UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO - CAMPUS SUR

CARRERA: INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del título de: INGENIERO DE SISTEMAS

TEMA:

AUDITORÍA A LA ADMINISTRACIÓN DE LA RED DE DATOS WAN DENOMINADA SOPORTE Y MONITOREO DE LA PLATAFORMA DE CLIENTES IMPLEMENTADA POR TELECOMUNICACIONES FULLDATA CÍA. LTDA. BASADA EN EL MARCO DE TRABAJO COBIT 4.1

AUTORES:

CARLOS ANDRÉS ALVEAR NIACATA

LEONARDO PATRICIO YÁNEZ CÁCERES

DIRECTOR:

JORGE ENRIQUE LÓPEZ LOGACHO

Quito, mayo de 2013

DECLARACIÓN

Nosotros Carlos Andrés Alvear Niacata, Leonardo Patricio Yánez Cáceres, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

----------	**----------**
Carlos Andrés Alvear Niacata	**Leonardo Patricio Yánez Cáceres**
C.I. 1715629588	**C.I. 1720857240**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por los señores: Carlos Andrés Alvear Niacata y Leonardo Patricio Yánez Cáceres, bajo mi dirección.

Ing. Jorge Enrique López Logacho
Director de Tesis

AGRADECIMIENTOS

Agradezco profundamente a todos aquellos que han contribuido a la culminación de este trabajo; principalmente a Dios que guía mi vida día a día y ha sido mi principal fortaleza, a mis padres Fabiola y Claudio a quienes debo la persona que soy y el apoyo incondicional, al Ing, Jorge López, por su guía, paciencia y conocimientos que nos ayudaron a culminar este proyecto y a mis amigos que siempre estuvieron presentes.

Carlos Andrés

Agradezco a Dios por darme la fuerza para concluir este proyecto y no desampararme en ningún momento de mi vida.

Al Ingeniero Jorge López por su apoyo incondicional y guía a través de la realización de nuestra tesis.

A mis padres, hermanos, familiares y amigos por su preocupación, aliento y apoyo durante el desarrollo de este proyecto.

Leonardo Patricio

CONTENIDO

RESUMEN

Hoy en día las tecnologías de la información y comunicaciones constituyen parte esencial dentro de cualquier organización empresarial, dado que manejan el bien más importante de una empresa que es la información, pero la mayoría de empresas subestiman el valor que se le debe dar a las áreas informáticas y de comunicaciones dentro de la gestión empresarial y la manera en como los objetivos de TI van de la mano con los objetivos de la empresa, por lo que se hace necesario recoger, agrupar y evaluar información sobre el manejo de TI para determinar en qué nivel de madurez se encuentra los procesos de administración de cierto sistema informático o área de TI con la finalidad de que los recursos se utilicen eficazmente y se acoplen con los fines de la organización.

Por lo que se han creado normas y estándares que brindan un lineamiento de cómo se deben llevar los procesos que envuelven a la gestión de la información, en este caso se tomó en cuenta a COBIT como metodología para la realización de una auditoria pues ha desarrollado un conjunto de objetivos de control que se encuentran aceptados para las TI y vinculados con la gestión del negocio.

Los objetivos de control de COBIT se encuentran clasificados en cuatro dominios:

- Planear y Organizar
- Adquirir e Implementar
- Entregar y Soporte
- Supervisar y Evaluar

Estos dominios buscan siempre mejorar continuamente de manera cíclica para alcanzar niveles adecuados en los procesos dentro de la administración de TI.

INTRODUCCIÓN

La presente tesis muestra la realización de un proceso de Auditoría a la Gestión Administrativa de la Red de Datos WAN con la cual la empresa FULLDATA CIA. LTDA., presta servicios de soporte y monitoreo a sus diferentes clientes, mediante la aplicación de la metodología presentada por el estándar COBIT. El proceso de auditoría llevado a cabo se basa en la selección de los Objetivos de Control detallados de cada uno de los Procesos COBIT que tienen relación directa con la Administración de procesos acoplándolos a las necesidades de la empresa.

En el Capítulo I, se presenta el Plan de Tesis sugerido, mostrando el planteamiento del problema, objetivo general y específicos, el alcance del proyecto y l metodología a implementarse. Sirviendo como una guía base para la presentación del proyecto.

El Capítulo II, contiene el Marco Teórico en el cual se reúnen conceptos e información detallada y puntual sobre la Gestión de Redes y el marco de trabajo COBIT la metodología en la que se basó la auditoria.

