentales.
• Ajustar los requerimientos mínimos para ocupar los cargos relacionados con el manejo del sistema de red de datos, para cumplir con esto con el cumplimiento de perfiles ajustándose a la normatividad y lograr desempeño adecuado de los funcionarios.
• Elaborar un plan de contingencia que subsane la ausencia del personal encargado del manejo del aspecto físico de la red de datos para evitar que los procesos sean afectados y se asigne la responsabilidad de estas funciones a personas idóneas.</td></tr>
</table>

Tabla 9. Hallazgo 4 CHDN

	HALLAZGO CENTRO HOSPITAL DIVINO NIÑO		**REF** **HHDN_O4**
PROCESO AUDITADO	Funcionamiento del aspecto físico de la red de datos		**PÁGINA** 1 DE 1
RESPONSABLE	LUIS ALBERTO REYNEL ARAUJO		
MATERIAL DE SOPORTE	COBIT		
DOMINIO	Planear y Organizar (PO)	**PROCESO**	Administrar la Inversión en TI (PO5)

DESCRIPCIÓN:

- No se realiza un proceso de toma de decisiones que de prioridad para la asignación de recursos a la adquisición de elementos tecnológicos que contribuyan con el mejoramiento del sistema de red de datos.
- No existen política para elaboración y mantenimiento de un buen presupuesto que sea utilizado en la adquisición de elementos que contribuyan con el sistema de red de datos.

La alta gerencia no tienen en cuenta al área de sistemas para la toma de decisiones para la adquisición de nuevas tecnologías, ni tampoco para la elaboración del presupuesto.

REF_PT:

CUESTIONARIOS_CHDN**/PLAN_PO5** (ANEXO 4).
E_AUDIO**/A_CHDN_04.**

CONSECUENCIAS:

- Al no existir un proceso de toma de decisiones que de prioridad a la asignación de recursos para adquisición de elementos tecnológicos para la red de datos se limita el óptimo funcionamiento del sistema de red y sus procesos no serán los más adecuados.
- Al no existir políticas que permitan elaborar y administrar un buen presupuesto para adquirir elementos que contribuyan al mejoramiento del sistema de red de datos se limita la adquisición necesaria de herramientas y con ello el desempeño general del sistema de red de datos.
-

RIESGO:

- **Probabilidad de ocurrencia:** $= 71{,}43\%$
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Implementar un proceso de toma de decisiones donde se brinde la prioridad necesaria a la asignación de recursos para adquirir elementos tecnológicos que ayuden al mejoramiento de la red física de datos y con ello optimizar los procesos informáticos de la entidad.
- Estudiar e implementar políticas donde se permita elaborar y administrar un buen presupuesto que sea utilizado para adquirir aquellos elementos tecnológicos necesarios para optimizar los procesos donde se involucre el sistema de red de datos.

Tabla 10. Hallazgo 5 CHDN

	HALLAZGO CENTRO HOSPITAL DIVINO NIÑO	**REF**
		HHDN_O5

PROCESO AUDITADO	Funcionamiento del aspecto físico de la red de datos	**PÁGINA**		
		1	DE	1
RESPONSABLE	LUIS ALBERTO REYNEL ARAUJO			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planear y Organizar (PO)	**PROCESO**	Evaluación y Análisis de Riesgos (PO9)	

DESCRIPCIÓN:

- No existen política y procedimientos para analizar y gestionar el riesgo del sistema de red de datos y para los elementos que lo conforman.
- No existe un plan de contingencia para contrarrestar un evento que afecte la conexión física de la red de datos.
- No existen políticas para adquirir pólizas de elementos que constituyen el aspecto físico de la red de datos.

Debido a que la solución a eventos que afecte la red de datos se han ido realizando cada vez que esto sucede, no se lleva ningún registro todo se realiza de modo empírico, El área de sistemas al tener rotación de personal no se puede designar a una persona específica para realizar documentación.

REF_PT:
CUESTIONARIOS_CHDN**/PLAN_PO9** (ANEXO 5).
E_AUDIO**/A_CHDN_05.**
CONSECUENCIAS:

- Al no existir política ni procedimientos para analizar y gestionar el riesgo del sistema físico de la red de datos y los elementos que lo conforman se pierde un actuar inmediato frente a las amenazas y se puede tomar una mala decisión en caso de un evento que atente contra la red de datos.
- Al no existir un plan de contingencia que actué en contra de un evento que afecte directamente a la red de datos se deja de lado mecanismos que ayuden a recomponer y reactivar procesos importantes donde el desempeño de la red de datos sea primordial.
- Al no existir políticas que se encaminen a la adquisición de pólizas para elementos que constituyen el aspecto físico de la red de datos se ve afectado el aseguramiento de estos a futuro y se afectara la pronta reconexión y restauración del sistema de red.

RIESGO:

- **Probabilidad de ocurrencia:** $= 100\%$
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Elaborar políticas y procedimientos para el análisis y la gestión del riesgo para el sistema físico de la red de datos debido a que si alguno de sus elementos esta en amenaza se tome decisiones oportunas y adecuadas que no llegue afectar en alta magnitud a la red de datos.
- Elaborar un plan de contingencia que ayude a dar soporte a la red física de datos para obtener mecanismos que ayuden a la recomponer y reactivar los procesos que se vean afectados para el sistema de red de datos.
- Implementar políticas para la adquisición de pólizas de los elementos que conforman el aspecto físico de la red de datos y con ello asegurar estos elementos a futuro y además se facilite restauración y reconexión del sistema de red de datos.

Tabla 11. Hallazgo 6 CHDN

	HALLAZGO CENTRO HOSPITAL DIVINO NIÑO	**REF**
		HHDN_O6

PROCESO AUDITADO	Funcionamiento del aspecto físico de la red de datos	**PÁGINA**		
		1	DE	1
RESPONSABLE	LUIS ALBERTO REYNEL ARAUJO			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquirir e Implementar (AI)	**PROCESO**	Adquirir y Mantener Software Aplicativo (AI2)	

DESCRIPCIÓN:

- No existe software que se utilice para monitorear la conexión de la red de datos en su aspecto físico.
- No se tiene ningún tipo de software para monitorear la conexión física de la red de datos.
- No existe mantenimiento para software de monitoreo de la red física de datos.

Debido al manejo institucional que tiene la E.S.E. Centro Hospital Divino Niño no se escucha las sugerencias del área de sistema en cuanto a la compra de un software con las características que se recomienda por ellos.

REF_PT:

CUESTIONARIOS_CHDN**/ADQ_AI2** (ANEXO 6).
E_AUDIO**/A_CHDN_06.**

CONSECUENCIAS:

- Al no existir software que se utilice para monitorear la conexión física de la red de datos se pierde el control de la conexión global de la red y con ello no permitiría identificar errores de conexión y agilizar mecanismos de reconexión.

RIESGO:

- **Probabilidad de ocurrencia:** $= 100\%$
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Adquirir software adecuado para monitorear la conexión física de la red de datos y con ello tener visión clara de la actividad de la red de datos.
- Llevar el proceso de mantenimiento periódico del software para monitoreo de la red física de datos y con ello asegurar el optimo funcionamiento de esta herramienta.

Tabla 12. Hallazgo 7 CHDN

	HALLAZGO CENTRO HOSPITAL DIVINO NIÑO	**REF**
		HHDN_O7

PROCESO AUDITADO	Funcionamiento del aspecto físico de la red de datos	**PÁGINA**		
		1	DE	1
RESPONSABLE	LUIS ALBERTO REYNEL ARAUJO			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquirir e Implementar (AI)	**PROCESO**	Adquirir y Mantener la infraestructura Tecnológica (AI3)	

DESCRIPCIÓN:

- No existe la implementación del procedimiento de múltiples cotizaciones a diferentes proveedores dentro de las políticas para adquisición de hardware.
- No existe conocimiento por parte de la gran mayoría de funcionarios sobre las políticas de adquisición de hardware.
- No existe documentación sobre las políticas de mantenimiento que se realiza a los equipos de cómputo.
- No se realiza acta de recepción por parte de la persona encargada del mantenimiento del equipo que se va a revisar y reparar.
- No existe documentación del proceso de mantenimiento de equipos de cómputo.
- No existe manual de funciones para el personal encargado de realizar mantenimiento preventivo y correctivo de los equipos de cómputo.
- No existe dentro del personal de mantenimiento un funcionario que tenga especialidad en la reparación de monitores.
- No se tiene una implementación adecuada del centro de computo.
- No existe proceso de mantenimiento para los elementos como switches, servidores y routers.
- No existe un procedimiento específico para el mantenimiento de la red de datos.
- No se tiene una implementación adecuada de cableado estructurado.
- No se tiene planos del cableado estructurado que se extiende por la entidad.
- No se realiza seguimiento adecuado de los elementos como: servidores, routers y switches ya que las hojas de vida no recolectan la información necesaria.

Falta de documentación en todo sentido tanto en el área de Talento humano como en el área de sistemas, donde no se tiene ningún tipo de procedimiento o manual de funciones ni de actividades.

La gerencia no se preocupa por el área de sistemas en general aún se tiene el pensamiento de que comprar computadores es invertir en sistemas.

La falta de personal y de documentación producen pérdidas de tiempo a la hora de actuar para contener algún evento que ponga en riesgo la red de datos.

REF_PT:

CUESTIONARIOS_CHDN**/ADO_AI3** (ANEXO 7).
E_FOTOGRAFICA**/IMG_1-IMG_10.**
E_FOTOGRAFICA**/IMG_11-IMG_13.**
E_AUDIO**/A_CHDN_7.**

CONSECUENCIAS:

- Al no existir múltiples cotizaciones para el proceso de adquisición de hardware se puede presentar sobregasto que atenta contra el presupuesto en general de la entidad y el presupuesto destinado a tecnologías de información.
- Al no existir conocimiento de las políticas de adquisición de hardware por parte de la mayoría de los funcionarios se pierde sentido de pertenencia por la entidad y sus intereses.
- Al no existir documentación sobre las políticas de mantenimiento que se realiza a los equipos de computo se pierde la guía directa de que hacer en este proceso y se presenta retrasó en las actividades.
- Al no existir la elaboración de un acta o documento escrito por parte de la persona encargada de hacer la recepción de equipos de cómputo para su respectiva revisión y reparación se carece de información para los objetivos que se plantean en el mantenimiento tanto correctivo o preventivo.
- Al no existir documentación sobre el mantenimiento de los equipos de cómputo se pierde guía de ejecución de este proceso y control de antecedentes.
- Al no existir manual de funciones para el personal encargado de hacer mantenimiento de los equipos de cómputo no se optimiza las actividades que deben realizarse en este proceso puesto que no hay responsable concreto para estas funciones.
- Al no existir dentro del personal de mantenimiento un funcionario especializado en reparación de monitores se estancan los procesos de corrección para las terminales de trabajo y se puede presentar gastos mayores para su reparación puesto que la entidad no cuenta con el personal para esta área.
- Al no existir la conformación ideal y adecuada del centro de computo se atenta contra la normatividad que busca en muchos aspectos brindar seguridad para la información y optimización de procesos.
- Al no existir el proceso de mantenimiento para los elementos como swiches, routers y servidores se atenta contra el buen funcionamiento de estos elementos y contra el cuidado que se les debe brindar ya son pieza fundamental de la red de datos.
- Al no existir un proceso de mantenimiento especifico de la red de datos se atenta contra su optimo funcionamiento y prevención de sucesos que perjudiquen los procesos que relacionan al sistema de red de datos.
- Al no existir la implementación adecuada de cableado estructurado se atenta contra la normatividad que ajusta objetivos de calidad para las entidades en lo que concierne a fiabilidad de la transmisión de datos y el respectivo orden de cada uno de los elementos de la red de datos.
- Al no tener planos del cableado estructurado que se extiende por la entidad se carece de visión inmediata para una eventual toma de decisiones donde se involucre nueva incorporación de elementos a la red de datos.
- Al no hacer seguimiento adecuado de los elementos como son routers, switches y servidores mediante hojas de vida ajustadas a recolectar la información suficiente se pierden los antecedentes que a futuro se deben utilizar para prevención y corrección de eventos que afecten el funcionamiento de estos elementos o equipos.

