PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE ESMERALDAS



ESCUELA INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TÉSIS DE GRADO

TEMA: "EVALUACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA BASADO EN ESTÁNDARES DE CONTROL INTERNO CASO: EMPRESA NATIONALTIRE EXPERTS S.A"

PREVIO OBTENCIÓN DEL TÍTULO DE

INGENIERO EN SISTEMAS Y COMPUTACIÓN

AUTOR:

YNGE VANESSA CEDEÑO RODRÍGUEZ

ASESOR:

ING. SUSANA PATIÑO

ESMERALDAS, 2017

Trabajo de Tesis Aprobado luego de haber dado
Cumplimiento a los requisitos exigidos por el Reglamento
De Grado de la PUCESE previa obtención del título de
INGENIERO EN SISTEMAS Y COMPUTACIÓN

_____

Presidente de Tribunal de Graduación

_____

Lector 1

_____

Lector 2

_____

Director de Escuela

_____

Director de Tesis

_____

Fecha

Esmeraldas, 24 de mayo del 2017

AUTORÍA

Yo, Ynge Vanessa Cedeño Rodríguez portadora de C.I# 080236438-0 declaro que este trabajo de titulación **"EVALUACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA BASADO EN ESTÁNDARES DE CONTROL INTERNO CASO: EMPRESA NATIONAL TIRE EXPERTS S.A"** es de mi autoría, en virtud de ello me responsabilizo de su contenido, veracidad, respetando los derechos intelectuales de terceros, al mismo tiempo cedo mis derechos de propiedad intelectual a la Pontificia Universidad Católica del Ecuador sede Esmeraldas PUCESE según lo establecido por la Ley de Propiedad Intelectual vigente.

_____

Vanessa Cedeño Rodríguez

CI#082364380

DEDICATORIA

Dedico este trabajo, a mis hijos que constituyen parte importante de mi vida y apoyo para seguir adelante, a mi Madre que siempre con su apoyo y dedicación me ha guiado con sus incentivos y consejos en la culminación de mis metas especialmente esta. Los amo.

AGRADECIMIENTO

Agradezco enormemente a mi Dios que siempre me guía, y que está presente en todo lo que realizo, en cada uno de mis pasos llenándome de fortaleza con su amor incondicional, a mis padres amados, a mi esposo e hijos que son mi orgullo, sin ellos no soy nada.

A mis profesores que me dieron todos los conocimientos que he adquirido a lo largo de esta carrera, y por los que hoy soy una profesional, y a mi asesora Ing. Susana gracias por su paciencia, asesoría y orientación.

A la empresa National Tire Experts S.A, por darme toda su ayuda en la realización de esta investigación, que espero sirva para impulsar más su desarrollo en el mercado, y me alegra ser parte de ello, gracias por haberme hecho parte de la gran familia que es Tire Experts.

RESUMEN

El presente proyecto efectúa una evaluación de los procesos de control interno del área de TI y su manejo dentro de la empresa. El mismo sugiere implementar un modelo de gestión, en el cual se determinan los niveles de eficacia y cumplimiento de los procesos.

Su ejecución propone la aplicabilidad de un marco metodológico a través de objetivos de control para Información y Tecnologías Relacionadas (COBIT 5), estableciendo estrategias que permitan la evolución de los procesos e implementación de nuevas políticas en el mejoramiento de la infraestructura de TI y redistribución eficiente de los recursos.

Se pudo identificar los puntos críticos que afectan la infraestructura tecnológica de la organización a través de una matriz de riesgos e investigación de campo en base a encuestas, entrevista y guía de observación, obteniendo una percepción global de sus fortalezas y debilidades.

En base a estos hallazgos obtenidos de la evaluación, se llegó a la conclusión que la empresa no cumple con todos los lineamientos de gestión y mantenimiento de la infraestructura de TI, acarreando riesgos altos y niveles de confianza mínimos.

Finalmente gracias a la aplicación de Cobit se plantearon estrategias a través de la aplicación de normativas que permitirán a la empresa alcanzar una transformación óptima en la administración y gestión de los procesos de TI, minimizando riesgos en la infraestructura.

Palabras clave: EVALUACIÓN, INFRAESTRUCTURA TECNOLÓGICA, ESTÁNDARES DE CONTROL INTERNO, COBIT.

ABSTRACT

This project carries out an evaluation of the internal control processes of the IT area and its management within the company. It suggests implementing a management model, in which the levels of effectiveness and compliance of the processes are determined.

Its execution proposes the applicability of a methodological framework through control objectives for Information and Related Technologies (COBIT 5), establishing strategies that allow the evolution of the processes and implementation of new policies in the improvement of the IT infrastructure and efficient redistribution of the resources.

It was possible to identify the critical points that affect the organization's technological infrastructure through a risk matrix and field research based on surveys, interview and observation guide, obtaining a global perception of its strengths and weaknesses.

Based on these findings from the evaluation, it was concluded that the company does not comply with all the management and maintenance guidelines of the IT infrastructure, entailing high risks and minimum levels of confidence.

Finally, thanks to the application of Cobit, strategies were proposed through the application of regulations that will allow the company to achieve an optimal transformation in the administration and management of IT processes, minimizing risks in the infrastructure.

Keywords: EVALUATION, TECHNOLOGICAL INFRASTRUCTURE, INTERNAL CONTROL STANDARDS, COBIT.

TABLA DE CONTENIDO

APROBACION MIEMBROS DEL TRIBUNAL……I
AUTORÍA……II
DEDICATORIA…,……..III
AGRADECIMIENTO……..IV
RESUMEN……V
ABSTRACT……VI
INTRODUCCIÓN I
Presentación de la Investigación 1
Planteamiento del Problema.....2
Justificación 3
Objetivos.....5
CAPITULO I 6
MARCO DE REFERENCIA 6
1.1. Antecedentes 6
1.2. Bases teóricas científicas.....8
1.2.1 Auditoría Informática 8
1.2.1.1 Factores que influyen en una Auditoría Informática.....8
1.2.2 Infraestructura Tecnológica.....9
1.2.2.1 Definición.....9
1.2.3 ¿Qué es el Gobierno de TI? 10
1.2.3.1 Evaluación del gobierno del TI en las Empresas 10
1.2.4 Control Interno 10
1.2.5 Seguridad de la información.....11
1.2.5.1 Sistema de gestión de seguridad (SGSI).....11
1.2.5.2 Fundamentos ISO 27001 y su aplicación en las empresas 11
1.2.6 COBIT (Control Objectives for Information and related Technology).....12
1.2.6.1 Transición de COBIT de la V4.1 a la V5.0.....13
1.2.6.2 Objetivos de Control COBIT 5.0.....14
1.2.6.3. Atributos de Capacidad de Procesos……..15
1.2.6.4. Mapeo de Metas y Procesos relacionados con las TI…….16
1.2.7 El Riesgo…….18
1.2.7.1. Matriz de Riesgos.....18
1.2.7.2 Indicadores de Riesgo.....19
1.2.7.3 Aplicación de la Matriz de Riesgo.....21
CAPITULO II 24

2. MATERIALES Y MÉTODOS.....24
2.1. Descripción del lugar.....24
2.2. Métodos y Técnicas que se emplearon 25
2.3. Población y Muestra de estudio 25
2.4 Técnicas de procesamiento y análisis estadístico de datos empleados 27
2.5. Normas éticas 27
CAPÌTULO III.....28
RESULTADOS.....28
3.1 Análisis e Interpretación de Datos 28
3.2. Análisis e interpretación de resultados de la encuesta 31
4.1.2 Análisis de la Entrevista y Guía de Observación 32
CAPÍTULO IV.....34
4. PROPUESTA.....34
4.1 Informe de Evaluación de la Infraestructura de TI.....34
4.1.1 Ubicación.....34
4.1.2 Organigrama Estructural.....34
4.1.3 Recurso Humano.....35
4.1.4 Infraestructura de TI.....35
4.1.5 Seguridad Física y Lógica.....38
4.1.6 Redes y Comunicaciones.....40
4.1.8 Servicio Web e Internet.....41
4.1.9 Topología de Red.....42
4.1.10 Detección de problemas de infraestructura.....42
4.2 Definición del Marco de Control Interno para evaluar los procesos tecnológicos 43
4.2.1 Marcos Metodológicos y Estándares de Control Interno Tecnológico.....43
4.2.2 Evaluación de los Objetivos de Control de COBIT 5.0 en relación con la empresa National Tire Experts S.A.....44
4.2.3. Objetivos corporativos vs objetivos de negocio.....45
4.2.4 Determinación del nivel de madurez de los procesos del área de TI de la Empresa National Tire Experts S.A 49
4.2.4.1 Dominio: Evaluar, Orientar y Supervisar (EDM) 49
4.2.4.2 Dominio: Alinear, Planear y Organizar (APO).....50
4.2.4.3 Dominio: Construir, Adquirir y Operar (BAI).....52
4.2.4.4 Dominio: Entregar Servicio y Soporte (DSS).....53
4.2.4.5 Dominio: Monitorear, Evaluar y Valorar (MEA) 54
4.5.1 Análisis de evaluación de Riesgos.....56
4.6 Estrategias de Implementación.....66

4.6.1 Estrategia de Implementación 1: Definir un Plan Estratégico de TI 66
4.6.2 Estrategia de Implementación 2: Asegurar la Capacitación y el Soporte a Usuarios .67
4.6.3 Estrategia de Implementación 3: Definir el modelo de Gobierno 68
4.6.4 Estrategia de Implementación 4: Definir normativas y procesos de TI.....69
4.6.5 Estrategia de Implementación 5: Implementar Gestión de Riesgos de TI.....70
4.6.6 Estrategia de Implementación 6: Implementación de la gestión Continuidad del Negocio 71
4.6.7 Estrategia de Implementación 7: Implementación de herramientas automatizadas de TI.....72
4.6.8 Diseño de un propuesta de una Topología de Red……74
4.7 Informe Final de Evaluación de Infraestructura...……..75
4.7.1 Alcance…..……..75
4.7.2 Metodología…-..……75
4.7.3 Evidencias Encontradas……...76
4.7.3.1 Proceso EDM: Evaluar, Orientar y Supervisar……..….76
4.7.3.2 Proceso APO: Alinear, Planear y Organizar……..……...……..77
4.7.3.3 Proceso BAI: Construir, Adquirir y Operar……...…….78
4.7.3.4 Proceso DSS: Entregar, Servicio y Soporte……..……...…….78
4.7.3.5 Proceso MEA: Monitorear, Evaluar y Valorar…...……...……...79
4.7.4 Estrategias o Plan de Acción…....……..…….…..80
4.7.4.1 Definir un Plan Estratégico de TI 80
4.7.4.2 Asegurar la Capacitación y el Soporte a Usuarios 80
4.7.4.3 Definir el modelo de Gobierno 81
4.7.4.4 Definir normativas y procesos de TI.....81
4.7.4.5 Implementar Gestión de Riesgos de TI.....81
4.7.4.6 Implementación de la gestión Continuidad del Negocio.....82
4.7.4.7 Implementación de herramientas automatizadas de TI 82
CAPITULO 5.....83
5. CONCLUSIONES Y RECOMENDACIONES 83
5.1 Conclusiones 83
5.2 Recomendaciones.....84
6. REFERENCIAS.....85
ANEXO A: Encuesta a los empleados Administrativos de la Empresa National Tire Experts S.A
ANEXO B1: Entrevista al encargado del departamento informático de la Empresa National Tire Experts S.A
ANEXO B2: Guía de Observación

ÍNDICE DE TABLAS

TABLA 1. NIVELES DE CAPACIDAD DE PROCESOS COBIT……...15
TABLA 2.MAPA DE MATRIZ DE RIESGOS……..…….....20
TABLA 3.RIESGOS DE ENTORNO……...…….……...……..…21
TABLA 4 RIESGOS DE TALENTO HUMANO……...…….....21
TABLA 5. RIESGOS FISICOS……..…….....21
TABLA 6. RIESGOS DE PROCESOS INTERNOS…….....22
TABLA 7. RIESGOS DE SEGURIDAD……...…….……....22
TABLA 8. RIESGOS DE INFRAESTRUCTURA TECNOLOGICA…….....23
TABLA 9.DISPOSITIVOS DE INFRAESTRUCTURA DE TI OFICINA MATRIZ…….....35
TABLA 10. DISPOSITIVOS DE INFRAESTRUCTURA DE TI SUCURSALES…….....37
TABLA 11.CUADRO COMPARATIVO DE MARCO METODOLÓGICO…….....43
TABLA 12.OBJETIVOS COMPARATIVOS VS OBJETIVOS DE NEGOCIO…….....45
TABLA 13. MAPEO ENTRE OBJETIVOS RELACIONADOS CON TI EN COBIT 5 CON PROCESOS 46
TABLA 14. ANÁLISIS DE OBJETIVOS DE DOMINIO EVALUAR, ORIENTAR Y SUPERVISAR (EDM)…….49
TABLA 15. TABLA 14.1 .ANÁLISIS DE OBJETIVOS DE DOMINIO ALINEAR, PLANEAR Y ORGANIZAR (APO)……...……...……50
TABLA 14. 2 ANÁLISIS DE OBJETIVOS DE DOMINIO CONSTRUIR, ADQUIRIR Y OPERAR (BAI)…….....…...……...……...52
TABLA 14.3 ANÁLISIS DE OBJETIVOS DE DOMINIO ENTREGAR SERVICIO Y SOPORTE (DSS)……..…….... 53
TABLA 14.4. ANÁLISIS DE OBJETIVOS DE DOMINIO MONITOREAR, EVALUAR Y VALORAR (MEA)……..…….....54
TABLA 15. NIVEL DE RIESGOS SEGÚN PROCESOS DE CONTROL COBIT…….…... 56
TABLA 16. MATRIZ DE RIESGO EMPRESA NATIONAL TIRE EXPERTS S.A……...58
TABLA 16.1.ACTIVIDADES DE ESTRATEGIAS DE IMPLEMENTACIÓN 1: DEFINIR UN PLAN ESTRATÉGICO DE TI……..…67
TABLA 16.2. ACTIVIDADES ESTRATEGIA DE IMPLEMENTACIÓN 2: ASEGURAR LA CAPACITACIÓN Y EL SOPORTE A USUARIOS…..…… ……..……68
TABLA 16.3.ACTIVIDADES ESTRATEGIA DE IMPLEMENTACIÓN 3: DEFINIR EL MODELO DE GOBIERNO……...……...69
TABLA 16.4 .ACTIVIDADES ESTRATEGIA DE IMPLEMENTACIÓN 4: DEFINIR NORMATIVAS Y PROCESOS DE TI.....70
TABLA 16.5.ACTIVIDADES ESTRATEGIA DE IMPLEMENTACIÓN 5: IMPLEMENTAR GESTIÓN DE RIESGOS DE TI……..……..…71
TABLA 16.6.ACTIVIDADES ESTRATEGIA DE IMPLEMENTACIÓN 6: DE LA GESTIÓN CONTINUIDAD DEL NEGOCIO.....72

TABLA 16.7.ACTIVIDADES ESTRATEGIA DE IMPLEMENTACIÓN 7: DE HERRAMIENTAS AUTOMATIZADAS DE TI.....73

INDICE DE GRÁFICOS

GRAFICO 1. ESTADO DE LOS EQUIPOS COMPUTACIONALES DE NATIONALTIRE EXPERTS.....28
GRAFICO 2 . TIEMPO DE RESPUESTA A INCIDENCIAS DE LOS EQUIPOS 29
GRAFICO 3 . VELOCIDAD DEL SERVICIO DE INTERNET 30
GRAFICO 4. NIVEL DEL SERVICIO DE TI 30
GRAFICO 5. NIVEL DE SERVICIO DE CAPACITACIÓN A USUARIOS 31

INDICE DE FIGURAS

FIGURA 1. MODELO DE REFERENCIA DE COBIT 5.....14
FIGURA 2. ATRIBUTOS DE CAPACIDAD DE PROCESOS 16
FIGURA 3 MAPEO ENTRE METAS CORPORATIVAS DE COBIT 5 Y METAS RELACIONADAS CON TI 17
FIGURA 4. MAPA DE LOCALIDADES 24
FIGURA 5. ECUACIÓN NO PROBABILÍSTICA 26
FIGURA 6. ORGANIGRAMA DE LA EMPRESA NATIONAL TIRE EXPERTS S.A.....34
FIGURA 7. PÁGINA CORPORATIVA NATIONAL TIRE EXPERTS S.A.....41
FIGURA 7. TOPOLOGÍA DE RED NATIONAL TIRE EXPERTS S.A.....42
FIGURA 8. TOPOLOGÍA DE RED PROPUESTA PARA LA EMPRESA NATIONAL TIRE EXPERTS S.A.....74

INTRODUCCIÓN

Presentación de la Investigación

La organización administrativa de las empresas está definida la gran parte del tiempo por Sistemas Informáticos, debido al tipo de información que se maneja, se administra y se gestiona. Para evitar ser vulnerables a pérdidas de datos, infiltraciones es necesaria su automatización buscando herramientas como la auditoria que ayuden en el control y seguridad de la gestión de TI (Tecnologías de la Información). (Achina, 2015)

En este enfoque, se puede mencionar que la auditoría es capaz de identificar y/o evaluar los procesos de una organización, creando estrategias que permitan una reorganización de los mismos de forma efectiva. Con el fin de determinar cómo se distribuyen los recursos con los que cuenta, y emitir soluciones.

En muchos casos la auditoria no es tomada como una inversión, sino como un gasto. En consecuencia, el cuidado, mantenimiento y control de los procesos tecnológicos de la organización pasa a segundo plano produciéndose consecuencias irreparables. Por ende se debe aplicar medidas preventivas que sean debidamente difundidas, para no permitir que existan pérdidas económicas que incidan fuertemente en el desarrollo de los procesos de las instituciones. (Gómez, 2013)

La implementación de metodologías de control permite la verificación y valoración de los sistemas, procedimientos informáticos, así como también el uso, efectividad y protección de equipos, para una acertada toma de decisiones.

La aplicación de un marco metodológico como COBIT, proporciona las directrices necesarias para identificar los requerimientos de los procesos de control, ayuda al perfeccionamiento de los mismos, mejorando la infraestructura, la calidad del servicio y el éxito en el cumplimiento de las metas la organización. (Isaca, 2008)

Además, este proyecto presenta una visión estratégica de cómo evolucionan tecnológicamente los procesos, y se mejora el rendimiento de las empresas. Con el fin de reestructurar las funciones, reducir costos y ofrecer lineamientos que permitan brindar un servicio de calidad.

Planteamiento del Problema

Las TIC`s juegan un papel primordial en las organizaciones debido a que su implementación requiere tanto de preparación como de la adquisición de infraestructura, fomentando la rentabilidad de las mismas. (Peirano y Suárez, 2005)

En la empresa National Tire Experts S.A, la infraestructura del área tecnológica es limitada, no está ligada a estándares que le ayuden a una administración efectiva de sus procesos. Así mismo, no posee políticas claras en cuanto al manejo y seguridad, lo que preocupa enormemente a sus directivos ya que la información es relevante para el crecimiento de la organización.

Debido a que es una empresa dedicada a la comercialización de neumáticos y servicios automotrices, y aunque posee un renombre a nivel nacional e internacional, el no contar con la tecnología adecuada ha provocado, incremento de riesgos, disminución del rendimiento operativo y la pérdida de competitividad en el mercado automotriz.

Por este motivo, pone en consideración que uno de los puntos de mayor relevancia para el crecimiento del negocio, es la inserción de la tecnología, aplicando normativas y metodologías nuevas que permitirán evaluar la forma en que se realiza la gestión de la información, identificando los niveles de eficiencia en los procesos de control que actualmente manejan y si estos serán o no los adecuados.

Para ello existen estándares metodológicos que garantizan políticas aplicadas a los procesos de auditoría de los cuales se pueden mencionar: ITIL (Information Technology Infrastructure Library), COSO (Committee of Sponsoring Organizations), COBIT (Control Objectives for Information and related Technology), ISO 27000.

Mediante un análisis previo se determinará cuál de ellos podrá ser aplicado para la solución de esta problemática, con el fin de proponer estrategias, encontrar una mejor solución y realizar una valoración de la infraestructura tecnológica del área de TI de la organización.

JUSTIFICACIÓN

Debido al avance que existe en el mundo, respecto a la ejecución de herramientas tecnológicas para la automatización de procesos, ya sea en instituciones gubernamentales y/o particulares, nace la exigencia de que a menudo estos sean incluidos en sus empresas para obtener una mejora en los procedimientos de los diferentes departamentos y adentrarse en el mundo de la tecnología.

Para garantizar una gestión eficaz de los recursos existe un elemento primordial, que es precisamente; el poseer información en el momento oportuno, que a su vez sea completa y confiable. Al mismo tiempo mejorar la calidad de los servicios y adecuarse constantemente al entorno que le rodea, tomando en consideración que la empresa debe encontrarse siempre en un nivel competitivo en el uso de tecnologías, con herramientas que maximicen sus recursos (Redondo, Llopart, y Duran, 1996).

Además será de mucha importancia debido a que se identificarán las fortalezas, oportunidades, debilidades y amenazas que tiene la empresa, proporcionando así los elementos necesarios para mantener una optimización de tiempo y recursos eficiente, haciendo que los procedimientos sean proactivos y evitar la reducción del rendimiento operativo.

De igual forma, llevando un buen manejo de la información, de la red y del sistema, la organización puede superar los retrasos en los tiempos de respuesta propiciando una mayor productividad, contrarrestando las dificultades y sobre todo reforzando el ambiente tecnológico planteando acciones estratégicas del negocio. (Hernández, 2010, p. 34)

Por medio de la elaboración de esta evaluación se pretende determinar la eficiencia de los procesos, de los recursos, de la información de la empresa, del nivel de rendimiento tecnológico y administrativo de la misma, vigilando el debido procesamiento y almacenamiento de la información, mediante uso de tecnologías que son necesarias para el desarrollo de las TI en la empresa.

