AUDITORIA A LA INFRAESTRUCTURA FISICA DE RED Y EQUIPOS DE COMPUTO DE LA NOTARÍA PRIMERA DE TÚQUERRES

EULER REMIGIO BASANTE MORA
GILBERTH ANDREY IPAZ

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

AUDITORIA A LA INFRAESTRUCTURA FISICA DE RED Y EQUIPOS DE COMPUTO DE LA NOTARÍA PRIMERA DE TÚQUERRES

EULER REMIGIO BASANTE MORA
GILBERTH ANDREY IPAZ

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

Director
ING. MANUEL BOLAÑOS GONZALEZ

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

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado son responsabilidad de los autores.

Artículo 1 del Acuerdo No. 324 de octubre 11 de 1966, emanado del honorable Consejo Directivo de la Universidad de Nariño.

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

Artículo 13 del Acuerdo No. 005 de 2010 emanado del honorable Consejo Académico.

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

Jurado

_____

Jurado

San Juan de Pasto, febrero 2016

DEDICATORIA

***A Dios**, por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.*

*.**A mis padres,** por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor; por los ejemplos de perseverancia y constancia que los caracterizan y que me han infundado siempre, por el valor mostrado para salir adelante.*

***Finalmente a los maestros**, aquellos que marcaron cada etapa de nuestro camino universitario, y que me ayudaron en asesorías y dudas presentadas en la elaboración de la tesis*

AGRADECIMIENTOS

A Dios, *por darme la oportunidad de vivir y por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.*

A mis maestros, *por su gran apoyo y motivación para la culminación de nuestros estudios profesionales y para la elaboración de esta tesis; al ingeniero FRANSISCO SOLARTE apoyo ofrecido en este trabajo; al ingeniero MANUEL BOLAÑOS por su tiempo compartido y por impulsar el desarrollo de nuestra formación profesional.*

A mis amigos, *que nos apoyamos mutuamente en nuestra formación profesional y brindarnos buenos momentos de calidez personal, de compañerismo, de aprendizaje, de crecimiento personal que marcaron nuestras vidas para bien nuestro y de la sociedad, mil gracias.*

Al Doctor ***CARLOS ARTEMIO RUANO VILLOTA*** *(Notario Primero del Circulo de Túquerres) Por permitirnos aplicar y ampliar nuestros conocimientos en LA NOTARÍA PRIMERA y Brindarnos su confianza y apoyo.*

Dios los Bendiga

EULER REMIGIO BASANTE MORA

GILBERTH ANDREY IPAZ

RESUMEN

El presente trabajo realiza una auditoria a la infraestructura física de red y equipos de cómputo de la Notaría Primera de Túquerres, con el objetivo principal de identificar fallos, riesgos y amenazas para minimizar el impacto y probabilidad de ocurrencia, para mejorar el funcionamiento de la entidad.

El trabajo identifico el estado actual de la planta tecnológica existente en la Notaría Primera de Túquerres necesaria para el funcionamiento de la red computacional existente en la entidad, realiza el proceso de análisis y evaluación de riesgos en la Notaría Primera de Túquerres que permitan valorar la probabilidad e impacto que causaría cada uno de los riesgos generando la matriz respectiva.

Este trabajo de auditoría informática, realizó un análisis minucioso para proteger el activo más importante que hoy en día poseen las entidades gubernamentales como es el activo de la información generando planes de mejoramiento y planes de contingencia.

El trabajo de auditoría se basó en el estándar COBIT (Objetivos de Control para Información y Tecnologías Relacionadas) que brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, presentando las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución.

ABSTRACT

This paper performs an audit to physical network infrastructure and computer equipment First of Túquerres Notaría, with the main objective of identifying failures, risks and threats to minimize the impact and likelihood of occurrence, to improve the functioning of the entity.

The work identified the current state of the existing technology plant in the First Túquerres necessary for the operation of the existing computer network in the state notary performs the process of analysis and risk assessment in the First Túquerres Notaría to gauge the probability and impact would cause each of the risks generating the respective matrix.

This work computer audit, conducted a thorough analysis to protect the most important asset today have government entities such as the asset information generating improvement plans and contingency plans.

The audit work was based on the standard COBIT (Control Objectives for Information and related Technology) that provide good practice through a framework of domains and processes, presenting activities in a manageable and logical structure. COBIT best practices represent the consensus of experts. They are strongly focused on control and less on execution.

TABLA DE CONTENIDO

LISTA DE FIGURAS

INTRODUCCIÓN

Siempre ha existido la preocupación por parte de las organizaciones por optimizar todos los recursos con que cuenta la entidad, sin embargo, por lo que respecta a la tecnología de informática, es decir, software, hardware, sistemas de información, investigación tecnológica, redes locales, bases de datos, ingeniería de software, telecomunicaciones, etc. esta representa una herramienta estratégica que representa rentabilidad y ventaja competitiva frente a sus similares en el mercado, en el ámbito de los sistemas de información y tecnología un alto porcentaje de las empresas tiene problemas en el manejo y control, tanto de los datos como de los elementos que almacena, procesa y distribuye.

El propósito de la revisión de la auditoría en informática, es el verificar que los recursos, es decir, información, energía, dinero, equipo, personal, programas de cómputo y materiales son adecuadamente coordinados y vigilados por la gerencia o por quien ellos designen.

Durante años se ha detectado el despilfarro de los recursos o uso inadecuado de los mismos, especialmente en informática, se ha mostrado interés por llegar por llegar a la meta sin importar el costo y los problemas de productividad.

IDENTIFICACION DEL PROBLEMA

TITULO DEL PROYECTO

AUDITORIA A LA INFRAESTRUCTURA FISICA DE RED Y EQUIPOS DE COMPUTO DE LA NOTARÍA PRIMERA DE TÚQUERRES

LINEA DE INVESTIGACION

Este proyecto corresponde a la línea de investigación Auditoria en redes.

DESCRIPCION DEL PROBLEMA

Planteamiento del problema: la Notaría Primera de Túquerres, es una entidad que busca la satisfacción total de todos los usuarios, mediante la oportunidad, trasparencia, seguridad jurídica y calidad en los servicios notariales realizados, contando con un talento humano competente, acorde con la confiabilidad que se otorga como guardadores de la fe pública, por lo cual es de suma importancia hacer una auditoria a la infraestructura física y tecnológica para que la comunicación y almacenamiento de la información entre los diferentes procesos de la entidad se realice de forma eficiente y eficaz garantizando veracidad e integridad de la información.

Formulación del problema: ¿Cómo la aplicación de una auditoria a la infraestructura física de red y equipos de cómputo de la notaría primera de Túquerres, aportara soluciones a problemas existentes en la transmisión y almacenamiento de datos entre las diferentes áreas de la entidad?

OBJETIVOS

Objetivo general

Aplicar auditoria a la infraestructura física de red y equipos de cómputo de la notaría primera de Túquerres con el fin de identificar fallos, riesgos y amenazas para minimizar el impacto y probabilidad de ocurrencia.

Objetivos específicos

- Identificar el estado actual de la infraestructura del cableado en parte física de la red de datos, en la notaría primera de Túquerres.
- Identificar el estado actual de la planta tecnológica existente en la notaría primera de Túquerres necesaria para el funcionamiento de la red computacional existente en la entidad.
- Definir los riesgos, vulnerabilidades y amenazas existentes en cuanto al mal manejo la infraestructura física de red y equipos de cómputo de la notaría primera de Túquerres
- Realizar el proceso de análisis y evaluación de riesgos que permitan valorar la probabilidad e impacto que causaría cada uno de los riesgos generando la matriz respectiva.
- Ejecutar las pruebas necesarias que permitan evidenciar las vulnerabilidades, riesgos y amenazas existentes en cuanto a deficiencias en funcionamiento de la infraestructura física de red y equipos de cómputo de la notaría primera de Túquerres.
- Presentar los resultados de las evaluaciones de la auditoria en el informe final, y elaborar el plan de mejora que será sustentado y entregado a la notaría primera de Túquerres.

JUSTIFICACION

La Notaría Primera de Túquerres siendo una entidad gubernamental presenta unas exigencias de alto nivel en prestación de servicio, la red de datos actualmente está en funcionamiento pero en ningún momento se le a realizado auditoria ni a la parte física ni a la parte tecnológica.

La ejecución de la auditoria en la notaría primera de Túquerres, se evidencia como necesaria con el fin de mejorar la administración de la red evitando fallos

continuos al momento de ejecutar procesos que utilicen la red y trasmisión de datos con el propósito de generar un plan de mejoramiento, plan de contingencia, en caso de cualquier eventualidad que conlleven a evitar retrasos en el desarrollo de actividades

ALCANCE Y DELIMITACION.

La auditoría se llevara a cabo con el propósito de analizar y evaluar el cumplimiento de las normas de instalación del cableado estructurado según el estándar Cobit, para determinar si este cumple sus funciones de manera eficiente y eficaz, en la Notaría Primera de Túquerres

1 MARCO TEORICO

1.1 ANTECEDENTES

A finales del siglo pasado la auditoria se creó únicamente para el sector financiero generando la auditoría contable pero poco a poco se fue incluyendo a la auditoria a diferentes procesos y actividades de las empresas y instituciones en general con el fin de mejorar su eficiencia, eficacia, seguridad, calidad, rentabilidad.

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.

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.

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.

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 dieciocho 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.

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

- Auditoría informática a nivel de los sistemas e indicadores de funcionamiento del hardware y software en la empresa Dispropan S.A.S. del departamento de Nariño y Putumayo, realizado por: Johana Lorena Hernández Benavides
- 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 del centro Hospital Divino Niño, realizado por: Luis Alberto Reynel Araujo.
- Técnicas de auditoria de sistemas aplicadas al proceso de contratación y páginas web en entidades oficiales del departamento de Nariño, realizado por: Luis Carlos Chávez.

1.2 CONCEPTOS GENERALES SOBRE AUDITORIA.

Es un examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo.

Mario G. Piattini y Emilio del Paso tienen el siguiente concepto: *"Es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas"*[1].

La palabra auditoría proviene del latín "*auditorius"*, y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír, y el diccionario lo define como "revisor de cuentas colegiado". El auditor tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del

[1] (PIATTINI & DEL PESO, 2001, p. 4)

señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

1.3 TIPOS DE AUDITORIA

La auditoría, como cualquier otra disciplina toma características diferentes de acuerdo al campo de acción en que se desenvuelven. Sin embargo, el objeto final debe responder a la definición general de la auditoría.