RIESGO:
- **Probabilidad de ocurrencia:** $= 26{,}53\%$
- **Impacto según relevancia del proceso:** Bajo

RECOMENDACIONES:

- Implementar dentro del proceso de adquisición de hardware el requisito de múltiples cotizaciones para con ello proteger el presupuesto de la entidad destinado a tecnologías de información.
- Dar a conocer las políticas de adquisición de hardware a los funcionarios para tener mayor sentido de pertenencia por los intereses de la entidad.
- Documentar las políticas de mantenimiento de los equipos de cómputo para consolidar la guía del proceso a seguir y con ello agilizar las actividades correspondientes.
- Implementar el diligenciamiento de un acta o documento adecuado para facilitar el mantenimiento de los elementos de cómputo y así facilitar el trabajo a la persona encargada del proceso para la respectiva revisión y reparación.
- Implementar la documentación sobre el mantenimiento de los equipos de cómputo se permite actuar más rápido ante este tipo de eventos ya que se facilita por la recolección de antecedentes.
- Incorporar dentro del manual de funciones las actividades pertinentes para lo que concierne al mantenimiento de equipos de cómputo ya que así se optimizara este proceso debido a que se asigna responsabilidad directa.
- Capacitar al personal encargado para el mantenimiento de equipos de computo sobre la reparación y mantenimiento de monitores para evitar se estanque el funcionamiento de las terminales de trabajo y además ahorras gastos que generarían reparación en otro lugar diferente a la entidad.
- Implementar el centro de cómputo con características adecuadas y normatividad correspondiente para lograr optimización de procesos y seguridad de la información que es vital para la entidad.
- Implementar el proceso de mantenimiento de los elementos como: swiches, routers y servidores para garantizar su óptimo funcionamiento y cuidado ya que son elementos fundamentales en la constitución de la red de datos.
- Implementar el proceso específico para el mantenimiento de la red de datos y así se prevengan los sucesos que puedan perjudicar procesos que se relacionen con el sistema de red de datos.
- Implementar y ajustar la entidad a un correcto esquema de cableado estructurado para que no se atente contra la normatividad para alcanzar los objetivos de calidad que debe poseer la entidad por la importancia de la información que se maneja.
- Elaborar los planos del cableado estructurado que se extiende por la entidad para tener facilidad de análisis al momento de una eventual toma de decisiones para mejorar el sistema de red de datos con incorporación de nuevos elementos en su aspecto físico.
- Elaborar hojas de vida adecuadas para recolectar información que sirva para el optimo seguimiento de los equipos como: servidores, routers y switches y con ello prevenir y corregir inconvenientes a futuro.

Tabla 13. Hallazgo 8 CHDN

	HALLAZGO CENTRO HOSPITAL DIVINO NIÑO	**REF**
		HHDN_O8

PROCESO AUDITADO	Funcionamiento del aspecto físico de la red de datos	**PÁGINA**			
		1	DE	1	
RESPONSABLE	LUIS ALBERTO REYNEL ARAUJO				
MATERIAL DE SOPORTE	COBIT				
DOMINIO	Entrega de Servicios y Soportes (DS)	**PROCESO**	Administración de instalaciones (DS12)		

DESCRIPCIÓN:

- No existen política adecuadas en el campo de seguridad referente al acceso y salida de las instalaciones donde se encuentran los elementos que conforman el aspecto físico de la red de datos.
- Dentro de las políticas de seguridad para el acceso a las instalaciones no se tiene en cuenta la identificación, autenticación y autorización de los individuos que ingresan.
- No se realizan requisas tanto al personal que ingresa como sale de las instalaciones.
- No se tiene en cuenta dentro de las políticas de seguridad de la entidad el procedimiento de escolta de visitantes para controlar sus acciones en las instalaciones.
- No existe políticas para brindar seguridad de las instalaciones ante eventos naturales o ambientales.
- No se adquiere pólizas para asegurar las perdidas que se ocasionen dentro de las instalaciones ante cualquier tipo de desastre para los elementos que conforman el aspecto físico de la red de datos.
- No existe la instalación de dispositivos en el lugar donde se ubican los servidores (detectores humo, supresores de fuego) que permitan detectar y prevenir incendios.
- No existe la instalación de cámaras que permitan monitorear el interior de las instalaciones de la entidad.

La seguridad no ha sido un fuerte en la institución y no se maneja ningún tipo de seguridad ni realizado ninguna inversión en el área de sistemas y en la E.S.E. Centro Hospital Divino Niño, falta de documentación sobre políticas y controles de seguridad.

REF PT:
CUESTIONARIOS_CHDN**/ESS_DS12** (ANEXO 8).
E_AUDIO**/A_CHDN_8.**

CONSECUENCIAS:

- Al no existir políticas adecuadas en el campo de la seguridad referente al acceso y salida de las instalaciones de la entidad donde se encuentran los elementos fundamentales de la red de datos como: servidores, switches y routers se corre el riesgo de sufrir robos, atentados o pérdida de información que es vital para la entidad.
- Al no existen políticas adecuadas en el campo de la seguridad referente a la identificación, autenticación y autorización de los individuos que ingresan a las instalaciones de la entidad da

lugar a que se atente contra los elementos de la entidad incluyendo la red física de datos.

- Al no controlar el acceso y salida de personas de la entidad mediante requisas no se puede detectar elementos que se utilicen para sabotear los procesos de la red de datos o hurto de los mismos.
- Al no tener en cuenta dentro de las políticas de seguridad de la entidad el procedimiento de escolta de visitantes se corre el riesgo de sufrir robos y sabotajes que afecten la red de datos.
- Al no existir políticas para seguridad de las instalaciones ante cualquier evento natural o ambiental no se disminuye riesgos de desastres que puedan afectar el desempeño y aspecto físico de la red de datos.
- Al no existir pólizas para asegurar las perdidas que se ocasionen dentro de las instalaciones ante cualquier tipo de desastre de los elementos que conforman el aspecto físico de la red de datos en este caso de presentarse un fortuito tardara mucho tiempo en recomponer el sistema de red.
- Al no existir instalación de dispositivos como son (detectores de humo, supresores de fuego) en el cuarto de servidores se corre el riesgo de sufrir un incendio.
- Al no existir instalación de cámaras en el interior de la entidad no se pueden registrar las actividades sospechosas que atenten contra la entidad.

RIESGO:

- **Probabilidad de ocurrencia:** = 90.9%
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Crear políticas adecuadas en el campo de seguridad referente al acceso y salida de las instalaciones para evitar hurtos de los elementos que conforman el sistema físico de la red de datos.
- Crear políticas adecuadas en el campo de seguridad referente a la identificación, autenticación y autorización de los individuos que ingresan a las instalaciones para impedir que se atente contra los elementos de la entidad incluyendo los elementos que hacen parte del aspecto físico de la red de datos.
- Controlar el acceso y salida de la entidad por medio de requisas para detectar que personas ajenas a la entidad realicen sabotaje a los procesos de la red de datos y también detección de hurto de aquellos elementos que conforman el aspecto físico de la red de datos.
- Implementar en la entidad el procedimiento de escolta para visitantes y con esto evitar hurto de elementos y sabotaje de los elementos que posee la estructura física de la red de datos.
- Tener en cuenta dentro de las políticas de seguridad de la entidad el procedimiento de escolta de visitantes para impedir robos, sabotajes en contra de la entidad.
- Implementar en la entidad políticas para dar mayor seguridad a las instalaciones ante cualquier evento natural o ambiental para disminuir los riesgos de desastres que atenten contra el óptimo desempeño y el aspecto físico en general de la red de datos.
- Adquirir pólizas de seguros para los elementos que constituyen el aspecto físico de la red de datos ya que si se presenta un evento inesperado que atente contra el sistema de red de datos no se tarde mucho tiempo en recomponer y poner en marcha el sistema.
- Instalar dispositivos como son (detectores de humo, supresores de fuego) en el cuarto de servidores para evitar un eventual incendio.
- Instalar cámaras en el interior de la entidad para registrar las actividades sospechosas de los individuos que ingresan.

Tabla 14. Hallazgo 9 CHDN

	HALLAZGO CENTRO HOSPITAL DIVINO NIÑO	**REF**
		HHDN_O9

PROCESO AUDITADO	Funcionamiento del aspecto físico de la red de datos	**PÁGINA**		
		1	DE	1
RESPONSABLE	LUIS ALBERTO REYNEL ARAUJO			
MATERIAL DE SOPORTE	COBIT			

DOMINIO	Monitorear y Evaluar (ME)	**PROCESO**	Evaluar lo adecuado del control interno(ME2)

DESCRIPCIÓN:

- No existen políticas ni procedimientos que se encaminen a monitorear la seguridad del aspecto físico de la red de datos.
- No existe descripción detallada de los procedimientos de monitoreo para la seguridad del aspecto físico de la red de datos que se deben aplicar.
- No existen políticas que contemplen la periodicidad adecuada para efectuar procesos de monitoreo.
- No existen políticas que contemplen quien debe ejecutar el monitoreo.
- No existen documentaciones de las políticas de monitoreo.
- No existe conocimiento para el personal encargado de administrar la red de datos sobre políticas y procedimientos de monitorear la seguridad del aspecto físico de la red de datos.
- No se realizan auditorias de ningún tipo para evaluar el desempeño de la parte eléctrica, ventilación del centro de computo y utilización de normas de cableado estructurado.

Falta de documentación en el área de sistemas, no se puede pedirle al personal encargado de que encargarse ni de qué manera hacerlo todo toca con los conocimientos que se manejen por parte de los funcionarios.

No existe ningún plan de auditorías para verificar el estado y desempeño de la red de datos ni del área de sistemas como tal.

REF_PT:

CUESTIONARIOS_CHDN**/MON_ME2** (ANEXO 9).
E_AUDIO**/A_CHDN_9.**

CONSECUENCIAS:

- Al no existir políticas ni procedimientos que se encaminen al monitoreo de la seguridad del aspecto físico de la red de datos se pierde el seguimiento de la actividad de la red de datos y con ello se carece del nivel correctivo y preventivo de eventos que afecten su buen funcionamiento.