Conviene subrayar que la metodología que se aplica en este proyecto sugiere emplear los recursos mediante la aplicación de estándares de control y buenas prácticas como: COBIT,

ITIL, ISO/IEC 27002. De esta manera se puedan definir los riesgos y mejorar el desempeño de los procesos proporcionando un gobierno de TI eficiente, que brinde ventajas competitivas de negocio asegurando la calidad y seguridad de la información.

Renovar la administración de los procedimientos con calidad de servicio constituye a COBIT 5 como soporte en el avance de la metodología a proponer. Es vital que las necesidades que existen en la empresa, incrementen las deficiencias que evitan el óptimo desarrollo de un proyecto, organización y administración de las tecnologías y así lograr un estándar de calidad tecnológica, gestionando los mejores intereses para el beneficio del negocio.

OBJETIVOS

Objetivo General

Evaluar la Infraestructura tecnológica de la Empresa National Tire Experts S.A mediante un análisis de riesgo aplicado a los servicios tecnológicos.

Objetivos Específicos

- ✓ Detallar el marco y estándares de control interno tecnológico.
- ✓ Medir la calidad del servicio mediante la aplicación de una encuesta de nivel de satisfacción a los empleados de National Tire Experts S.A
- ✓ Utilizar un marco de control interno para la evaluación de los procesos tecnológicos.
- ✓ Describir las estrategias de implementación mediante la presentación de un informe de auditoría.

CAPITULO I

MARCO DE REFERENCIA

1.1. Antecedentes

Junto con la evolución de las tecnologías de la información han surgido necesidades en distintos sectores empresariales. Así, estas tecnologías se han convertido en elementos esenciales para la automatización de procesos tecnológicos y para el cumplimiento de las metas proyectadas por las organizaciones.

Se considera que varias organizaciones reconocen los grandes beneficios de las TI, pero también conocen que es necesario controlar y administrar todos los riesgos que se lleguen a manifestar. (Estrella y Alvear, 2013)

Por otro lado, es bueno tener presente que los riesgos empresariales no solo provienen del exterior de la entidad, sino que además pueden localizarse internamente, en gran parte producidos por el manejo descuidado de las actividades administrativas y el descontento de las operativas. (Vega, 2006)

El aporte potencial que la tecnología ha brindado a las organizaciones, ha modificado la forma en la que se desarrollan en el mercado, manifestándose innovaciones significativas adaptándola de forma rápida y eficaz a los cambios. Además, la optimización de los procesos de trabajo, contribuyen al desarrollo del modelo empresarial haciendo imprescindible la implementación de auditorías. (Villardefrancos y Rivera, 2006)

Al escuchar sobre auditoria se puede precisar, en muchos casos que está vinculado con procesos contables, de los cuales se derivan diversos modelos, normas y estándares de auditoría. Dichas normas han ayudado a las instituciones a medir el peligro o vulnerabilidad de sus procedimientos de control, mejorando su infraestructura organizacional y sobre todo efectivizando sus recursos tecnológicos. (Vega, 2006)

Hay que destacar que en muchos estudios las empresas han optado por realizar la autogestión de sus procesos, integrando auditorías internas y de forma permanente, debido a que el costo que implica la contratación de auditorías externas es elevado.

Como Gaita y Reinaudi (2012) enfatizan en su estudio, que la implementación de la auditoría interna permite detectar errores, de los cuales efectúen acciones correctivas garantizando la integridad, conservación de sus sistemas de gestión, veracidad y seguridad de la información.

Existen muchos estándares para la gestión de la infraestructura interna que ayudan a obtener un mejor desempeño en el área de TI, los cuales focalizan los sectores de mayor riesgo, reorganizando sus funciones. Así mismo, en algunos estudios se recomienda que a través de la aplicación de Outsoursing, se pueda medir el grado de satisfacción del usuario y mejorar la productividad de las entidades. (Analuisa y Erazo (2007); Rivera y Zambrano (2015))

Se evidencian en otras auditorias informáticas, como la desarrollada por Pirela (2005), que a pesar de tener ciertos procesos y funciones bien definidos, el departamento de TI no posee un sistema de gestión que le ayude a efectivizar el control de sus actividades. Por esto, elaboró un análisis de control de riesgos que permitió mejorar sus tiempos de respuesta y la calidad de servicios que presta, con la ayuda de Cobit como herramienta metodológica.

Muchas empresas en el ámbito nacional e internacional desconocen si un proceso está alcanzando los requerimientos necesarios en base a la comparación de sus prácticas de control contra empresas similares.

Por esto considerando que COBIT es una herramienta para el control interno y debido a su versatilidad ha sido adoptado por muchas organizaciones. Sus normativas ayudan a fortalecer las funciones empresariales produciendo concordancia y equilibrio entre los procesos con la finalidad de alcanzar sus objetivos. (Rivera y Zambrano, 2015)

1.2. BASES TEÓRICAS CIENTÍFICAS

1.2.1 Auditoría Informática

Su actividad principal es la de proporcionar lineamientos que ayuden al desarrollo de la funcionalidad de las áreas de una empresa que permitan la reducción de costos, aumentar la rentabilidad y obtener beneficios mediante la valoración de procesos administrativos institucionales. (Vega, 2006, pág. 6)

A la auditoria informática se la puede tomar como un análisis minucioso que tiene como finalidad reestructurar los procesos en cuestión de eficacia, rendimiento y salvaguardando la correcta utilización de la información de una sección, un organismo o una entidad.

La verificación del cumplimiento de especificaciones o procesos permite obtener una visión global de la situación interna de las organizaciones, a través de técnicas que identifiquen si son aplicados correctamente y cumplen con las metas propuestas, que impidan correr riesgos permanentes ocasionando pérdidas sustanciales que impidan su desarrollo.

1.2.1.1 Factores que influyen en una Auditoría Informática

Según lo que define Villardefrancos y Rivera (2006) se puede analizar que los puntos con mayor influencia en la auditoria informática son:

- ✓ Leyes gubernamentales.
- ✓ Políticas internas de la empresa.
- ✓ Gestión de la utilización de equipos computacionales.
- ✓ Altos costos debido a errores.
- ✓ Pérdida de información y de capacidades de procesamiento de datos, aumentando así la posibilidad de toma de decisiones incorrectas.
- ✓ Valor del hardware, software y personal.
- ✓ Necesidad de mantener la privacidad y confidencialidad de las transacciones de la entidad.

Estos factores deben ser tomados en consideración antes de realizar una auditoría para evitar un efecto negativo en la organización, proporcionando una retroalimentación de los procesos, usando su influencia negativa en favor de la misma a través de estrategias.

1.2.2 Infraestructura Tecnológica

1.2.2.1 Definición

La infraestructura de TI, se define como los recursos adquiridos por una empresa con el fin de mejorar la funcionalidad de sus procesos, adaptados a los requerimientos del mismo, ajustando un presupuesto destinado por la administración, brindando servicios de calidad, midiendo el incremento de las capacidades tecnológicas y operativas de la empresa. (Leal y Bermúdez, 2006)

Se puede considerar que la infraestructura tecnologica ayuda a las empresas a utilizar adecuadamente la tecnologia, apoyandose en las plataformas existentes, además brinda servicios entre equipos y aplicaciones, logrando que estos dispositivos funcionen en forma estructurada y organizada, reduciendo los costos y sobre todo potencializando los recursos que poseen las organizaciónes.

Ofreciendo servicios tales como:

- Administración de dispositivos mediante plataformas tecnológicas permitiendo la conexión de departamentos y usuarios dentro del ambiente digital.
- Conectividad que brinda la comunicación entre los diferentes usuarios de la empresa por medio de interconexión de datos, voz, videos, etc.
- Seguridad de los datos, a través de la administración de respaldos, manejo adecuado de la información y resguardo de los mismos
- Capacitación en el manejo de recursos tecnológicos (uso de sistemas, manejo de equipos, etc.)
- Proyecto de infraestructura tecnológica, que den un enfoque del manejo y la inversión en el desarrollo tecnológico de la organización.

1.2.3 ¿Qué es el Gobierno de TI?

Es la responsabilidad del alto mando directivo, que especifica esquemas de decisión y compromiso para impulsar un comportamiento deseable de las organizaciones. El cuál es el encargado de Evaluar Políticas, Dirigir políticas de los planes y Monitorear el rendimiento de las operaciones de las necesidades del negocio. (Analuisa y Erazo, 2007)

En definitiva, el gobierno de TI es rentable para la empresa debido a que ayuda a minimizar los efectos que produce el avance tecnológico, optimizando los recursos, garantizando que los servicios sean de calidad para que los procesos sean reestructurados estratégicamente logrando la meta esperada.

1.2.3.1 Evaluación del gobierno del TI en las Empresas

Se considera importante el uso de estándares de TI con el fin de cumplir con los requerimientos del negocio y que estos sean regulados de forma comprensible proporcionando estrategias que permitan un ambiente propicio, evaluar su eficiencia y el desempeño de los procesos. (Gómez, 2013)

Se considera que para una mejor organización administrativa de las empresas en el gobierno de TI se debe verificar las opciones que tienen los directivos para definir prioridades y tomar las mejores decisiones; así también evaluar de progreso de los procesos administrativos a fin de que se logren las metas empresariales.

1.2.4 Control Interno

Se refleja por medio de normativas que se aplican a las unidades directivas de la organización, para la implementación de herramientas que direcciones y constaten el cumplimiento de los cambios en el desempeño interno y determinar si existe resguardo de los procedimientos financieros y administrativos. (Álvarez y Ezzard, sf)

Analizando este contexto el control interno asegura el éxito de la gestion de las funciones de la organización a traves de lineamientos establecidos y formalizar las operaciones aun no definidas, reformando fallas que se presenten y haciendo buen uso de los recursos, administrandolos de manera eficiente.

1.2.5 Seguridad de la información

La utilización de las TI permite que la comunicación con clientes se efectúan mediante acuerdos vía web, todas la facilidades que hoy en día existen ha ayudado a que se desarrollen con más facilidad. Sin embargo, esto ocasiona que día tras día sean inermes a las amenazas, que pueden llegar a ser inseguros para la organización influyendo en las actividades. (Clavijo, 2006)

Se puede considerar que el impacto producido por la seguridad de la Información en las personas, puede ser diferente según el punto de vista, ayuda a que la información sea controlada a través de herramientas que potencializan el resguardo de la información haciéndola confiable, reduciendo deficiencias que puedan producir costos elevados, perdida de información e incluso la quiebra de ciertas organizaciones.

1.2.5.1 Sistema de gestión de seguridad (SGSI)

Según www.iso27000.es (2016), el SGSI es una herramienta que permite la dirección de la seguridad de la información de una empresa, realizando la debida asignación de materiales y herramientas, siguiendo una normativa con la cual los procesos sean retroalimentados aplicando los lineamientos de la organización.

Se define al SGSI según la norma ISO 27001, en el que se nombran los estándares y mejores prácticas de seguridad de la información, (Ladino, Villa y López, 2011, p. 333)

En conclusión se puede decir que la falta de seguridad de la información en las entidades requiere la aplicación de ciertas herramientas de seguridad que reduzcan las deficiencias en el control y gestión del manejo de la información, por tal motivo las empresas priorizan la implementación de medidas de seguridad minimizando incidentes y garantizar la prolongación de sus actividades en el mercado.

1.2.5.2 Fundamentos ISO 27001 y su aplicación en las empresas

El SGSI toma como elementos de entrada los requerimientos de seguridad de los datos, a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen las metas de la empresa.

Las organizaciones pueden realizar la petición de una auditoria a cualquier entidad, teniendo en consideración todos los requerimientos en cuanto a seguridad se refiere determinando responsabilidades, definir cuáles son los procesos a evaluar mediante el discernimiento de los empleados que forman parte de este proceso e identificación de problemas y su impacto.

Conforme a lo planteado, se analiza el ejemplo puntual de Ladino, Villa, y López(2011, p. 338), en el cual se toma como caso práctico una certificación de la ISO 27000 aplicado a una entidad pública, en la cual se determina que es muy difícil renovar el modo de trabajar de las personas de la entidad. Además cuando se revisa si las normas se están cumpliendo, después de tantos intentos se determinó que los usuarios no realizaban trabajos ya efectuados con antelación. Debido a esto la directiva tomo la decisión de aplicar nuevas directrices para forzarlos a ejecutar dichos procesos.

1.2.6 COBIT (Control Objectives for Information and related Technology)

Cobit publicó su versión 4.1 en 2007 y finalizó con la versión 5 a finales del 2011 y su respectiva publicación en el 2012. (Achina, 2015)

Con el fin de satisfacer las necesidades y/o requerimientos de una organización el Marco Metodológico Cobit, proporciona un enfoque estructurado de sus objetivos de control para determinar la confiabilidad de la información, la disponibilidad de los recursos y las disposiciones en la seguridad de los datos.

Además ayuda a precisar el grado de exactitud y competencia de los procesos de forma integral, como también la efectividad y la eficacia en la forma como se maneja la información, a través de la implementación de los objetivos de control de TI en los diferentes procesos mejorando las expectativas de la organización y evitar riesgos.

Es decir que, COBIT indica que la administración de la información se organiza mediante la interrelación entre el procesamiento de las TI, los requerimientos con las metas de la organización a fin de conseguir estrategias que permitan un óptimo funcionamiento de los procesos.

1.2.6.1 Transición de COBIT de la V4.1 a la V5.0

Según menciona Isaca (2012), la versión Cobit 4.1 está ligados gestionar las funciones de aplicabilidad de las TI en esta edición propone 34 objetivos de control que están organizados en 4 dominios: Planificación y Organización, Adquisición e Implementación, Entrega y Soporte y Supervisión y Evaluación; en su nueva edición mejorada suministra un enfoque integrador entre la gobernabilidad y la dirección o gestión de tecnologías y obtener un equilibrio en el rendimiento y los niveles de control de procesos que debe tener la organización.

Se determina a continuación una explicación breve de cada uno extraída de Isaca (2012):

Planear y Organizar (PO)

En este dominio se trata de definir la planificación y la organización determinando las estrategias que ayuden a definir si se cumplen o no con las metas de la organización.

Adquirir e Implantar (AI)

Cuando se lleva a cabo la estrategia se propone establecer resultados y determinar cómo van a ser aplicados y relacionados en el desarrollo administrativo de una organización.

Entregar y Dar Soporte (DS)

Se refiere a entrega de los requerimientos de los servicios que son todos los procedimientos de preparación, confiabilidad y persistencia, donde estos servicios sean proporcionados estableciendo procedimientos requeridos por la organización.

Monitorear y Evaluar (ME)

La valoración de los procedimientos del negocio debe ejecutar verificaciones reglamentarias en el tiempo en las cuales se determinarán condición y su idoneidad en cuanto al control de requerimientos.

1.2.6.2 Objetivos de Control COBIT 5.0

Los objetivos que proporciona COBIT, ayudan a los altos dirigentes de una compañía a encontrar una respuesta de cómo y de qué forma se administran sus procesos.

Estos procesos poseen una guía que proporciona normativas regularizadas para garantizar que las funciones y aplicaciones de las entidades se cumplan adecuadamente, obteniendo una disminución considerable de riesgos e impactos que mediante esta metodología sean identificados y debidamente reformados, cumpliendo los objetivos corporativos.

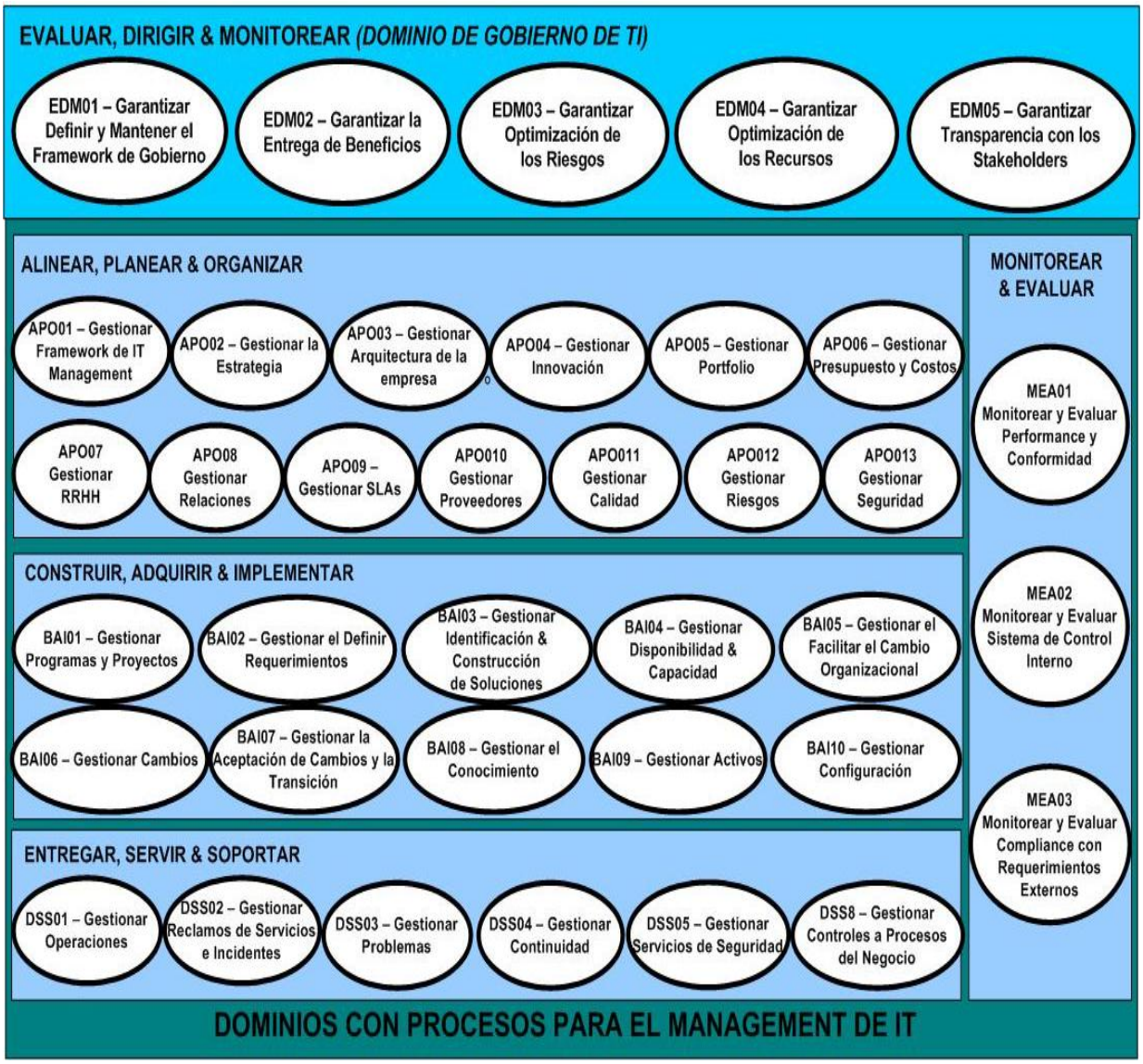


Figura 1. Modelo de Referencia de COBIT 5 (ISACA, 2012)

1.2.6.3. Atributos de Capacidad de Procesos

Según ISACA (2013) con el fin de medir o evaluar el nivel en el que un proceso de control se encuentra definido, establece ciertos atributos mediante los cuales se determinan el grado de capacidad de los procesos desde el Nivel 0 hasta el Nivel 5, definiendo cual es la situación actual analizado con relación del nivel que sin ser el óptimo pueda asegurar la ejecución de las necesidades principales de la organización.

A continuación se definen los niveles de capacidad de procesos basados en el estándar ISO/IEC 15504.

Tabla 1.

Niveles de Capacidad de Procesos COBIT

NIVELES DE CAPACIDAD DE PROCESOS COBIT 5.0	
Nivel 0 : Incompleto	El proceso no se ha implementado o no alcanza su objetivo. De este nivel existe mínima o ninguna certeza de éxito regular del objetivo
Nivel 1: Ejecutado	El proceso aplicado alcanza su objetivo
Nivel 2: Gestionado	El proceso ejecutado se aplica de forma administrada (programada, controlada, adaptada) , sus procesos de trabajo se instauran, controlan y continúan de forma adecuada
Nivel 3: Establecido	Este proceso administrado esta aplicado utilizando uno ya especificado con capacidad de obtener los resultados de proceso
Nivel 4: Predecible	Este proceso establecido se encuentra en los niveles específicos para obtener los resultados del proceso
Nivel 5: Optimizado	El proceso predecible se mejora continuamente para cumplir con los objetivos de los negocios tanto actuales como futuros.