En el Capítulo III, se presenta la Situación Actual de la Empresa así como la administración de riegos mediante la metodología MAGERIT, la cual permite la gestión de riesgos.

En Capítulo IV, se plantea la Auditoria en general, así como los procesos aplicables de cada uno de los dominios de COBIT y las herramientas que se aplicaran a la auditoria.

En el Capítulo V, se presenta la ejecución de la auditoria mediante la aplicación de los procesos adecuados para la Administración de la red WAN de Soporte y Monitoreo acorde a los dominios de COBIT.

En el Capítulo VI, se presentan las conclusiones y recomendaciones en base a la aplicación de la auditoria y las diferentes entrevistas y cuestionarios aplicados al personal de la empresa.

CAPÍTULO 1

PLAN DE TÉSIS

1.1 Tema

Auditoría a la Administración de la Red de Datos WAN denominada Soporte y Monitoreo de la plataforma de clientes implementada por Telecomunicaciones FULLDATA Cía. Ltda. Basada en el Marco de Trabajo COBIT 4.1.

1.2 Planteamiento del Problema

El problema se basa en el desconocimiento de los estándares internacionales respecto a la dirección y control de la Tecnología de Información de la empresa, sin tener claro la necesidad del aseguramiento del valor de TI proporcionado por Telecomunicaciones FULLDATA Cía. Ltda., por lo que la administración, organización, supervisión y control de los elementos involucrados en la interconexión no son evaluados correctamente para proporcionar un nivel de servicio acorde a las necesidades del cliente.

Por estos motivos el manejo de servicios de TI que brinda la empresa necesita una mejor estructura de prestación de los mismos para tener un entendimiento de las necesidades dentro de la red empresarial y el área administrativa a las cuales se da soporte técnico, debido al movimiento del negocio las soluciones tienen que ser rápidas y eficaces.

1.3 Objetivos del Proyecto

Objetivo General

Realizar una Auditoria a la Administración de la Red de Datos WAN de Soporte y Monitoreo, utilizando el Marco de Trabajo COBIT 4.1, con el fin de presentar las actividades de control en una estructura manejable y lógica, alineando TI con los objetivos del negocio de Telecomunicaciones FULLDATA Cía. Ltda.

Objetivos Específicos

- Analizar y diagnosticar la situación actual de la Administración de la Red de Datos WAN que brinda soporte y monitoreo, implementada por Telecomunicaciones FULLDATA Cia. Ltda., para lo cual se tomará como referencia 3 clientes de los cuales se obtendrá los resultados finales.
- Plantear mejores prácticas para la Administración de la Red de Datos WAN de soporte y monitoreo implementada por Telecomunicaciones FULLDATA Cía. Ltda.
- Proponer nuevos procesos y actividades que ayudarán a identificar los controles que se requieren para garantizar la seguridad de la información.

1.4 Justificación del Proyecto

Mediante la auditoría basada en la aplicación de la metodología presentada por el estándar COBIT, Telecomunicaciones FULLDATA Cía. Ltda., podrá proponer mejoras que permitan minimizar o eliminar los problemas actuales en la Administración de la Red de Datos WAN de soporte y monitoreo, desarrollando prácticas adecuadas, siendo la gestión de TI un factor crítico para estimular el control y progreso, estableciendo un vínculo con los requerimientos del negocio.

El proceso de auditoría a realizarse se basa en la selección de los Objetivos de Control detallados de cada uno de los procesos COBIT que tienen relación directa con la gestión de las Redes Informáticas.

Los Objetivos de Control proporcionados por el Marco de Referencia COBIT nos sirven para realizar un plan de Auditoria en la Administración de la Red de Datos WAN que brinda el servicio de soporte y monitoreo a los diferentes clientes, con los resultados que se obtendrán del nivel actual de la Administración en Telecomunicaciones FULLDATA Cía. Ltda., estará en capacidad de proponer mejoras que permitan minimizar o eliminar los problemas que se presenten en las interconexiones.

1.5 Alcance del Proyecto

Telecomunicaciones FULLDATA Cía. Ltda., es una empresa que provee soluciones integrales para necesidades puntuales, buscando una proyección en las compañías que contratan los servicios y soluciones de avanzada, para contribuir al desarrollo de las mismas.