- Al no existir descripción detallada de los procesos de monitoreo que se deben realizar al aspecto físico del sistema de red de datos se carece de hacer seguimientos óptimos y precisos que contribuyan al buen funcionamiento de la red de datos.
- Al no existir la contemplación de la periodicidad con la que se debe realizar los procesos de monitoreo para seguimiento del aspecto físico de la red de datos se ocasiona perdida del seguimiento en tiempo adecuado y recomendado para realizar ajustes correctivos y preventivos.
- Al no existir políticas que contemplen quien debe ser el responsable del proceso de monitoreo para la seguridad del aspecto físico de la red de datos se pierde ejecución en las funciones que se debe cumplir ante el proceso ya que no habrá quien rinda cuentas de estas actividades.
- Al no existir la documentación de las políticas de monitoreo para la seguridad física de la red de datos se pierde información guía que agilice este proceso.
- Al no existir conocimiento de políticas y procedimientos de monitoreo para los empleados encargados de administrar el aspecto físico de la red de datos se pierde ejecución de actividades claves para prevenir y corregir problemas con la red de datos.
- Al no realizar auditorias de ningún tipo para los aspectos relacionados con la red física de datos no se puede concluir una idea real del funcionamiento de la red física de datos.

RIESGO:

- **Probabilidad de ocurrencia:** 100%
- **Impacto según relevancia del proceso:** Alto

RECOMENDACIONES:

- Elaborar e implementar políticas y procedimientos adecuados para el monitoreo de la seguridad del aspecto físico de la red de datos para tener un seguimiento que ayude a generar procesos preventivos y correctivos.
- Implementar dentro de las políticas de monitoreo del aspecto físico de la red datos una descripción detallada de los procesos a trabajar, con ello se elaborara seguimientos óptimos y precisos que optimicen el funcionamiento de la red de datos.
- Contemplar el periodo en el que se deba realizar el monitoreo dentro de las políticas de la seguridad del aspecto físico de la red de datos, para que el tiempo empleado sea el adecuado y se pueda realizar las respectivas prevenciones y correcciones.
- Asignar las funciones de monitorear la seguridad del aspecto físico de la red de datos a personal especifico, con ello se priorizara la ejecución de estas tareas y se sabrá quien responderá ante estas actividades.
- Documentar las políticas para seguridad de la red física de datos y con ello utilizar esta información como herramienta ágil para ejecutar este proceso.
- Dar a conocer a los funcionarios encargados de la administración de la red de datos las políticas de monitoreo para el seguimiento de la seguridad del aspecto físico de la red de datos, para lograr ejecución dentro de lo correctivo y preventivo dentro de lo que atente al sistema de red de datos.
- Realizar auditorias del sistema físico de la red de datos para así lograr tener la visión mas clara de la situación que presenta la red de datos y mejorar los aspectos que sean necesarios.

3.2.4. Informe de Auditoria.

✓ **Objetivos**

Realizar auditoria de sistemas a la infraestructura física de la red de datos de la E.S.E. Centro Hospital Divino Niño, con el fin de evidenciar las vulnerabilidades de seguridad física a las que se encuentra expuesta la información que utilizan dicha entidad.

✓ **Objetivos Específicos**

- Analizar y evaluar políticas de control de riesgos dentro de la entidad.

- Analizar las políticas existentes en la entidad que garantizan la seguridad física de la información.

- Establecer el estado de las políticas que garantizan la continuidad en el proceso de comunicación de la red de datos de la sede principal de la E.S.E. Centro Hospital Divino Niño.

- Aportar información que permita a la entidad auditada implementar las medidas necesarias, para garantizar que los procesos realizados por sus usuarios tengan como materia prima información confiable, integra y confidencial, que asegure la trasparencia en los procesos.

- Analizar las instalaciones físicas que las entidades poseen, que garantizan la seguridad de la información.

✓ **Limitaciones.** La auditoria se realizo con completa normalidad, sin embargo cabe resaltar que en ningún momento se tuvo acceso a servidores en funcionamiento, un routers o switches ya que esto no hacia parte de los lineamientos de la auditoria, ni se tuvo acceso a alguna información en cuanto al hardware de la red de datos e información, como planos de red por lo que no existe ningún plano, inventario de hardware de equipos de comunicaciones debido a que la mayoría son del proveedor de internet, lo que impidió diagnosticar el proceso de normas y certificación de puntos de la red montada en la sede principal de la E.S.E. Centro Hospital Divino Niño.

✓ **Resultados de la Auditoría.** A continuación se presentan los resultados de la auditoría aplicada a la infraestructura física de la red de datos de la sede principal de la E.S.E Centro Hospital Divino Niño, también se presentan las recomendaciones de mejoramiento para cada uno de los procesos COBIT auditados.

- **DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)**

➢ **Proceso COBIT PO1: Definir un Plan Estratégico de TI.**

○ **Hallazgo**

No existe un grupo encargado de evaluar y estudiar el desempeño de la red de datos en su aspecto físico.

No existen políticas ni procedimientos relacionados con la conformación adecuada de la arquitectura y del aspecto físico de la red de datos.

REF HHDN_01 (Tabla 6)

○ **Recomendaciones**

Conformar un grupo determinado de funcionarios que evalúen y estudien el desempeño de la red física de datos para con ello tomen decisiones oportunas y adecuadas en la eventualidad de no cumplir objetivos planteados.

Elaborar e implementar políticas y procedimientos relacionados con la conformación de la arquitectura y del aspecto físico de la red de datos para ajustar los servicios de red a las necesidades propias que necesite la entidad.

➢ **Proceso COBIT PO3: Determinar la dirección tecnológica.**

○ **Hallazgo**

No existen políticas ni procedimientos relacionados con el estudio o análisis de nuevas tecnologías y elementos que sean implementados para el mejoramiento de la red de datos.

No se lleva un registro documentado de los estudios de nuevas tecnologías y elementos que pueden ser incorporados al sistema de la red de datos.

REF HHDN_02 (Tabla 7)

○ **Recomendaciones**

Crear políticas que estén relacionadas con la búsqueda de nuevas tecnologías y elementos que mejoren el desempeño del sistema de red de datos.

Documentar los estudios que se realicen de nuevas tecnologías y elementos que mejoren el desempeño de la red de datos para lograr implementarlas en el futuro con mayor facilidad.

➢ **Proceso COBIT PO4: Definición de la Organización y de las Relaciones de TI.**

- **Hallazgo**

No existe manual de funciones o procedimientos específico para los trabajadores encargados de la administración y mantenimiento del aspecto físico de la red de datos.

No existe dentro del manual de funciones la definición o descripción de los cargos relacionados con el manejo del aspecto físico del sistema de red de datos.

No existen dentro del manual de funciones especificaciones de requisitos mínimos que deban cumplir las personas para ocupar los cargos relacionados con el manejo del aspecto físico de la red de datos.

No existe un plan de contingencia que se ejecute cuando se presente ausencia de los funcionarios encargados de manejar el aspecto físico de la red de datos.

REF HHDN_03 (Tabla 8)

- **Recomendaciones**

Elaborar el manual de funciones o procedimientos especifico para los trabajadores encargados del manejo y administración del aspecto físico de la red de datos y con esto se oriente al personal para un óptimo funcionamiento y desempeño de las tareas que se deben realizar en este campo.

Implementar dentro del manual de funciones o procedimientos para los trabajadores encargados del manejo y administración del aspecto físico de la red de datos las descripciones o definiciones adecuadas, para no perder una guía concreta para la ejecución de tareas fundamentales.

Ajustar los requerimientos mínimos para ocupar los cargos relacionados con el manejo del sistema de red de datos, para cumplir con esto con el cumplimiento de perfiles ajustándose a la normatividad y lograr desempeño adecuado de los funcionarios.

Elaborar un plan de contingencia que subsane la ausencia del personal encargado del manejo del aspecto físico de la red de datos para evitar que los procesos sean afectados y se asigne la responsabilidad de estas funciones a personas idóneas.

- **Proceso COBIT PO5: Administrar la Inversión en TI.**

  - **Hallazgo**

No se realiza un proceso de toma de decisiones que de prioridad para la asignación de recursos a la adquisición de elementos tecnológicos que contribuyan con el mejoramiento del sistema de red de datos.

No existen política para elaboración y mantenimiento de un buen presupuesto que sea utilizado en la adquisición de elementos que contribuyan con el sistema de red de datos.

REF HHDN_04 (Tabla 9)

  - **Recomendaciones**

Implementar un proceso de toma de decisiones donde se brinde la prioridad necesaria a la asignación de recursos para adquirir elementos tecnológicos que ayuden al mejoramiento de la red física de datos y con ello optimizar los procesos informáticos de la entidad.

Estudiar e implementar políticas donde se permita elaborar y administrar un buen presupuesto que sea utilizado para adquirir aquellos elementos tecnológicos necesarios para optimizar los procesos donde se involucre el sistema de red de datos.

- **Proceso COBIT PO9: Evaluación y Análisis de Riesgos.**

  - **Hallazgo**

No existen política y procedimientos para analizar y gestionar el riesgo del sistema de red de datos y para los elementos que lo conforman.

No existe un plan de contingencia para contrarrestar un evento que afecte la conexión física de la red de datos.

No existen políticas para adquirir pólizas de elementos que constituyen el aspecto físico de la red de datos.

REF HHDN_05 (Tabla 10)

  - **Recomendaciones**

Elaborar políticas y procedimientos para el análisis y la gestión del riesgo para el sistema físico de la red de datos debido a que si alguno de sus elementos esta en

amenaza se tome decisiones oportunas y adecuadas que no llegue afectar en alta magnitud a la red de datos.

Elaborar un plan de contingencia que ayude a dar soporte a la red física de datos para obtener mecanismos que ayuden a la recomponer y reactivar los procesos que se vean afectados para el sistema de red de datos.

Implementar políticas para la adquisición de pólizas de los elementos que conforman el aspecto físico de la red de datos y con ello asegurar estos elementos a futuro y además se facilite restauración y reconexión del sistema de red de datos.

- **DOMINIO ADQUISICIÓN E IMPLEMENTACIÓN (AI)**

➢ **Proceso COBIT AI2: Adquirir y Mantener Software Aplicativo.**

○ **Hallazgo**

No existe software que se utilice para monitorear la conexión de la red de datos en su aspecto físico.

No se tiene ningún tipo de software para monitorear la conexión física de la red de datos.

No existe mantenimiento para software de monitoreo de la red física de datos.

REF HHDN_06 (Tabla 11)

○ **Recomendaciones**

Adquirir software adecuado para monitorear la conexión física de la red de datos y con ello tener visión clara de la actividad de la red de datos.

Llevar el proceso de mantenimiento periódico del software para monitoreo de la red física de datos y con ello asegurar el optimo funcionamiento de esta herramienta.

➢ **Proceso COBIT AI3: Adquirir y Mantener la infraestructura Tecnológica.**

○ **Hallazgo**

No existe la implementación del procedimiento de múltiples cotizaciones a diferentes proveedores dentro de las políticas para adquisición de hardware.

No existe conocimiento por parte de la gran mayoría de funcionarios sobre las políticas de adquisición de hardware.

No existe documentación sobre las políticas de mantenimiento que se realiza a los equipos de cómputo.

No se realiza acta de recepción por parte de la persona encargada del mantenimiento del equipo que se va a revisar y reparar.

No existe documentación del proceso de mantenimiento de equipos de cómputo.

No existe manual de funciones para el personal encargado de realizar mantenimiento preventivo y correctivo de los equipos de cómputo.