Nota: (ISACA., 2013)

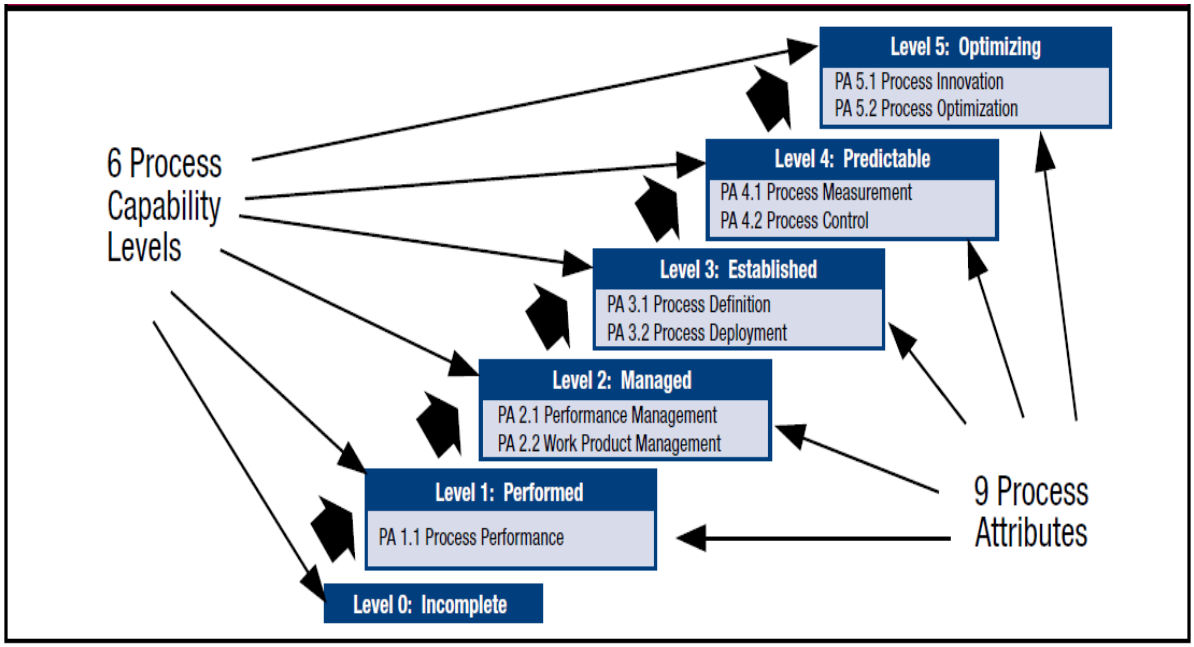


Figura 2. Atributos de Capacidad de Procesos (ISACA., 2013)

1.2.6.4. Mapeo de Metas y Procesos relacionados con las TI

Con el fin de conocer cuáles serán los objetivos o procesos importantes para las empresas, Cobit hace referencia a un alineación de los objetivos de TI mediante un Mapeo en que se detallan los 37 objetivos de Cobit categorizando con (P) como elementos principales y con (S) los secundarios cuando el proceso incide en el proceso pero menos importante identificados en la Figura 3.

			Enterprise Goal																
			Stakeholder value of business investments	Portfolio of competitive products and services	Managed business risk (safeguarding of assets)	Compliance with external laws and regulations	Financial transparency	Customer-oriented service culture	Business service continuity and availability	Agile responses to a changing business environment	Information-based strategic decision making	Optimisation of service delivery costs	Optimisation of business process functionality	Optimisation of business process costs	Managed business change programmes	Operational and staff productivity	Compliance with internal policies	Skilled and motivated people	Product and business innovation culture
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
		IT-related Goal	Financial					Customer					Internal					Learning and Growth	
Financial	01	Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	IT compliance and support for business compliance with external laws and regulations			S	P											P		
	03	Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
	04	Managed IT-related business risk			P	S			P	S		P			S		S	S	
	05	Realised benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
	06	Transparency of IT costs, benefits and risk	S		S		P				S	P		P					
Customer	07	Delivery of IT services in line with business requirements	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Adequate use of applications, information and technology solutions	S	S	S			S	S		S	S	P	S		P		S	S
Internal	09	IT agility	S	P	S			S		P			P		S	S		S	P
	10	Security of information, processing infrastructure and applications			P	P			P								P		
	11	Optimisation of IT assets, resources and capabilities	P	S						S		P	S	P	S	S			S
	12	Enablement and support of business processes by integrating applications and technology into business processes	S	P	S			S		S		S	P	S	S	S			S
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	P	S	S			S				S		S	P				
	14	Availability of reliable and useful information for decision making	S	S	S	S			P		P		S						
	15	IT compliance with internal policies			S	S											P		
Learning and Growth	16	Competent and motivated business and IT personnel	S	S	P			S		S						P		P	S
	17	Knowledge, expertise and initiatives for business innovation	S	P				S		P	S		S		S			S	P

Figura 3.**Mapeo entre Metas corporativas de COBIT 5 y Metas relacionadas con TI** (Isaca, 2012)

1.2.7 El Riesgo

El riesgo puede definirse como la vulnerabilidad o daño que experimentan las instituciones en cualquier actividad u operación que se efectúe dentro de la misma.

En este contexto, ese riesgo puede proporcionar afectaciones de gran magnitud en las organizaciones si no son mitigados a tiempo, como pérdida de información, e incluso la quiebra. Debido a esto existen herramientas que ayudan a detectarlas y emitir procedimientos adecuados para evitarlas a corto, mediano y largo plazo.

1.2.7.1. Matriz de Riesgos

En toda entidad es necesario tener en cuenta la adaptabilidad de herramientas de análisis de riesgos aplicadas a sus procesos, las cuales definan el cumplimiento de políticas en cada una de las operaciones tecnológicas que se desarrollan en la empresa.

Para identificar los puntos de riesgo de cada proceso de una evaluación, se toma en cuenta una matriz de Riesgos. Con la cual se logra determinar los problemas existentes con el fin de evaluarlos para tener información que permita minimizar su efecto en los procesos de la organización.

Los objetivos para el análisis de riesgos de TI son los siguientes (Jaramillo, 2013):

- Identificar, determinar y restablecer funciones de control de administración de riesgos
- Conocer la realidad de los procesos llevados a cabo por el área de TI
- Establecer la metodología adecuada y valoración de Riesgos de TI.
- Informar sobre los riesgos que se lleguen a identificar en la empresa
- Monitorear los riesgos a fin de garantizar la integridad, confidencialidad y confiabilidad de la información.

1.2.7.2 Indicadores de Riesgo

Los indicadores son aquellos que definen la forma y cómo serán medidos los riesgos, dependiendo de qué tan a menudo se presente un suceso. Estos indicadores deben ser identificados analizando sus atributos en relación con el riesgo y que sean medibles.

Los indicadores de riesgo utilizados en este proyecto son Frecuencia, Impacto y Tolerancia los cuales se describen a continuación:

Frecuencia

La frecuencia es el número de ocurrencias de hecho o suceso en un periodo de tiempo. Los niveles de frecuencia se definen de la siguiente forma:

1: Altamente Improbable.

2: Improbable

3: Eventual

4: Probable

5: Altamente Probable.

Impacto

Efecto probable o cierto, positivo o negativo, directo o indirecto, reversible o irreversible, de naturaleza social, económica y/o ambiental que se deriva de una o varias acciones con origen en las actividades de la organización.

Los niveles de impacto dentro de la organización se han definido de la siguiente manera: (Siles y Mondelo, 2012)

1: Muy Baja.

2: Baja

3: Moderada.

4: Alto

5: Muy Alto.

Tolerancia al Riesgo

Una vez definidos el impacto y la frecuencia de riesgos en la organización, se procede a establecer la tolerancia, que sería la capacidad de aceptar riesgo. Para esto se estableció trabajar con un rango de ponderaciones. Para determinar la ponderación de cada uno de los riesgos que se van a identificar se va a utilizar la siguiente fórmula: (Siles y Mondelo, 2012)

Dónde: **P:** Ponderación. **F:** Frecuencia. **I:** Impacto.

Los rangos de tolerancia al riesgo basados en la ponderación son los siguientes

Muy Bajo: Rango [1-2]

Bajo: Rango [3-4]

Medio: Rango [5-6-8-9]

Alto: Rango [10-12-15-16]

Muy Alto: Rango [20-25]

Definidos los rangos ya se puede definir una matriz/mapa de riesgos base para el estudio como la detallada a continuación

Tabla 2.

Mapa de Matriz de Riesgos

IMPACTO	5.- Muy Alto	5	10	15	20	25
	4.- Alto	4	8	12	16	20
	3.- Medio	3	6	9	12	15
	2.-Bajo	2	4	6	8	10
	1.- Muy Bajo	1	2	3	4	5
MAPA/ MATRIZ DE RIESGOS		1. Altamente Improbable	2.Improbable	3. Eventual	4. Probable	5 Altamente Probable
		FRECUENCIA				

Nota: (Jaramillo, 2013)

1.2.7.3 Aplicación de la Matriz de Riesgo

Con el fin de encontrar solución a los riesgos que se presentan en la organización que impiden el buen manejo, gestión de los procesos de TI y metas del negocio, a continuación se detalla los riesgos encontrados en la evaluación de esta investigación en la aplicación de entrevistas y observación al encargado del Área de TI, que son evaluados en la Tabla 16.

Entorno

Tabla 3.

Riesgos de Entorno

Código	Riesgo
E1	Limitación de medidas preventivas por desastres naturales
E2	Falta de mantenimiento permanente de las instalaciones eléctricas

Talento Humano

Tabla 4.

Riesgos de Talento Humano

Código	Riesgo
TH01	Falta de personal especializado de TI
TH02	La capacitación de los empleados de TI es mínima
TH03	Documentación de planificación de capacitación del personal regular

Físico

Tabla 5

Riesgos Físicos

Código	Riesgo
F01	Hardware no adecuado para el desempeño de funciones
F02	Espacio físico limitado para equipos e infraestructura

F03	Falta de estrategias preventivas contra daños
F04	Falta de documentación de requerimientos del área de TI
F05	Ausencia de políticas de uso de HW
F06	Falta de políticas de acceso a usuarios

Procesos Internos

Tabla 6.

Riesgos de Procesos Internos

Código	**Riesgo**
PI01	Falta de políticas de control de incidentes internos
PI02	Falta de definición de soporte de TI de las aplicaciones de la organización
PI03	Falta de manuales y procedimientos de configuración en el manejo de aplicaciones

Seguridad

Tabla 7.

Riesgos de Seguridad

Código	Riesgo
S01	Seguridad en el manejo de la Información
S02	Seguridad de Control de Accesos al personal en todas las áreas de la organización
S03	Falta de plan de contingencias

S04	Políticas de respaldo de información

Infraestructura Tecnológica

Tabla 8.

Riesgos de Infraestructura Tecnológica

Código	Riesgo
ITE01	Carencia de políticas y funcionalidades en la adquisición de equipos
ITE02	Organización de procesos de control de cambios a nivel de software
ITE03	Organización de procesos de control de cambios a nivel de hardware
ITE04	Conexiones de Red inestables

En este punto se instaura la posibilidad de ocurrencia de riesgos y su efecto, acreditándolas y haciendo una valoración con el propósito de la escala de riesgo y las actividades a desarrollarse.

En él se detalla los riesgos identificados según el nivel de ocurrencia y el efecto que producen en la organización.

CAPITULO II

2. MATERIALES Y MÉTODOS

Con el fin de generar un orden, en las diversas fases requeridas para realizar una evaluación de infraestructura tecnológica en la empresa National Tire Experts S.A, surge la necesidad de basarse en una metodología. Esto se hace en función de mantener una estrecha relación entre cada una de las etapas del proyecto y de esta forma obtener información necesaria.

2.1. Descripción del lugar

National Tire Experts S.A es una empresa comercializadora de neumáticos y servicios automotrices, con reconocimiento a nivel nacional, asociado a la empresa líder en el mercado ecuatoriano e internacional Continental Tire Andina, cuenta con 130 empleados distribuidos en las localidades de Santo Domingo de los Tsáchilas, Esmeraldas, Quevedo, Babahoyo, Quito, Cuenca.

Se considera que para este proyecto debido los procesos y la información relevante se realiza en la Matriz se centrará en la localidad de:

Ciudad o Municipio: Santo Domingo

Departamento, Estado o provincia: Santo Domingo de los Tsáchilas

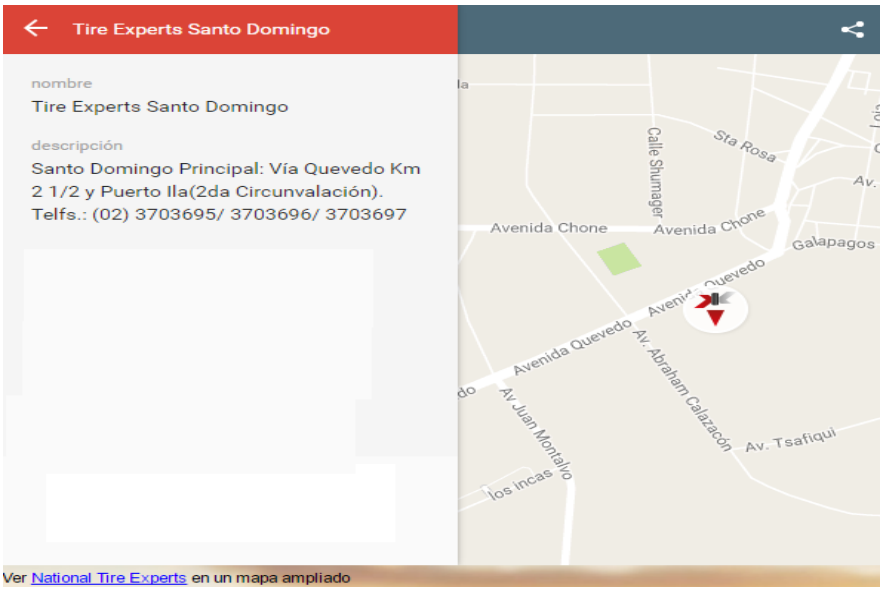


Figura 4. Mapa de localidades NationalTire Experts,(2016.).
Recuperado de : http://www.tire-experts.com.ec/cparrales/nuestros-locales.html

2.2. Métodos y Técnicas que se emplearon

Técnicas

Durante el desarrollo de la investigación se utilizarán las técnicas de la entrevista, encuesta y la observación directa.

Entrevista: Dirigida al encargado del Área tecnológica de la empresa a fin de obtener datos importantes del sistema, su funcionamiento, inventario de equipos, formas de almacenamiento de información y otros aspectos que se consideran necesarios para el desarrollo de los procesos de la auditoria **(Anexo B1).**

Observación: Se utilizó una guía de Observación, la cual permitió cerciorarse de la eficiencia de los procesos de la organización, como se maneja la información, documentos del área tecnológica, con el objeto de establecer una existencia y autenticidad. La observación hará más confiable la obtención de la información y evidencias **(Anexo B2).**

Encuesta: Dirigida al personal administrativo de la empresa National Tire Experts S.A, con el fin de identificar/evaluar las falencias en la infraestructura tecnológica de la empresa y determinar la forma con la que se manejan los mismos **(Anexo A).**

Debido a los resultados que se desea obtener, las variables utilizadas en esta encuesta son cualitativas que ayudan a que el analisis y la tabulacion de los datos sea precisa para su evaluación, está apoyado en base a la encuesta de nivel de satisfacción empleada en la metodología de Díaz (2011).

2.3. Población y Muestra de estudio

La población para este estudio está dada por 110 empleados que desarrollan cargos administrativos, manejan equipos tecnológicos y cualquier tipo de información primordial para la empresa.

Debido al tamaño de la población se determina el cálculo de la muestra para este trabajo de investigación es Aleatoria el cual ayudó a la obtención de información relevante debido a esto se utilizó la siguiente fórmula.

$$\boldsymbol{n = \frac{N\sigma^2\ Z^2}{(N-1)\ e^2 + \ \sigma^2\ Z^2}}$$

Figura 5. Ecuación no Probabilística (Aguilar, 2005)

n = Tamaño de la muestra

N = Población

$\boldsymbol{\sigma}$ **=** Desviación estándar de la población, generalmente cuando no se tiene su valor suele utilizarse un valor constante de 0,5

Z: Valor obtenido mediante niveles de confianza, si no se tiene su valor se lo toma en relación al 95 % de confianza que equivale a 1,96 (es el más usual)

e: Límite aceptable de error muestral, cuando no se tiene su valor suele utilizarse un valor que varía entre 1% (0,01) y el 9% (0,09)

Aplicando la fórmula:

N= 110 empleados

σ = 0,5

e=0,06

Z= 1.96

$$n = \frac{110\ \ (0.5^2)(1{,}96^2)}{(110-1)(0.06^2) + \ (0.5^2)(1{,}96^2)}$$

$$n = \frac{105{,}644}{0{,}3924 + \ 0{,}9604}$$

$$n = \frac{105{,}644}{1{,}3528}$$

n = 78,09 **Tamaño de la muestra 78 empleados**

2.4 Técnicas de procesamiento y análisis estadístico de datos empleados

Para efectuar la recolección de datos se realizó encuestas dirigidas a la población descrita en el apartado anterior, entrevistas, y fichas de observación para toda la información de la cual se tome evidencias de puntos relevantes para la investigación.

Se desarrolló cuestionarios para la aplicación de entrevistas y encuestas con el fin de lograr un mejor análisis de los datos recolectados se va a utilizar la técnica de estadística descriptiva utilizando hojas de cálculo y graficación de los resultados.

2.5. Normas éticas

Para el planteamiento y ejecución de las encuestas de este trabajo de investigación se guardará absoluta confidencialidad, de los datos personales así como también de la información requerida que se obtenga de los encuestados.

CAPÌTULO III
RESULTADOS

3.1 Análisis e Interpretación de Datos

Para la evaluación del control interno de la infraestructura de la organización, se determinó la aplicación de una encuesta de Nivel de Satisfacción dirigida a los empleados de National Tire Experts S.A, con la finalidad de medir la calidad de servicio que el área tecnológica proporciona a los usuarios dicha encuesta fue realizada a través de un formulario Web ejecutada el 6 y 7 de Febrero del año en curso.

A continuación se detalla los resultados y el análisis de los datos obtenidos en la encuesta, de las cuales se tomó en cuenta cinco preguntas como los más relevantes para esta investigación **(Anexo A)**.

P1: ¿Con que frecuencia su equipo computacional sufre problemas en su funcionamiento?

Análisis: La mayor parte de los usuarios tienen problemas o daños en los equipos de trabajo, que hacen difícil la realización de sus actividades diarias como se puede apreciar en el Gráfico 1.

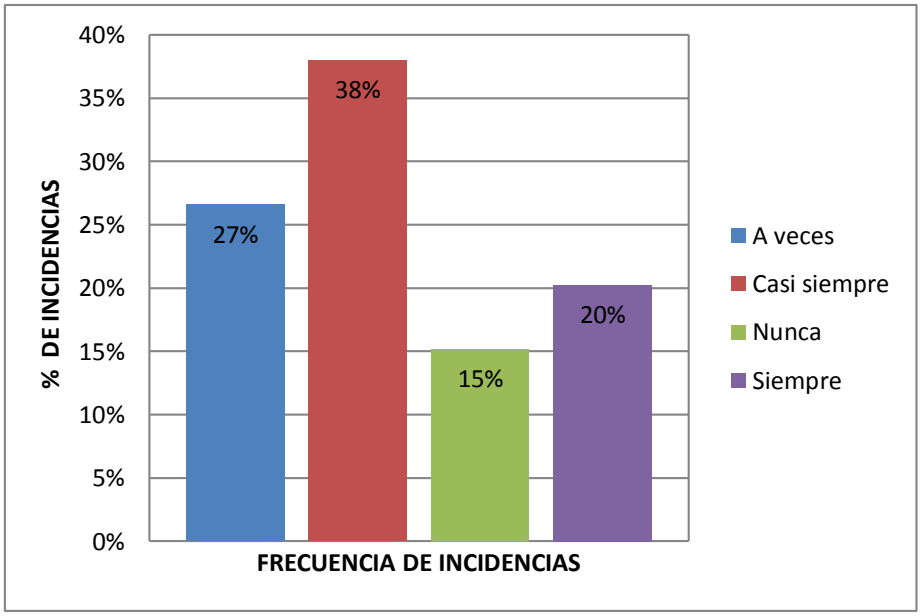


Grafico 1.Estado de los equipos computacionales de National Tire Experts

P2: ¿El área tecnológica da respuesta rápida a incidencias o problemas en su equipo computacional?

Análisis: En el Gráfico 2 se evidencia que el área tecnológica no responde a tiempo las incidencias presentadas por los usuarios, los cuales también se pueden asociar a la cantidad de incidencias que se presentan en los equipos computacionales sean estas de hardware o software como se apreció en el Gráfico 1.

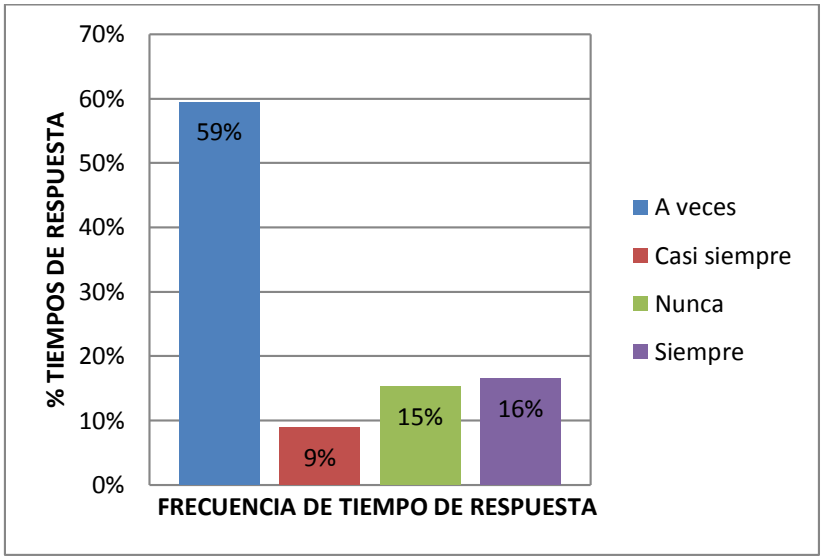


Grafico 2 . Tiempo de Respuesta a Incidencias de los equipos

P3: ¿Cómo usted considera que es el servicio de Internet que maneja la empresa?

Análisis: Debido a su importancia en el continuo desarrollo de las actividades de las empresas, el internet es uno de los servicios más usados, según el Gráfico 3, se puede apreciar la inconformidad de los usuarios con este servicio, evidenciando que el servicio que otorga el ISP (Internet Provider Service) contratado por la institución es no cumple con los requerimientos de la organización.

Este punto se puede considerar en relación con el estado o funcionalidad en que se encuentran los equipos computacionales de cada usuario.