1.3.1 Según la relación de dependencia del auditor

- **Auditoría de primera parte (auditoría interna[2]):** se realiza por miembros de la propia organización o por otras personas que actúen de parte de esta, para fines internos. Proporcionan información para la dirección y para las acciones correctivas, preventivas o de mejora.
- **Auditoría de segunda parte (auditoría externa[3]):** se realiza por los clientes de la organización o por otras personas que actúen de parte de este, cuando existe un contrato. Proporcionan confianza al cliente en la organización suministradora.
- **Auditoría de tercera parte (auditoría externa[3]):** se realiza por organizaciones competentes de certificación para obtener la certificación del sistema de gestión de calidad. Proporcionan confianza a los clientes potenciales de la organización.

1.3.2 Según el campo de actuación: entre las auditorias más relevantes hay:

- **Auditoría administrativa:** revisa y evalúa si los métodos, sistemas y procedimientos que se siguen en todas las fases del proceso administrativo aseguran el cumplimiento con políticas, planes, programas, leyes y

[2] La auditoría interna es la realizada con recursos materiales y personas que pertenecen a la empresa auditada. Los empleados que realizan esta tarea son remunerados económicamente. La auditoría interna existe por expresa decisión de la Empresa, o sea, que puede optar por su disolución en cualquier momento.

[3] La auditoría externa es realizada por personas afines a la empresa auditada; es siempre remunerada. Se presupone una mayor objetividad que en la auditoría interna, debido al mayor distanciamiento entre auditores y auditados.

reglamentaciones que puedan tener un impacto significativo en la operación de los reportes y asegurar que la organización los esté cumpliendo y respetando. Es el examen metódico y ordenado de los objetivos de una empresa de su estructura orgánica y de la utilización del elemento humano a fin de informar los hechos investigados. Su importancia radica en el hecho de que proporciona a los directivos de una organización un panorama sobre la forma como está siendo administrada por los diferentes niveles jerárquicos y operativos, señalando aciertos y desviaciones de aquellas áreas cuyos problemas administrativos detectados exigen una mayor o pronta atención.

- **Auditoría operativa:** es el examen posterior, profesional, objetivo y sistemático de la totalidad o parte de las operaciones o actividades de una entidad, proyecto, programa, inversión o contrato en particular, sus unidades integrantes u operacionales específicas. Su propósito es determinar los grados de efectividad, economía y eficiencia alcanzados por la organización y formular recomendaciones para mejorar las operaciones evaluadas. Relacionada básicamente con los objetivos de eficacia, eficiencia y economía.
- **Auditoría financiera:** Es un proceso cuyo resultado final es la emisión de un informe, en el que el auditor da a conocer su opinión sobre la situación financiera de la empresa, este proceso solo es posible llevarlo a cabo a través de un elemento llamado evidencia de auditoria, ya que el auditor hace su trabajo posterior a las operaciones de la empresa. La Auditoría Financiera es la más conocida de todas, pues es la requerida por las empresas y es la que ha presentado el máximo desarrollo.

1.4 AUDITORÍA EN INFORMATICA

Es un examen que se realiza con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y metas del negocio.

Existe pues, un cuerpo de conocimientos, normas, técnicas y buenas practicas dedicadas a la evaluación y aseguramiento de la calidad, seguridad, razonabilidad, y disponibilidad de la INFORMACION tratada y almacenada a través del computador y equipos afines, así como de la eficiencia, eficacia y economía con que la administración de un ente están manejando dicha INFORMACION y todos los recursos físicos y humanos asociados para su adquisición, captura, procesamiento, transmisión, distribución, uso y almacenamiento. Todo lo anterior con el objetivo de emitir una opinión o juicio, para lo cual se aplican técnicas de auditoria de general aceptación y conocimiento técnico específico

Es conocida como auditoria de sistemas, teniendo como objetivo evaluar sistemas informáticos en forma integral, los procedimientos y seguridad de los equipos electrónicos o hardware de los programas o software que posea la empresa sean propios o de modalidad de servicios.

Analiza 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

1.4.1 Objetivos de la auditoria informática: el objetivo de la auditoría informática persigue es la evolución de un sistema informático para emitir una opción sobre la fiabilidad y exactitud de los datos procesados, así como detectar y corregir errores encontrados y asegurar la continuidad del soporte automatizado de la gestión y por ultimo elaborar un recomendación de plan de acción.

La Auditoría Informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

Esta es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas

sean confiables y con un buen nivel de seguridad. Además debe evaluar todo: informática, organización de centros de información, hardware y software.

1.4.2 Alcance de la Auditoría Informática: el alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoria informática, 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.

Aplicación: la auditoría de sistemas analiza todos los procedimientos y métodos de la empresa con la intención de mejorar su eficacia.

Que audita: líneas y redes de las instalaciones informática.

Para que se audita: examinar y analizar 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.

La información es considerada un activo tan o más importante que cualquier otro en una organización.

1.4.3 Fases de la auditoria informática: para que los resultados de una auditoria sean óptimos, esta deberá estar basada en alguna metodología ampliamente conocida para la realización de auditorías. En general las faces en que se desarrolla toda auditoria, son:

- **Planeación:** aquí se debe planificar como realizar la auditoria, con los pasos a seguir, además de tener claro las herramientas a ocupar para la recolección, procesamiento y presentación de los datos necesarios para la auditoria, cabe destacar que el planteamiento está estrictamente ligado a los objetivos específicos de la auditoria.

- **Ejecución:** en esta fase se plantea el trabajo a realizar, recopilando y analizando los datos, es decir, tomar información y procesarla de acuerdo a los objetivos de la auditoría.
- **Informe de auditoría:** aquí se presentan de forma clara, coherente y entendible las conclusiones de la auditoria, que dicho sea de paso es el resultado de procesamiento de la información y se compone de las sugerencias realizadas en la base a lo observado y a las reglas aplicadas para enmarcar a la auditoria (estándares).

1.4.4 Finalidad de la auditoría: el propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de los resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados, en los servicios que proporcionan los sistemas computacionales de la entidad.

1.4.5 Control interno y auditoria informática: este es el seguimiento a las recomendaciones emitidas a la auditoria, es revisar si están cumpliendo a cabalidad lo que se implementó con el fin de reducir los errores y que estos no persistan o estén apareciendo o desapareciendo.

Estos están estrechamente ligados con el control interno de la empresa que es el plan de la organización de todos los métodos y procedimientos que son relativos y que están directamente relacionados con salvaguardar los activos y la confiabilidad de los registros financieros.

Además del control interno, también existe el control interno informático que es el que controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la dirección de la organización y la dirección de informática.

1.4.6 Tipos de controles internos: los controles informáticos se dividen en las siguientes categorías:

- **Controles preventivos**: para tratar de evitar el hecho, como por ejemplo que un software de seguridad impida los accesos no autorizados al sistema.
- **Controles detectivos**: cuando fallan los preventivos para tratar de conocer cuanto antes del evento.
- **Controles correctivos**: facilitan la vuelta a la normalidad cuando se han producido incidencias.

1.4.7 Técnicas para la auditoria informática: existen muchas herramientas para la ejecución de una auditoria informática, están ayudan a la gestión de examinar que tan eficientes y eficaces son los controles del área evaluada, entre las herramientas más usada para auditar están:

- Cuestionarios
- Entrevistas
- Formularios Checklist
- Formularios virtuales
- Software de interrogación
- Fotografías o tomas de valor
- Diseños de flujos y de la red de información
- Planos de distribución e instalación
- Certificados, garantías, otros del software
- Historia de cambios y mejoras

1.4.8 Principales pruebas y herramientas para efectuar una auditoria informática: al elaborar una auditoria informática el auditor puede realizar las siguientes pruebas:

- **Pruebas Clásicas:** consiste en probar las aplicaciones/sistemas con datos de prueba, observando la entrada, la salida esperada, y la salida obtenida. Existen paquetes que permiten la realización de estas pruebas.

- **Pruebas sustantivas:** aportan al auditor informático las suficientes evidencias y que se pueda formar un juicio. 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**: determinan si un sistema de control interno funciona adecuadamente según la documentación, según declaran los auditados y según las políticas y procedimientos de la organización.

1.5 COBIT (*Control Objectives for Information and related Technology*).

La Organización ISACA *(Information Systems Audit and Control Association*), se formo 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

[4] www.degerencia.com/articulos/los_cinco_componentes_del_control_interno.

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.

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

1.5.1 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:

1.5.1.1 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, 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.

1.5.1.2 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:

1.5.1.3 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:

1.5.1.4 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

1.5.1.5 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.

1.5.1.6 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.

1.5.1.7 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.

1.5.1.8 PO8 Asegurar el cumplimiento con los requerimientos externos

- PO8.1 Definición y mantenimiento de procedimientos para la revisión de requerimientos externos,
- PO8.2 Leyes, regulaciones y contratos
- PO8.3 Revisiones regulares en cuanto a cambios
- PO8.4 Búsqueda de asistencia legal y modificaciones
- PO8.5 Seguridad y privacidad
- Propiedad intelectual
- Flujo de datos externos y criptografía

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:

1.5.1.9 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.

1.5.1.10 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.

1.5.1.11 PO11 Administración de calidad

- PO11.1 Sistema de administración de calidad
- PO11.2 Estándares y prácticas de calidad
- PO11.3 Estándares de desarrollo y de adquisición
- PO11.4 Enfoque en el cliente de TI
- PO11.5 Mejora continua
- PO11.6 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.

1.5.2 **Dominio: adquisición e implementación (AI):** para llevar a cabo la estrategia de TI, las soluciones deben ser identificadas, desarrolladas o

adquiridas, así como implementadas e integradas dentro del proceso del negocio. Este dominio cubre cambios y mantenimiento realizado a sistemas existentes.

Procesos:

1.5.2.1 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.

1.5.2.2 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.

1.5.2.3 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.

1.5.2.4 AI4 Facilitar la operación y el uso

- AI4.1 Plan para soluciones de operación
- AI4.2 Transferencia de conocimiento a la gerencia del negocio
- AI4.3 Transferencia de conocimiento a usuarios finales.
- AI4.4 Transferencia de conocimiento al personal de operaciones y soporte

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.