El presente trabajo muestra la realización de un proceso de Auditoría a la Administración de la Red de Datos WAN de soporte y monitoreo mediante la aplicación de la metodología presentada por el Marco de Trabajo COBIT, donde se analizará el estado actual de la gestión de seguridad determinando los procesos COBIT que permitirán llevar a cabo el desarrollo de la presente auditoría, siguiendo las recomendaciones de COBIT, este documento expone los Objetivos de Control detallados que tienen relación con la administración en un ambiente de T.I., y que contribuyan a alcanzar los objetivos del negocio.

Una vez efectuada las pruebas se aplicará una evaluación del cumplimiento de las mismas para cada uno de los Objetivos de Control permitiendo al final obtener el nivel actual de la Administración de Red de Datos WAN. En base a esto se presentará la situación actual de los Objetivos de Control que cumplen los requerimientos y sobre los que no cumplen se plantearán mejores prácticas para la gestión de la Red de Datos WAN de soporte y monitoreo implementada por Telecomunicaciones FULLDATA Cía. Ltda., proponiendo nuevos procesos y actividades que ayudaran a identificar los controles que se requieren para garantizar la seguridad de la información.

Como resultado de la auditoría se realizará el informe técnico y ejecutivo, donde se presentará una descripción de la situación actual de las áreas donde se encuentran las mayores debilidades en cuanto a la administración en la Red de Datos WAN de soporte y monitoreo y se expondrán recomendaciones para su atenuación o superación definitiva.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Gestión de Redes [2]

La gestión de redes incluye la administración, organización, supervisión, y control del hardware, software y los elementos humanos para monitorizar, probar, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable[1].

Objetivos de la Gestión de Redes:

- Garantizar un servicio continuo.
- Capacidad para superar o evitar fallas.
- Capacidad para monitorear y diagnosticar condiciones no satisfactorias.
- Monitoreo del rendimiento esperado.
- Expansión y reconfiguración dinámica.
- Mejorar la seguridad de la red.
- Manejo Integrado de la red.
- Centralización de la gestión con implementación distribuida.
- Reducir costo operacional de la red.
- Incrementar la flexibilidad de operación e integración.
- Fácil uso de la red.

2.1.1 Modelo de Gestión ISO[2]

El modelo de gestión ISO clasifica las tareas de los sistemas de gestión en cinco áreas funcionales. La tarea del encargado de gestionar una red empresarial será evaluar la plataforma de gestión a utilizar en cuanto a la

[1] Introducción a la Gestión de Redes,http://lacnic.net/documentos/lacnicx/Intro_Gestion_Redes.pdf

[2] Ramón Jesús Millan Tejedor, Gestión de Redes, Consultoría Estratética en Tecnologías de la Información, http://www.ramonmillan.com/tutoriales/gestionred.php

medida en que dicha plataforma resuelva la problemática de gestión en cada una de estas áreas:

- Gestión de configuración.
- Gestión de rendimiento.
- Gestión de contabilidad.
- Gestión de fallos.
- Gestión de seguridad.

2.1.1.1 Gestión de Configuración

El objetivo de la gestión de configuración es obtener datos de la red y utilizarlos para incorporar, mantener y retirar los distintos componentes y recursos a integrar. Consiste en la realización de tres tareas fundamentales:

- Recolección automatizada de datos sobre el inventario y estado de la red, tales como versiones de software y hardware de los distintos componentes.
- Cambio en la configuración de los recursos.
- Almacenamiento de los datos de configuración.

2.1.1.2 Gestión de Rendimiento

La gestión de prestaciones o del rendimiento tiene como objetivo principal el mantenimiento del nivel de servicio que la red ofrece a sus usuarios, asegurándose de que está operando de manera eficiente en todo momento. La gestión de prestaciones se basa en cuatro tareas:

- Recogida de datos o variables indicadoras de rendimiento, tales como el troughput de la red, los tiempos de respuesta o latencia, la utilización de la línea, etc.
- Análisis de los datos para determinar los niveles normales de rendimiento.
- Establecimiento de umbrales, como indicadores que fijan los niveles mínimos de rendimiento que pueden ser tolerados.

- Determinación de un sistema de procesado periódico de los datos de prestación de los distintos equipos, para su estudio continuado.

2.1.1.3 Gestión de Contabilidad

La gestión de contabilidad tiene como misión la medida de parámetros de utilización de la red que permitan a su explotador preparar las correspondientes facturas a sus clientes. Entre las tareas que se deben realizar en esta área, están:

- Recolección de datos sobre la utilización de los recursos.
- Establecimiento de cuotas.
- Cobro a los usuarios con las tarifas derivadas de la utilización de los recursos.