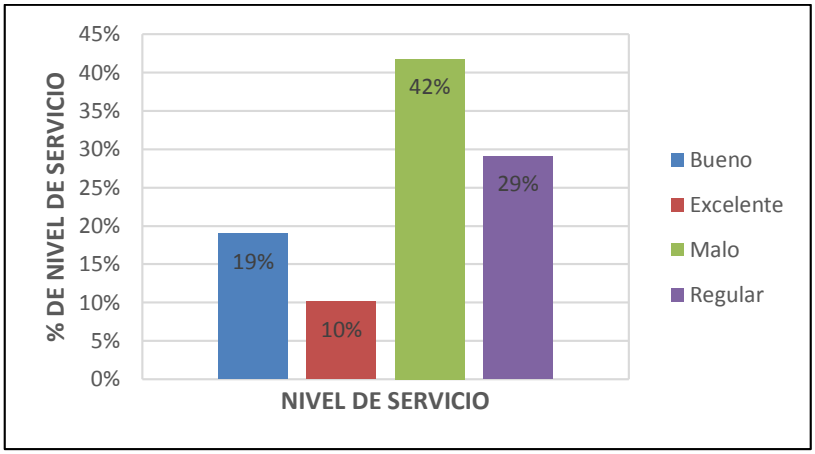


Grafico 3 **.** Velocidad del Servicio de Internet

P5: ¿Cómo considera el servicio brindado por el área de tecnología?

Análisis: Según los resultados los usuarios se sienten conformes con la atención que brinda el encargado del área ante las incidencias que se presentan en sus equipos sean estos de hardware y software como se evidencia en el Gráfico 4.

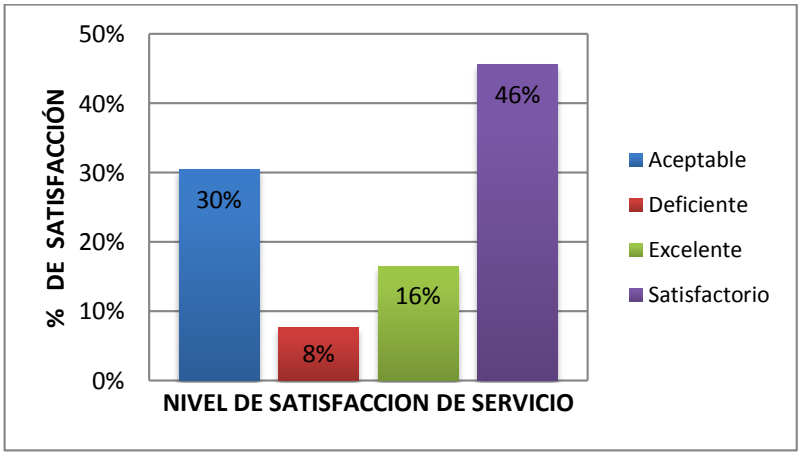


Grafico 4. **Nivel del Servicio de TI**

P6: ¿Qué piensa usted de la capacitación que proporciona el área tecnológica relacionada con Tecnologías de la Información?

Análisis: El nivel de capacitación de la empresa en general satisface los requerimientos de los usuarios como se puede distinguir en el Grafico 5, aunque existe un pequeño porcentaje que no posee conocimientos definidos en el uso adecuado de las aplicaciones y esto puede

incidir en hallazgo de nuevas incidencias en los equipos y el manejo inapropiado hardware y software.

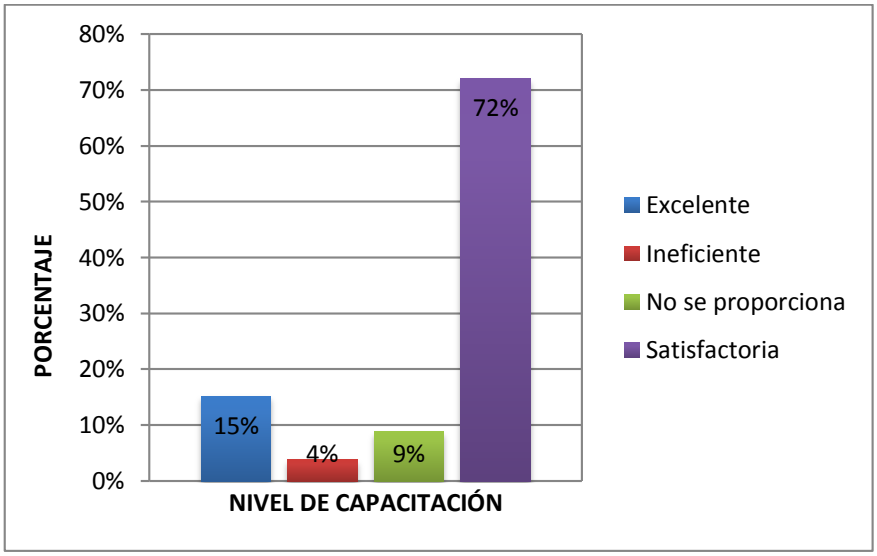


Grafico 5.Nivel de Servicio de Capacitación a Usuarios

3.2. Análisis e interpretación de resultados de la encuesta

Debido a que la empresa National Tire Experts S.A, tiene como objetivo seguir siendo un referente comercial en el mercado Automotriz, considera que lo más importante para el desarrollo de la misma es el brindar un servicio de calidad con calidez a sus clientes.

Mediante la implementación de nueva Infraestructura, la organización está interesada en buscar métodos que le ayuden a evolucionar en el campo tecnológico, que en la actualidad es muy necesario para el mejoramiento de sus procesos de control interno y administración de los mismos.

Por este motivo, para esta propuesta se considera necesaria la aplicación de COBIT 5.0, el cual con ayuda de sus objetivos de control proporciona un enfoque general de cada uno de los procesos, de las aplicaciones y la estructura de la empresa, relacionándolos con los objetivos del negocio obteniendo una mejora continua.

4.1.2 Análisis de la Entrevista y Guía de Observación

Después de la aplicación del cuestionario utilizado para la entrevista al encargado del área de tecnología de la empresa. Se realizó un análisis que consta de varios categorías siguiendo como pauta los objetivos de control proporcionados por Cobit, para la aplicación de la auditoría en cuanto a seguridad, políticas de control interno, planes, etc.

Además con la aplicación de la guía de observación, se tomó en cuenta las observaciones y hallazgo de evidencias necesarias para definir las falencias encontradas, definir riesgos, analizarlos y proponer soluciones **(Anexo B1 y B2).**

Según lo observado se puede determinar que la empresa no tiene procesos definidos, tiene carencia de control en la distribución de las funciones, desempeño y soporte en el área tecnológica. Los procesos carecen de políticas y planificación permitiendo un desequilibrio en su funcionalidad existiendo desorganización.

La seguridad es de vital importancia para una empresa por eso se requiere estar protegido frente a cualquier eventualidad sean estas eléctricas, de datos, de desastres naturales, eventuales, entre otras.

Haciendo necesario la aplicación de políticas de seguridad que eviten que la infraestructura de la organización se encuentre en riesgo.

National Tire Experts está implementando normativas de seguridad en la prevención de incendios, desastres, etc. A pesar de esto necesita establecer políticas definidas que sean analizadas y probadas a fin de que puedan ser aplicadas según las necesidades de la institución.

En cuanto a seguridad de la información, el encargado del área tecnológica indicó que existe cierto nivel de prevención por la aplicación de técnicas básicas de reguardo de los datos, como respaldos en medios externos. Además manifestó que no existe un presupuesto para la implementación de equipamiento y software que permita un control de seguridad efectivo que habría evitado pérdida de información y por ende costos elevados a la organización.

También se pudo apreciar que el proceso de autenticación de usuarios no es seguro, debido a que el área de tecnología carece de infraestructura complementaria, que permita un control eficiente de las aplicaciones, red, servicios tecnológicos, resguardo de información, entre otros.

CAPÍTULO IV

4. PROPUESTA

4.1 INFORME DE EVALUACIÓN DE LA INFRAESTRUCTURA DE TI

Empresa: National Tire Experts S.A
Área: Tecnológica

4.1.1 Ubicación

Las oficinas de la empresa National Tire Experts S.A están ubicadas en Santo Domingo de los Tsáchilas en su oficina Matriz, además tiene actualmente cinco sucursales, en Esmeraldas, Babahoyo, Quevedo, Quito y Cuenca.

En la oficina Matriz se localiza el personal Administrativo, Financiero y Tecnológico.

4.1.2 Organigrama Estructural



Figura 6. Organigrama de la empresa National Tire Experts S.A Autor: Vanessa Cedeño

4.1.3 Recurso Humano

El personal del área de tecnología lo conforma una persona, entre sus responsabilidades o funciones podemos mencionar las siguientes:

- Controlar el funcionamiento del Sistema Informático a todos los usuarios.
- Administrar la red, control de accesos, conexión de los equipos, control del sistema de video vigilancia a través de Internet.
- Brindar soporte de los programas, aplicaciones de la oficina matriz y de las sucursales de forma remota.
- Controlar el acceso a información y manejo del correo institucional.
- Contratación de servicios de HW y SW de la organización previa autorización de Gerencia Financiera.
- Mantenimiento de equipos (computadores).
- Instalación de software necesario para el correcto funcionamiento de los equipos.
- Control del servidor y respaldo de información.

4.1.4 Infraestructura de TI

A continuación se detalla los componentes de la infraestructura tecnológica de la empresa, en la que se incluye la especificación de todos los activos.

La empresa posee un servidor en la oficina matriz además cuenta con 30 equipos de escritorio y dos portátiles distribuidos de la siguiente forma:

OFICINA MATRIZ

Tabla 9.

Dispositivos de Infraestructura de TI oficina Matriz

RESGUARDO DE INFORMACION					
Equipo	**Marca**	**Capacidad**	**Memoria**	**Procesador**	**Departamento**
Servidor	HP	500GB	4GB	CORE 2.53	Área de TI
Portátil	HP	500GB	4GB	CORE I5	Encargado de TI

DISPOSITIVOS POR DEPARTAMENTOS					
Portátil	Samsung	1Tb	4GB	CORE I5	Gerencia General
Computador de escritorio	COMPAQ s25212y	250GB	1GB	Athlon 64 (V) 2.2 GHz	Jefe de Matriz
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Vendedor Interno 1
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Vendedor Interno 2
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Vendedor externo
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Asistente de Marketing
Portátil	HP	500GB	2GB	Intel Dual Core	Gerencia LVT
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Vendedor Interno 1
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Asistente de crédito
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Tesorero
Computador de escritorio	HP	500GB	2GB	Intel Core I5	Contador
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Inventario
Computador de escritorio	Clon	250GB	2GB	Intel Celeron	Bodega
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Jefe Nacional de Crédito y Cobranzas
Portátil	HP	1tb	4GB	Intel Core i7	Encargado del área de Sistemas
Computador de escritorio	Clon	500gb	2GB	Intel Celeron	Gerencia Financiera
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Gerencia PLT
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Jefe RRHH
Computador de escritorio	Clon	250GB	2GB	Intel Celeron	Asistente de RRHH
Computador de escritorio	Clon	250GB	1GB	Intel Celeron	Jefe de Taller
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Dep. Legal
Computador de escritorio	Clon	250GB	2GB	Intel Celeron	Jefe de Crédito Matriz
Computador de escritorio	Clon	500GB	2GB	Intel Celeron	Compras Públicas 1
Computador de escritorio	Clon	250GB	2GB	Intel Celeron	Compras Públicas 2
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Asistente de Crédito
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Recaudador
Computador de escritorio	Clon	250GB	2GB	Intel Celeron	Logística
Computador de escritorio	Clon	250GB	1GB	Intel Celeron	Ajustador1
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Ajustador2

Computador de escritorio	Clon	250GB	2GB	Intel Celeron	Jefe de Marketing
Computador de escritorio	Clon	500GB	2GB	Intel Celeron	Reencauche
Computador de escritorio	Clon	250GB	2GB	Intel Celeron	Compras Públicas 2
EQUIPOS DE REDES					
SWITCH	D-LINK , 24 PUERTOS				
2 ROUTER	D-LINK				
EQUIPOS DE SEGURIDAD					
CAMARAS DE VIDEO VIGILANCIA			6		
DVR			1		
CIRCUITO DE ALARMAS			1		
SENSOR DE PANICO			1		

SUCURSALES (5 oficinas a nivel nacional)

Tabla 10.

Dispositivos de Infraestructura de TI Sucursales

Dispositivos por departamentos					
Portátil	Samsung	1Tb	4GB	CORE I5	Vendedor
Computador de escritorio	COMPAQ s25212y	250GB	1GB	Athlon 64 (V) 2.2 GHz	Jefe
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	CAJA 1
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	CAJA 2
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Vendedor externo
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Asistente de Crédito
Computador de escritorio	Clon	250GB	1GB	Intel Celeron	Jefe de Taller
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Bodega
Computador de escritorio	Clon	250GB	2GB	Intel Dual Core	Logística
Computador de escritorio	Clon	250GB	1GB	Intel Celeron	Ajustador
Computador de escritorio	Clon	250GB	1GB	Intel Celeron	Recaudador
EQUIPOS DE REDES					
ACCESS POINT	D-LINK				
ROUTER	D-LINK				
EQUIPOS DE SEGURIDAD					
CAMARAS DE VIDEO VIGILANCIA			3		
DVR			1		
CIRCUITO DE ALARMAS			1		
SENSOR DE PANICO			1		

4.1.5 Seguridad Física y Lógica

En cuanto a la parte de seguridad física de la entidad no cuenta con servicio de guardianía, debido a esto cualquier persona puede acceder a las instalaciones.

El acceso a las oficinas es libre, no existe ningún tipo de seguridad, el espacio destinado al área de TI es sumamente reducido, se encuentra separado por cubículos con otros departamentos, no cuenta con un ambiente ventilado para el correcto funcionamiento de los equipos además se puede acceder físicamente al servidor sin ningún tipo de restricción, aunque el acceso lógico a este no es posible debido a que cuenta con una contraseña de acceso a la cual solo tiene acceso el encargado del área.

No existe rack para la instalación y resguardo de equipos de comunicación estos se localizan sobre un escritorio, ocasionando un caos en la organización del cableado además de no contar con seguridad en caso de siniestros, no existen UPS para prevenir descargas eléctricas, los equipos se encuentran conectados con regletas lo que puede producir riesgos de apagones.

El equipo de seguridad en la oficina matriz cuenta con seis cámaras IP con sistema de video vigilancia, manejado y manipulado por el encargado del área de TI. El sistema funciona correctamente, de igual manera el sistema de alarmas está controlado por una empresa de seguridad permanente las 24 horas del día.

Cada usuario tiene acceso a su equipo de trabajo a través de contraseñas y otra para el manejo de información en el sistema, cada vez que se lo requiere o cuando hay el ingreso de personal nuevo se le proporciona una.

El equipo de seguridad en las sucursales cuenta con tres cámaras IP con sistema de video vigilancia, manejado y manipulado por el encargado del área de TI desde la oficina matriz. El sistema funciona correctamente, de igual manera el sistema de alarmas está controlado por una empresa de seguridad permanente las 24 horas del día.

4.1.6 Redes y Comunicaciones

Matriz

El espacio destinado como área de TI, es muy reducido no posee nivel de seguridad física debido a que se encuentra en un cuarto compartido con otros departamentos por módulos o cubículos, no existe un rack para el posicionamiento de los equipos de comunicación, por lo tanto se encuentran colocados provisionalmente en un escritorio a la intemperie.

El área consta de un servidor, en el cual se almacena y administra el sistema de información además del manejo de respaldo de la institución, en el cual el encargado de TI realiza el control de accesos de usuarios y contraseñas.

Los equipos con los que cuenta actualmente no cumplen con los requerimientos de área, por lo tanto necesita una actualización e implementación de nueva infraestructura tecnológica que proporcione un mejor desempeño de las funciones del área y manejo de los recursos.

Sucursales

La red instalada en cada sucursal es completamente inalámbrica, todo el sistema de redes es manejado desde la matriz por el encargado del área de TI, no existe un rack para el posicionamiento de los equipos de comunicación, por lo que se encuentran colocados provisionalmente en el piso.

Los equipos con los que cuenta actualmente las sucursales necesitan actualización e implementación de nueva infraestructura tecnológica que proporcione un mejor desempeño de las funciones de cada departamento y manejo de los recursos.

4.1.7 Software

Matriz

Actualmente la empresa adquirió un sistema Administrativo – Financiero llamado CADILAC, desarrollado por la empresa AGIPRO, la cual se encarga del mantenimiento de forma externa.

En cuanto al software, siete equipos de escritorio funcionan a través de Windows XP los cuales presentan problemas de activación de producto, las portátiles usan Windows 8 y el resto de equipos usan Windows Vista, por lo tanto deben ser actualizados para que todos se encuentren debidamente estandarizados.

El software de soporte con el que trabaja el servidor es con el S.O Windows Server 2003, su página web corporativa www.tire-experts.com.ec y correo electrónico institucional nombreUsuario.apellidoUsuario@tire_experts.com.ec

El software utilizado para la realización de respaldos que utiliza la empresa es Paragon Backup & Recovery. Cabe indicar que solo cuatro de los equipos cuentan con licencia original de S.O y antivirus.

Sucursales

El sistema está instalado en el servidor en la oficina matriz por lo que es utilizado a través de Internet y monitoreado por el encargado del área de TI mediante acceso remoto.

En cuanto al software, los equipos de escritorio dos funcionan a través de Windows XP los cuales presentan problemas de activación de producto, el resto de equipos usan Windows Vista, por lo tanto deben ser actualizados para que todos se encuentren debidamente estandarizados.

Cabe indicar que solo uno de los equipos cuenta con licencia original de S.O y antivirus.

4.1.8 Servicio Web e Internet

Matriz

El servicio de Internet con el que cuenta la empresa es proporcionado por un plan corporativo de CNEL contratado e implementado en la oficina matriz y en cada una de las sucursales las cuales se conectan al sistema a través de Internet.

También cuenta con su propio sitio web, por el cual promociona sus productos y servicios.

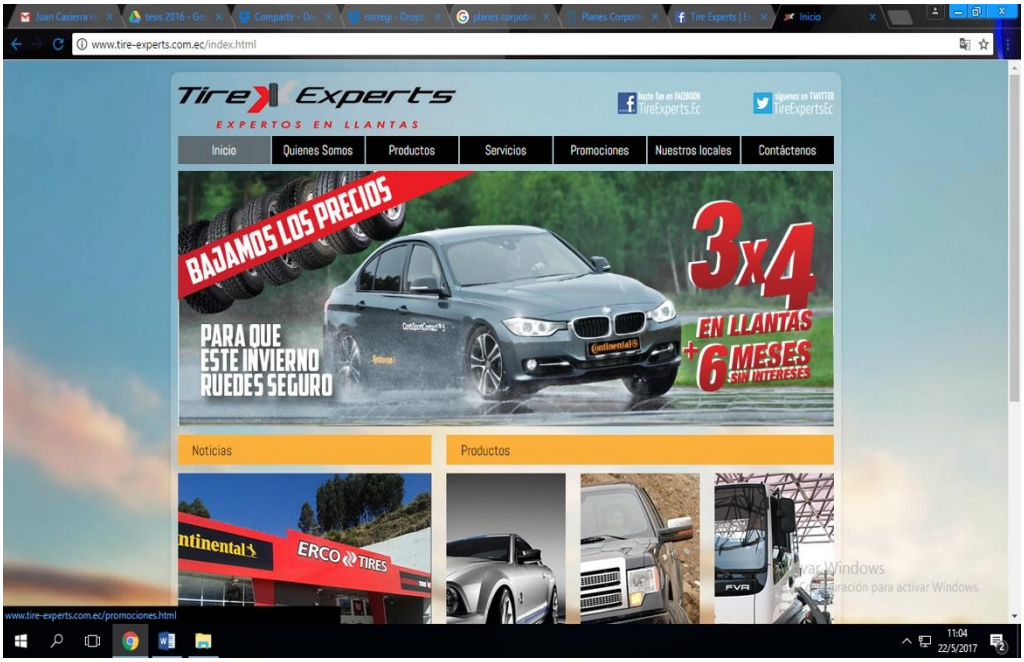


Figura 7. Página corporativa National Tire Experts S.A

Sucursales

La mayor parte del tiempo las sucursales se ven en la obligación de interrumpir sus funciones debido a la caída del servicio de Internet ocasionando la inconformidad y descontento constante de los usuarios, debido que se conectan al sistema a través de Internet.

4.1.9 Topología de Red

Actualmente la empresa cuenta con un ISP CNT corporativo, con una conexión de ancho de banda de 2.75 Mbps de subida y 0.87 Mbps de bajada al que se conectan todos los equipos, cada localidad posee una cuenta de internet de la misma categoría. Cuando existe alguna eventualidad con el servicio de internet o se produce un apagón eléctrico las sucursales cuentan con un modem usb Claro para el funcionamiento de los equipos de caja.