1.5.2.5 AI5 Adquirir recursos

- AI5.1Control de adquisición
- AI5.2 Administración de contratos con proveedores
- AI5.3 Selección de proveedores
- AI5.4 Adquisición de recursos de TI

Objetivo: responder a los requerimientos del negocio de acuerdo con la estrategia de negocio, mientras se reducen los defectos y la repetición de trabajos en la prestación del servicio y en la solución

1.5.2.6 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.

1.5.2.7 AI7 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

1.5.3 **Dominio: entregar y dar soporte (DS):** en este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de

los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Procesos:

1.5.3.1 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.

1.5.3.2 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:

1.5.3.3 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

1.5.3.4 DS4 Asegurar el servicio continúo

- 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 probada y funcional, que esté alineado con el plan de continuidad del negocio y relacionada con los requerimientos de negocio

1.5.3.5 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

1.5.3.6 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.

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

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

1.5.3.9 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.

1.5.3.10 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.

1.5.3.11 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.

1.5.3.12 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.

1.5.3.13 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

1.5.4 **Dominio: monitorear y evaluar (ME):** todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio.

Procesos:

1.5.4.1 ME1 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.

1.5.4.2 ME2 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.

1.5.4.3 ME3 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.

1.5.4.4 ME4 Proveer auditoría 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

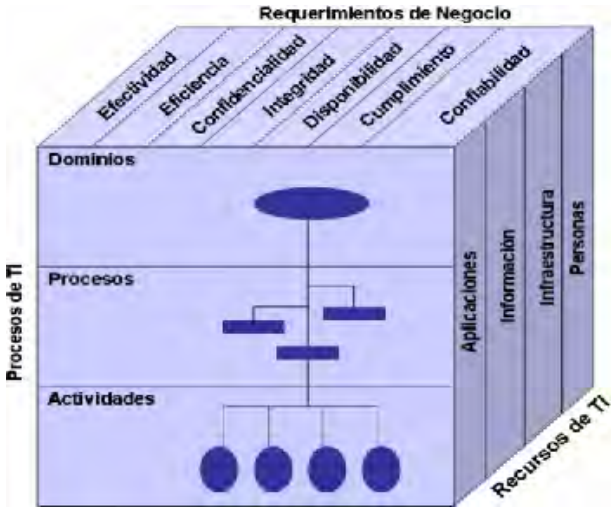
1.6 OBJETIVOS DE CONTROL

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



FUENTE: manual cobitT

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.

2. METODOLOGÍA

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 equipo 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 Auditoría 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.

- **Presentación del Informe Final**: se realizó un informe final 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.

- **Leyes y decretos comunes:** en este apartado se citaran las leyes y decretos que regularon el proceso de auditoría en las dos entidades.
- A los efectos del artículo 12 de la Ley 15/1999, el PROVEEDOR únicamente tratará los datos de carácter personal a los que tenga acceso conforme a las instrucciones del CLIENTE y no los aplicará o utilizará con un fin distinto al objeto del Contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el caso de que el PROVEEDOR destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del Contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

  - ✓ **DE NOTARÍA:** Las consagradas en el Art. 3 del D.L. 960 de 1970
  - ✓ [Numeral derogado por el artículo 46 del Decreto 2163 de 1970.]
  - ✓ [Numeral derogado por el artículo 46 del Decreto 2163 de 1970.]
  - ✓ Las demás funciones que les señalen las Leyes.
  - ✓ Depósitos: Art. 18 y 19 de la Ley 29 de 1973, articulo 46 Decreto Reglamentario 2148 de 1983, capitulo XI.

- **Misión**

Lograr la satisfacción total de todos los usuarios, mediante la oportunidad, trasparencia, seguridad jurídica y calidad en los servicios notariales realizados,

contando con un talento humano competente y comprometido dispuesto a prestar una orientación y asesoría completa, acorde con la confiabilidad que se nos otorga como guardadores de la fe pública

- **Visión**

Garantizar un excelente servicio mediante el compromiso de todos los empleados de la Notaría, para satisfacer las necesidades y expectativas de los usuarios y de los mismos empleados.

ORGANIGRAMA

Fig.2 Organigrama

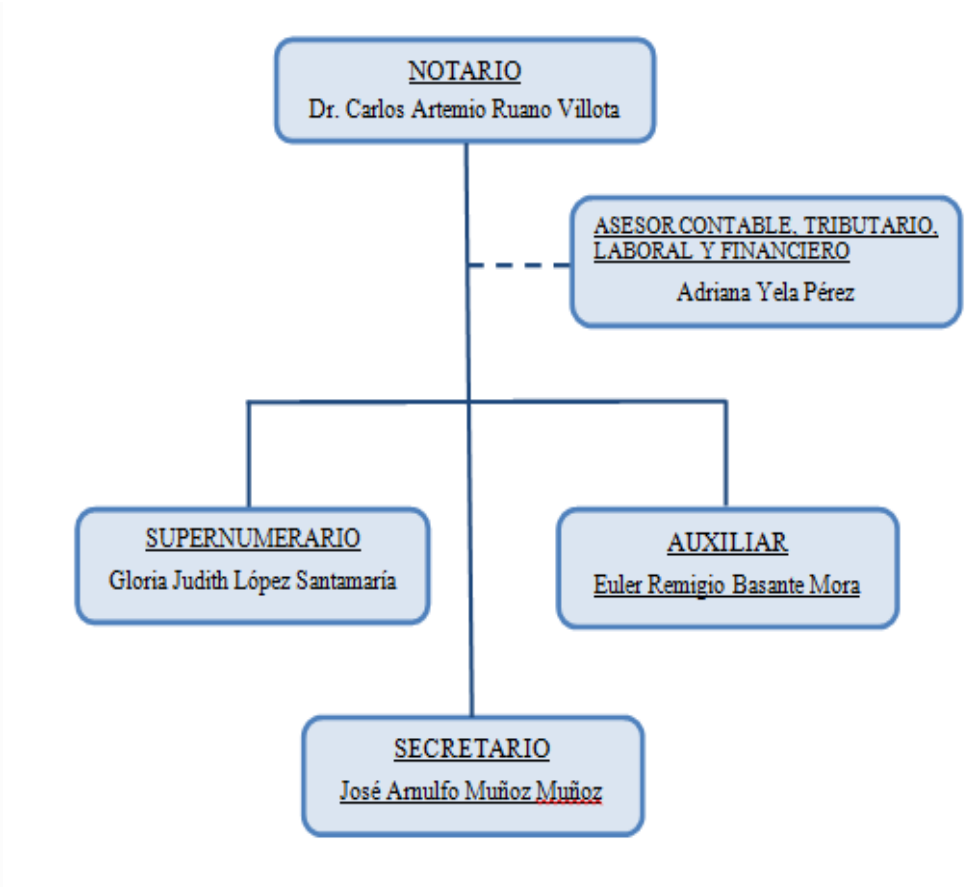
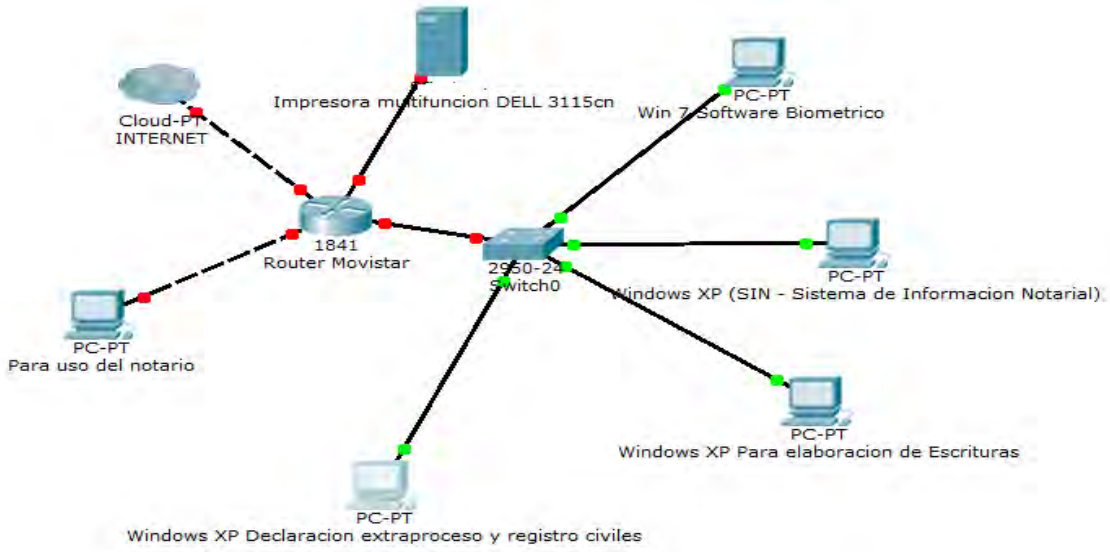


Fig. 3. Topología red



3.2. ARCHIVO CORRIENTE

Este archivo está compuesto por documentos directamente relacionados con el desarrollo del proyecto.

3.2.1 Plan de auditoría: las metodologías son necesarias para desarrollar cualquier tipo de proyecto de forma ordenada eficaz, razón por la que la metodología utilizada para la realización de la auditoria de sistemas dentro de **LA NOTARÍA PRIMERA DE TÚQUERRES.** Es de tipo cuantitativo/subjetivo, basado en un modelo matemático numérico, arrojando como resultado una lista de riesgos obtenidos del análisis de cada uno de los procesos a auditar teniendo en cuenta su importancia e impacto dentro del área de sistemas de ahí su calificación y recomendaciones realizadas.

La metodología aplicada en la realización de esta auditoría, se ejecutó de la siguiente manera:

Etapa1. Exploración del entorno: este primer paso se realizó con el fin de familiarizarse con el área de sistemas de **LA NOTARÍA PRIMERA DE TÚQUERRES**, se hace un estudio previo de los procesos a auditar obteniendo así las herramientas necesarias para una adecuada planeación de la auditoria, también en esta etapa se definen que elementos se utilizaron para elaborar la auditoria. Se realizaron varias visitas con el fin de conocer y observar los diferentes procesos, para identificarlos y auditarlos, a través de entrevistas abiertas se dio inicio a la recolección de información, dando el siguiente paso que fueron la aplicación de cuestionarios cuantificables con los funcionarios de los diferentes departamentos de **LA NOTARÍA PRIMERA DE TÚQUERRES.**

Etapa2. Planeación de las actividades de auditoria: aquí se realizó la planificación de todo el proceso de la auditoría, con las siguientes actividades:

- Se realizó un estudio previo del área de **LA NOTARÍA PRIMERA DE TÚQUERRES.** obteniendo información necesaria respecto al tema.
- Se identificó el alcance y los objetivos de la auditoria a realizar.
- Determinación de los recursos necesarios con los que se realizó la auditoria.
- Se elaboró el plan de trabajo.