No existe dentro del personal de mantenimiento un funcionario que tenga especialidad en la reparación de monitores.

No se tiene una implementación adecuada del centro de computo.

No existe proceso de mantenimiento para los elementos como switches, servidores y routers.

No existe un procedimiento específico para el mantenimiento de la red de datos.

No se tiene una implementación adecuada de cableado estructurado.

No se tiene planos del cableado estructurado que se extiende por la entidad.

No se realiza seguimiento adecuado de los elementos como: servidores, routers y switches ya que las hojas de vida no recolectan la información necesaria.

REF HHDN_07 (Tabla 12)

- **Recomendaciones**

Implementar dentro del proceso de adquisición de hardware el requisito de múltiples cotizaciones para con ello proteger el presupuesto de la entidad destinado a tecnologías de información.

Dar a conocer las políticas de adquisición de hardware a los funcionarios para tener mayor sentido de pertenencia por los intereses de la entidad.

Documentar las políticas de mantenimiento de los equipos de cómputo para consolidar la guía del proceso a seguir y con ello agilizar las actividades correspondientes.

Implementar el diligenciamiento de un acta o documento adecuado para facilitar el mantenimiento de los elementos de cómputo y así facilitar el trabajo a la persona encargada del proceso para la respectiva revisión y reparación.

Implementar la documentación sobre el mantenimiento de los equipos de cómputo se permite actuar más rápido ante este tipo de eventos ya que se facilita por la recolección de antecedentes.

Incorporar dentro del manual de funciones las actividades pertinentes para lo que concierne al mantenimiento de equipos de cómputo ya que así se optimizara este proceso debido a que se asigna responsabilidad directa.

Capacitar al personal encargado para el mantenimiento de equipos de computo sobre la reparación y mantenimiento de monitores para evitar se estanque el funcionamiento de las terminales de trabajo y además ahorras gastos que generarían reparación en otro lugar diferente a la entidad.

Implementar el centro de cómputo con características adecuadas y normatividad correspondiente para lograr optimización de procesos y seguridad de la información que es vital para la entidad.

Implementar el proceso de mantenimiento de los elementos como: swiches, routers y servidores para garantizar su óptimo funcionamiento y cuidado ya que son elementos fundamentales en la constitución de la red de datos.

Implementar el proceso específico para el mantenimiento de la red de datos y así se prevengan los sucesos que puedan perjudicar procesos que se relacionen con el sistema de red de datos.

Implementar y ajustar la entidad a un correcto esquema de cableado estructurado para que no se atente contra la normatividad para alcanzar los objetivos de calidad que debe poseer la entidad por la importancia de la información que se maneja.

Elaborar los planos del cableado estructurado que se extiende por la entidad para tener facilidad de análisis al momento de una eventual toma de decisiones para mejorar el sistema de red de datos con incorporación de nuevos elementos en su aspecto físico.

Elaborar hojas de vida adecuadas para recolectar información que sirva para el optimo seguimiento de los equipos como: servidores, routers y switches y con ello prevenir y corregir inconvenientes a futuro.

- **DOMINIO- ENTREGAR Y DAR SOPORTE (DS)**

➢ **Proceso COBIT DS12: Administración de instalaciones.**

○ **Hallazgo**

No existe política adecuada en el campo de seguridad referente al acceso y salida de las instalaciones donde se encuentran los elementos que conforman el aspecto físico de la red de datos.

Dentro de las políticas de seguridad para el acceso a las instalaciones no se tiene en cuenta la identificación, autenticación y autorización de los individuos que ingresan.

No se realizan requisas tanto al personal que ingresa como sale de las instalaciones.

No se tiene en cuenta dentro de las políticas de seguridad de la entidad el procedimiento de escolta de visitantes para controlar sus acciones en las instalaciones.

No existe políticas para brindar seguridad de las instalaciones ante eventos naturales o ambientales.

No se adquiere pólizas para asegurar las perdidas que se ocasionen dentro de las instalaciones ante cualquier tipo de desastre para los elementos que conforman el aspecto físico de la red de datos.

No existe la instalación de dispositivos en el lugar donde se ubican los servidores (detectores humo, supresores de fuego) que permitan detectar y prevenir incendios.

No existe la instalación de cámaras que permitan monitorear el interior de las instalaciones de la entidad.

REF HHDN_08 (Tabla 13)

○ **Recomendaciones**

Crear políticas adecuadas en el campo de seguridad referente al acceso y salida de las instalaciones para evitar hurtos de los elementos que conforman el sistema físico de la red de datos.

Crear políticas adecuadas en el campo de seguridad referente a la identificación, autenticación y autorización de los individuos que ingresan a las instalaciones para

impedir que se atente contra los elementos de la entidad incluyendo los elementos que hacen parte del aspecto físico de la red de datos.

Controlar el acceso y salida de la entidad por medio de requisas para detectar que personas ajenas a la entidad realicen sabotaje a los procesos de la red de datos y también detección de hurto de aquellos elementos que conforman el aspecto físico de la red de datos.

Implementar en la entidad el procedimiento de escolta para visitantes y con esto evitar hurto de elementos y sabotaje de los elementos que posee la estructura física de la red de datos.

Tener en cuenta dentro de las políticas de seguridad de la entidad el procedimiento de escolta de visitantes para impedir robos, sabotajes en contra de la entidad.

Implementar en la entidad políticas para dar mayor seguridad a las instalaciones ante cualquier evento natural o ambiental para disminuir los riesgos de desastres que atenten contra el óptimo desempeño y el aspecto físico en general de la red de datos.

Adquirir pólizas de seguros para los elementos que constituyen el aspecto físico de la red de datos ya que si se presenta un evento inesperado que atente contra el sistema de red de datos no se tarde mucho tiempo en recomponer y poner en marcha el sistema.

Instalar dispositivos como son (detectores de humo, supresores de fuego) en el cuarto de servidores para evitar un eventual incendio.

Instalar cámaras en el interior de la entidad para registrar las actividades sospechosas de los individuos que ingresan.

- **DOMINIO – MONITOREAR Y EVALUAR (ME)**

➢ **Proceso COBIT ME2: Evaluar lo adecuado del control interno.**

o **Hallazgo**

No existen políticas ni procedimientos que se encaminen a monitorear la seguridad del aspecto físico de la red de datos.

No existe descripción detallada de los procedimientos de monitoreo para la seguridad del aspecto físico de la red de datos que se deben aplicar.

No existen políticas que contemplen la periodicidad adecuada para efectuar procesos de monitoreo.

No existen políticas que contemplen quien debe ejecutar el monitoreo.

No existen documentaciones de las políticas de monitoreo.

No existe conocimiento para el personal encargado de administrar la red de datos sobre políticas y procedimientos de monitorear la seguridad del aspecto físico de la red de datos.

No se realizan auditorias de ningún tipo para evaluar el desempeño de la parte eléctrica, ventilación del centro de computo y utilización de normas de cableado estructurado.

REF HHDN_09 (Tabla 14)

- **Recomendaciones**

Elaborar e implementar políticas y procedimientos adecuados para el monitoreo de la seguridad del aspecto físico de la red de datos para tener un seguimiento que ayude a generar procesos preventivos y correctivos.

Implementar dentro de las políticas de monitoreo del aspecto físico de la red datos una descripción detallada de los procesos a trabajar, con ello se elaborara seguimientos óptimos y precisos que optimicen el funcionamiento de la red de datos.

Contemplar el periodo en el que se deba realizar el monitoreo dentro de las políticas de la seguridad del aspecto físico de la red de datos, para que el tiempo empleado sea el adecuado y se pueda realizar las respectivas prevenciones y correcciones.

Asignar las funciones de monitorear la seguridad del aspecto físico de la red de datos a personal especifico, con ello se priorizara la ejecución de estas tareas y se sabrá quien responderá ante estas actividades.

Documentar las políticas para seguridad de la red física de datos y con ello utilizar esta información como herramienta ágil para ejecutar este proceso.

Dar a conocer a los funcionarios encargados de la administración de la red de datos las políticas de monitoreo para el seguimiento de la seguridad del aspecto físico de la red de datos, para lograr ejecución dentro de lo correctivo y preventivo dentro de lo que atente al sistema de red de datos.

Realizar auditorías del sistema físico de la red de datos para así lograr tener la visión más clara de la situación que presenta la red de datos y mejorar los aspectos que sean necesarios.

3.2.4.1. Evaluación de la usabilidad y del decreto 1151 de 2008 de Gobierno en Línea.

Tabla 15. Gobierno En Línea E.S.E. Centro Hospital Divino Niño

Nombre de la entidad:	E.S.E. Centro Hospital Divino Niño
Municipio:	Tumaco (Nariño)
Nit:	840.001.036-7
Dirección:	Barrio Unión Victoria Frente a los tanques de Ecopetrol
Teléfono:	7 27 15 56 - 7 27 04 04
Correo electrónico:	divinonino@esechdntumaco.gov.co
URL portal Web:	www.esechdntumaco.gov.co

CRITERIO	CUMPLE/NO CUMPLE
SOBRE LA ENTIDAD	
Información básica en el Portal del Estado Colombiano	**NO**
Misión y visión	**SI**
Objetivos y funciones	**SI**
Organigrama	**NO**
Localización física	**SI**
Teléfonos y/o líneas gratuitas y fax (con indicativo nacional e internacional)	**SI**
Correo electrónico de contacto o enlace al sistema de atención al ciudadano con que cuente la entidad	**NO**
Horarios y días de atención al público	**NO**
Directorio de funcionarios principales	**NO**
Directorio de entidades	**NO**
Directorio de agremiaciones y asociaciones	**NO**
NORMATIVIDAD	
Leyes/ Ordenanzas /Acuerdos	**NO**
Decretos	**NO**
Resoluciones, Circulares /u otros actos administrativos de carácter general	**NO**
PRESUPUESTO	
Presupuesto aprobado en ejercicio	**NO**
Información histórica de presupuestos	**NO**
POLITICAS, PLANES, PROGRAMAS Y PROYECTOS INSTITUCIONALES	
Políticas, planes o líneas estratégicas	**NO**
Programas y proyectos en ejecución	**NO**
Contacto con dependencia responsable	**NO**
TRAMITES Y SERVICIOS	
Listado de trámites y servicios	**NO**
CONTRATACION	
Información sobre la contratación	**NO**
CONTROL Y RENDICION DE CUENTAS	

Entes de control que vigilan a la entidad	**NO**
Informes de Gestión	**NO**
Metas e indicadores de gestión	**NO**
Plan de Mejoramiento	**NO**
SERVICIOS DE INFORMACION	
Información para niños	**NO**
Preguntas y respuestas frecuentes	**NO**
Boletines y publicaciones	**SI**
Noticias	**SI**
Calendario de actividades	**NO**
Glosario	**NO**
Política de privacidad y condiciones de uso	**NO**
Política editorial y de actualización	**NO**
Oferta de empleos	**NO**
ESTANDARES DE PRESENTACION	
Enlace al Portal del Estado Colombiano	**SI**
Fecha de la última actualización	**NO**
Número de Visitas	**SI**
División de los contenidos	**NO**
Uso de colores	**SI**
Manejo de vínculos	**SI**
ESTANDARES DE FUNCIONALIDAD	
Mapa del sitio	**NO**
Acceso a la página de inicio	**SI**
Acceso al menú principal	**SI**
Ruta de navegación	**NO**
ESTANDARES TECNICOS	
Nombre de dominio	**SI**
Marcación y/o etiquetado	**NO**
Uso de navegadores	**SI**
MECANISMOS DE INTERACCIÓN	
Servicios de información al ciudadano	**NO**
Buzón de contacto, peticiones, quejas y reclamos	**NO**
Seguimiento a solicitudes, peticiones, quejas y reclamos.	**NO**
Mecanismo de búsqueda	**NO**
Suscripción a servicios de información al correo electrónico o RSS	**NO**
Encuestas de opinión	**SI**
Información en audio y/o video	**SI**
Servicios de atención en línea	**NO**
Mecanismos de participación	**NO**
Ayudas	**NO**
Avisos de confirmación	**NO**