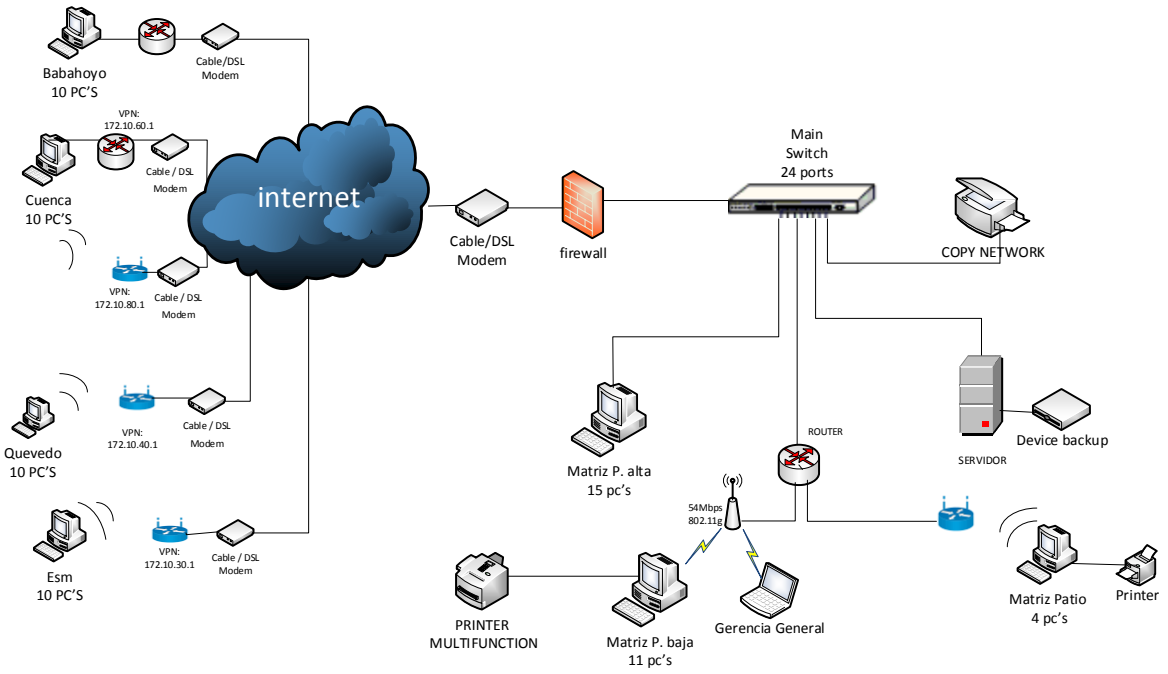


Figura 7. Topología de Red National Tire Experts S.A Autor: Vanessa Cedeño

4.1.10 Detección de problemas de infraestructura

Existe una sobrecarga de funciones asignadas al encargado del área de TI, el solo contar con una persona para todos los procesos, ocasiona la deficiencia en el servicio de soporte a usuarios, y el manejo adecuado de la seguridad física y lógica tanto de la información como de la infraestructura.

En cuanto a tecnología se refiere, para la empresa no es un punto de mayor relevancia la capacitación a los usuarios en esta área, esto limita su capacidad de resolución de problemas elementales, resultando indispensable la presencia y conocimientos del encargado de TI, proporcionando que las actividades propias del área en ciertos casos no las pueda cumplir a tiempo.

El S.O de los equipos en su mayoría no se encuentran debidamente licenciados, por lo que la empresa debe analizar su adquisición inmediata.

El espacio asignado a la infraestructura no es el adecuado, cuenta con un espacio reducido para los equipos, el acceso es libre para cualquier usuario, no existe un ambiente fresco con el cual los equipos no estén expuestos a sobrecargas, además el tipo de red usada en la organización debe ser estandarizada, con la finalidad que todos los procesos sean llevados por una misma línea.

4.2 Definición del Marco de Control Interno para evaluar los procesos tecnológicos

Existen varios estándares para el desarrollo de buenas prácticas de control, que son implementados en las empresas con la finalidad de obtener un mejoramiento en la gestión administrativa de sus procesos para ello se determina un la comparación de los marcos de control.

4.2.1 Marcos Metodológicos y Estándares de Control Interno Tecnológico

Tabla 11.
Cuadro comparativo de marcos metodológicos

ITIL	COSO	ISO 27001	COBIT
Information Technology and Infrastructure Library	Organización de Tecnologías de la Información COSO	Proveedores de cualquier tipo de servicio de seguridad	Control Objectives for Information and related Technology
Es un estándar ligado a la gestión de Servicios de TI	Control interno de administración con respecto al logro de objetivos	Normas para determinar un sistema de seguridad de información en contexto de riesgos de la organización	Enfoque estructurado de buenas prácticas a través de dominios y procesos
Ofrece servicios de calidad obteniendo la satisfacción del cliente	Mide el nivel de madurez aplicando mejores practica en la administración de software	Sistemas de administración de seguridad de información	Alinea metas de negocio mediante modelos de madurez que ayudan a los auditores

Posee dos 43 libros centrales, cubriendo el área de soporte de servicio	Posee 3 objetivos de control Interno, 5 componentes y 17 factores	39 categorías entre otros controles añadidos total de 133	Tiene 34 procesos de TI con 210 objetivos de control

Nota: (Estrella y Alvear, 2013). Evaluacion Técnica Informática del Sistema de Informacion de la empresa COSSFA, utilizando el estàndar internacional COBIT.

Según el cuadro comparativo de la Tabla 11 evidencia que las características del marco de referencia Cobit ponderan sobre los otros marcos, gracias a su adaptabilidad con las metas de negocio permite un control interno eficiente, así como también el establecimiento de políticas claras.

4.2.2 Evaluación de los Objetivos de Control de COBIT 5.0 en relación con la empresa National Tire Experts S.A

Los Niveles de Madurez de la compañía mediante los procesos de dominio que plantea COBIT 5.0, determina en qué nivel de gestión se encuentran los procedimientos que son o que van a ser ejecutados.

La detección de estos procesos, se llevó a cabo mediante la investigación de funciones, normativas, documentos proporcionados mediante entrevistas con el encargado del área de TI, el Ing. Marco Galarraga.

Para la selección de los objetivos de control que sean relevantes para el proceso de gestión en el Gobierno de TI, se identificaron los objetivos que se encuentran alineados con los procesos de Cobit como muestra en la Tabla 12.

Luego de alinear totalmente los objetivos de la organización con los de Cobit, se procedió a realizar un mapeo, en el cual se identificó los objetivos que aportan de manera significativa al proceso y que fueron tomados en consideración para el análisis.

Para la aplicación del mapeo detallado en la Tabla 13, se designó una valoración de 5 para los procesos principales (P) y 1 para los secundarios (S), con el fin de identificar fácilmente cuales son los objetivos que contribuyeron de forma significativa con las metas de gobierno relacionando (P) como las más relevantes y (S) las de menor relevancia.

4.2.3. Objetivos corporativos vs objetivos de negocio

Tabla 12.

Objetivos corporativos vs objetivos de negocio

OBJETIVOS CORPORATIVOS COBIT		OBJETIVOS DE NEGOCIO				
		Incrementar la productividad y rentabilidad de la empresa, reduciendo costes de producción.	Extensión del negocio, creando nuevos locales para promover fuentes de trabajo logrando la expansión a nivel nacional	Mejorar la calidad del servicio, con personal altamente calificado y mejora continua de los procesos de negocio	Estimular asociaciones estratégicas promoviendo el desarrollo de consolidación del mercado.	Lograr el crecimiento de la organización en el aérea automotriz obteniendo liderazgo tecnológico
1.	Valor para las partes interesadas de las inversiones de negocio		X			X
2.	Cartera de productos y servicios competitivos					
3.	Riesgos de negocio gestionados (salvaguarda de activo)	X				
4.	Cumplimiento de leyes y regulaciones externas			X		
5.	Transparencia financiera	X				
6.	Cultura de servicio orientada al cliente			X		
7.	Continuidad y disponibilidad del servicio de negocio	X			X	X
8.	Respuestas ágiles a un entorno de negocio cambiante					
9.	Toma estratégica de Decisiones basadas en información					
10.	Optimización de costes de entrega del servicio					
11.	Optimización de la funcionalidad de los procesos de negocio	X				
12.	Optimización de los costes de los procesos de negocio	X	X			
13.	Programas gestionados de cambio en el negocio					
14.	Productividad operacional y de los empleados	X	X	X		
15.	Cumplimiento con las políticas internas					
16.	Personal entrenado y motivado					
17.	Cultura de innovación del producto y del negocio		X		X	X

Nota: (ISACA, 2012). COBIT 5. Un Marco de Negocio para el Gobierno y la Gestion de la empresa.)

Tabla 13.

Mapeo entre Objetivos relacionados con TI en COBIT 5 con procesos

Mapeo entre Objetivos relacionados con TI en COBIT 5 con procesos																			
			Objetivo relacionado con TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro	Disponibilidad de información útil y relevante para la toma de	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
Procesos de COBIT 5			**Financiera**						**Cliente**		**Interna**							**Aprendizaje y Crecimiento**		**VALORACION**
Evaluar, Orientar y Monitorizar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	5	1	5	1			5		1	1	1	1	1	1	1	1	1	26
	EDM02	Asegurar la Entrega de Beneficios	5		1		5	5	5	1			1	1	1	1		1	5	32
	EDM03	Asegurar la Optimización del Riesgo	1	1	1	5		5	1	1		5			1	1	5	1	1	29
	EDM04	Asegurar la Optimización de los Recursos	1		1	1	1	1	1	1	5		5		1			5	1	24
	EDM05	Asegurar la Transparencia hacia las partes interesadas	1	1	1			5	5						1	1	1		1	17

Tabla 13.

Mapeo entre Objetivos relacionados con TI en COBIT 5 con procesos (continuación)

Alinear, Planificar y Organizar	**APO01**	Gestionar el Marco de Gestión de TI	5	5	1	1			1		5	1	5	1		1	5	5	5	41
	APO02	Ge1tionar la E1trategia	5		1	1	1		5	1	1		1	1	1	1	1	1	5	26
	APO03	Ge1tionar la Arquitectura Empresarial	5		1	1				1	5	1	1	1		1			1	17
	A5O04	Gestionar la Innovación	1			1	5			5	5		5	1		1			5	34
	APO05	Gestionar el Portafolio	5		1	1	5	1					1		5				1	19
	APO06	Gestionar el Presupuesto y los Costes	1		1	1	5	5	1	1			5		1					21
	APO07	Gestionar los Recursos Humanos	5	1	1	1			1		1	1	5		5		1	5	5	32
	APO08	Gestionar las Relaciones	5					1	5				1		1				5	18
	APO09	Gestionar los Acuerdos de Servicio	1						5	1			1		1	5	1			15
	A5O10	Ge1tionar lo1 5roveedore1		1		5	1	1	5	1	5	1	1		1	1	1		1	25
	APO11	Ge1tionar la Calidad	1	1		1	5		5	1	1		1		5	1	1	1	1	25
	A5O12	Ge1tionar el Rie1go		5		5		5	1	1	1	5			5	1	1	1	1	32
	APO13	Ge1tionar la 1eguridad		5		5		5	1	1		5				5				27
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	5		1	5	1						1		1			1	1	16
	BAI02	Gestionar la Definición de Requisitos	5	1	1	1	1		5	1	1	1	1	5	1	1			1	26
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	1			1	1		5	1			1	1	1	1			1	14
	BAI04	Ge1tionar la Disponibilidad y la Capacidad				1	1		5	1	1		5		1	5			1	21
	BAI05	Gestionar la introducción de Cambios Organizativos	1		1		1		1	5	1		1	1	1				1	14

Tabla 23.

Mapeo entre Objetivos relacionados con TI en COBIT 5 con procesos (continuación)

	BAI06	Gestionar los Cambios			1	5	1		5	1	1	5	1	1	1	1	1		1	25
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				1	1		1	5	1			5	1	1	1		1	18
	BAI08	Gestionar el Conocimiento	1				1		1	1	5	1	1			1		1	5	18
	BAI09	Gestionar los Activos		1		1		5	1		1	1	5			1	1			17
	BAI10	Ge1tionar la Configuración		5		1		1		1	1	1	5			5	1			21
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		1		5	1		5	1	1	1	5			1	1	1	1	24
	DSS02	Gestionar las 5eticiones y los Incidentes del Servicio				5			5	1		5				1	5		1	23
	DSS03	Gestionar los Problemas		1		5	1		5	1	1		5	1		5	1		1	27
	DSS04	Gestionar la Continuidad	1	1		5	1		5	1	1	1	1	1		5	1	1	1	26
	DSS05	Gestionar los Servicios de Seguridad	1	5		5			1	1		1	1	1		1	1			18
	DSS06	Gestionar los Controles de los Procesos del Negocio		1		5			5	1		1	5	1		1	5	1	1	27
Supervisar, Evaluar y Valorar (MEA)	MEA01	Supervisar, evaluar y valorar el rendimiento y la conformidad.		1			1	1	5		1				5	5		5		24
	MEA02	Supervisar, evaluar y valorar el sistema de control interno	5	1		5			1	1	1	5			5		1	1		26
	MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos.		5	1			1		1			5			5	5			23

Nota. Tomada como referencia de (ISACA, 2012)

4.2.4 Determinación del nivel de madurez de los procesos del área de TI de la Empresa National Tire Experts S.A

A continuación la evaluación y análisis de cada dominio según la clasificación de los objetivos de control de COBIT 5.0, definidos en la tabla anterior, aplicables para la ejecución de la auditoría a la empresa National Tire Experts S.A.

Tabla 14.

Análisis de Objetivos de dominio Evaluar, Orientar y Supervisar (EDM)

EDM01: Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno:	**0 Proceso Incompleto**
	No existe un modelo estratégico de toma de decisiones para que las TI sean efectivas y estén alineadas con el entorno externo e interno de la empresa y los requerimientos de las partes interesadas. No existe un sistema de gobierno de TI. Los riesgos y beneficios al usuario, resultado de decisiones estratégicas importantes se reconocen de forma intuitiva. **Fuente: Entrevista dirigida al encargado del área de TI.**
EDM02: Asegurar la entrega de beneficios	**0 Proceso Incompleto**
	Hay un control de presupuestos pero no se proyectan ni controlan beneficios. No existe un portafolio de iniciativas de TI Los presupuestos de proyectos individuales son gestionados y controlados. Sin embargo no se gestionan los beneficios de las inversiones en TI. **Fuente: Entrevista dirigida al encargado del área de TI.**
EDM03: Asegurar la optimización del Riesgo	**0 Proceso Incompleto**
	No cumple. En su organización no cuenta con una visión de riesgo, aun no se han tomado decisiones al respecto y no se ha realizado todas las evaluaciones de riesgos a los que se expone la TI de la organización **Fuente: Entrevista dirigida al encargado del área de TI.**

EDM4 Asegurar la optimización de recursos	0 Proceso Incompleto
	No existe un planificación de recursos, la aprobación de estos recursos son realizadas por la gerencia Financiera, no existe presupuestos definidos. **Fuente: Entrevista dirigida al encargado del área de TI.**

4.2.4.2 Dominio: Alinear, Planear y Organizar (APO)

Tabla 14.1

Análisis de Objetivos de dominio Alinear , Planear y Organizar (APO)

APO01 Gestionar el marco de trabajo de Administración de TI	1 Proceso Ejecutado
	No existe un plan estratégico de tecnología definido y alineado. Existe la necesidad de establecer políticas, lineamientos y procedimientos, debido a que estos no están debidamente documentados. **Fuente: Entrevista dirigida al encargado del área de TI.**
APO02 Gestionar la Estrategia	**0 Proceso Incompleto**
	Se han determinado las diferentes estrategias que pueden ser planteadas para mejoramiento del entorno de TI. No se han documentado, ni se han asignado responsabilidades. **Fuente: Guía de Observación aplicada en el área de TI.**
APO04 Gestionar la Innovación	**1 Proceso Ejecutado**
	EL área de TI, ha analizado las debilidades y deficiencias del departamento en cuanto a innovación tecnológica. No posee un plan definido pero se ha planteado soluciones para mejora de los servicios e innovación de las tecnologías ya utilizada **Fuente: Guía de Observación aplicada en el área de TI**

APO06 Gestionar el presupuesto y los costos	**0 Proceso Incompleto**
	Existe la necesidad de identificar y asignar presupuestos y costos. Estos costos pueden reasignarse pero no está definida una estructura de asignación de responsabilidades que definan los costos y presupuestos generadores de valor para cada recurso. **Fuente: Entrevista dirigida al encargado del área de TI**
APO07.Gestionar los Recursos Humanos:	**0 Proceso Incompleto**
	Existe una sola persona encargada de área de tecnología, la carga laboral es grande. Por ende este recurso es limitado, falta definir ciertas funciones del área para poder mitigar cualquier riesgo que se presente. El área no cuenta con una planificación de mantenimiento, capacitación o entrenamiento del personal, estos procesos se realizan de forma informal. **Fuente: Entrevista dirigida al encargado del área de TI**
APO10 Gestionar los proveedores	**0 Proceso Incompleto**
	No existe un proceso que defina las condiciones estándares de los proveedores de servicio. Por ende tampoco está definido el proceso de selección de los mismos los riesgos y la prestación de servicio es informal. **Fuente: Entrevista dirigida al encargado del área de TI**
APO11 Gestionar la Calidad	**0 Proceso Incompleto**
	No existen recursos definidos para ejecutar un plan de aseguramiento de la calidad de los procesos de la organización, el personal no cuenta con conocimientos para desarrollo de aplicaciones. **Fuente: Entrevista dirigida al encargado del área de TI**
APO12 Gestionar los Riesgos	**0 Proceso Incompleto**
	Los riesgos asociados a los procedimientos de la organización no están definidos. No se han tenido en cuenta los efectos producidos por la vulnerabilidad de seguridad. La administración del riesgo no forma parte de los procesos de servicios de TI esenciales de la empresa. Además no se ha determinado una matriz de gestión de riesgos. **Fuente: Entrevista y Guía de Observación dirigida al encargado del área de TI**

APO13 Gestionar la seguridad	1 Proceso Ejecutado
	Existen aplicaciones que garantizan la seguridad de la información, mediante los servidores , pero no existe ninguna política definida y debidamente documentada de monitoreo en cada proceso , no existen controles que detecten fallas de seguridad **Fuente: Entrevista dirigida al encargado del área de TI**

4.2.4.3 Dominio: Construir, Adquirir y Operar (BAI)

Tabla 14. 2

Análisis de Objetivos de dominio Construir , Adquirir y Operar (BAI)

BAI02 Gestionar la Definición de Requerimientos	0 Proceso Incompleto
	No hay un proceso definido para el mantenimiento y adquisición de requerimientos de TI. No existe una planificación para este proceso, en cuanto a infraestructura de forma periódica. Los sistemas pasan un periodo de prueba realizadas por los usuarios para su debida aprobación. **Fuente: Entrevista dirigida al encargado del área de TI**
BAI03 Gestionar la Identificación y Construcción de Soluciones	**0 Proceso Incompleto**
	La identificación de soluciones depende de cada experiencia , no existen requerimientos estructurados que ayuden a definir soluciones tecnológicas **Fuente: Entrevista dirigida al encargado del área de TI**
BAI06 Gestionar los Cambios	**0 Proceso Incompleto**
	Estos procesos no están estructurados, los cambios no son realizados de acuerdo a cronogramas definidos. No existen políticas de cambios en el sistema, del personal de manejo de la configuración o programas en la empresa. **Fuente: Guía de observación aplicada al área de TI**

4.2.4.4 Dominio: Entregar Servicio y Soporte (DSS)

Tabla 14.3

Análisis de Objetivos de dominio Entregar Servicio y Soporte (DSS)

DSS01 Gestionar las Operaciones	**1 Proceso Ejecutado**
	Se puede evidenciar que existe una alta dependencia de las habilidades del encargado el área tecnológica, se registran logs de servidores de correo, y aplicaciones, pero no son utilizados para asegurar el control de acceso a los usuarios en aplicaciones que no son de carácter laboral. Los procesos de mantenimiento de la infraestructura no están documentados y dependen de la disponibilidad del encargado de área. Los altos ejecutivos están desarrollando un plan de implementación de medidas de seguridad en la infraestructura pero aún no se tiene un modelo concreto **Fuente: Guía de observación aplicada al área de TI**
DSS02 Gestionar las solicitudes de Servicio e Incidentes	**0 Proceso Incompleto**
	EL área tecnológica trata de realizar y abastecer la demanda de incidentes de los usuarios, no poseen una estructura específica para el soporte. Existe la necesidad de contar con personal adicional con el cual se pueda abastecer la demanda, y así poder obtener una administración de atención de soporte a usuario eficiente. Los procesos no se documentan, no existe un estándar ni tampoco un registro formal. **Fuente: Guía de observación y entrevista aplicada al área de TI**
DSS03 Gestionar los problemas	**0 Proceso Incompleto**
	No existe conciencia sobre la necesidad de gestión de los problemas, no se han realizado ningún intento de identificar las causas de los incidentes. Existe la necesidad de asesorías que resuelvan la causa, pero no hay asignación de responsabilidad de gestión de problemas. **Fuente: Guía de observación y entrevista aplicada al área de TI**

DSS04 Gestionar la Continuidad	**0 Proceso Incompleto**
	No existe un plan de continuidad de TI. Las prácticas de continuidad emergen, el triunfo depende de cada individuo, existe el compromiso de mantener la continuidad del servicio. **Fuente: Guía de observación y entrevista aplicada al área de TI**
DSS05 Gestionar los Servicios de Seguridad	**1 Proceso Ejecutado**
	La necesidad de seguridad es ilimitada. Los servicios a terceros no cumplen con todos los requerimientos de seguridad de la organización. Aun no se han asignado los roles de seguridad y la supervisión de seguridad de accesos físicos y lógicos de los usuarios y las aplicaciones. **Fuente: Guía de observación aplicada al área de TI**
DSS06 Gestionar los Controles de Procesos de Negocio	**0 Proceso Incompleto**
	Los procesos de TI no están definidos, los mismos que deben ser mapeados con los procesos de negocio de la empresa. No se ha realizado ningún proceso u operación adecuada para la gestión y el control del aseguramiento de la información. **Fuente: Guía de observación y entrevista aplicada al área de TI**

4.2-4.5 Dominio: Monitorear, Evaluar y Valorar (MEA)

Tabla 14.4.