Etapa3. Realización las actividades de la auditoria: en esta etapa se realizaron las diferentes actividades implantadas en la etapa anterior, mediante la aplicación de técnicas junto con la aplicación de diferentes herramientas que garantizo el cumplimiento de los objetivos propuestos para la ejecución de la auditoria. En esta etapa se realizaron las siguientes actividades:

Elaboración del plan de auditoría, a través de COBIT permitiendo así la identificación de los procesos y objetivos de control evaluados. Se elaboran cuadros de definición de fuentes de conocimiento, que facilitan la identificación clara de la fuente de obtención de las pruebas.

Se aplicaron entrevistas con preguntas abiertas y preguntas cerradas para la obtención de información general de la empresa, para luego elaborar diferentes cuestionarios cuantitativos para cada uno de los procesos seleccionados dentro de los dominios del COBIT a auditar.

Se realizó la identificación de vulnerabilidades, riesgos y amenazas, y su valoración con respecto a la probabilidad e impacto mediante la utilización del COBIT (modelo para auditoría y control de sistemas de información).

- ✓ Identificar las vulnerabilidades, riesgos y amenazas existentes en el sistema.
- ✓ Valorar los riesgos según la escala definida para la probabilidad e impacto.

- ✓ Identificación de hallazgos. Mediante el formato de hallazgos, se asigna la probabilidad de ocurrencia e impacto para los riesgos encontrados.

- ✓ Elaboración de la matriz de probabilidad e impacto, que permitió identificar los riesgos altos que necesitan mitigarse de manera urgente mediante un plan correctivo.

Etapa 4. Presentación del informe final: etapa en la cual se realizó el informe final que contiene todos los procesos evaluados con la descripción del comportamiento que estos tienen dentro de la empresa o los hallazgos encontrados con sus respectivas recomendaciones que permitan mitigarlos al máximo. Este informe se presentó y se entregó al ingeniero de sistemas de **LA NOTARÍA PRIMERA DE TÚQUERRES.** Para que tomen las respectivas correcciones a implantar mediante un plan de mejoramiento.

3.2.2 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

- **Fuentes Primarias:** las fuentes primarias en el desarrollo de esta auditoría se poseen las siguientes:

- ✓ Entrevista, dirigida al ingeniero de sistemas de **LA NOTARÍA PRIMERA DE TÚQUERRES.**
- ✓ Ejecución de los cuestionarios en todas áreas de **LA NOTARÍA PRIMERA DE TÚQUERRES**
- ✓ Manuales, que estén relacionados con los procesos que se manejan en el área de sistemas en **LA NOTARÍA PRIMERA DE TÚQUERRES.**
- **Fuentes secundarias:** para el desarrollo de este proyecto de auditoría, se cuenta con la vasta gama de libros referenciales y la web, por lo anterior se podrá consultar temas relacionados con auditorías informáticas de seguridad de la red de datos, información relacionada con software para la auditoria de redes, Etc.

- **Plan de pruebas:** el plan de Pruebas permite anotar todas las observaciones durante el proceso de la auditoria de manera secuencial, este contiene lo siguiente: Prueba, Proceso, tipo y acción de la prueba.

3.2.3 Programa de auditoría: para la ejecución de la auditoria a la infraestructura física de la red de datos y equipos de **LA NOTARÍA PRIMERA DE TÚQUERRES**, se utiliza la metodología COBIT de ISACA , que cubre 210 objetivos de control clasificados en 4 dominios y 35 procesos. De los cuales se aplican los siguientes:

3.2.3.1 Dominio planificación y organización (PO): la Planificación y el dominio de Organización cubren el empleo de tecnología y como puede esta ser mejor utilizada en una empresa para ayudar a alcanzar los objetivos de la empresa. Esto también destaca la forma de organización que la infraestructura tecnológica y la TI debe tomar para alcanzar los resultados óptimos.

Procesos de dominio planificación y organización (PO)

- PO1 definir un plan estratégico de TI
- PO3 determinar la dirección tecnológica
- PO4 definir los procesos, organización y relaciones de TI

- PO9 evaluar y administrar los riesgos de TI

PO1 definir un plan estratégico de TI: la planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. La función de TI y los interesados del negocio son responsables de asegurar que el valor óptimo se consigue desde los proyectos y el portafolio de servicios. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido. La estrategia de negocio y prioridades se reflejarán en portafolios y se ejecutarán por los planes estratégicos de TI, que especifican objetivos concisos, planes de acción y tareas que están comprendidas y aceptadas tanto por negocio como por TI.

- **Que satisface el requerimiento del negocio de:** sostener o extender los requerimientos de gobierno y de la estrategia del negocio, al mismo tiempo que se mantiene la transparencia sobre los beneficios, costos y riesgos
- **Enfocándose en:** la incorporación de TI y de la gerencia del negocio en la traducción de los requerimientos del negocio a ofertas de servicio, y el desarrollo de estrategias para entregar estos servicios de una forma transparente y rentable.

- **Se logra con:**
  - ✓ El compromiso con la alta gerencia y con la gerencia del negocio para alinear la planeación estratégica de TI con las necesidades del negocio actuales y futuras
  - ✓ El entendimiento de las capacidades actuales de TI
  - ✓ La aplicación de un esquema de prioridades para los objetivos del negocio que cuantifique los requerimientos del negocio
- **Objetivos de control:** definir un plan estratégico de TI que satisfaga el requerimiento de negocio de TI de sostener o extender la estrategia de

negocio y los requerimientos de gobierno al mismo tiempo que se mantiene la transparencia sobre los beneficios, costos y riesgos.

- **PO1.3 Evaluación del desempeño y la capacidad actual:** evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades
- **PO1.4 Plan estratégico de TI:** crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operativos. Define cómo se cumplirán y medirán los objetivos y recibirán una autorización formal de los interesados. El plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de obtención, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI

2 **PO3 Determinar la dirección tecnológica:** aprovechar al máximo la tecnología disponible o tecnología emergente satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica.

- **Que satisface el requerimiento del negocio de**: contar con sistemas aplicativos estándares, bien integrados, rentables y estables, así como recursos y capacidades que satisfagan requerimientos de negocio, actuales y futuros.

- **Enfocándose en:** la definición e implementación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas

- **Se logra con:** el establecimiento de un foro para dirigir la arquitectura y verificar el cumplimiento

  El establecimiento de un plan de infraestructura tecnológica equilibrado versus costos, riesgos y arquitectura de información.

- **Objetivos de control:** se busca actualizar regularmente aspectos referentes a la arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias, con el fin de que la empresa aproveche al máximo sus recursos tecnológicos.

  PO3.1 Planeación de la dirección: analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiada tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio. También identificar en el plan qué tecnologías tienen el potencial de oportunidades de negocio. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración los aspectos de contingencia de los componentes de la infraestructura.

3 **PO4 Definir los procesos de TI, organización y relaciones de TI:** la Prestación de servicios de TI se realiza a través de una organización conveniente en número y habilidades con tareas y responsabilidades definidas y comunicadas.

- **Que satisface el requerimiento del negocio de:** agilizar la respuesta a las estrategias del negocio mientras se cumplen los requerimientos de gobierno y se establece en puntos de contacto definidos y competentes

- **Enfocándose en:** el establecimiento de estructuras organizacionales de TI transparentes, flexibles y responsables, y en la definición e implementación

de procesos de TI con dueños, y en la integración de roles y responsabilidades hacia los procesos de negocio y de decisión.

- **Se logra con:**

  - ✓ La definición de un marco de trabajo de procesos de TI
  - ✓ La definición de un cuerpo y una estructura organizacional apropiada.
  - ✓ La definición de roles y responsabilidades

- **Objetivos de control:** se busca definir el personal de la tecnología de información, los roles, las funciones y responsabilidades, permitiendo el buen funcionamiento de servicios que satisfagan los objetivos del área de Sistemas que concuerden los de la empresa.

  Teniendo en cuenta los siguientes objetivos de control:

  - **PO4.6 Responsabilidad de aseguramiento de calidad de TI:** 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 Políticas y procedimientos para personal contratado: 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

4 **PO9 Evaluar y administrar los riesgos de TI:** se refiere a crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales acordados. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar.

- **Que satisface el requerimiento del negocio de:** analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas del negocio.

- **Enfocándose en:** la elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales.

- **Se logra con:**

  - ✓ La garantía de que la administración de riesgos este incluida completamente en los procesos.
  - ✓ La realización de evaluaciones de riesgo.
  - ✓ La recomendación y comunicación de planes de acción para remediar riesgos.

- **Objetivos de control:** se encargan de identificar, analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de la empresa, con el objetivo de asegurar el logro de los objetivos de TI, con la estabilidad y el funcionamiento de las comunicaciones de la red.

  Se deben adoptar estrategias de mitigación de riesgos para minimizarlos a un nivel aceptable de acuerdo a los siguientes objetivos de control:

  - **PO9.1 Alineación de la administración de riesgos de TI y del negocio**: 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 IT**: 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.

3.2.3.2 DOMINIO: Adquisición e implementación (AI)

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

Procesos de dominio adquisición e implementación:

- AI3. Adquirir y mantener infraestructura tecnológica

1 **AI3 Adquirir y mantener la infraestructura tecnológica:** proporcionar las plataformas apropiadas para soportar aplicaciones de negocios debido al costo y a la importancia de los elementos que constituyen la red física de datos es prioritaria tanto la adquisición como el mantenimiento de estos elementos fundamentales para el proceso tecnológico de la entidad.

- **Que satisface el requerimiento del negocio de:** adquirir y dar mantenimiento a una infraestructura integrada y estándar de TI.

- **Enfocándose en:** proporcionar plataformas adecuadas para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología.

- **Se logra con:**

  - ✓ El establecimiento de un plan de adquisición de tecnología que se alinea con el plan de infraestructura tecnológica.
  - ✓ La planeación de mantenimiento de la infraestructura.
  - ✓ La implantación de medidas de control interno, seguridad y auditabilidad.