3.2.4.2. Medición y evaluación de la usabilidad del portal web de la E.S.E. Centro Hospital Divino Niño.

Tabla 16. Usabilidad E.S.E Centro Hospital Divino Niño

Institución:		**E.S.E. Centro Hospital Divino Niño**		
Url:		**www.esechdntumaco.gov.co**		
Evaluador:		**Luis Alberto Reynel Araujo**		
Fecha:		**16/03/2012**		
Nota:		**5,18**		
20%		**1. Usabilidad**	**5,611**	**1,1222**
	40%	**1.1 Comprensibilidad Global del Sitio**	**6,889**	**2,7556**
		1.1.1 Esquema de Organización Global	**3,33**	
		1.1.1.1 Mapa del Sitio	0	
		1.1.1.2 Índice Global (por Temas, etc.)	4	
		1.1.1.3 Tabla de Contenidos	5	
		1.1.2 Calidad en el Sistema de Etiquetado	**5,5**	
		1.1.2.1 Etiquetado Textual	6	
		1.1.2.2 Etiquetado con Iconos	5	
		1.1.3 Visita Guiada	**N/A**	
		1.1.3.1 Visita Convencional	N/A	
		1.1.3.2 Visita Virtual (con Tecnología VR)	N/A	
		1.1.4 Página Principal	**8,167**	
		1.1.4.1 Navegabilidad de la página principal	10	
		1.1.4.2 Impacto de la página principal	**6,333**	
		1.1.4.2.1 La página principal refleja la idea del sitio	6	
		1.1.4.2.2 La página principal deja claro que puedo hacer en el sitio	6	
		1.1.4.2.3 La página principal se ve bien al deshabilitar las imágenes	7	
		1.1.5 Consistencia de la navegación	**7**	
	10%	**1.2 Mecanismos de Ayuda y Retroalimentación en línea**	**1**	**0,1**
		1.2.1 Calidad de la Ayuda	**3**	
		1.2.1.1 Ayuda Explicatoria acerca del sitio	3	
		1.2.1.2 Ayuda de la Búsqueda	3	
		1.2.2 Indicador de Ultima Actualización	**1**	
		1.2.2.1 Global (de todo el sitio Web)	0	
		1.2.2.2 Restringido (subsitio o página)	0	
		1.2.2.3 Por noticias (Solo ultimas noticias)	3	
		1.2.3 Directorio de Enlaces	**0**	
		1.2.3.1 Enlaces a sitios de Interés	0	
		1.2.3.2 Enlaces a asociaciones de interés	0	
		1.2.4 Facilidad FAQ	**0**	
	10%	**1.3 Aspectos de Interfaces y Estéticos**	**7,278**	**0,7278**
		1.3.1 Cohesividad al Agrupar los Objetos de Control Principales	**6**	
		1.3.2 Permanencia y Estabilidad en la Presentación de los Controles Principales	**7**	
		1.3.2.1 Permanencia de Controles Directos	7	

		1.3.2.2 Permanencia de Controles Indirectos	6	
		1.3.2.3 Estabilidad	10	
		1.3.3 Preferencia Estética	**7**	
		1.3.4 Uniformidad en el Estilo del sitio	**6**	
	10%	**1.4 Misceláneas**	**3**	**0,3**
		1.4.1 Soporte a Lenguaje Extranjero	**0**	
		1.4.2 Descarga de contenidos	**N/A**	
		1.4.2.1 Descarga de contenidos a multidispositivo	N/A	
		1.4.2.2 Descarga de contenidos	N/A	
		1.4.3 Intrusión publicitaria	**6**	
	15%	**1.5 Usabilidad de los Textos**	**10**	**1,5**
		1.5.1 Textos adaptados para la Web	**5,333**	
		1.5.1.1 Textos breves	5	
		1.5.1.2 Textos escaneables	6	
		1.5.1.3 Estilo de escritura conciso	5	
	15%	**1.6 Clasificación de la información**	**5,5**	**0,825**
		1.6.1 Categorías	5,5	
		1.6.1.1 Claridad de las categorías	6	
		1.6.1.2 Cohesión de las categorías	5	
10%		**2. Accesibilidad**	**6,75**	**0,675**
	70%	**2.1 Accesibilidad para usuarios con discapacidades**	**3,5**	**2,45**
		2.1.1 Discapacidades visuales	**7**	
		2.1.1.1 Posibilidad de modificar el tamaño de las fuentes	7	
		2.1.1.2 Combinaciones de color (para usuarios con ceguera al color)	N/A	
		2.1.1.3 Markup claro para poder ser leído por un lector de pantalla	N/A	
		2.1.1.4 Etiquetas ALT en todas las imágenes	6	
		2.1.2 Discapacidades auditivas	**0**	
	20%	**2.2 Acceso a navegadores no gráficos**	**N/A**	**0,07**
	10%	**2.3 Acceso Multidispositivo**	**10**	**1**
15%		**3. Funcionalidad**	**5,435**	**0,8152**
	50%	**3.1 Aspectos de Búsqueda**	**3,75**	**1,875**
		3.1.1 Mecanismo de Búsqueda en el Sitio	**2,5**	
		3.1.1.1 Búsqueda Restringida (por secciones)	0	
		3.1.1.2 Búsqueda Global	5	
		3.1.2 Búsqueda siempre disponible	**5**	
	50%	**3.2 Aspectos de Navegación y Exploración**	**7,119**	**3,5595**
		3.2.1 Navegabilidad Local (de subsitio)	**6,5**	
		3.2.1.1 Nivel de Interconexión	5	
		3.2.1.2 Orientación	6	
		3.2.1.2.1 Indicador del Camino	7	
		3.2.1.2.2 Etiqueta de la Posición Actual	8	
		3.2.2 Navegabilidad Global	**7**	
		3.2.2.1 Acoplamiento entre Subsitios	7	
		3.2.3 Objetos de Control Navegacional	**7,333**	
		3.2.3.1 Permanencia y Estabilidad en la Presentación deControles Contextuales	10	
		3.2.3.1.1 Permanencia de los Controles Contextuales	10	
		3.2.3.1.2 Estabilidad	10	
		3.2.3.2 Nivel de Desplazamiento	**10**	

		3.2.3.2.1 Desplazamiento Vertical	10	
		3.2.3.2.2 Desplazamiento Horizontal	10	
		3.2.4 Predicción Navegacional	**2**	
		3.2.4.1 Enlace con Título (enlace con texto explicatorio)	2	
		3.2.4.2 Calidad de la Frase del Enlace	2	
		3.2.5 Funciones Misceláneas y Específicas del Dominio	**7**	
40%		**4 Contenidos**	**4,594**	**1,8389**
	30%	**4.1 Información Institucional**	**3,5**	**1,05**
		4.1.1 Plan de acción	**4**	
		4.1.1.1 Planes de acción actual	8	
		4.1.1.2 Planes de acción futuros	0	
		4.1.2 Información sobre las dependencias	**2**	
		4.1.2.1 Funciones de las dependencias	0	
		4.1.2.2 Horario de atención de las dependencias	4	
		4.1.3 Valores Institucionales	**4,5**	
		4.1.3.1 Misión y Visión	9	
		4.1.3.2 Historia	0	
	18%	**4.2 Información sobre las directivas institucionales**	**5**	**0,9**
		4.2.1 Curriculum de los directivos	**0**	
		4.2.1.1 Intereses institucionales	**3**	
		4.2.1.2 Hoja de Vida	0	
		4.2.2 Información de contacto	**10**	
		4.2.2.1 Email directivo	10	
	13%	**4.3 Información sobre las dependencias**	**3**	**0,39**
		4.3.1 Objetivos	**3**	
		4.3.2 Funciones	**3**	
	13%	**4.4 Información sobre beneficios a usuarios**	**4,333**	**0,5633**
		4.4.1 Lista de beneficios	**3**	
		4.4.2 Descripción de los beneficios	**7**	
		4.4.3 Información adicional	**3**	
	13%	**4.5 Información de contacto de la institución**	**4,75**	**0,6175**
		4.5.1 Ubicación	**2**	
		4.5.1.1 Como llegar (transportes, distancias, etc.)	6	
		4.5.1.2 Mapa Geográfico	0	
		4.5.1.3 Mapa Interno	0	
		4.5.2 Contacto con responsables / asesores	**7,5**	
		4.5.2.1 Nombre	10	
		4.5.2.2 Correo	10	
		4.5.2.3 Teléfono	10	
		4.5.2.4 Fax	0	
	13%	**4.6 Información para externos a la institución**	**7**	**0,9**
		4.6.1 Claridad de Misión y Visión	**9**	
		4.6.2 Información geográfica	**5**	
7.5%		**5. Confiabilidad**	**2,519**	**0,1889**
	50%	**5.1 Ausencia de Deficiencias y Errores**	**4,556**	**2,2778**
		5.1.1 Errores de Enlaces	**7**	
		5.1.1.1 Enlaces Rotos	7	
		5.1.1.2 Enlaces Inválidos	7	
		5.1.1.3 Enlaces no Implementados	7	
		5.1.2 Errores o Deficiencias Varias	**6,667**	

		5.1.2.1 Deficiencias o cualidades ausentes debido a diferentes navegadores	10	
		5.1.2.2 Nodos Web Muertos (sin enlaces de retorno)	**5**	
		5.1.2.3 Nodos Destinos (inesperadamente) en Construcción	5	
		5.1.3 Enlaces externos a instituciones prestigiosas	**0**	
	25%	**5.2 Utilización de estándares W3C**	**0**	**0**
		5.2.1 HTML	0	
		5.2.2 CSS	0	
	25%	**Actualización periódica de la información**	**3**	**0,75**

7.5%		**6. Eficiencia**	**7,167**	**0,5375**
	60%	**6.1 Accesibilidad de Información**	**7,5**	**4,5**
		6.1.1 Soporte a Versión sólo Texto	N/A	
		6.1.2 Legibilidad al desactivar la Propiedad Imagen del Browser	**7,5**	
		6.1.2.1 Imagen con Título	9	
		6.1.2.2 Legibilidad Global	6	
	20%	**6.2 Rendimiento**	**8**	**1,6**
	20%	**6.3 Tiempo de descarga**	**6**	**1.2**

La calificaciones bajas de deben a que el portal web no cumple a cabalidad con el lineamiento de gobierno en línea, posee inconsistencias y errores, además de carecer de los siguientes servicios e información.