Análisis de Objetivos de dominio Monitorear, Evaluar y Valorar (MEA)

MEA01 Monitorear , Evaluar y Valorar el Desempeño y Conformidad	**0 Proceso Incompleto**
	La empresa no cuenta con un proceso de monitoreo. No existen reportes oportunos y precisos que indiquen el avance de los objetivos de la empresa. **Fuente: Entrevista dirigida al encargado del área de TI**

MEA02 Monitorear, Evaluar y Valorar el Sistema de Control Interno	**0 Proceso Incompleto**
	Carece de procesos de monitoreo de la efectividad de los controles internos de la organización. Existe falta de conciencia de aseguramiento de control interno de TI. El área de TI reconoce la necesidad de un registro y gestión en el manejo de la información, sin embargo no se han definido proceso de evaluación y recolección. **Fuente: Guía de observación y entrevista aplicada al área de TI**
MEA03 Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos	**0 Proceso Incompleto**
	La organización no cuenta con un sistema de control interno que regule los requerimientos externos y su cumplimiento. Existe la necesidad de administrarlo de forma regular. No se han asignado responsabilidades formales que permitan hacer un seguimiento de la efectividad del control interno. **Fuente: Guía de observación y entrevista aplicada al área de TI**

4.5 Análisis de Riesgo de los procesos existentes

4.5.1 Análisis de evaluación de Riesgos.

Se puede apreciar en la tabla 15, los riesgos que se clasificaron en las Tabla 3 en Entorno (E), Tabla 4 Talento Humano (TH), Tabla 5 Físico (F), Tabla 6 Procesos Internos (PI), Tabla 7 Seguridad(S) y Tabla 8 Infraestructura Tecnológica (ITE), determinando su nivel de Impacto, y relacionados con los objetivos de control proporcionados por COBIT, los mismos que fueron seleccionados en la Tabla 13.

Para determinar el nivel de impacto que produce cada riesgo definido en la matriz dependiendo del impacto, frecuencia y Tolerancia son codificados en Muy alto (5), Alto (4), Medio (3), Bajo (2) y Muy bajo (1).

Tabla 15.

Nivel de Riesgos según procesos de control COBIT

Proceso	Muy Alto	Alto	Medio	Bajo	Muy Bajo
APO. Alinear , Planear y Organizar	3	6	4	1	0
EDM. Evaluar, Orientar y Supervisar	0	5	1	0	0
DSS. Entregar Servicio y Soporte	2	4	3	1	1
BAI. Controlar, Adquirir y Operar	1	0	1	0	0
MEA. Monitorear, Evaluar y Valorar	1	0	3	0	0
TOTALES	8	15	12	2	1

Luego de haber culminado el análisis de riesgos como lo muestra la Tabla 12, se pudo evidenciar aquellos que necesitan reforzarse y los que están debidamente controlados.

Poniendo más atención en reorganizar sus procesos de acuerdo al efecto que producen cada uno de ellos en la organización, reasignando de mejor manera los recursos adaptándolos a los requerimientos que se presenten a corto, mediano y largo plazo.

Se debe tener mayor énfasis por parte de la Gerencia a los elementos que se identificaron con un riesgo Muy Alto, Alto y Medio, debido a que estos son una parte fundamental del fortalecimiento del negocio.

Se deben tomar decisiones acertadas para aquellas propuestas de las que se puedan obtener beneficios para la empresa, impulsando un mejor entorno en la aplicación de las mismas. Además se debe considerar que deben estar vinculadas a las estrategias planteadas y con las metas propuestas por el área de TI.

Otro paso importante es el de establecer el avance de los procesos nuevos y corregir los que están hechos y así asegurar que los mismos se encuentren en un progreso continuo.

Se deben instaurar medios que ratifiquen la gestión precisa de las necesidades que puedan producirse de acuerdo a los procedimientos regulados por los organismos de control de la compañía.

Según el análisis de los elementos de riesgo, alineados con los objetivos de control de Cobit se instauran estrategias que le permitirán a la empresa implementar procesos que mediante su aplicación aseguren una mejora continua de los procesos.

Tabla 16.
Matriz de Riesgo Empresa National Tire Experts S.A

4. 5 Matriz de Riesgo Empresa National Tire Experts S.A																						
Nº de Riesgo	*Tipo de riesgo*	*Riesgo*	*DOMINIOS COBIT*	*Síntoma*	Frecuencia					Impacto					Ponderación					Codificación	*Propuesta*
					Altamente Improbable.	Improbable	Eventual	Probable	Altamente Probable.	*Muy Baja*	Baja	Moderada.	Alto	Muy Alto.	Muy Bajo	Bajo	*Medio*	*Alto*	*Muy Alto*		
					1	2	3	4	5	1	2	3	4	5	(1-2)	(3-4)	(5-9)	(10-16)	(20-25)		
E1	Entorno	Limitación de medidas preventivas por desastres naturales	APO12	En caso de ocurrir un desastre natural, la empresa no cuenta con procesos de prevención ante estos eventos. Ocasionando pérdidas y gastos para la compañía	1					5					5					Medio	Incluir en el plan estratégico lineamientos o políticas sobre medidas preventivas ante desastres
E2	Entorno	Falta de mantenimiento permanente de las instalaciones eléctricas	DSS03	El mantenimiento de las instalaciones de forma periódica permitirá que la operatividad de los sistemas de la organización funcione de forma efectiva previniendo problemas futuros	2					1					2					Muy Bajo	Generar políticas de mantenimiento de la infraestructura eléctrica de la compañía
TH01	Talento Humano	Falta de personal especializado de TI	APO07	El no contar con todo el personal adecuado para cumplir con los requerimientos del área de TI, no permite que el soporte y la atención a los usuarios sea eficiente y rápida	4					4					16					Alto	Generar Herramientas estándar ligado a capacitaciones a los empleados en el uso de estas.

Tabla 16.
Matriz de Riesgo Empresa National Tire Experts S.A (Continuación)

(continuacion) 4. 5 Matriz de Riesgo Empresa National Tire Experts S.A																						
Nº de Riesgo	*Tipo de riesgo*	*Riesgo*	*DOMINIOS COBIT*	*Síntoma*	Frecuencia					Impacto					Ponderación					Codificación	*Propuesta*
					Altamente Improbable.	Improbable	Eventual	Probable	Altamente Probable.	*Muy Baja*	Baja	Moderada.	Alto	Muy Alto.	Muy Bajo	Bajo	*Medio*	*Alto*	*Muy Alto*		
					1	2	3	4	5	1	2	3	4	5	(1-2)	(3-4)	(5-9)	(10-16)	(20-25)		
TH02	Talento Humano	La capacitación de los empleados de TI es mínima	APO07	La falta de planificación en la asignación de recursos y el mejoramiento de los conocimientos de los empleados del área de TI , permite que no se cumpla con los lineamientos y estándares en el manejo de herramientas y aplicaciones que esta área necesita tener	3					3					9					Medio	Crear políticas de capacitación , con alcances y sus objetivos
TH03	Talento Humano	Documentación de planificación de capacitación del personal regular	APO07	No existe una documentación que permita la distribución de la capacitación del personal en cuanto a sistema y aplicaciones que utilizan los usuarios en las diferentes funciones que desempeñan	1					3					3					Bajo	Elaborar la documentación que distribuya mediante cronogramas los procesos de capacitación de cada uno de los empleados en las herramientas que utiliza
F01	Físicos	Hardware no adecuado para el desempeño de funciones	EDM04 APO04	Existen muchas carencias en ciertos procesos y equipos utilizados en el área de TI que limitan el desempeño normal y efectivo de sus funciones	5					3					15					Alto	Los usuarios deben hacer uso del software que esté de acuerdo con la capacidad de los equipos, también se podría analizar la obtención de nuevos equipos.

Tabla 16.
Matriz de Riesgo Empresa National Tire Experts S.A (Continuación)

(continuacion) 4. 5 Matriz de Riesgo Empresa National Tire Experts S.A																						
Nº de Riesgo	*Tipo de riesgo*	*Riesgo*	*DOMINIOS COBIT*	*Síntoma*	Frecuencia					Impacto					Ponderación					Codificación	*Propuesta*
					Altamente Improbable.	Improbable	Eventual	Probable	Altamente Probable.	*Muy Baja*	Baja	Moderada.	Alto	Muy Alto.	Muy Bajo	Bajo	*Medio*	*Alto*	*Muy Alto*		
					1	2	3	4	5	1	2	3	4	5	(1-2)	(3-4)	(5-9)	(10-16)	(20-25)		
F02	Físicos	Espacio físico limitado para equipos	EDM04	El no tener un espacio adecuado para la instalación y funcionalidad de equipos para el área no permite que se implementen nuevos herramientas , aplicaciones y equipos necesarios para el control, gestión y organización de todas las funciones que el área de TI debe realizar	5					3					15					Alto	Elaborar un diseño de una nueva infraestructura analizando los lineamientos y los requerimientos del negocio.
F03	Físicos	Falta de estrategias preventivas contra daños	APO02	No existe un control en la distribución estrategias que impidan el mal uso de la infraestructura de la compañía mediante políticas que ayuden con la continuidad del negocio	3					3					9					Medio	Detectar los posibles causas de fallas y en base a esto desarrollar estrategias preventivas
F04	Físicos	Falta de documentación de requerimientos del área de TI	APO06 BAI02	La asignación de recursos físicos no se ha distribuido de acuerdo a los necesidades del área de TI , la debida documentación de estos requerimientos proporcionará una asignación optima de los equipos y recursos	4					2					8					Medio	Realizar la documentación de los requerimientos de la organización

Tabla 16.

Matriz de Riesgo Empresa National Tire Experts S.A (Continuación)

(continuacion) 4. 5 Matriz de Riesgo Empresa National Tire Experts S.A																						
Nº de Riesgo	*Tipo de riesgo*	*Riesgo*	*DOMINIOS COBIT*	*Síntoma*	Frecuencia					Impacto					Ponderación					Codificación	*Propuesta*
					Altamente Improbable.	Improbable	Eventual	Probable	Altamente Probable.	*Muy Baja*	Baja	Moderada.	Alto	Muy Alto.	Muy Bajo	Bajo	*Medio*	*Alto*	*Muy Alto*		
					1	2	3	4	5	1	2	3	4	5	(1-2)	(3-4)	(5-9)	(10-16)	(20-25)		
F05	Físicos	Ausencia de políticas de uso de HW	DSS02	La documentación de la políticas para el uso de HW, permite una mejor organización en la revisión y manteniendo de herramientas y formas de cómo debe ser el uso y manejo de los recursos	2					3					6					Medio	Formalizar la Documentación de políticas de revisión de equipos
F06	Físicos	Falta de políticas de acceso a usuarios	DSS03 DSS05 APO01	No existe un control efectivo de lineamientos o normas para la utilización y acceso de información y de equipos de usuarios no autorizados. Puede ocasionar perdida de información e infiltraciones que pueden ser perjudiciales para la empresa	2					5					10					Alto	Definir políticas de control de acceso a la información de usuarios y documentarlo.
PI01	Procesos Internos	Falta de políticas de control de incidentes internos	DSS06 MEA02	Existe una persona para dar soporte a todos los usuarios de la empresa. Muchos de los departamentos son desatendidos y la respuesta a estos incidentes es lenta. La falta de personal y la ausencia de normativas de control de incidentes produce muchas veces suspensión de actividades	4					5					20					Alto	Implementar y documentar políticas y procesos manejo de incidentes en la empresa

Tabla 16.
Matriz de Riesgo Empresa National Tire Experts S.A (Continuación)

(continuacion) 4. 5 Matriz de Riesgo Empresa National Tire Experts S.A																						
Nº de Riesgo	*Tipo de riesgo*	*Riesgo*	*DOMINIOS COBIT*	*Síntoma*	Frecuencia					Impacto					Ponderación					Codificación	*Propuesta*
					Altamente Improbable.	Improbable	Eventual	Probable	Altamente Probable.	*Muy Baja*	Baja	Moderada.	Alto	Muy Alto.	Muy Bajo	Bajo	*Medio*	*Alto*	*Muy Alto*		
					1	2	3	4	5	1	2	3	4	5	(1-2)	(3-4)	(5-9)	(10-16)	(20-25)		
PI02	Procesos Internos	Falta de definición de soporte de TI de las aplicaciones de la organización	DSS02	Existe falta de implementación de lineamientos para el uso de aplicaciones, incluyendo capacitación, seguridades, etc. que ayudarían en la organización del área con el fin de que las soluciones sean atendidas de forma efectiva	3					3					9					Medio	Asignar un soporte para herramientas de la organización
PI03	Procesos Internos	Falta de manuales y procedimientos de configuración en el manejo de aplicaciones	DSS02	El usuario no puede dar solución a dudas o incidentes sobre herramientas de la organización. Debido a la no existencia de manuales de usuario para esto. YA que siempre se debe pedir solución al experto de la herramienta, haciendo que el usuario dependa específicamente de otra persona para realizar cualquier tarea	2					2					4					Bajo	Crear manuales de usuario para herramientas de la organización
S01	Seguridad	Seguridad en el manejo de la Información	APO13 DSS05	La seguridad de la información no es resguardada adecuadamente, por ende se han presentado varias eventualidades en su manejo, respaldo y resguardo de la información.	5					5					25					Muy Alto	Evaluar los procesos que ya están definidos y plantear nuevos a fin de que determine qué políticas deben ser implementadas para luego formalizarlas

Tabla 16.
Matriz de Riesgo Empresa National Tire Experts S.A (Continuación)

(continuacion) 4. 5 Matriz de Riesgo Empresa National Tire Experts S.A																								
Nº de Riesgo	*Tipo de riesgo*	*Riesgo*	*DOMINIOS COBIT*	*Síntoma*	Frecuencia					Impacto					Ponderación					Codificación	*Propuesta*
					Altamente Improbable.	Improbable	Eventual	Probable	Altamente Probable.	*Muy Baja*	Baja	Moderada.	Alto	Muy Alto.	Muy Bajo	Bajo	*Medio*	*Alto*	*Muy Alto*		
					1	2	3	4	5	1	2	3	4	5	(1-2)	(3-4)	(5-9)	(10-16)	(20-25)		
S02	Seguridad	Seguridad de Control de Accesos al personal en todas las aéreas de la organización	DSS01 DSS05	La seguridad en el ingreso a las instalaciones del área de TI es mínimo, no existe un control en los diferentes niveles d acceso a personal externo a la compañía					5					5					25	Muy alto	Formalizar políticas de control de acceso a personas ajenas a la organización
S03	Seguridad	Falta de plan de contingencias	EDM03 DSS01	No existe un plan que permita la prevención de cualquier eventualidad que se presente en la infraestructura del área de TI, El encargado de TI no conoce los lineamientos que debe seguir en caso de siniestros					3					3					9	Medio	Implementar un plan de contingencias
S04	Seguridad	Políticas de respaldo de información	DSS05 APO01	El área de TI posee procesos para generar los respaldos de información planificadamente acción relevante para la organización, pero no está documentado, no posee políticas que ayuden a que estos procesos se lleven de manera adecuada.					3					4					12	Alto	Crear y analizar políticas para cada proceso de respaldo de información con el fin de mantener una organización del proceso

Tabla 16.
Matriz de Riesgo Empresa National Tire Experts S.A (Continuación)

(Acontinuacion) 4. 5 Matriz de Riesgo Empresa National Tire Experts S.A																					
Nº de Riesgo	*Tipo de riesgo*	*Riesgo*	*DOMINIOS COBIT*	*Síntoma*	Frecuencia					Impacto					Ponderación					Codificación	*Propuesta*
					Altamente Improbable.	Improbable	Eventual	Probable	Altamente Probable.	*Muy Baja*	Baja	Moderada.	Alto	Muy Alto.	Muy Bajo	Bajo	*Medio*	*Alto*	*Muy Alto*		
					1	2	3	4	5	1	2	3	4	5	(1-2)	(3-4)	(5-9)	(10-16)	(20-25)		
ITE01	Infraestructura tecnológica	Carencia de políticas y funcionalidades en la adquisición de equipos	APO04 APO06 EDM02	No existe normativas que ayuden a la gestión de procesos en la adquisición de equipos e infraestructura tecnológica	4					3					12					Alto	Implementar políticas de gestión en la adquisición de equipos e infraestructura debidamente documentada
ITE02	Infraestructura tecnológica	Organización de procesos de control de cambios a nivel de software	EDM04 APO04 APO06	Cuenta con ciertos procesos de control de cambios de software, aunque estos procesos sean manejados desde Gerencia Financiera, no se lleva un control de la adquisición de aplicaciones debidamente licenciadas , no existen procesos debidamente documentados	4					3					12					Alto	Analizar los cambios de SW que se van a realizar , se debe considerar las ventajas y desventajas de las aplicaciones comparándolas con las actuales y analizar su factibilidad
ITE03	Infraestructura tecnológica	Organización de procesos de control de cambios a nivel de hardware	EDM04 APO04	Cuenta con ciertos procesos de control de cambios de hw, aunque estos sean manejados desde Gerencia Financiera, no existen procesos debidamente documentados	3					4					12					Alto	Analizar los cambios de SW que se van a realizar , se debe considerar las ventajas y desventajas de las aplicaciones comparándolas con las actuales y analizar su factibilidad

Tabla 16.

Matriz de Riesgo Empresa National Tire Experts S.A (Continuación)

(continuacion) 4. 5 Matriz de Riesgo Empresa National Tire Experts S.A																						
Nº de Riesgo	*Tipo de riesgo*	*Riesgo*	*DOMINIOS COBIT*	*Síntoma*	Frecuencia					Impacto					Ponderación					Codificación	*Propuesta*
					Altamente Improbable.	Improbable	Eventual	Probable	Altamente Probable.	*Muy Baja*	Baja	Moderada.	Alto	Muy Alto.	Muy Bajo	Bajo	*Medio*	*Alto*	*Muy Alto*		
					1	2	3	4	5	1	2	3	4	5	(1-2)	(3-4)	(5-9)	(10-16)	(20-25)		
ITE04	Infraestructura tecnológica	Conexiones de Red inestables	APO10 APO12 BAI03	Las interrupciones en la conexión de internet son muy frecuentes en las diferentes sucursales de la organización, esto ocasiona perdida de transmisión de datos , fallas en la comunicación e interrupción de procesos	5					5					25					Muy Alto	Analizar las falencias en el servicio de Internet contratado por la organización a fin de verificar cuales son las causas, y analizar la contratación de un nuevo proveedor de internet.

4.6 Estrategias de Implementación

Después de la evaluación detallada de los objetivos de control de COBIT y la matriz de gestión de riesgos, se planteó ciertas estrategias de implementación, con el fin de que sean tomadas en cuenta por la organización para el mejoramiento de los procesos de TI en las diferentes áreas de la empresa.

Se han categorizado en 7 estrategias las cuales se detallan a continuación:

1.- Definir un Plan Estratégico

2.-Asegurar la capacitación y Soporte a usuarios

3.-Definir el modelo de Gobierno

4.- Definir normativas y procesos de TI

5.-Implementar Gestión de Riesgos de TI

6.-Implementación de la gestión Continuidad del Negocio

7.-Implementacion de herramientas automatizadas de TI

4.6.1 Estrategia de Implementación 1: Definir un Plan Estratégico de TI

Los diferentes departamentos de la organización, colaborarán para determinar los puntos relevantes de TI que deben ser tomados en cuenta para establecer una planificación Estratégica, que fomente aspectos importantes a los objetivos estratégicos de la organización.

Este plan debe detallar como va a influir las TI en la aplicación de los servicios, cuáles serán sus objetivos, definir responsabilidades, formas de ejecución de funciones, actividades y recursos, presupuestos y todos los requerimientos legales. En los cuales se identifiquen puntos importantes en el establecimiento de políticas contribuyan y vayan de la mano con las metas del negocio para su debida aprobación.

Tabla 16.1.

Actividades de Estrategias de Implementación 1: Definir un Plan Estratégico de TI

Aplicada a Objetivos Cobit: **EDM01-EDM02-EDM03-EDM04-APO01-APO02-APO04-APO06-DSS04**
Actividades : 1. Establecer las metas tácticas de la organización en el área de TI 2. Vincular las metas de la organización con las de TI 3. Crear normas de definición de estrategias en cuanto a tecnología, Riesgos, Administrativas, Financieras, etc. 4. Crear un ámbito de administración y seguimiento en base a planificaciones. 5. Incluir en el Plan Estratégico las funciones del área de TI

4.6.2 Estrategia de Implementación 2: Asegurar la Capacitación y el Soporte a Usuarios

Para la implementación de esta estrategia, la organización deberá plantear una distribución efectiva de niveles de entrenamiento a los usuarios, identificando sus niveles de conocimiento, habilidades y las necesidades de la organización a corto y largo plazo.

Determinar la difusión de asignación de instructores y medir los periodos para cada programa de capacitación, mantener un registro de cada actividad por categorías.
Además deberá contar con la elaboración de evaluaciones con las cuales se pueda medir el desempeño de los usuarios en la mejoras de sus funciones, otro punto importante es el clasificar los requerimientos de los usuarios con el fin de mitigar incidentes que se presenten en el proceso de entrenamiento.

Se garantizará la éxito de esta estrategia desarrollando informes a Gerencia para un monitoreo permanente de cada actividad y poder corregir cualquier falla que se presente.

Tabla 16.2.

Actividades Estrategia de Implementación 2: Asegurar la Capacitación y el Soporte a Usuarios

Aplicada a Objetivos Cobit: **APO06- APO07 - DSS02 – DSS03**
Actividades : 1. Establecer y posicionar los requerimientos de entrenamiento a los usuarios 2. Crear un plan de entrenamiento de acuerdo a los requerimientos. 3. Desarrollar acciones de entrenamiento, tutores y entendimiento. 4. Localizar y registrar incidentes de soporte e información 5. Evaluar, analizar y hacer una valoración de necesidades 6. Informar incidentes para su seguimiento

4.6.3 Estrategia de Implementación 3: Definir el modelo de Gobierno

Primeramente se debe instaurar una delegación estratégica, la cual ayude a que el Gobierno de TI sea utilizado adecuadamente, estableciendo una relación estrecha, regulando la estructura de actividades de TI. Por otro lado, se debe verificar la ejecución de normas y lineamientos que ayudarán en el éxito de las metas y estrategia planteada.

Constituir y aplicar funciones, determinando relaciones y competencias las cuales deben adaptarse a las actividades de TI con la estructura de la organización y notificarlas.

Tabla 16.3.