- **Objetivos de control:** se busca satisfacer con los requerimientos de la empresa, el área de sistemas debe contar un plan operativo donde se garantice el buen funcionamiento, mantenimiento y cumplimiento de los estándares de la infraestructura tecnológica para dar soporte a los diferentes procesos dentro de la empresa.

  Toma en consideración los siguientes objetivos de control:

- **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.
- **AI3.2 Protección y disponibilidad del recurso de infraestructura:** Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por

todos aquellos que desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso.

- **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.

3.2.3.3 Dominio - entregar y dar soporte (DS)

Contar con una definición documentada hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto a los procesos también incluye el monitoreo.

Procesos de dominio ENTREGAR Y DAR SOPORTE

- Administración de instalaciones (DS12).

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.

- **Que satisface el requerimiento del negocio de:** proteger los activos de cómputo y la información del negocio minimizando el riesgo de la interrupción del servicio.

- **Enfocándose en:** proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo.

- **Se logra con:**

  - ✓ Implementando medidas de seguridad física.

  - ✓ Seleccionando y administrando las instalaciones**.**

- **Objetivos de control:** se busca controlar la seguridad de la empresa, el área de sistemas debe contar un plan de seguridad donde se garantice el buen funcionamiento, mantenimiento y

cumplimiento de los estándares de la infraestructura tecnológica para dar seguridad a los diferentes activos dentro de la empresa.

- **DS12.1 Selección y Diseño del Centro de Datos:** definir, seleccionar, 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 óptima y cumpla con las necesidades del servicio.
- **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.
- **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.

3.2.3.4 Dominio monitorear y evaluar (ME)

Procesos de dominio monitorear y evaluar

- ME2 Supervisar y evaluar el control interno

1. **ME2 Supervisar y evaluar el control interno:** establecer un programa de control interno efectivo para TI requiere de un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-Evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las

leyes y regulaciones aplicables teniendo en cuenta los siguientes objetivos de control.

- **Que satisface el requerimiento del negocio de:** proteger el logro de los objetivos de TI y cumplir las leyes y reglamentos relacionados con TI
- **Enfocándose en:** el monitoreo de los procesos de control interno para las actividades relacionadas con TI e identificar las acciones de mejoramiento.
- **Se logra con:**
  - ✓ La definición de un sistema de controles internos integrados en el marco de trabajo de los procesos de TI.
  - ✓ Monitorear y reportar actividades de los controles internos sobre TI.
  - ✓ Reportar las excepciones de control a la gerencia para tomar acciones.
- **Objetivos de control:** monitorear y evaluar el control interno que satisfaga el requerimiento de negocio de TI de proteger el logro de los objetivos de TI y cumplir con las leyes y regulaciones relacionadas con TI
  - **ME2.7 Acciones correctivas:** identificar, iniciar, rastrear e implementar acciones correctivas derivadas de los controles de evaluación y los informes.

3.3 CUADROS FUENTES DE CONOCIMIENTO

- Fuentes de conocimiento y plan de pruebas
- Descripción de los cuadros de cuestionarios y entrevistas

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

REF: identificación del cuadro de Definición.

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

OBJETO DE ESTUDIO: identificación de la parte a evaluar

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

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

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

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

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

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

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

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

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

Cuadro de cuestionarios y entrevistas

DOMINIO: Planeación y Organización (PO)

PROCESO: PO1 Definir un Plan Estratégico de TI.

Notaría 1 SNR SUPERINTENDENCIA DE NOTARIADO & REGISTRO La guarda de la fe pública	Tipo de Registro: Cuadro de Definición de Fuentes de Conocimiento, Pruebas de Análisis y Auditoria.	
Entidad Auditada:	NOTARÍA PRIMERA DE TÚQUERRES	
Área Auditada:	**SISTEMAS**	**Ref: PO1-1**
Objeto de Estudio	**Funcionamiento red de datos y equipos de cómputo**	
Responsables:	EULER REMIGIO BASANTE MORA GILBERTH ANDREY IPAZ	
Material de Soporte:	COBIT	
DOMINIO: Planeación y Organización (PO)		
PROCESO: PO1 Definir un Plan Estratégico de TI.		
Descripción de la Actividad/Prueba: Determinar Fuentes de Conocimiento, Determinar las Pruebas de Análisis del Sistema y las Pruebas de Auditoria definidas en la Metodología Cobit.		

Fuentes de Conocimiento	**REPOSITORIO DE PRUEBAS APLICABLES**	
	De Análisis	**De Ejecución**
- Entrevista al ingeniero encargado del área de sistemas de la NOTARIA PRIMERA DE TUQUERRES	-Analizar la estructura y organización de la empresa. -Analizar plan estratégico de la	-Revisión detallada de plan estratégico de la empresa - Revisión detallada de plan de gestión de la empresa -Revisión detallada de la

- Entrevista a los diferentes funcionarios de la NOTARIA PRIMERA DE TUQUERRES -plan estratégico de la empresa la NOTARIA PRIMERA DE TUQUERRES -Arquitectura de Red la NOTARIA PRIMERA DE TUQUERRES. -Presupuesto para infraestructura tecnológica.	empresa -Analizar el plan de contingencia para el área de sistemas -Analizar plan de gestión de la empresa -Análisis del plan de infraestructura tecnológica. -Analizar soluciones tecnológicas existentes en la empresa.	Arquitectura de red, de las políticas y aplicación de las normas. -Revisión detallada de los planes de contingencia, el cumplimiento de estas, el conocimiento por el personal. -Revisar detalladamente el plan de equipos de red y de computo -Revisar soluciones tecnológicas en cuanto a la parte de la red de datos.

Cuadros de cuestionarios y entrevistas:

Ver anexo cuestionarios y entrevistas PO3

Ver anexo cuestionarios y entrevistas PO4

Ver anexo cuestionarios y entrevistas PO9

Ver anexo cuestionarios y entrevistas AI3

Ver anexo cuestionarios y entrevistas DS12

Ver anexo cuestionarios y entrevistas ME2

3.4 RECOLECCIÓN DE INFORMACIÓN.

Entrevistas y cuestionarios

3.4.1 Cuestionario cuantitativo: permite definir preguntas tomando como base el cuadro de definición de fuente de conocimiento. El cuestionario presenta tres

opciones de respuesta (SI, NO, NA (No Aplica)), permitiendo así calificar el proceso entre 1 a 5, teniendo en cuenta el nivel de importancia de la pregunta, bajo criterio de los auditores, la sumatoria del puntaje de las preguntas da el total de la encuesta, se califica las columnas del SI, las del NO y las NA, sumando el puntaje de las preguntas. La fuente permite identificar los responsables bien sea una determinada persona o cualquier medio del cual se tomó la información para calificar.

Los ítems que se encuentran en este formato son:
REF: identificación del cuadro de Definición.

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

OBJETO DE ESTUDIO: identificación de la parte a evaluar

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

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

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

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

PREGUNTA: listado de preguntas que serán evaluadas.

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

FUENTE: de donde se obtiene la información

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

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

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

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

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

% Total de Riesgo = 100 - % de Riesgo

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

1% - 30% = Riesgo Bajo

31% - 70% = Riesgo Medio

71% - 100% = Riesgo Alto

Riesgo bajo: deficiencias bajas en grado de importancia mayor, fáciles de solucionar a largo plazo.

*Riesgo medio: s*e debe tomar medidas de solución o mejora en un determinado periodo de tiempo.

Riesgo alto: se debe establecer soluciones inmediatas para reducir el riesgo sin afectar los objetivos del caso de estudio.

Entonces, se calcula así:

% de Riesgo Total = 100 - % de Riesgo

El resultado obtenido, permitió formular conclusiones acerca de funcionamiento del proceso evaluado, teniendo en cuenta que este toma validez con la obtención de pruebas, que verifique los resultados de la encuesta.

Recolección de información

DOMINIO PLANEACION Y ORGANIZACIÓN

CUESTIONARIO PO1

	CUESTIONARIO CUANTITATIVO					
REF: PLAN PO1						
ENTIDAD AUDITADA		NOTARÍA PRIMERA TÚQUERRES		**PAGINA**		
				1	**DE**	**1**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Funcionamiento de la red de datos y equipos de cómputo			
RESPONSABLES		EULER REMIGIO BASANTE MORA GILBERTH ANDREY IPAZ				
MATERIA L DE SOPORTE		COBIT				
DOMINIO	Planeación y Organización (PO)	**PROCESO**	PO1 Definir un Plan Estratégico de TI.			

PREGUNTA	**SI**	**NO**	**NA**	**OBSERVACION**
1. ¿Considera que la estrategia de la tecnología de la información está alineada con el desarrollo del negocio?		**4**		**ANEXO2**
2. ¿Existe inventario de la infraestructura tecnológica instalada?		**5**		**ANEXO2**
3¿Se están optimizando el uso de los recursos?		**5**		**ANEXO2**
4¿Las personas de la organización entienden los objetivos de las TI?	**2**			Existe dependencia hacia el ingeniero ya que es el único

				encargado
5¿Cree que la calidad de los sistemas que se tienen implementados es buena?	**2**			**ANEXO2**
6¿considera que el plan estratégico existente para realizar copias de respaldo es bueno?		**5**		Existe dependencia hacia el ingeniero ya que es el único encargado
7¿Le parece que el mantenimiento preventivo que se está realizando a la infraestructura tecnológica es apropiado?		**5**		Existe dependencia hacia el ingeniero ya que es el único encargado
8 ¿La inversión realizada por gerencia en infraestructura tecnológica es apropiada?	**2**			**ANEXO2**
9 ¿En caso de problema en red, el protocolo para superar el fallo es conveniente?		**4**		**ANEXO2**
10 ¿Existen planes de contingencia adecuados en caso de daño de hardware necesario para administrar la Red de datos?		**5**		Existe dependencia hacia el ingeniero ya que es el único encargado
TOTAL	**6**	**33**		
TOTAL CUESTIONARIO		**39**		

PORCENTAJE DE RIESGO:= $\frac{6*100}{39}$= 15.38%

% de Riesgo Total = 100 – 15.38 = 84.62%

Por lo tanto el porcentaje de riesgo es **ALTO.**

Cuadros cuantitativos de procesos:

Ver anexo cuantitativo PO3

Ver anexo cuantitativo PO4

Ver anexo cuantitativo PO9

Ver anexo cuantitativo AI3

Cuestionarios de control:

ENTREGAR Y DAR SOPORTE (DS)