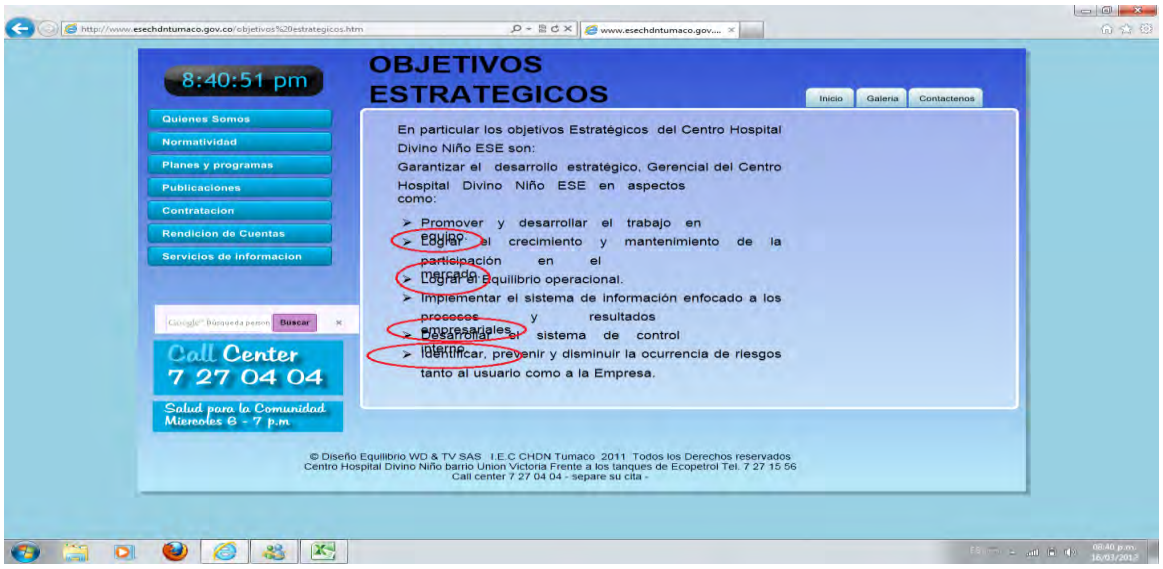
- Mapa del sitio.
- Organigrama.
- No existe un correo electrónico de contacto o enlace con el sistema de atención al ciudadano.
- No existe ningún tipo de directorio de funcionarios, de entidades, ni de agremiaciones.
- No existen horarios ni días de atención al público.
- No se muestra ningún tipo de información sobre Leyes/ Ordenanzas /Acuerdos, decretos, resoluciones, circulares /u otros actos administrativos de carácter general.
- Presupuesto aprobado en ejercicio.
- Información Histórica de presupuestos
- Políticas, planes, programas y proyectos en ejecución, ni contacto con la dependencia responsable.
- No hay listado de servicios que ofrece la entidad.
- No se encuentra ningún tipo de información sobre contrataciones, licitaciones.
- Falta de los informes de gestión, metas e indicadores, planes de mejoramiento. No se publican los resultados sean mensuales o trimestrales confrontado con las metas.
- No existe información para niños, preguntas y respuestas frecuentes, calendarios de actividades, glosario, política de privacidad y condiciones de uso.
- Fecha de última actualización.

- Contenido desorganizado.
- Enlace al portal del estado colombiano www.gobiernoenlinea.gov.co.
- Falta de un mecanismo de búsqueda interna.
- No existe un servicio de atención en línea.
- No existe ningún tipo de ayuda en el portal web
- No existe soporte a Lenguaje Extranjero.
- La combinación de colores es muy mala y no tienen nada que ver con los colores institucionales.
- Falta la Historia de la institución.
- No se sabe con claridad cual es el fin del portal web.
- Errores de ortografía

Figura 2. Error en la distribución de texto 1.

Error en el contenido de la misión institucional que se encuentra dentro del despliegue de la opción “Quienes Somos” en el menú principal de la página

Figura 3. Error en la distribución de texto 2.

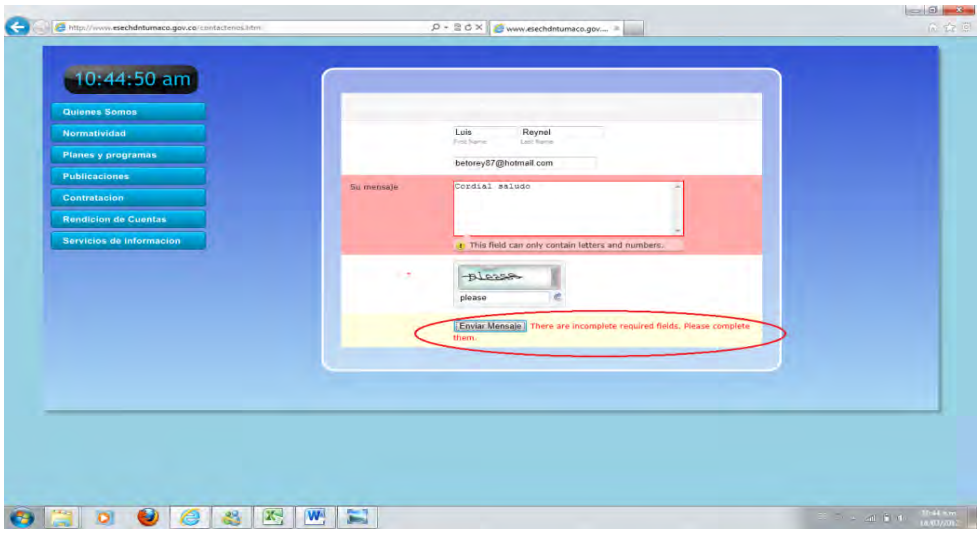


Cuatro errores de distribución del texto que hace referencia al contenido de “OBJETIVOS ESTRATÉGICOS” que se despliega de la opción “QUIENES SOMOS” situada en el menú principal de la página

Figura 4. Links deshabilitados.

Tres opciones del menú principal de la página se encuentran deshabilitadas “Normatividad”, “Contratación” y “Rendición de cuentas”.

Figura 5. Error de conexión.

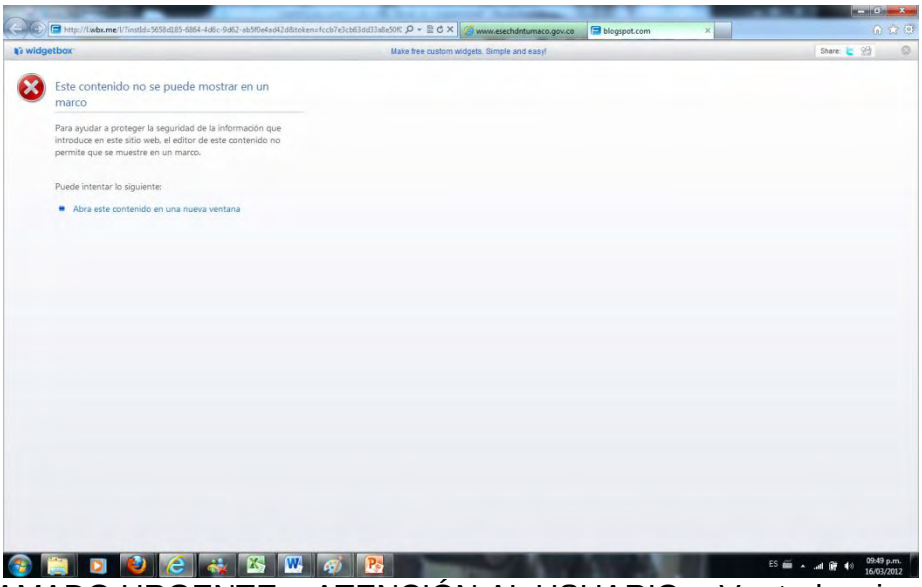


Opción “Contáctenos” la cual se encuentra en el menú principal de la página.

Figura 6. Link deshabilitados 2.

Se encuentran en estado deshabilitado las tres opciones “PREGUNTAS FRECUENTES”,”BOLETINES Y PUBLICACIONES”,”OFERTA DE EMPLEO” que se despliegan del botón “Servicios de información ”.

Figura 7. Error de enlace



Ruta (LLAMADO URGENTE – ATENCIÓN AL USUARIO-> Ver todo mi perfil).

Figura 8. Salud Pública

"SALUD PUBLICA" esta deshabilitada la cual se encuentra dentro del despliegue de la opción "Planes y programas" situada en el menú principal de la página.

3.2.4.3. Pruebas a realizar en la página web.

- **Spiders, Robots, y Crawlers:** Esta fase del proceso de recopilación de información consiste en navegar y capturar recursos relacionados con la aplicación que está siendo probada

- **Reconocimiento mediante motores de búsqueda:** Los motores de búsqueda, como Google, pueden utilizarse para descubrir incidencias relacionadas con la estructura de la aplicación web, o páginas de error producidas por la aplicación que han sido expuestas públicamente.

- **Identificación de puntos de entrada de la aplicación:** La enumeración tanto de la aplicación como de su entorno es un proceso clave antes de que cualquier tipo de ataque comience. Esta sección ayudara a identificar y catalogar cada sección de la aplicación que deba ser objeto de investigación una vez concluya el proceso de enumeración y acotación

- **Pruebas del receptor de escucha de la BD:** Durante la configuración del servidor de base de datos, muchos administradores de bases de datos no tienen en consideración la seguridad del receptor de escucha de la base de datos. Este componente podría revelar información sensible como por ejemplo las configuraciones o las instancias de base de datos en ejecución en caso de encontrarse incorrectamente configurado o analizado mediante técnicas manuales o automáticas. La información mostrada podría ser de gran utilidad a la hora de realizar seguidamente otras pruebas que supongan un mayor impacto.

- **Archivos antiguos, copias de seguridad y sin referencia:** Los ficheros redundantes, legibles y descargables de un servidor web, como por ejemplo antiguos, copias de seguridad y renombrados, son una fuente importante de información. Es necesario verificar la existencia de estos ficheros porque podrían contener partes importantes del código fuente, rutas de instalación así como contraseñas tanto de las aplicaciones como de las bases de datos.

- **Interfaces de administración de la infraestructura y de la aplicación:** Muchas aplicaciones utilizan una ruta común para los paneles de administración que podrían ser utilizados para adivinar o realizar fuerza bruta sobre contraseñas de administración. Estas pruebas se realizan para buscar interfaces de administración y para comprobar la posibilidad de explotarlos para conseguir acceso a funcionalidades de administración.

- **Métodos HTTP y XST:** En este punto se comprueba que el servidor web no este configurado para permitir los órdenes (métodos) HTTP potencialmente peligrosos y que no es posible el Cross Siete Tracking (XST).

- **Pruebas de Fuerza Bruta**: Cuando un ataque de diccionario falla, la persona a cargo de las pruebas puede intentar utilizar métodos de fuerza bruta para conseguir autenticación. Las pruebas de fuerza bruta no son fáciles de llevar a cabo, debido al tiempo requerido y el posible bloqueo de la persona que esté realizando las pruebas.

- **INYECCION SQL:** Un ataque de Inyección SQL consiste en la inserción o "inyección" de datos en una consulta SQL desde un cliente de la aplicación. El éxito en una inyección SQL puede leer datos sensibles de la base de datos, modificar los datos (insertar/actualizar/borrar), realizar operaciones de administración sobre la base de datos (como reiniciar el DBMS), recuperar el contenido de un archivo del sistema de archivos del DBMS y, en algunos casos, ejecutar ordenes en el sistema operativo. Los ataques de inyección SQL son un tipo de ataques de inyección, en los que ordenes SQL son inyectados en texto para afectar la correcta realización de una consulta SQL predefinida.