Actividades Estrategia de Implementación 3: Definir el modelo de Gobierno

Aplicada a Objetivos Cobit: **EDM01-EDM02-EDM03-EDM04-APO01-APO02-APO03- APO07-APO11 – APO13 – BAI03- BAI04 – DSS04 –DSS05 –MEA01-MEA02-MEA03.**
Actividades : 1. Crear y vincular el entorno del Gobierno de TI con las metas de la organización 2. Desarrollar funciones para los miembros de la delegación de TI 3. Instaurar funciones y responsabilidades de TI 4. Establecer responsabilidades de sistemas procesos e información 5. Ajustar las estructura de la organización a las actividades de TI y formalizarlas

4.6. 4 Estrategia de Implementación 4: Definir normativas y procesos de TI

Para implementar esta estrategia la organización deberá identificar normas y procesos que tengan relación del área de TI con otras áreas, impulsando la cooperación, ejecución y renovación permanente de los procesos.

Fomentar el ordenamiento de procesos y normas de TI que permitan reforzar los puntos estratégicos de las TI, haciendo que estos puntos sean relevantes para las operaciones de la organización, notificando debidamente a la Dirección y a los usuarios de la empresa las políticas a fin de que sean documentadas y formalizadas.

Tabla 16.4

Actividades Estrategia de Implementación 4: Definir normativas y procesos de TI

Aplicada a Objetivos Cobit: **APO01-APO06- APO10-APO13 – BAI02 –BAI6-DSS02 –DSS03- DSS04 – DSS05 – DSS06 –MEA01 –MEA02 –MEA03**
Actividades : 1. Crear y desarrollar procesos y normativas relacionadas con TI en otros departamentos 2. Instaurar un ámbito de procedimientos para la actualización de políticas de TI 3. Alinear los procedimientos y lineamientos en un ámbito de control 4. Plantear, formalizar y ejecutar normas y procesos de TI

4.6.5 Estrategia de Implementación 5: Implementar Gestión de Riesgos de TI

Establecer las metas de TI y definir la administración de los riesgos, identificando cuál de los objetivos está ligado a un hecho de riesgo.

Para efectivizar el punto anterior la organización debe emplear un análisis de riesgos, que identifique qué efecto produce este punto en la organización, estructurar funciones de control que permitan priorizar la ejecución de un plan de acción de riesgos que permita monitorear constantemente el impacto de algún evento que se pueda producir.

Tabla 16.5.

Actividades Estrategia de Implementación 5: Implementar Gestión de Riesgos de TI

Aplicada a Objetivos Cobit: **APO12-APO13 – BAI02 – BAI03 - BAI6- DSS02 – DSS03- DSS04 – DSS05 – DSS06 –MEA02 –MEA03**
Actividades : 1. Reconocer y desarrollar los objetivos internos del área de TI y su entorno de riesgo 2. Efectuar una evaluación de riesgo de TI 3. Evaluar los efectos de los riesgos presentados 4. Categorizar por niveles y realizar una planificación de las funciones de control 5. Crear presupuestos para la ejecución de planes de acción ante riesgos 6. Realizar un seguimiento de los planes estratégicos

4.6.6 Estrategia de Implementación 6: Implementación de la gestión Continuidad del Negocio

La empresa National Tire Experts debe instaurar un Ámbito de trabajo que permita ser la base de ejecución e implementación de proyectos de restablecimiento de contingencias, en este ámbito se debe gestionar la prolongación de las tareas.

Promover la distribución de competencias de los servicios en la ejecución de planes de recuperación y plan de contingencias que permitan mitigar el impacto que se llegara a producir debido a la suspensión de actividades debido a desastres. Realizar pruebas periódicas para mantener la continuidad de las TI, fortaleciendo este proceso y sobre todo mantenerlo en vigencia.

Tabla 16.6.

Actividades Estrategia de Implementación 6: Implementación de la gestión Continuidad del Negocio

Aplicada a Objetivos Cobit: **DSS01 - DSS04**
Actividades : 1. Crear un plan de colaboración incluyendo a todas las áreas de la organización 2. Analizar los riesgos que enfrenta la organización 3. Desarrollar una evaluación de los efectos y niveles de riesgos 4. Establecer acciones de disminución de riesgos 5. Realizar monitoreo continuo de los proyectos de continuidad 6. Entrenar e informar a los usuarios 7. Realizar pruebas continuas 8. Realizar un proceso de control de cambios para que estos proyectos tengan validez.

4.6.7 Estrategia de Implementación 7: Implementación de herramientas automatizadas de TI

El uso de Herramientas automatizadas debe permanecer alineadas con las necesidades de la organización, en donde se administre, gestione y controle la seguridad en las áreas de TI. Además debe identificar cuál de estas herramientas es requerida como soporte de los demás departamentos de la empresa.

La empresa debe definir si la aplicación de la(s) herramientas sean adecuadas para su implementación, y estas a su vez deben ser documentadas, debidamente registradas y que sirvan como soporte para el personal de TI y de la organización en general.

Tabla 16.7.

Actividades Estrategia de Implementación 7: Implementación de herramientas automatizadas de TI

Aplicada a Objetivos Cobit: **DSS02 –DSS03– DSS06**
Actividades : 1. Ofrecer a los usuarios herramientas que ayuden a identificar y gestionar los sistemas. 2. Identificar cuáles son las áreas con mayor requerimiento de herramientas. 3. Realizar una evaluación de factibilidad, efecto y estimación de costos en la implementación de las herramientas. 4. Hacer uso de una herramienta automatizada para registrar y documentar todos los procesos efectuados por el personal de TI y de la organización.

4.6.8 DISEÑO DE UNA PROPUESTA DE UNA TOPOLOGÌA DE RED

Como se puede apreciar en la topología propuesta en la figura 8, se estableció una restructuración del diseño anterior, separando el área de servidores de la red de datos mediante la implementación de una zona desmilitarizada o DMZ, que garantiza que los servidores no se encuentren en conexión directa con la red, que todos los departamentos o sectores de la red no tengan fácil acceso a ellos creando una zona segura de vulnerabilidades y ataques.

Esta propuesta tiene como finalidad a una mejor utilización de los recursos, brindar una mejor conectividad entre los equipos informático y rendimiento de aplicaciones.

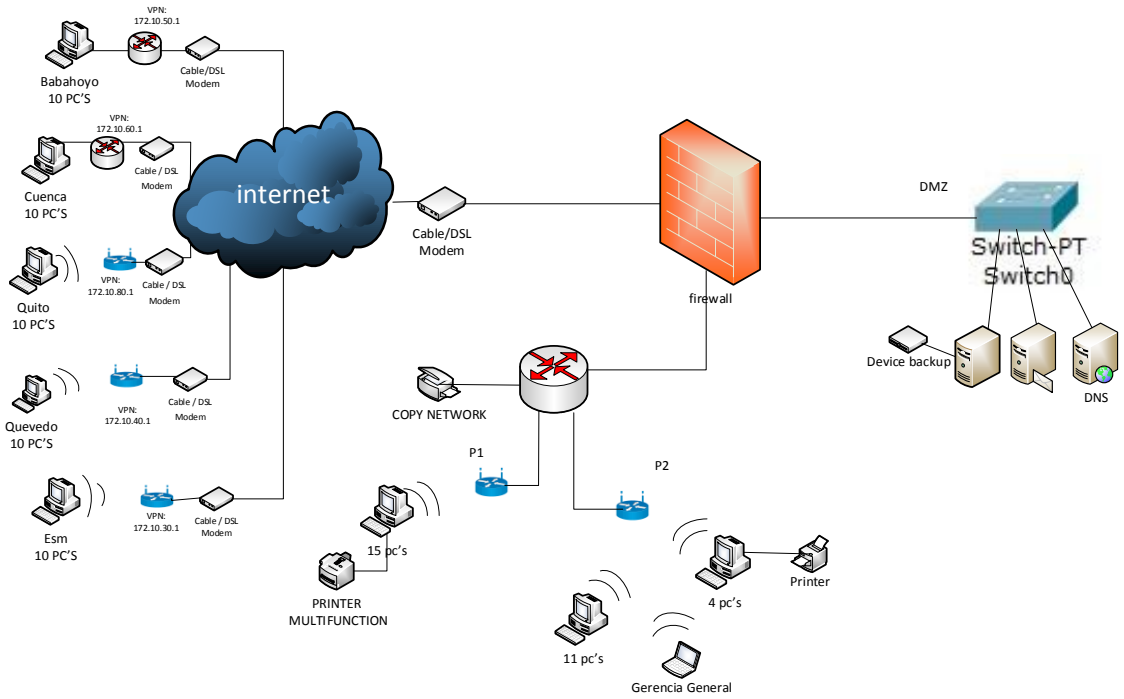


Figura 8. Topología de red propuesta para la empresa National Tire Experts S.A Autor: Vanessa Cedeño

INFORME FINAL

4.7 INFORME FINAL DE EVALUACION DE INFRAESTRUCTURA

EMPRESA: National Tire Experts S.A

4.7.1 ALCANCE: Evaluar la situación actual de la Infraestructura de TI de la Empresa National Tire Experts S.A

4.7.2 METODOLOGIA: La Metodología aplicada en este proyecto es el Marco de Referencia COBIT V5.0 el cual mediante sus objetivos de control, permite identificar el grado de madurez de los procesos de la organización evaluando si estos son aplicables o no.

Los niveles de capacidad de los procesos definidos para esta evaluación son:

Nivel 0: Incompleto El proceso no se ha implementado o no alcanza los objetivos
Nivel 1: Ejecutado El proceso aplicado alcanza su objetivo
Nivel 2: Gestionado El proceso ejecutado se realiza en forma controlada y/o adecuada
Nivel 3: Establecido Utiliza uno ya establecido para definir los resultados
Nivel 4: Predecible Se encuentra en los niveles específicos
Nivel 5: Optimizado Se mejora continuamente para cumplir con los objetivos actuales y futuros.

Además, de la ejecución de COBIT, se aplicaron encuestas de nivel de satisfacción al personal administrativo de la compañía, entrevistas al encargado del área de TI y la aplicación de una guía de observación que sirvieron de herramientas para la obtención adecuada de la información requerida.

Se inició con un análisis de riesgos mediante una matriz, tomando en consideración los procesos que COBIT, de los cuales fueron seleccionados y evaluados 25 objetivos, que proporcionaron la determinación de la situación actual de la empresa en cuanto a infraestructura y gestión de los procesos de negocio se refiere.

De las evidencias que fueron encontradas se procedió con el análisis de los hallazgos encontrados, mediante la presentación de los resultados, especificando criterios acerca de estos resultados y el planteamiento de las estrategias o planes de acción.

4.7.3 EVIDENCIAS ENCONTRADAS

Los procesos seleccionados y ejecutados en esta evaluación se detallan a continuación:

4.7.3.1 PROCESO EDM: EVALUAR, ORIENTAR Y SUPERVISAR

Proceso Incompleto 0:

- No existe un modelo estratégico de toma de decisiones para que las TI sean efectivas y estén alineadas con el entorno externo e interno de la empresa y los requerimientos de las partes interesadas.

- No existe un sistema de gobierno de TI. Los riesgos y beneficios al usuario, resultado de decisiones estratégicas importantes se reconocen de forma intuitiva.

- Hay un control de presupuestos pero no se proyectan ni controlan beneficios. No existe un portafolio de iniciativas de TI. Los presupuestos de proyectos individuales son gestionados y controlados, sin embargo no se gestionan los beneficios de las inversiones en TI.

- La organización no cuenta con una visión de riesgo, aun no se han tomado decisiones al respecto y no se ha realizado todas las evaluaciones de riesgos a los que se expone el área de TI de la organización.

- Además no existe una planificación de recursos, debido a que la empresa no cuenta con presupuestos definidos, su aprobación depende de la gerencia Financiera.

4.7.3.2 PROCESO APO: ALINEAR, PLANEAR Y ORGANIZAR

Proceso Ejecutado 1:

- Existe un plan estratégico pero no se encuentra alineado con el área de tecnología. Existe la necesidad de establecer políticas, lineamientos y procedimientos, debido a que estos no están debidamente documentados.

- En el área de TI se han analizado las debilidades y deficiencias del departamento del cual se encontró que en cuanto a innovación tecnológica no posee un plan definido pero se ha planteado soluciones para mejora de los servicios e innovación de las tecnologías ya utilizadas.

- Existen aplicaciones que garantizan la seguridad de la información, mediante los servidores, pero no existe ninguna política definida de monitoreo en cada proceso, ni controles que detecten fallas de seguridad

Proceso Incompleto 0:

- Existe una sola persona encargada de área de tecnología, por ende este recurso es limitado, falta definir ciertas funciones del área para poder mitigar cualquier riesgo que se presente o a su vez analizar presupuesto para la adquisición de nuevo personal de apoyo en el área.

- El área no cuenta con una planificación de mantenimiento, capacitación o entrenamiento del personal, estos procesos se realizan de forma informal. Además no existe un proceso que defina las condiciones de los proveedores de servicio. Por ende tampoco está definido el proceso de selección de los mismos.

- Los riesgos asociados a los procedimientos de la organización no están definidos. No se han tenido en cuenta los efectos producidos por la vulnerabilidad en la seguridad de la información.

- La administración del riesgo no forma parte de los procesos de servicios de TI esenciales de la empresa, por ende no se ha determinado una matriz de gestión de riesgos.

4.7.3.3 PROCESO BAI: CONSTRUIR, ADQUIRIR Y OPERAR

Proceso Incompleto 0:

- La identificación de soluciones depende de cada experiencia, no existen requerimientos estructurados que ayuden a definir soluciones tecnológicas

- Estos procesos no están estructurados, los cambios no son realizados de acuerdo a cronogramas definidos. No existen políticas de cambios en el sistema, del personal de manejo de la configuración o programas en la empresa.

4.7.3.4 PROCESO DSS: ENTREGAR SERVICIO Y SOPORTE

Proceso Ejecutado 1:

- Se pudo evidenciar que existe una alta dependencia de las habilidades del encargado el área tecnológica, los usuarios no se encuentran en capacidad de solucionar cualquier inconveniente que se presente.

- Los procesos de mantenimiento de la infraestructura no están documentados y dependen de la disponibilidad del encargado de área. Los altos ejecutivos están desarrollando un plan de implementación de medidas de seguridad en la infraestructura pero aún no se tiene un modelo concreto.

- Existe un registro de logs para el control de acceso a aplicaciones, pero no son utilizados para asegurar el control de acceso a los usuarios en aplicaciones que no son de carácter laboral.

- La necesidad de seguridad es ilimitada. Los servicios a terceros no cumplen con todos los requerimientos de seguridad de la organización. Aun no se han

asignado los roles de seguridad y la supervisión de accesos físicos y lógicos de los usuarios y las aplicaciones.

Proceso Incompleto 0:

- El área tecnológica trata de realizar y abastecer la demanda de incidentes de los usuarios, pero no posee una estructura específica para el soporte. Existe la necesidad de contar con personal adicional con el cual se pueda abastecer la demanda, y así poder obtener una administración de atención de soporte a usuario eficiente. Los procesos no se documentan, debido a que no existe un estándar ni tampoco un registro formal.

- No existe conciencia sobre la necesidad de gestión de los problemas, no se han realizado ningún intento de identificar las causas de los incidentes. Se necesita de asesorías que resuelvan la causa, pero no hay asignación de responsabilidad de gestión de problema.

4.7.3.5 PROCESO MEA: MONITOREAR, EVALUAR Y VALORAR

Proceso Incompleto 0:

- La empresa no cuenta con un proceso de monitoreo de la efectividad de los controles internos de la organización, debido a la falta de conciencia de aseguramiento de control interno de TI.

- No existen reportes oportunos y precisos que indiquen el avance de los objetivos de la empresa.

- El área de TI reconoce la necesidad de un registro y gestión en el manejo de la información, sin embargo no se han definido procesos de evaluación y recolección que ayude a la organización con un sistema de control interno que regule los requerimientos externos y su cumplimiento.

- No se han asignado responsabilidades formales que permitan hacer un seguimiento de la efectividad del control interno.

4.7.4 ESTRATEGIAS O PLAN DE ACCIÒN

4.7.4.1 Definir un Plan Estratégico de TI

Los diferentes departamentos de la organización, deben colaborar para determinar los puntos relevantes de TI que deben ser tomados en cuenta para establecer una planificación Estratégica, que fomente aspectos importantes a los objetivos estratégicos de la organización.

Este plan debe detallar cómo influirá las TI en la aplicación de los servicios, cuáles serán sus objetivos, definir responsabilidades, formas de ejecución de funciones, actividades, recursos, presupuestos y todos los requerimientos legales. En los cuales se identifiquen puntos importantes en el establecimiento de políticas que contribuyan y estén alineadas con las metas del negocio para su debida aprobación.

4.7.4.2 Asegurar la Capacitación y el Soporte a Usuarios

Para la implementación de esta estrategia, la organización deberá plantear una distribución efectiva de niveles de entrenamiento a los usuarios, identificando sus niveles de conocimiento, habilidades y las necesidades de la organización a corto y largo plazo.

Determinar la difusión de asignación de instructores y medir los periodos para cada programa de capacitación, mantener un registro de cada actividad por categorías.

Además deberá contar con la elaboración de evaluaciones con las cuales se pueda medir el desempeño de los usuarios en la mejoras de sus funciones, otro punto importante es el clasificar los requerimientos de los usuarios con el fin de mitigar incidentes que se presenten en el proceso de entrenamiento.

Se garantizará el éxito de esta estrategia desarrollando informes a Gerencia para un monitoreo permanente de cada actividad y poder corregir cualquier falla que se presente.

4.7.4.3 Definir el modelo de Gobierno

Primeramente se debe instaurar una delegación estratégica, la cual ayude a que el Gobierno de TI sea utilizado adecuadamente, estableciendo una relación estrecha, regulando la estructura de actividades de TI. Por otro lado, se debe verificar la ejecución de normas y lineamientos que ayudarán en el éxito de las metas y las estrategias planteadas.

Constituir y aplicar funciones, determinando relaciones y competencias las cuales deben adaptarse a las actividades de TI con la estructura de la organización y notificarlas.

4.7.4.4 Definir normativas y procesos de TI

Para implementar esta estrategia la organización deberá identificar normas y procesos que tengan relación del área de TI con otras áreas, impulsando la cooperación, ejecución y renovación permanente de los procesos.

Fomentar el ordenamiento de procesos y normas de TI que permitan reforzar los puntos estratégicos, haciendo que estos puntos sean relevantes para las operaciones de la organización, notificando debidamente a la Gerencia y a los usuarios de la empresa las políticas a fin de que sean documentadas y formalizadas.

4.7.4.5 Implementar Gestión de Riesgos de TI

Establecer las metas de TI y definir la administración de los riesgos, identificando cuál de los objetivos está ligado a un hecho de riesgo.

Para efectivizar el punto anterior la organización debe emplear un análisis de riesgos, que identifique qué efecto produce este punto en la organización, estructurar funciones de control que permitan priorizar la ejecución de un plan de acción de riesgos que monitoree constantemente el impacto de algún evento que se pueda producir.

4.7.4.6 Implementación de la gestión Continuidad del Negocio

La empresa National Tire Experts debe instaurar un ámbito de trabajo que permita ser la base de ejecución e implementación de proyectos de restablecimiento de contingencias, en este ámbito se debe gestionar la prolongación de las tareas.

Promover la distribución de competencias de los servicios en la ejecución de planes de recuperación y plan de contingencias que permitan mitigar el impacto que se llegara a producir debido a la suspensión de actividades debido a desastres.

Realizar pruebas periódicas para mantener la continuidad de las TI, fortaleciendo este proceso y sobre todo mantenerlo en vigencia.

4.7.4.7 Implementación de herramientas automatizadas de TI

El uso de herramientas automatizadas debe permanecer alineadas con las necesidades de la organización, en donde se administre, gestione y controle la seguridad en las áreas de TI. Además se debe identificar cuál de estas herramientas es requerida como soporte de los demás departamentos de la empresa.

También debe definir si la aplicación de la herramienta sea adecuada, a su vez debe ser documentada, debidamente registrada sirviendo de soporte para el personal de TI y de la organización en general.

El planteamiento de estas estrategias de implementación, busca dar a la empresa una pauta en la reorganización de los procesos, controlando el manejo de los recursos, y gestión de seguridad de la información, estableciendo el mejoramiento de la infraestructura logrando llegar a un grado de evolución de los servicios que ofrece a un nivel alto a mediano plazo y un excelente manejo de la información con la finalidad de obtener una ventaja competitiva.

CAPITULO 5

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- COBIT por sus características, principios de control y gestión, prevalece ante otros marcos debido a que su uso garantiza un mejor gobierno de TI, proporcionando una visión clara de la situación tecnológica actual de la organización, asegurando que las metas del negocio se cumplan.

- En la evaluación de Infraestructura mediante Cobit se determinó que la gran parte de los procesos se encuentran en un nivel 0 o Incompleto.

- El principal logro en la aplicación de una metodología de control interno de TI es el uso de técnicas de recolección de datos, encaminando a la institución al cumplimiento de las metas propuestas y control de los procesos tecnológicos.

- Una infraestructura apropiada, disminuirá las vulnerabilidades de los recursos garantizando el desarrollo regular de funciones y procesos tecnológicos de las organizaciones.

- La Implementación de estrategias ayudará a la empresa a alcanzar un grado de madurez superior en el control de los procesos basados en el Marco Metodológico.

- La Administración de Riesgos de TI es importante ya que es una aproximación científica del comportamiento de los riesgos, anticipando posibles pérdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero de las pérdidas que puedan ocurrir.

5.2 Recomendaciones

- La evaluación realizada en este proyecto de investigación provee sugerencias y e indicaciones, que sirven como base para una mejora en la administración de los procesos analizados en el área de TI de la empresa National Tire Experts S.A que deben ser considerados para su implementación.

- Se deben realizar evaluaciones periódicas con el fin de mantener actualizado, con el fin de verificar si existe o no mejoría en los procesos y tomar decisiones.

- La empresa National Tire Experts debe realizar una revisión exhaustiva de las funciones y procedimientos en cuanto a seguridad se refiere, debe poner mayor énfasis en este punto ya que si no cumple con ciertos lineamientos la empresa seguirá teniendo pérdidas de las cuales no podrá recuperarse.