CUESTIONARIO DE CONTROL CC1

Notaría 1 SNR SUPERINTENDENCIA DE NOTARIADO & REGISTRO La guarda de la fe pública	NOTARÍA PRIMERA DE TÚQUERRES	TÚQUERRES
Cuestionario de Control	**CC1**	
Dominio	Entrega de Servicios y Soportes	
Proceso	DS12: Administración de Instalaciones.	
Objetivo de Control	SEGURIDAD CENTRO DE COMPUTO	

Cuestionario

Pregunta	**SI**	**NO**	**N/A**
¿Las instalaciones (cubículos y oficinas) fueron diseñadas o adaptadas específicamente para funcionar como un centro de cómputo?		4	**ANEXO1**
¿Se tiene una distribución del espacio adecuada, de forma tal que facilite el trabajo y no existan distracciones?		4	**ANEXO1**
¿Existe suficiente espacio dentro de las instalaciones de forma que permita una circulación fluida?	3		**ANEXO1**
¿Existen lugares de acceso restringido?		5	**ANEXO1**

¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?		5	**ANEXO1**
¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de censores?	3		**ANEXO1**
¿Existen señalizaciones adecuadas en las salidas de emergencia y se tienen establecidas rutas de evacuación?		4	**ANEXO1**
¿Se tienen medios adecuados para extinción de fuego en el centro de cómputo?	4		**ANEXO1**
¿Se cuenta con iluminación adecuada y con iluminación de emergencia en casos de contingencia?		3	**ANEXO1**
¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?	4		**ANEXO1**
¿Se tiene un lugar asignado para papelería y utensilios de trabajo?	3		**ANEXO1**
¿Son funcionales los muebles instalados dentro del centro de cómputo: archiveros, mesas de trabajo, etc.?		3	**ANEXO1**
¿Existen prohibiciones para fumar, consumir alimentos y bebidas?	4		**ANEXO1**
¿Se cuenta con suficientes carteles en lugares visibles que recuerdan estas prohibiciones?	3		**ANEXO1**
¿Con cuanta frecuencia se limpian las instalaciones? Semanal		3	**ANEXO1**
Mensual			**ANEXO1**
Anual			**ANEXO1**
¿Se cuenta en los cuartos de comunicaciones con piso falso?		4	**ANEXO1**
¿Con cuanta frecuencia se limpian los ductos de aire y la cámara de aire que existe debajo del piso falso (si existe)? Semanal		4	**ANEXO1**

Mensual			
Anual		4	**ANEXO2**
TOTAL	24	43	
TOTAL CUESTIONARIO	67		

PORCENTAJE DE RIESGO:= $\frac{24*100}{67}$= 35.82%

% de Riesgo Total = 100 – 35.82= 64.18

Por lo tanto el porcentaje de riesgo es **MEDIO.**

Cuadros de control de procesos:

Ver anexo control DS12 CC2

Ver anexo control DS12 CC3

Ver anexo control DS12 CC4

Ver anexo control ME2 CC1

2.5 LISTA DE RIESGOS

- **Riesgos Dominio Planeación Y Organización**

PO1 Definir un Plan Estratégico de TI

R1. No existe un grupo encargado de evaluar y estudiar el desempeño de la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.

R2. No existen políticas ni procedimientos relacionados con la conformación adecuada de la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.

PO3 Determinar la Dirección Tecnológica

R3 No existe un plan de la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.

R4 No hay un inventario actualizado de la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.

R5 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

R6 No se realizan simulacros con los planes de contingencia en caso de fallas de software o hardware en la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.

R7. No hay un cronograma de mantenimientos preventivos a la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.

PO4 Definición de la Organización y de las Relaciones de TI

R8 El manual de funciones del personal del área de sistemas no se actualiza con frecuencia, con sus respectivas funciones, descripción de cargo y requerimientos, personal responsable.

R9 En caso de falta del personal clave en la parte de Redes de datos no se tiene planes de contingencia para su reemplazo en caso de ausencia o no está documentado.

PO9 Evaluación y Análisis de Riesgos

R10 No existe el plan de evaluación de riesgos del área de sistemas de la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.

R11 No existe un plan de contingencia ni de seguridad para contrarrestar un evento que afecte la conexión física de la red de datos

R12 No se cuenta con pólizas de seguros para el manejo del riesgo

Riesgos Dominio ADQUISICION E IMPLEMENTACION (AI)

AI3 Adquirir y Mantener la infraestructura Tecnológica

R13 No existe documentación sobre las políticas de mantenimiento que se realiza a la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.

R14 No existe conocimiento por parte de la gran mayoría de funcionarios sobre las políticas de adquisición de hardware.

R15 No existe documentación del proceso de mantenimiento de la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.

R16 No existe manual de funciones para el personal encargado de realizar mantenimiento preventivo y correctivo de la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.

R17 No se tiene una implementación adecuada de cableado estructurado.

R18 No se tiene planos del cableado estructurado que se extiende por la entidad.

R19 No se realiza seguimiento adecuado de los elementos como: servidores, routers y switches ya que las hojas de vida no recolectan la información necesaria.

Riesgos Dominio ENTREGAR Y DAR SOPORTE (DS)

DS12 Administración de instalaciones

R20 No existen políticas 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.

R21 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

R22 La parte de cableado de la red de datos se encuentra con cables sueltos, fuera de canaletas, no sigue un estándar definido.

R23 No existen prohibiciones para fumar, consumir alimentos y bebidas, falta suficientes carteles en lugares visibles.

R24 Con poca frecuencia se revisan y calibran los controles ambientales.

R25 No se tiene un plan de emergencia si falla los controles ambientales.

R26 No se Realizan simulacros con la planta eléctrica.

R27 No se tienen medidas implementadas en caso de falla del sistema de seguridad del área de sistemas

Riesgos Dominio MONITOREAR Y EVALUAR (ME)

ME2 Evaluar lo adecuado del control interno

R28 No existen políticas ni procedimientos que se encaminen a monitorear la seguridad de la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.

R29 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.

R30 No se realizan auditorias de ningún tipo para evaluar el desempeño de la parte eléctrica, ventilación del centro de cómputo y utilización de normas de cableado estructurado.

3.6 VALORACIÓN DE RIESGOS

Notaría 1 SNR SUPERINTENDENCIA DE NOTARIADO & REGISTRO	**VALORACIÓN DE RIESGOS**						**REF**
							VLRN_1
N°	**RIESGOS/VALORACIÓN**	**PROBABILIDAD**			**IMPACTO**		**DOMINIO**
		A	**M**	**B**	**L**	**M**	**C**
R1	No existe un grupo encargado de evaluar y estudiar el desempeño de la infraestructura tecnológica	X				**X**		PO1 (3)

R2	No existen políticas ni procedimientos relacionados con la conformación adecuada de la arquitectura de la infraestructura tecnológica	X				**X**		PO1(3)
R3	No existe un plan de la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.	**X**					**X**	PO 3(1)
R4	No hay un inventario actualizado de la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES	X				**X**		PO 3(1)
R5	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	**X**			X			PO 3(1)
R6	No se realizan simulacros con los planes de contingencia en caso de fallas de software o hardware en la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES	**X**			X			PO 3(1)

R7	No hay un cronograma de mantenimientos preventivos a la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.	X				**X**		PO3 (1)
R8	El manual de funciones del personal del área de sistemas no se actualiza con frecuencia, con sus respectivas funciones, descripción de cargo y requerimientos, personal responsable.		X		X			PO4 (6)
R9	En caso de falta del personal clave en la parte de Redes de datos no se tiene planes de contingencia para su reemplazo en caso de ausencia o no está documentado.	X					**X**	PO4(13)
R10	No existe el plan de evaluación de riesgos del área de sistemas de la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES.	**X**			**X**			PO9 (1) PO9 (3)
R11	No existe un plan de contingencia ni de seguridad para contrarrestar un evento que afecte la conexión física de la red de datos.		X				X	PO9(4) PO9(5)
R12	No se cuenta con pólizas de seguros para el manejo del riesgo		X			X		PO9(6)

R13	No existe documentación sobre las políticas de mantenimiento que se realiza a la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES		X		X			AI3 (3)
R14	No existe conocimiento por parte de la gran mayoría de funcionarios sobre las políticas de adquisición de hardware.			X	X			AI3 (1)
R15	No existe documentación del proceso de mantenimiento de la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES	**X**				X		AI3 (3)
R16	No existe manual de funciones para el personal encargado de realizar mantenimiento preventivo y correctivo de la infraestructura física de la red y de los equipos de cómputo en la NOTARÍA PRIMERA DE TÚQUERRES		**X**			X		AI3 (3)
R17	No se tiene una implementación adecuada de cableado estructurado			X		X		AI3 (3)
R18	No se tiene planos del cableado estructurado que se extiende por la entidad.			X	X			AI3 (3)

R19	No se realiza seguimiento adecuado de los elementos como: servidores, routers y switches ya que las hojas de vida no recolectan la información necesaria		X				X	AI3 (3)
R20	No existen políticas 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	X					X	DS12(2) DS12(3)
R21	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	X				X		DS12(2) DS12(3)
R22	la parte de cableado de la red de datos se encuentra con cables sueltos, fuera de canaletas, no sigue un estándar definido			X			X	DS12(1) DS12(5)
R23	No existen prohibiciones para fumar, consumir alimentos y bebidas, falta suficientes carteles en lugares visibles			X			X	DS12(5)
R24	Con poca frecuencia se revisan y calibran los controles ambientales			X	X			DS12(5)

3.7 MATRIZ DE IMPACTO CON RIESGOS ENCONTRADOS EN PROCESO

Matriz de Probabilidad e impacto

Según el MECI este componentes primordial en el desarrollo de la auditoria ya que permite determinar el nivel de riesgo de cada uno de los hallazgos encontrados, tanto cualitativa como cuantitativamente. Por medio de esta clasificación se puede observar cuál de los riegos es catastrófico, importante, moderado o aceptable y a su vez el respectivo valor del riesgo.

Probabilidad				
	Alto(3)	**Riesgo Moderado (15)**	**Riesgo Importante (30)**	**Riesgo Inaceptable (60)**
	Medio(2)	**Riesgo Tolerable (10)**	**Riesgo Moderado (20)**	**Riesgo Importante (40)**
	Bajo(1)	**Riesgo Aceptable (5)**	**Riesgo Tolerable (10)**	**Riesgo Moderado (20)**
		Bajo(leve)(5)	**Medio(moderado)(10)**	**Alto(catastrófico)(20)**
		Impacto		

4. HALLAZGOS

A continuación se describirán los hallazgos encontrados la NOTARÍA PRIMERA DE TÚQUERRES.