Algunas Herramientas de automatización para realizar auditorías web son:

- **Acunetix:** un escáner de vulnerabilidades que permite analizar la seguridad de las aplicaciones Web de una manera sencilla. Basta con configurar la url/ip/puerto donde se encuentra la aplicación, y seleccionar el perfil de ataque para lanzar un escáner.

Se pueden probar vulnerabilidades de tipo Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection, Code Execution, Directory Traversal, HTTP Parameter Pollution, File Inclusion, Script Source Code Disclosure, CRLF Injection, Cross Frame Scripting (XFS), PHP Code Injection, XPath Injection, Path Disclosure (Unix and Windows), LDAP Injection, Cookie Manipulation, Arbitrary File creation, Arbitrary File deletion, Email Injection, File Tampering, URL redirection, Remote XSL inclusion, DOM XSS, MultiRequest Parameter Manipulation : Blind SQL/XPath Injection, Input Validation, Buffer Overflows, Sub-Domain Scanning, permite escanear puertos abiertos, métodos habilitados, fuzzear en busca de archivos no linkados, comprobar listados de directorios, y un largo etc.

- **Asp-audit:** Esta herramienta es utilizada para encontrar o buscar errores de seguridad en configuraciones de aplicaciones ASP.NET.

- **DirBuster:** Es una herramienta desarrollada en JAVA que nos permite encontrar aquellos directorios y archivos que se encuentren en los servidores WEB y que no tengan los permisos asignados correctamente. Se usa la técnica de "Fuerza Bruta" la cual consiste en hacer peticiones hasta que le servidor nos deje descargar o acceder a dicho archivo o directorio respetivamente.

- **Grabber:** Es un escáner para aplicaciones web, básicamente detecta algunas vulnerabilidades de los sitios webs, esta aplicación es sencilla y no es rápida pero es muy portable y adaptable. Está diseñado para escanear sitos pequeños como lo serían foros ,blogs, etc.. no grandes aplicaciones web ya que llevaría mucho tiempo y se llenaría el ancho de banda de nuestra red. Puede detectar las siguientes vulnerabilidades: Cross-Site Scripting SQL Injection File Inclusion Backup files check Simple AJAX check Hybrid analysis/Crystal ball JavaScript source code analyzer.

Mantra (OWASP Mantra Security Framework): es una aplicación de código abierto que cuenta con herramientas hacking. add-ons y scripts basados en firefox y chromium. Este "toolkit" esta enfocado en general a personas interesadas en el ámbito de la seguridad web, bien pueden usarla desde personas que apenas están empezando o personas que ya tengan mucha experiencia en el tema. Las herramientas que ofrece Mantra se agrupan en las siguientes categorías :

- **Recopilación de Información:** En este grupo podrán encontrar add-ons para obtener información especifica de la aplicaciones web , como su dirección ip, la ubicacion fisica del servidor(FlagFox), mostrar los archivos que fueron cargados para mostrar la pagina, ir directamente el acceso a los scripts y hojas de estilo incluidos en la página web actual(JSView), destapa tecnologías de base utilizadas en sitios web como la CMS, sistemas de comercio electrónico, frameworks de JavaScript, etc herramientas de análisis(Wappalyzer).

- **Editores**: Herramientas para editar y depurar código (Firebug).

- **Utilidades de red:** Estas aplicaciones nos permitirán utilizar un cliente FTP/SFTP(Fire FTP), un cliente SSH(Fire SSH), manejar base de datos SQLite(SQLite Manager), controlar la Cache de DNS, supervisar todo el trafico entrante y saliente HTTP entre el navegador y los servidores web(HTTP Fox).

- **Miscelánea:** Aplicaciones que tienen como objetivo complementar o facilitar el uso de otras aplicaciones, aca podemos encontrar add-ons como Greasemonkey, Greasefire, FlipperURL, Session Manager, CacheToggle, entre otras.

- **Solicitud de Auditoria:** Como su nombre lo indica en este grupo encontraremos aplicaciones que facilitan la auditoria de vulnerabilidades, incluso ver y editar las cookies, analizar los XSS, algunas de las aplicaciones son TamperData, RESTClient, SQL Inject Me, FireCookie, Cookie Monster, Fireforce, Me XSS, etc, etc....

- **Proxy:** se encuentran aplicaciones muy sencillas como FoxyProxy , que facilitan el anonimato.

Las pruebas antes descritas no se pudieron realizar por que el servicio de hosting el cual albergaba la página se venció y no fue levantado durante el periodo de auditoria.

3.2.4.4. Informe Gerencial de auditoria.

Doctora: Ana Lucia Castillo.

Gerente Centro Hospital Divino Niño. Luego de realizar las distintas pruebas y aplicar las metodologías de auditoria que se tenía como objetivo principal evaluar el decreto 1151 del 14 de abril de 2008 que trata sobre los lineamientos de Gobierno En Línea y auditar la infraestructura física de la red de datos de la sede principal se observó lo siguiente:

Análisis del comité de gobierno en línea. La E.S.E. Centro Hospital Divino Niño hasta la fecha no ha conformado un comité de gobierno en línea.

Análisis fase de información

No se cumple con los siguientes ítems:

- Mapa del sitio.
- Organigrama.
- No existe un correo electrónico de contacto o enlace con el sistema de atención al ciudadano.
- No existe ningún tipo de directorio de funcionarios, de entidades, ni de agremiaciones.
- No existen horarios ni días de atención al público.
- No se muestra ningún tipo de información sobre Leyes/ Ordenanzas /Acuerdos, decretos, resoluciones, circulares /u otros actos administrativos de carácter general.
- Presupuesto aprobado en ejercicio.
- Información Histórica de presupuestos
- Políticas, planes, programas y proyectos en ejecución, ni contacto con la dependencia responsable.
- No hay listado de servicios que ofrece la entidad.
- No se encuentra ningún tipo de información sobre contrataciones, licitaciones.
- Falta de los informes de gestión, metas e indicadores, planes de mejoramiento. No se publican los resultados sean mensuales o trimestrales confrontado con las metas.

- No existe información para niños, preguntas y respuestas frecuentes, calendarios de actividades, glosario, política de privacidad y condiciones de uso.
- Fecha de última actualización.
- Contenido desorganizado.
- Enlace al portal del estado colombiano www.gobiernoenlinea.gov.co.
- Falta de un mecanismo de búsqueda interna.
- No existe un servicio de atención en línea.
- No existe ningún tipo de ayuda en el portal web
- No existe soporte a Lenguaje Extranjero.
- La combinación de colores es muy mala y no tienen nada que ver con los colores institucionales.
- Falta la Historia de la institución.

Se debe de destacar que se ha designado a una persona para que se haga cargo del portal web y comenzar con la aplicación de los lineamientos de gobierno en línea, además que de que cuenta con el apoyo del área de sistemas.

Auditoria a la infraestructura física de la red de datos de la sede principal
Los resultados de la auditoria a la infraestructura física de la red de datos será resumido y agrupados por cada uno de los dominios del COBIT.

- **DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)**

En cuanto la parte de planificación y organización como tal se encontró de que se realiza muy poco, los problemas se van solucionando de acuerdo a como van apareciendo.

Hace falta un manual de funciones que sea diseñado para el área de sistemas.

No se encontró ningún tipo de políticas y procedimientos para dar mantenimiento ni solución a ningún tipo de problema que presente la red de datos.

Falta diseñar planes de contingencia que ayuden a los encargados de la red de datos contrarrestar de manera rápida algún daño en la red de datos, se debe de empezar a realizar estudios de análisis de riegos.

Aunque no existe ningún proceso para el estudio de nuevas tecnologías el personal del área de sistemas en cabeza del coordinador mantiene investigando y dando a conocer a la gerencia sobre nuevas tecnologías y soluciones que puedan ayudar a mejorar la calidad del servicio de la red de datos.

- **DOMINIO ADQUISICIÓN E IMPLEMENTACIÓN (AI)**

No se maneja ningún tipo de software que ayude a determinar problemas en la red, esto representa pérdida de tiempo en el momento de encontrar y solventar de manera más rápida los problemas que se presenten.

Aunque no existe un manual para el mantenimiento de la infraestructura tecnológica, el personal encargado del área de sistemas tiene los conocimientos suficientes y aportan soluciones eficazmente.

- **DOMINIO- ENTREGAR Y DAR SOPORTE (DS)**

Se debe de tener en cuenta que cuando se tiene una buena administración de las instalaciones el servicio tienen a mejorar en el caso de la E.S.E. Centro Hospital Divino Niño no existe ningún tipo de políticas seguridad de acceso, los equipos de comunicación de la red de datos están en áreas que no son recomendables, el lugar donde se encuentra el servidor principal y un sitwch de comunicación no cuenta con ningún tipo de seguridad tipo detectores de humo, supresores de fuego que permitiría detectar y prevenir incendios.

Se destaca que los funcionarios del área de sistemas tienes conocimiento de esta problemática y ya se han empezado a comunicar con la alta gerencia para solicitar los equipos necesarios para prevenir cualquier inconveniente en este lugar.

- **DOMINIO – MONITOREAR Y EVALUAR (ME)**

No se realiza ningún tipo de monitoreo a la red de datos, debido a que no existe ningún procedimiento, proceso o política que así lo exija, aun asi el equipo del área de sistemas conoce bien la red de datos y pueden dar respuesta rápida a cualquier inconveniente

RECOMENDACIONES

- Conformar un grupo determinado de funcionarios que evalúen y estudien el desempeño de la red física de datos para con ello tomen decisiones oportunas y adecuadas en la eventualidad de no cumplir objetivos planteados.

- Elaborar e implementar políticas y procedimientos relacionados con la conformación de la arquitectura y del aspecto físico de la red de datos para ajustar los servicios de red a las necesidades propias que necesite la entidad.

- Crear políticas que estén relacionadas con la búsqueda de nuevas tecnologías y elementos que mejoren el desempeño del sistema de red de datos.

- Documentar los estudios que se realicen de nuevas tecnologías y elementos que mejoren el desempeño de la red de datos para lograr implementarlas en el futuro con mayor facilidad.

- Elaborar el manual de funciones o procedimientos específico para los trabajadores encargados del manejo y administración del aspecto físico de la red de datos y con esto se oriente al personal para un óptimo funcionamiento y desempeño de las tareas que se deben realizar en este campo.

- Implementar dentro del manual de funciones o procedimientos para los trabajadores encargados del manejo y administración del aspecto físico de la red de datos las descripciones o definiciones adecuadas, para no perder una guía concreta para la ejecución de tareas fundamentales.

- Ajustar los requerimientos mínimos para ocupar los cargos relacionados con el manejo del sistema de red de datos, para cumplir con esto con el cumplimiento de perfiles ajustándose a la normatividad y lograr desempeño adecuado de los funcionarios.

- Elaborar un plan de contingencia que subsane la ausencia del personal encargado del manejo del aspecto físico de la red de datos para evitar que los

- procesos sean afectados y se asigne la responsabilidad de estas funciones a personas idóneas.