- Para la empresa es útil y necesario la creación de un Plan Estratégico y de Contingencias para el área de TI, que sirva de apoyo para gestionar los procesos del área de forma adecuada y organizada, logrando un mejor desempeño del proceso y del personal que hace uso de ella.

- La Gerencia debe plantear un presupuesto específico en la adquisición y mantenimiento de infraestructura para el área de TI debido a que los requerimientos son ilimitados y no son abastecidos, además la empresa necesita equipos y aplicaciones que permitan que las actividades del área se realicen con eficiencia proporcionando así un nivel de calidad de servicio óptimo.

- Se recomienda incentivar a los usuarios a seguir los lineamientos de seguridad y responsabilidad con su equipo de trabajo. Para mantener un balance en la gestión de riesgos de TI se debe comunicar periódicamente las oportunidades que lo beneficien y los riesgos que lo afecten.

- Poner atención a los criterios evaluados en este proyecto con el propósito de obtener una mejora continua, con procesos inclusivos y controlados apoyados en los lineamientos que COBIT proporciona a través de sus objetivos de control

6. REFERENCIAS

Achina, G. I. (2015). *Análisis y Desarrollo de un Plan de Administración de Infraestructura Interna Basados en Dominios de COBIT para la empresa Softeflex S.A.* Obtenido de http://www.dspace.uce.edu.ec/handle/25000/4226?mode=full

Aguilar, B. S. (enero-agosto de 2005). Formulas para el càlculo de la muestra en investigaciones de salud. *Secretarìa de Salud del Estado de Tabasco*, 333-338. Obtenido de http://www.redalyc.org/pdf/487/48711206.pdf

Agustin. (3 de Julio de 2015). *slideshare.net*. Obtenido de Introducción, • Auditoria Informática o de Sistemas: http://es.slideshare.net/jhzcueva/auditoria-informtica-o-de-sistemas-introduccin

Álvarez, G., & Ezzard, R. R. (s.f.). *Auditoría a la Gestión de las Tecnologías y Sistemas de Información.* Obtenido de http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/indata/Vol6_n1/pdf/auditoria.pdf

Analuisa, E. V., & Erazo, L. T. (Junio de 2007). Auditoria Informática al Departamento de Tecnologías de la Informacion (T.I) de Hidroapute. Quito.

Berná, M. J., & Maciá, P. F. (10 de Julio de 2015). Gobierno y Gestión TI, de la teoría a la experiencia. *Departamento de Tecnología Informática y Computación Universidad de Alicante*.

Bustamante, M. C. (2017). Conectores para redacción de textos. Obtenido de https://mimundoele2.files.wordpress.com/2016/07/conectores-generales.pdf

Clavijo, D. C. (enero-junio de 2006). Políticas de seguridad informática. *Universidad Libre*, págs. 86-92.

Contraloria General del Estado Ecuatoriano. (12 de junio de 2002). Ley Orgánica de la Contraloría Gneral del Estado(LOCGE) . *Decreto ejecutivo Nº548*.

Coraisaca, A. J., & Llumiquinga, P. C. (2012). Trabjo de Grado "Aplicación de COBIT 4.1 en la auditoría de una aplicación Financiera tipo Web de una Institución Financiera". *Escuela Politecnica Nacional*.

Del Peso, N. (2012). *Auditoria de tecnologías y Sistemas de Información.* RA-MA S.A.

Del Peso, N. E., Del Peso, M., & Piattini, V. M. (2008). *Auditoria de Tecnologías y Sistemas de Información.* Alfaomega Ra-Ma.

Díaz, T. G. (3 al 13 de Octubre de 2011). *http://es.slideshare.net/*. Obtenido de http://es.slideshare.net/Tabodiaz/auditoria-informatica-al-departamento-de-ti?qid=0e5f0f42-91ca-44b0-a804-b8c6d29fda5e&v=&b=&from_search=2

Estrella, Z. E., & Alvear, M. S. (Enero de 2013). *Evaluación Técnica Informáica del Sistema de Información de la empresa COSSFA,utilizando el estámdar internacional COBIT.*

Estrella, Z. E., & Alvear, M. S. (2013). Evaluacion Técnica Informática del Sistema de Informacion de la empresa COSSFA, utilizando el estàndar internacional COBIT.

Fernández, G. N. (Octubre de 2005). *Importancia de la auditoría informática.* Obtenido de Universidad Nacional Autónoma de México: http://www.enterate.unam.mx/Articulos/2005/octubre/auditoria.htm

Gaita, C., & Reinaudi, R. (25,26 y 27 de Septiembre de 2012). *El control financiero permanente.Auditoria continua o auditoria desarrollada de modo continuo. Evaluacion de los controles.Evaluación de los riesgos.La informacón necesaria*. Obtenido de http://www.tcuentaslp.gob.ar/wp-content/uploads/2011/01/Auditorias-Financieras-Una-visión-superadora-.pdf

Gómez, E. J. (7 de Octubre de 2013). El Rol de la Auditoría de Sistemas de Información en la evaluación del gobierno de tecnologías de Información en las organizaciones. Bogotá, Colombia.

Hernández, A. A. (25 de julio de 2010). Auditoria Informática y Gestion de Tecnologias de Informacion y Comunicación (TICs). 34. Obtenido de Universidad Centrooccidental Lissandro Alvarado: http://www.redalyc.org/articulo.oa?id=88019355001

Isaca. (2007). *COBIT 4.1 ,IT Governance Institute*. Obtenido de http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf

Isaca. (Octubre de 2008). *Alineando COBIT 4.41, ITIL v3, ISO/MEC 27002 en Beneficio del Negocio.* Obtenido de http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2.7.pdf

ISACA. (2012). COBIT 5. Un Marco de Negocio para el Gobierno y la Gestion de la empresa. 2.

Isaca. (2012). COBIT 5.A Business Framework for Government and Business Management. 2.

ISACA. (2013). *Guia de Auto-Evaluación Usando COBIT 5.* Obtenido de https://www.isaca.org/Journal/archives/2016/Volume-1/Pages/how-cobit-5-improves-the-work-process-capability-of-auditors-spanish.aspx

Jaramillo, A. J. (2013). *"Propuesta de Gestión del Riesgo de Infraestructura Tecnológica Basada en COBIT, para la empresa SOFT WAREHOUSE S.A.".* Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/6247/T-PUCE-6426.pdf?sequence=1&isAllowed=y

Jaramillo, A. J. (2013). *PROPUESTA DE GESTIÓN DEL RIESGO DE INFRAESTRUCTURA TECNOLÓGICA BASADA EN COBIT, PARA LA EMPRESA SOFT WAREHOUSE S.A.* Obtenido de http://repositorio.puce.edu.ec/handle/22000/6247?show=full

Ladino, A. M., Villa, S. P., & López, E. A. (abril de 2011). FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS. 338. Obtenido de http://www.redalyc.org/articulo.oa?id=84921327061

Leal, S. A., & Bermúdez, J. (2006). Análisis situacional de la infraestructura tecnológica del tribunal supremo de justicia. *Universidad Privada Dr. Rafael Belloso Chacín*, págs. 1-17.

NationalTire Experts. (2016). *Mapa de localización de NationalTire Experts S.A*. Obtenido de http://www.tire-experts.com.ec/cparrales/nuestros-locales.html

Navarro, E. d., & Plalttini, M. G. (2008). *Auditoría informática : un enfoque práctico.* España: RA- MA.

Peirano, F., & Suárez, D. (Junio de 2005). *"Las TICs mejoran el desempeño de las PyMEs.Somos capaces de explicar cómo lo hacen?".* Obtenido de https://www.researchgate.net/profile/Diana_Suarez11/publication/237732346_Las_TICs_mejoran_el_desempeno_de_las_PyMEs_Somos_capaces_de_explicar_como_lo_hacen/links/568cfbf308aeb488ea32472f.pdf

Pirela, A. (septiembre-diciembre de 2005). Estudio de un caso de control interno . *Universidad Privada Dr. Rafael Belloso Chacín* , pág. 483.

Redondo, D. R., Llopart, P. X., & Duran, J. D. (1996). AUDITORIA DE GESTION. *Universidad de Barcelona (España)*.

Rodríguez, L. M., Pineiro, S. C., & De Llano, M. P. (2013). Mapa de Riesgos: Identificación y Gestión de Riesgos. *Revista Atlántica de Economía – Volumen 2*.

Rovayo, R. T. (2011). Auditoría Informática y Seguridad de la Información de BDO.

Sahibudin, A. M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in Order to. *Conference on Modelling & Simulation.*, 749-753. Obtenido de Design a Comprehensive IT Framework in Organizations.

Siles, R. P., & Mondelo, E. P. (2012). *Guía de Gestión de Proyectos para Resultados PM4R, 2012.* 2ª edición, BID-INDES. Obtenido de http://es.scribd.com/doc/13889837/Gestion-de-Riesgosla-Matriz-de-Riesgos

Sunagua, D., & Ángel, F. (2013). Auditoría de Seguridad de Información. *Fides Et Ratio [online]*, 19-30.

Vásquez, B. D. (Julio de 2011). Proyecto de Tesis: "Desarrollo de un Plan de administración de Infraestructura Interna Basados en Dominios COBIT para la empresa UNIPLEX S.A". Quito, Pichincha, Ecuador.

Vega, G. M. (2006). Las Auditorias de información en las organizaciones. *Ciencias de la Información*, 3-14. Obtenido de http://oai.redalyc.org/articulo.oa?id=181418190001.

Villardefrancos, Á. M., & Rivera, Z. (2006). La auditoria como proceso de control: concepto y tipología. *Ciencias de la Información, 37()*, 53-59.

WWW.ISO27000.ES. (2016). *Sistema de Gestion de la seguridad de la información.* Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

ANEXO A

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE ESMERALDAS (PUCESE)

ENCUESTA A LOS EMPLEADOS ADMINISTRATIVOS DE LA EMPRESA NATIONAL TIRE EXPERTS S.A

Objetivo: Determinar el grado de satisfacción de los servicios a los usuarios de la Red/sistema de la empresa NationalTire Experts S.A

Marque con una (x) la respuesta que corresponda.

1.- ¿Con que frecuencia su equipo computacional sufre problemas en su funcionamiento?

Nunca ☐
A veces ☐
Casi siempre ☐
Siempre ☐

2.- ¿El servicio da respuesta rápida a incidencias o problemas en su equipo computacional?

Nunca ☐
A veces ☐
Casi siempre ☐
Siempre ☐

3.- ¿Cómo usted considera que es el servicio de Internet que maneja la empresa?

Malo ☐
Regular ☐
Bueno ☐
Excelente ☐

4.- ¿Considera que el área de tecnología cumple con puntualidad con todos los trabajos de soporte o relacionado con informática?

Nunca ☐
Rara vez ☐
Ocasionalmente ☐
Generalmente ☐
Siempre ☐

5.- ¿Cómo considera el servicio brindado por el área de tecnología?

Deficiente ☐
Aceptable ☐
Satisfactorio ☐
Excelente ☐

6.- ¿Qué piensa usted de la capacitación que proporciona el área tecnológica relacionada con Tecnologías de la Información?

No se proporciona ☐
Es ineficiente ☐
Satisfactoria ☐
Excelente ☐

ANEXO B

(ANEXO B1)

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE ESMERALDAS (PUCESE)

ENTREVISTA AL ENCARGADO DEL DEPARTAMENTO INFORMÁTICO DE LA EMPRESA NATIONAL TIRE EXPERTS S.A

PREGUNTAS	N/A	SI	NO	OBSERVACIONES
PLANEACIÓN				
1.- ¿El área de tecnologías de la Información cuenta con políticas establecidas en TI?			x	No, el área carece de políticas internas.
2.- ¿Se ha realizado una planificación estratégica del adecuado uso de la TI?			x	No, si existe planificación estratégica pero no incluye al área de TI.
3.- ¿Existe un plan operativo anual?			x	No, se está planificando una propuesta pero aún no se ha concretado, ni tampoco formalizado
4.- ¿Existe un seguimiento continuo a la política de desarrollo tecnológico y planes operativos anuales?			x	No.
5.- ¿Se cuenta con un plan de infraestructura de redes de datos y eléctrico?			X	
6.- ¿En los últimos 12 meses se ha realizado algún tipo de auditoría en esta área?			X	El área de TI no, solo en el área financiera
7.- ¿De qué tipo? Interna Externa		X		Externa, solo en el área financiera
8 - ¿Existe planes de contingencia del software, de la red y del personal informático?			X	

A. POLÍTICA GLOBAL DE SEGURIDAD				
A1.- ¿Ha tenido la posibilidad de perder información sensible de la organización a causa de algún ataque informático?		X		Si, debido a que no existe un procesos definidos, ni las seguridades necesarias
A2.- ¿Cree que el área está protegida ante la intrusión de hackers informáticos?			X	Faltan recursos para implementar herramientas de protección intrusos
A3.- ¿Tiene conocimiento de las políticas de seguridad orientadas a conservar la integridad, confidencialidad y disponibilidad de la información?		X		Si tengo, conocimiento pero no hay un procedimiento definido para la aplicación y planificación.
A4.- ¿Se hace algún tipo de revisión de los sistemas de información de forma periódica?		X		Si, por parte del proveedor del sistema
A5.- ¿Existen controles que detecten posibles fallas de seguridad?			X	No existen
A6.- ¿Se ha definido el nivel de acceso de los usuarios? Es decir, a que recursos tienen acceso y a que recursos no		X		Si. Cada usuario posee contraseñas para el uso del sistema de información
A7.- ¿Se han definido modelos de amenaza de los que permita identificar y planificar de forma correcta la mejor manera de mitigar las amenazas a las aplicaciones o sistemas de información de la empresa?			X	No, se han definido aun
A8.- ¿Utiliza alguna metodología, técnica o método para la identificación y análisis de vulnerabilidades en el sistema de información de la empresa?			X	No, contamos con ninguna metodología
B. AGRESIONES FÍSICAS EXTERNAS				
B1. ¿Existen filtros y estabilizadores eléctricos en la red eléctrica de suministro a los servidores?			X	No existen recursos asignados

B2. ¿Tienen instaladas fuentes de alimentación redundantes?			X	No existen recursos asignados
B3. ¿Tienen instalados sistemas de información interrumpida?			X	No.
B4. ¿Está preparada la organización para superar cualquier eventualidad que interrumpa las actividades habituales que involucra el uso de las redes de datos o de comunicación?			X	No, Cuando existe cualquier eventualidad, se interrumpe las comunicaciones y toda actividad que tenga que ver con tecnología, debido a que todo se maneja desde la Matriz y por ende las sucursales se ven en la obligación de interrumpir sus actividades.
C. CONTROLES DE ACCESO FÍSICO				
C1.- ¿Existe algún control que impide el acceso físico a los recursos a personal no autorizado?			X	No, hay un control definido
C2. ¿Existe algún mecanismo físico que impida el uso de los sistemas de información a dispositivos o equipos no autorizados?			X	No, no existe
D. SERVIDORES				
D1.- ¿Existen SO servidores, que impiden el acceso a los datos a los usuarios no autorizados en la organización?		X		Si, existe un control de acceso, de usuarios externos
D2.- ¿Están los servidores protegidos en cuanto a inicio de sesión y accesos a través de la red?		X		Sí, todo está controlado a través de contraseñas
D3. ¿Se accede de forma remota?			X	No.
E. COPIA DE SEGURIDAD				
E1.- ¿Se realizan copias de datos? ¿Con qué periodicidad? Diariamente Semanalmente Mensualmente Semestral		X X		Si se realizan
E2. ¿Se prueba la integridad de las copias de seguridad?		X		Si cada vez que se realiza una copia nueva

E3.- ¿Ha probado restaurar alguna copia de seguridad?		X		Si
E4. ¿Ha tenido éxito en la restauración?		X		Sí, no ha existido ninguna complicación
E5.- ¿Existe un procedimiento para obtener las copias de seguridad?			X	No existe un procedimiento formalizado. Se aplican experiencias adquiridas
E6. ¿Está automatizado?		X		Si
E7.- ¿Se almacenan las copias de seguridad en un lugar de acceso restringido?		X		Si, están guardadas bajo llaves pero puede ser violentado, el lugar de almacenamiento no es muy seguro.
E8.- ¿Se almacena alguna copia fuera de las instalaciones de la empresa?		X		Si, se realizan algunas copias para seguridad de la información, se tienen dos copias resguardadas fuera de la institución.
F. MECANISMO DE IDENTIFICACIÓN Y AUTENTICACIÓN				
F1.- ¿Existe un procedimiento de Identificación y autenticación de los usuarios administradores de los servidores?		X		Si.
F2.- ¿Está basado en contraseñas?		X		Si
F3.- ¿Las contraseñas se asignan de forma automática por el servidor?		X		Si, cuando existe un usuario que acceda por primera vez y cuando hay olvido.
F4. ¿Existe un procedimiento de cambio de contraseñas?		X		Si.
G. CONTROLES DE ACCESO				
G1.- ¿Existen controles para el acceso a los recursos?			X	No, los usuarios pueden accesar a cualquier aplicación o herramienta extra laboral sin ningún tipo de control
G2. ¿Existen ficheros de log o similares que registren los accesos autorizados y los intentos de acceso ilícitos?		X		Si existen, pero no se lleva un control sobre esto

G3. Una vez pasados los filtros de identificación, ¿Se han separado los recursos a los que tiene acceso cada usuario?			X	Solo cuando se accede al sistema no a los equipos
H. PLANES DE SEGURIDAD Y CONTINGENCIAS				
H1. ¿Se ha elaborado un plan de seguridad para salvaguarda de activos no tangibles (información) de la organización?			X	No existe, el no contar con talento humano extra en el área de TI es un limitante
H2 ¿Existe un responsable o responsables que coordinen las medidas de seguridad aplicables?			X	
H3.- ¿Se ha elaborado un plan de seguridad?			X	No, pero se tiene en mente trabajar en ello
H4. Se aplica en la organización	X			
H5 ¿Existe un presupuesto asignado para la seguridad en la información?	X			No existe
H6. ¿Cuál es la cuantía? No se asigna recursos Menos de mil Menos de 5 mil Menos de 10 mil Más de 10 mil	X			
H7. ¿Se han incluido en el mismo los aspectos relacionados con las comunicaciones?	X			
H8. ¿El mismo personal de área realiza el plan de seguridad?	X			
H9. ¿Existe un contrato de mantenimiento en el que se priorice la seguridad, los planes de contingencias del software y del personal informático?			X	No existe planificación
H10. ¿Dispone del personal informático involucrado directamente con la seguridad del sistema?			X	No, en el área de TI se requiere más personal debido a que el encargado de todas las funciones soy yo, no logro abastecer todo

				por ende existen retrasos en el soporte a usuarios y para el control de la seguridad.
I. ACCESO A INTERNET				
I1. ¿Existe una política definida para los accesos a Internet?			X	No, los usuarios tienen libertad para el uso de aplicaciones y acceso a internet
I2. ¿Se ha explicado claramente a los usuarios la política?			X	No hay políticas
I3. ¿Existe un acceso a Internet corporativo?		X		Sí, tenemos contratado el servicio de CNT para la conectividad en un plan corporativo
I4. ¿Está limitado el acceso por puesto?			X	Es un servicio Wireless
I5. ¿Existen controles sobre las páginas accedidas por cada puesto o usuario?			X	No, el usuario puede acceder a cualquier pagina
I6. ¿Se revisan las páginas accedidas para tomar medidas contra el usuario que no cumpla sus funciones?			X	No , hay un control sobre este punto
J. ATAQUES INFORMÁTICOS				
J1 ¿Ha identificado ataques generados desde el interior de la organización?		X		Sí, no contamos con una Antivirus con licencia, trabajamos con antivirus gratuitos. Se ha hablado con Gerencia Financiera para asignación de presupuesto pero no se ha autorizado en este y otros incidentes
J2. ¿Suele estar informado sobre las últimas noticias en cuanto a seguridad?		X		Si

(ANEXO B2)

GUIA DE OBSERVACIÓN

PREGUNTAS	N/A	SI	NO	OBSERVACIONES
De qué manera se hace el seguimiento de política de desarrollo tecnológico y planes operativos	X			En la organización no existen planes operativos, ni políticas de control definidas.
¿Quién elabora los planes de contingencia en el departamento?	X			La empresa no cuenta con un plan de contingencias
¿Qué metodología o técnica utiliza para identificar y analizar vulnerabilidades en los sistemas de información?			X	No existe ninguna metodología o técnica
¿De qué manera la organización realiza el punto B4?			X	No existe preparación, cuando existen estas eventualidades , el trabajo es interrumpido hasta la solución de problema
¿Qué tipos de controles se utilizan en el punto C1?			X	No existe control debido a que el área de TI se encuentra en un espacio abierto sin seguridades
¿Quién es el o los responsables del punto H2?		X		El responsable es el encargado del área de TI, pero no existe una planificación , ni asignación de responsabilidades que estén debidamente formalizadas

¿Con que periodicidad se elaboran planes operativos?	X			El área de TI no cuenta con planes operativos documentados.
¿Qué elementos o acciones se llevan a cabo desde la planeación operativa para responder por la seguridad de la información ante agentes internos o externos físicos o lógicos?	X			El área d TI no cuenta con planes operativos
¿Desde la planeación liderada por el área como responde a la necesidad de servicio de la información?	X			No existe un portafolio de servicios
Con que periodicidad se asesora a los usuarios sobre el correcto manejo de las herramientas tecnológicas			X	No existe la asesoría, los usuarios no tienen control de la información que descargan y de todas las aplicaciones que utilizan.
¿Existe proyectos en formulación y/o ejecución que permiten alianzas estratégicas con entidades del nivel regional, nacional internacional para la financiación de los proyectos que brindan acceso a herramientas tecnológicas? ¿Cuáles son?		X		Si existen alianzas, pero los proyectos aún no están bien definidos para su implementación