Dominios y Procesos Auditados en la NOTARÍA PRIMERA DE TÚQUERRES.

Los hallazgos encontrados en la NOTARÍA PRIMERA DE TÚQUERRES.

Se presentaran en el orden de los dominios y procesos auditados los cuales fueron:

Dominio - planificación 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).
- Evaluación y análisis de riesgos (PO9).

Dominio - adquisición e implementación (AI)

- 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).

4.1 MATRIZ DE PROBABILIDAD DE IMPACTO

Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso

Probabilidad				
	Alto(3)	Riesgo Moderado H5—PO3 H6—PO3 H10—PO9	Riesgo Importante: H1—PO1 H7—PO3 H2--PO1 H21-DS1 H4—PO3 H15—AI3	Riesgo Inaceptable H3—PO3 H9—PO4 H20—DS12
	Medio(2)	Riesgo Tolerable H8—PO4 H13-AI3 H28—ME2	Riesgo Moderado H12—PO9 H16—AI3 H27-DS12	Riesgo Importante H11—PO9 H19-AI3
	Bajo(1)	Riesgo Aceptable H14—AI3 H18—AI3 H24—DS12 H26—DS12	Riesgo Tolerable H17-AI3 H25-DS12	Riesgo Moderado H22—DS12 H23—DS12
		Bajo(leve)(5)	Medio(moderado)(10)	Alto(catastrófico)(20)
		Impacto		

Descripción del Formato de Hallazgos

- **ENTIDAD AUDITADA:** hace referencia al nombre de la entidad auditada.
- **REF:** cuestionario que determino el Hallazgo.
- **AREA AUDITADA:** se refiere al área de TI la cual será el objeto de estudio.
- **SISTEMA:** hace referencia al nombre del sistema actual de la entidad auditada.
- **RESPONSABLES:** hace referencia a los nombres del equipo encargado de la auditoría.

- **PROBABILIDAD:** hace referencia a la posibilidad de ocurrencia del riesgo.
- **IMPACTO:** hace referencia a las consecuencias que puede ocasionar a la entidad la materialización del riesgo.
- **DESCRIPCIÓN HALLAZGO:** se refiere a los detalles del hallazgo.
- **NIVEL DE RIESGO:** hace referencia al valor cualitativo o cuantitativo del riesgo.
- **CONSECUENCIA:** se refiere al efecto actual o futuro, que tendrá la organización, de no tomar las precauciones oportunas.
- **RECOMENDACIONES:** hace referencia a las descripciones correctivas de carácter preventivo.

Cuadro de Hallazgos:

Definir un plan estratégico de TI (PO1)

Notaría 1 SNR SUPERINTENDENCIA DE NOTARIADO & REGISTRO	**Hallazgos**	**Ref. Plan (PO)**	
Entidad Auditada:	NOTARÍA PRIMERA DE TÚQUERRES		
Área Auditada:	Sistemas	**Objeto de Estudio**	Funcionamiento de la red de datos y equipos de cómputo
Responsables: EULER REMIGIO BASANTE MORA - GILBERTH ANDREY IPAZ			
Material de Soporte: COBIT			
Dominio:	Planeación y Organización(PO)	**Proceso:**	Definir un plan estratégico de TI (PO1)
Descripción Hallazgo:			
R1. No existe un grupo encargado de evaluar y estudiar el desempeño de la infraestructura física de la red y de los equipos de cómputo en la			

NOTARIA PRIMERA DE TUQUERRES. R2. No existen políticas ni procedimientos relacionados con la conformación adecuada de la infraestructura física de la red y de los equipos de cómputo en la NOTARIA PRIMERA DE TUQUERRES	
Probabilidad :ALTA	**Impacto: MODERADO**
Nivel de Riesgo: IMPORTANTE	
Consecuencia:	
• Al no existir un grupo encargado de evaluar y estudiar el desempeño de la infraestructura física de la red y de los equipos de cómputo se pierde la claridad para tomar decisiones pertinentes. • 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 la infraestructura física de la red y de los equipos de cómputo	
Recomendaciones:	
• Conformar un grupo determinado de funcionarios que evalúen y estudien el desempeño de la infraestructura física de la red y de los equipos de cómputo para tomar decisiones oportunas y adecuadas en la eventualidad de no cumplir objetivos planteados. • Elaborar e implementar políticas y procedimientos relacionados con la conformación de la infraestructura física de la red y de los equipos de cómputo para ajustar los servicios de red a las necesidades propias que necesite la entidad	

Cuadros de Hallazgos:

Ver anexo hallazgos PO3

Ver anexo hallazgos PO4

5. INFORME EJECUTIVO

San Juan de Pasto 20 de febrero del 2016

DOCTOR:

CARLOS ARTEMIO RUANO VILLOTA

NOTARIO

REF: AUDITORIA INFORMATICA A LA INFRAESTRUCUTURA FISICA DE LA RED Y DE LOS EQUIPOS DE COMPUTO DE LA NOTARÍA PRIMERA DE TÚQUERRES

Presente.

Como es de su conocimiento la infraestructura física de la red y de los equipos de cómputo de la NOTARÍA PRIMERA DE TÚQUERRES, fue sometida a una auditoria de sistemas para evaluar su funcionalidad.

Después de realizar las pruebas sobre la infraestructura física de la red y de los equipos de cómputo de la NOTARÍA PRIMERA DE TÚQUERRES se relacionan algunos aspectos favorables generales extraídos del informe de la presente auditoría

Por lo tanto se podría decir que la infraestructura física de la red y de los equipos de cómputo de la NOTARÍA PRIMERA DE TÚQUERRES tiene un funcionamiento adecuado del 30% y el restante 70% de la red debe ser corregido y mejorado para lograr un porcentaje más alto de funcionalidad

EVALUACIÓN DEL HARDWARE DE EQUIPOS DE CÓMPUTO, DISPOSITIVOS MÓVILES Y REDES:

- no tiene un manejo adecuado de un inventario tecnológico, por lo cual es importante sugerir la creación de este inventario y mantenerlo actualizado

constantemente para llevar un control y/o registro adecuado de los activos de la entidad.

- es muy importante llevar un proceso documentado de los procesos de mantenimiento de hardware en la entidad con el fin de llevar un control de la vida útil de cada uno de los elementos tecnológicos de la NOTARÍA para futuras tomas de decisiones y mejoramientos de la empresa. la falta de mantenimiento preventivo y correctivo provoca lentitud y pérdida de hardware, generando perdida de información o peor aun cuando un equipo deja de funcionar generara más gastos.
- La NOTARÍA no maneja un sistema de actualización para los equipos existentes ni tampoco una documentación de los mismos, para lo cual se recomienda programar las actualizaciones de software que responda a las necesidades del trabajo a realizar en cada una de las sedes dependiendo de los equipos y las actualizaciones necesarias para no entorpecer las actividades diarias.

- Se recomienda mantener actualizados los planos de la red de voz y datos, donde se puede evidenciar los elementos de la red como gabinetes de comunicaciones, puestos de trabajo, puntos de red, cuellos de botella, entre otros, esto con el fin de identificar problemas y sorpresas que se pueden presentar y cambios que se pueden realizar

- no se encontró una documentación sobre cómo se lleva a cabo los procesos de adquisición de infraestructura tecnológica pero cabe resaltar que el personal está pendiente de cada una de las necesidades en cuanto a equipos necesarios y se tiene en cuenta la mejor opción a la hora de adquirir los equipos tecnológicos.

- no existe documentación de la gestión de red de comunicaciones, en caso de presentarse fallas, el no contar con planos de red, impide que se localice de manera inmediata el punto de fallo implicando pérdida de tiempo y

mayores gastos, teniendo en cuenta que los costos en materiales, mano de obra e interrupción de labores al hacer la búsqueda o hacer cambios en la infraestructura pueden ser muy altos.

Se recomienda que se cuente con un documento de gestión de red, el cual permita identificar objetivos encaminados a la monitorización del tráfico y la calidad del servicio, pautas que permitan prevenir, diagnosticar y resolver problemas de la red. Identificación de los usuarios de la red y el software, dar soporte a los usuarios, pautas de seguridad, gestión de los fallos producidos en la red, gestión de rendimiento y planificación.

Se recomienda además que los equipos activos (switche, router, etc) se acojan a la norma estándar, los equipos activos y cableados deben ser ubicados en una estructura abierta, basada en un rack o cerrada denominada gabinete.

EVALUACIÓN DE ÁREA INFORMÁTICA Y FUNCIONES DEL PERSONAL DE INFORMÁTICA:

- actualmente no se encuentra creada como tal el área de informática en la NOTARÍA PRIMERA por lo que se recomienda consolidarla con una persona encargada de esta área y de la creación y mantenimiento de todos los procesos necesarios a llevar, la persona encargada de esta área se recomienda sea una persona idónea en este campo que sepa el manejo de la infraestructura tecnológica y el manejo de los procesos para la misma, además de tener conocimientos en sistemas y procesos informáticos, ya que actualmente cuando se presentan problemas informáticos y tecnológicos el personal de la empresa debe de alguna manera buscar la solución con personal diferentes a los existentes en la empresa.

PLANES DE CONTINUIDAD

- La falta de un plan de contingencia formal expone a la entidad a fallas o interrupciones que harán que la compañía deje de prestar el servicio de calidad a sus usuarios o desestabilice el buen funcionamiento de la entidad.

- No existen usuarios y contraseñas para la identificación en el acceso al centro de cómputo del personal de la empresa y del personal exterior.

- Cualquier operario podría visualizar, modificar o eliminar la información perteneciente a la configuración de la red, generando así falta de integridad en la información.

Atentamente

EULER REMIGIO BASANTE MORA GILBERTH ANDREY IPAZ

Auditor Egresado Udenar **Auditor Egresado Udenar**

Recibí

CARLOS ARTEMIO RUANO VILLOTA_____

INFORME GENERAL DE LA AUDITORIA

Hallazgos:

REF: AUDITORIA INFORMATICA A LA INFRAESTRUCUTURA FISICA DE LA RED Y DE LOS EQUIPOS DE COMPUTO DE LA NOTARÍA PRIMERA DE TÚQUERRES

De nuestra consideración:

Nosotros, Euler Basante y Gilberth Ipaz nos dirigimos a usted para darle a conocer el dictamen preliminar de la Auditoría practicada A LA INFRAESTRUCUTURA FISICA Y DE LA RED Y DE LOS EQUIPOS DE COMPUTO DE LA NOTARÍA PRIMERA**.** La misma que se ha llevado a cabo desde el 10 de enero del 2016.