- Implementar un proceso de toma de decisiones donde se brinde la prioridad necesaria a la asignación de recursos para adquirir elementos tecnológicos que ayuden al mejoramiento de la red física de datos y con ello optimizar los procesos informáticos de la entidad.

- Estudiar e implementar políticas donde se permita elaborar y administrar un buen presupuesto que sea utilizado para adquirir aquellos elementos tecnológicos necesarios para optimizar los procesos donde se involucre el sistema de red de datos.

- Elaborar políticas y procedimientos para el análisis y la gestión del riesgo para el sistema físico de la red de datos debido a que si alguno de sus elementos esta en amenaza se tome decisiones oportunas y adecuadas que no llegue afectar en alta magnitud a la red de datos.

- Elaborar un plan de contingencia que ayude a dar soporte a la red física de datos para obtener mecanismos que ayuden a la recomponer y reactivar los procesos que se vean afectados para el sistema de red de datos.

- Implementar políticas para la adquisición de pólizas de los elementos que conforman el aspecto físico de la red de datos y con ello asegurar estos elementos a futuro y además se facilite restauración y reconexión del sistema de red de datos.

- Adquirir software adecuado para monitorear la conexión física de la red de datos y con ello tener visión clara de la actividad de la red de datos.

- Llevar el proceso de mantenimiento periódico del software para monitoreo de la red física de datos y con ello asegurar el optimo funcionamiento de esta herramienta.

- Implementar dentro del proceso de adquisición de hardware el requisito de múltiples cotizaciones para con ello proteger el presupuesto de la entidad destinado a tecnologías de información.

- Dar a conocer las políticas de adquisición de hardware a los funcionarios para tener mayor sentido de pertenencia por los intereses de la entidad.

- Documentar las políticas de mantenimiento de los equipos de cómputo para consolidar la guía del proceso a seguir y con ello agilizar las actividades correspondientes.

- Implementar el diligenciamiento de un acta o documento adecuado para facilitar el mantenimiento de los elementos de cómputo y así facilitar el trabajo a la persona encargada del proceso para la respectiva revisión y reparación.

- Implementar la documentación sobre el mantenimiento de los equipos de cómputo se permite actuar más rápido ante este tipo de eventos ya que se facilita por la recolección de antecedentes.

- Incorporar dentro del manual de funciones las actividades pertinentes para lo que concierne al mantenimiento de equipos de cómputo ya que así se optimizara este proceso debido a que se asigna responsabilidad directa.

- Capacitar al personal encargado para el mantenimiento de equipos de computo sobre la reparación y mantenimiento de monitores para evitar se estanque el funcionamiento de las terminales de trabajo y además ahorras gastos que generarían reparación en otro lugar diferente a la entidad.

- Implementar el centro de cómputo con características adecuadas y normatividad correspondiente para lograr optimización de procesos y seguridad de la información que es vital para la entidad.

- Implementar el proceso de mantenimiento de los elementos como: swiches, routers y servidores para garantizar su óptimo funcionamiento y cuidado ya que son elementos fundamentales en la constitución de la red de datos.

- Implementar el proceso específico para el mantenimiento de la red de datos y así se prevengan los sucesos que puedan perjudicar procesos que se relacionen con el sistema de red de datos.

- Implementar y ajustar la entidad a un correcto esquema de cableado estructurado para que no se atente contra la normatividad para alcanzar los objetivos de calidad que debe poseer la entidad por la importancia de la información que se maneja.

- Elaborar los planos del cableado estructurado que se extiende por la entidad para tener facilidad de análisis al momento de una eventual toma de decisiones para mejorar el sistema de red de datos con incorporación de nuevos elementos en su aspecto físico.

- Elaborar hojas de vida adecuadas para recolectar información que sirva para el optimo seguimiento de los equipos como: servidores, routers y switches y con ello prevenir y corregir inconvenientes a futuro.

- Crear políticas adecuadas en el campo de seguridad referente al acceso y salida de las instalaciones para evitar hurtos de los elementos que conforman el sistema físico de la red de datos.

- Crear políticas adecuadas en el campo de seguridad referente a la identificación, autenticación y autorización de los individuos que ingresan a las instalaciones para impedir que se atente contra los elementos de la entidad incluyendo los elementos que hacen parte del aspecto físico de la red de datos.

- Controlar el acceso y salida de la entidad por medio de requisas para detectar que personas ajenas a la entidad realicen sabotaje a los procesos de la red de datos y también detección de hurto de aquellos elementos que conforman el aspecto físico de la red de datos.

- Implementar en la entidad el procedimiento de escolta para visitantes y con esto evitar hurto de elementos y sabotaje de los elementos que posee la estructura física de la red de datos.

- Tener en cuenta dentro de las políticas de seguridad de la entidad el procedimiento de escolta de visitantes para impedir robos, sabotajes en contra de la entidad.

- Implementar en la entidad políticas para dar mayor seguridad a las instalaciones ante cualquier evento natural o ambiental para disminuir los riesgos de desastres que atenten contra el óptimo desempeño y el aspecto físico en general de la red de datos.

- Adquirir pólizas de seguros para los elementos que constituyen el aspecto físico de la red de datos ya que si se presenta un evento inesperado que atente contra el sistema de red de datos no se tarde mucho tiempo en recomponer y poner en marcha el sistema.

- Instalar dispositivos como son (detectores de humo, supresores de fuego) en el cuarto de servidores para evitar un eventual incendio.

- Instalar cámaras en el interior de la entidad para registrar las actividades sospechosas de los individuos que ingresan.

- Elaborar e implementar políticas y procedimientos adecuados para el monitoreo de la seguridad del aspecto físico de la red de datos para tener un seguimiento que ayude a generar procesos preventivos y correctivos.

- Implementar dentro de las políticas de monitoreo del aspecto físico de la red datos una descripción detallada de los procesos a trabajar, con ello se elaborara seguimientos óptimos y precisos que optimicen el funcionamiento de la red de datos.

- Contemplar el periodo en el que se deba realizar el monitoreo dentro de las políticas de la seguridad del aspecto físico de la red de datos, para que el tiempo empleado sea el adecuado y se pueda realizar las respectivas prevenciones y correcciones.

- Asignar las funciones de monitorear la seguridad del aspecto físico de la red de datos a personal específico, con ello se priorizara la ejecución de estas tareas y se sabrá quién responderá ante estas actividades.

- Documentar las políticas para seguridad de la red física de datos y con ello utilizar esta información como herramienta ágil para ejecutar este proceso.

- Dar a conocer a los funcionarios encargados de la administración de la red de datos las políticas de monitoreo para el seguimiento de la seguridad del aspecto físico de la red de datos, para lograr ejecución dentro de lo correctivo y preventivo dentro de lo que atente al sistema de red de datos.

- Realizar auditorías del sistema físico de la red de datos para así lograr tener la visión más clara de la situación que presenta la red de datos y mejorar los aspectos que sean necesarios.

CONCLUSIONES

- La auditoría de sistemas es una herramienta la cual permite conocer de manera profunda el funcionamiento de cualquier empresa o área la cual sea objeto de nuestro estudio por medio de evaluación de los procesos, técnicas, política, normas con el fin de encontrar vulnerabilidades de seguridad tanto a nivel físico como lógico, para poder realizar recomendaciones y planes de mejoramiento para cubrir estas falencias.

- La E.S.E. Centro Hospital Divino Niño desde la Gerencia hasta los funcionarios del área de sistemas son conscientes de que existen falencias las cuales quedan demostradas en este estudio.

- La E.S.E. Centro Hospital Divino Niño no cumple con los lineamientos establecidos en el decreto 1151 de Abril de 2008 para la implementación de la estrategia Gobierno En Línea, lo cual hace esta una de sus mayores falencias que deben de empezar a corregir de manera inmediata.

- Por medio de COBIT el auditor logra entender la importancia de la seguridad de la información y de cómo los ingenieros de sistemas deben de ser el brazo que este pendiente de esta seguridad de que los sistemas y procesos funcionen correctamente para que cumplan con el objetivo por el cual fueron implementados.

- Después de realizar la auditoria en la E.S.E. Centro Hospital Divino Niño el auditor pudo apreciar lo importante que son las TI para que esta y cualquier otra entidad pueda cumplir con todos sus objetivos, la importancia de saber buscar, analizar y procesar la información ya que de pequeños datos se puede obtener valiosa información la cual puede ayudar a mejorar cualquier proceso que se está realizando

- A pesar de que existen falencias el personal encargado del área de sistemas demuestra un total sentido de pertenencia con la empresa y están comprometidos con los procesos de mejoras, pero esto no solo depende de ellos si no del apoyo que pueda brindar la alta gerencia

BIBLIOGRAFÍA

ECHENIQUE GARCIA José A., Auditoria en informática, 2ª Ed., Mc GRAW-HILL, Mexico D.F., 2005.

GUSTIN Enith, SOLARTE Francisco Javier, HERNANDEZ Ricardo. Manual De Procedimientos para Llevar a la Práctica La Auditoría Informática y de Sistemas, Copyright © 2011.

PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: un enfoque práctico, 2ª Ed., Alfaomega/RA-MA, México D.F., 2001.

PINILLA F. José D., Auditoría informática: un enfoque operacional, ECOE, Bogotá, 1995

WEBGRAFIA

http://www.isaca-bogota.net/metodologias/cobit.aspx 281

http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html

http://www.monografias.com/trabajos39/la-auditoria/la-auditoria.shtml

https://www.owasp.org/index.php/OWASP_Mantra_-_Security_Framework.

http://www.gobiernoenlinea.gov.co/c/document_library/get_file?uuid=d724077d-7ad1-4c6f-82b2-5e35b5e043e3&groupId=10136

http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml

http://www.eduardoleyton.com/apuntes/UDP_COBIT.pdf

http://www.hacienda.go.cr/cifh/sidovih/uploads/Logo/COBIT.pdf

http://www.flu-project.com/escaneres-de-vulnerabilidades-web-cual-es-tu-preferido-parte-i.html

http://www.buenastareas.com/ensayos/Herramientas-De-Auditoria-De-Paginas-Web/1385892.html

ANEXOS

Los anexos se entregan en medio magnético y constan de:

- Cuadro de definición de fuentes de conocimiento: Se encuentran en la carpeta FUENTE _DE_CONOCIMIENTO_CHDN consta de archivos llamados ANEXOS y van desde ANEXO 1 hasta ANEXO 9.

- Hallazgos: Se encuentra una carpeta llamada HALLAZGOS_CHDN consta de archivos llamados HHDN y van desde HHDN_1 hasta HHDN_9

- Evidencias fotográficas: Se encuentra una carpeta llamada E_FOTOGRAFICA consta de archivos llamados IMG y van des IMG_1 hasta IMG_13

- Evidencias de audio: Se encuentra una carpeta llamada E_AUDIO consta de archivos llamados A_CHDN y van desde A_CHDN_01 hasta A_CHDN_09

- Cuestionarios: Se encuentra una carpeta llamada CUESTIONARIOS_CHDN consta de archivos llamados ANEXOS y van desde ANEXO 1 hasta ANEXO 9.

- Decreto 1151 de 2008: Se encuentra un documento en pdf en la carpeta anexos de nombre: “Decreto 1151 Abril14 de 2008”, donde se explica en que consiste el decreto.