Hallazgos en la seguridad física.

- No existe un plan de la infraestructura física de la red y de los equipos de cómputo actualizado.
- No se lleva un control y una actualización del plan de la infraestructura física de la red y de los equipos de cómputo, no está documentada.
- No existe manual de funciones o procedimientos específico para los trabajadores encargados de la administración y mantenimiento de la infraestructura física de la red y de los equipos de cómputo.
- No existen dentro del manual de funciones especificaciones de requisitos mínimos que deban cumplir las personas para ocupar los cargos relacionados con el manejo de la infraestructura física de la red y de los equipos de cómputo.
- No existe un plan de contingencia que se ejecute cuando se presente ausencia de los funcionarios encargados de manejar la infraestructura física de la red y de los equipos de cómputo

- En caso de falta del personal clave en la parte de Redes de datos de LA NOTARÍA PRIMERA, no se tiene planes de contingencia para su reemplazo en caso de ausencia O no está documentado.
- No se han hecho simulacros al respecto de funcionarios clave del área de red de datos de LA NOTARÍA PRIMERA.
- No se tiene actualizado ni documentado el plan de evaluación de riesgos del área de sistemas de la infraestructura física de la red y de los equipos de cómputo de LA NOTARÍA PRIMERA.
- No existe un plan de contingencia para contrarrestar un evento que afecte la infraestructura física de la red y de los equipos de cómputo no se encuentra debidamente documentado.
- No se cuenta con pólizas de seguros para el manejo del riesgo.
- Las deficiencias en los niveles de servicio en cuanto a la red de datos de NOTARÍA PRIMERA. No están identificadas.
- No existe documentación sobre las políticas de mantenimiento que se realiza a los equipos de cómputo.
- No existe manual de funciones para el personal encargado de realizar mantenimiento preventivo y correctivo de los equipos de cómputo.
- No se tiene una implementación adecuada del centro de cómputo.
- No existe un diagrama o planos del cableado estructurado que se extiende por la entidad de la red de datos de LA NOTARÍA PRIMERA.
- No se realiza seguimiento adecuado de los elementos como: servidores, routers y switches ya que las hojas de vida no recolectan la información necesaria.
- 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.

- Existe una parte de cableado de la red de datos que se encuentra con cables sueltos, fuera de canaletas, no sigue un estándar definido.

Recomendaciones:

De acuerdo a las falencias encontradas con respecto al Hardware, se

Expone las siguientes recomendaciones:

- Conformar un grupo determinado de funcionarios que evalúen y estudien el desempeño de la infraestructura física de la red y de los equipos de cómputo.
- Elaborar e implementar políticas y procedimientos de la infraestructura física de la red y de los equipos de cómputo.
- Llevar un inventario documentado y actualizado de la infraestructura física de la red y de los equipos de cómputo.
- Documentar los cambios o mejoras al plan de la infraestructura física de la red y de los equipos de cómputo.
- Elaborar el manual de funciones o procedimientos específicos para los trabajadores encargados del manejo y administración de la infraestructura física de la red y de los equipos de cómputo.
- Elaborar un plan de contingencia que subsane la ausencia del personal encargado del manejo de la infraestructura física de la red y de los equipos de cómputo.
- Tener planes de contingencia para el reemplazo del personal clave en la parte de Redes de datos en LA NOTARÍA PRIMERA, para así evitar contratiempos, en cuanto al reemplazo y demoras en el sistema de la red de datos.
- Elaborar políticas y procedimientos para el análisis y evaluación de riesgos del área de sistemas en la infraestructura física de la red y de los equipos de cómputo.

- Obtener pólizas de seguros para el manejo del riesgo, tanto para personal como para la infraestructura física de la red y de los equipos de cómputo, para así tener un respaldo en caso de accidentes fortuitos que se puedan presentar dentro de la NOTARÍA PRIMERA.
- Documentar las políticas de adquisición de la infraestructura física de la red y de los equipos de cómputo
- Realizar capacitaciones para los usuarios de la red.
- 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.
- 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.
- 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 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 y Documentar 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.
- Documentar los puntos de cableado donde se está encontrando daños, para saber el motivo que lo provoca y verificar si en ese punto se está realizando un posible sabotaje de la red.

- 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.
- Documentar las políticas para seguridad de la red física de datos y con ello utilizar esta información como herramienta ágil para ejecutar este proceso.
- Realizar auditorías de la infraestructura física de la red y de los equipos de cómputo 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

Con el desarrollo de este trabajo de grado se logró auditar lo referente a la infraestructura física de la red y de los equipos de cómputo de LA NOTARÍA PRIMERA identificando los riesgos y amenazas que presentan.

La auditoría que se realizó siguió el modelo de auditoria cobit, entrevistas a los ingenieros, administradores, aplicación de cuestionarios.

El presente trabajo realizado en la NOTARÍA PRIMERA DE TÚQUERRES reveló la situación actual en la que se encuentra.

Una vez aplicado el análisis de riesgos a los recursos la NOTARÍA PRIMERA DE TÚQUERRES se pudo conocer las amenazas, vulnerabilidades, que probabilidades hay de que ocurra, el nivel de riesgo al que está sujeto los recursos informáticos y nivel de impacto que ocasionaría cumpliendo con los objetivos impuestos en el inicio del proyecto

Los hallazgos de auditoria, cuestionarios de control interno, entrevistas y pruebas han sido herramientas apropiadas para la obtención de resultados que muestran las falencias a ser consideradas dentro del mejoramiento constante de la NOTARÍA PRIMERA DE TÚQUERRES

Se ha aportado una visión sobre la importancia de la AUDITORIA Y SEGURIDAD EN SISTEMAS centrándonos en la *infraestructura física de la red y de los equipos de cómputo de LA NOTARÍA PRIMERA*. Respecto al tiempo dedicado para realizar este trabajo no podemos estimar con precisión las horas invertidas puesto que ha habido meses en los que hemos dedicado gran cantidad de horas y otros que por diversos motivos, no han sido tantas como hubiésemos querido.

- La auditoría realiza 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 auditoría de sistemas es una herramienta la cual nos permite conocer de manera profunda el funcionamiento de cualquier empresa o área la cual se objetó de nuestro estudio.
- En LA NOTARÍA PRIMERA desde EL NOTARIO hasta los funcionarios de la entidad son conscientes de que existen falencias las cuales quedan demostradas en este estudio..
- En LA NOTARÍA PRIMERA se debe de dar mayor prioridad al Área de sistemas por ser esta un pilar fundamental en todos los procesos que se realizan en la entidad.
- Se deja a disposición de LA NOTARÍA PRIMERA los hallazgos y recomendaciones, las cuales son necesarias para continuar con el proceso de mejoramiento.
- Se debe buscar el mejoramiento continuo de la entidad por medio de nuevas auditorías a otras áreas.

RECOMENDACIONES

Como parte del proceso de control interno de toda entidad se debe realizar planificaciones y programas de auditoría de gestión que permitan evaluar los procedimientos de cada departamento, áreas y unidades, con la finalidad de establecer estrategias y mejoras en la calidad.

- Desarrollar indicadores que permitan evaluar el cumplimiento de metas y objetivos de cada agencia y de la Institución.
- Implementar indicadores de gestión de calidad y productividad que permitan disminuir los costos de no calidad, mejorar el servicio y elevar la productividad del personal.
- Es importante cuantificar la pérdida de tiempo que un empleado genera en su labor diaria a través de los resultados que arrojen los indicadores de gestión de la productividad.
- Se debe desarrollar planes y programas para establecerse como piñonera en el sistema mutual, a través de la creación de productos y servicios innovadores.
- Desarrollar auditorias de gestión continuas que permitan validar y evaluar la calidad de los procesos y los servicios.
- Implementar indicadores de productividad que permitan determinar indicadores de calidad del servicio y la satisfacción del cliente
- Realizar encuestas de medición y monitoreo, las cuales servirán como herramientas para recolección de los indicadores de gestión

BIBLIOGRAFIA

- 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.
- INGENIERO FRANCISCO NICOLAS SOLARTE SOLARTE. (Septiembre de 2010) Auditoria Informática y de Sistemas. Retrieved from http://auditordesistemas.blogspot.com/
- Murillo, Enrique (26 de marzo de 2013). «La Función del Auditor» (en español). AOB News. Consultado el 26 de marzo de 2013. Retrieved from. http://es.wikipedia.org/wiki/Auditor
- 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
- ROBERTO GÓMEZ LÓPEZ. Doctor en Economía (Dirección y Administración de Empresas). Retrieved from
- http://ucapanama.org/wp-content/uploads/2011/12/Generalidades-en-la-Auditoria.pdf.

BIBLIOWEB

- ISACA, COBIT 4.1 Castellano (En línea). En: ISACA Colombia (Bogotá). Disponible en la dirección electrónica: http://www.isaca-bogota.net/metodologias/cobit.aspx 281
- PARRA GALVIS, Andrés Felipe. Auditoria de sistemas de información (en línea). En: Guía Laboral Gerencie 2009: Agosto 27, 2008. Disponible en la dirección electrónica: http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html
- WIKIPEDIA. Objetivos de control para la información y tecnologías relacionadas (En línea). En: Wikipedia La enciclopedia Libre. Disponible en la dirección electrónica: http://es.wikipedia.org/wiki/COBIT
- http://www.monografias.com/trabajos39/la-auditoria/la-auditoria.shtml
- http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

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.

Administración: Elementos del proceso administrativo: previsión, planeación, organización, integración, dirección y control.

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: 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.

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.

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

COBIT (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, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

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.

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.

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

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

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.

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

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.

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.

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.

Software: Componentes inmateriales del computador como 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.

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.

ANEXOS

Remitirse al soporte de medio magnético CD o a la memoria USB para revisar los anexos.

- Anexos cuestionarios y entrevistas
- Anexos cuantitativos
- Anexos de control
- Anexos de hallazgos
- Anexos 1 fotografías
- Anexos 2 cuestionarios
- Anexos 3 entrevistas audio