2.1.1.4 Gestión de Fallos

La gestión de fallos tiene por objetivo fundamental la localización y recuperación de los problemas de la red. La gestión de problemas de red implica las siguientes tareas:

- Determinación de los síntomas del problema.
- Aislamiento del fallo.
- Resolución del fallo.
- Comprobación de la validez de la solución en todos los subsistemas importantes de la red.
- Almacenamiento de la detección y resolución del problema.

2.1.1.5 Gestión de Seguridad

La misión de la gestión de seguridad es ofrecer mecanismos que faciliten el mantenimiento de políticas de seguridad (orientadas a la protección contra ataques de intrusos). Entre las funciones realizadas por los sistemas de gestión de seguridad, están:

- Identificación de recursos sensibles en la red, tales como ficheros o dispositivos de comunicaciones.

- Determinación de las relaciones entre los recursos sensibles de la red y los grupos de usuarios.
- Monitorización de los puntos de acceso a los recursos sensibles de red.
- Almacenamiento de los intentos de acceso no autorizados a estos recursos, para su posterior análisis.

Se refiere esencialmente a los mecanismos que dispone el administrador de una red para monitorear los recursos, los permisos de uso de estos recursos asignados a cada usuario y el tipo de utilización a cada uno de estos.

Se relaciona con 2 aspectos de la seguridad del sistema:

La gestión de seguridad misma, que se refiere a la habilidad para supervisar y controlar la disponibilidad de facilidades de seguridad, y a reportar amenazas y rupturas en la seguridad. La seguridad de la gestión, que requiere de la habilidad para autentificar usuarios y aplicaciones de gestión, para así garantizar la confidencialidad e integridad de los datos y prevenir accesos no autorizados a la información. Para cumplir satisfactoriamente con la realización de estas tareas, es necesario tomar en consideración ciertas políticas de seguridad.

2.1.1.5.1 Políticas de Seguridad[3]

Las decisiones en cuanto a medidas de seguridad para una organización determinan, obviamente, que tan segura será la red y, además, qué nivel de funcionalidad ofrecerá y qué tan fácil será de usar. Se entiende como un grupo de normas cuyo fin es determinar que se puede o no hacer en lo referente a la operación de un sistema que involucre al área de seguridad de la información, estas normas son establecidas por el responsable del sistema de información.

Una política de seguridad puede ser prohibitiva, si todo lo que no está expresamente permitido está denegado, o permisiva, si todo lo que no está expresamente prohibido está permitido. Se puede considerar la primera

[3] Stalling W. (1995), Networkd Internetwork Security: Principles and Practice, s.e., Inc. New Jersey, Tesis Auditoría de la Gestión de seguridad en la red de Datos del Swissôtel basada en COBIT, EPN, 2006.

interpretación mejor que la segunda para mantener la seguridad de un sistema; en este caso la política contemplaría todas las actividades que se pueden realizar en los sistemas, y las omitidas serían consideradas ilegales.

Para que una política de seguridad se considere efectiva deberá tener en cuenta seis elementos claves para garantizar la información del sistema:

- Disponibilidad

Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica. Una variedad de ataques pueden resultar en la pérdida o reducción de la disponibilidad. Algunos de estos ataques pueden estar expuestos a acciones y medidas automáticas, tales como autenticación y encriptación, sin embargo otros requerirán de acciones físicas para prevenir o recuperarse de la pérdida de la disponibilidad de los elementos de un sistema distribuido.

- No repudio

Consiste en prevenir que ni el emisor ni el receptor puedan negar la transmisión de un mensaje. Además, cuando un mensaje es enviado, el receptor puede probar que el mensaje fue de hecho enviado por el supuesto emisor. De igual manera, cuando un mensaje es recibido, el emisor puede probar que el mensaje fue de hecho recibido por el supuesto receptor.

- Confidencialidad

La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario, la confidencialidad es también la protección de los datos transmitidos contra los ataques pasivos, con respecto a la entrega del contenido del mensaje se pueden identificar varios niveles de protección.

Otro aspecto de la confidencialidad es la protección del flujo de tráfico desde el análisis. Esto implica que un atacante no pueda observar el origen, el destino, la frecuencia, longitud, u otra característica del tráfico en una comunicación.

- Autenticidad

El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.

El servicio de autenticación concierne al aseguramiento de que una comunicación es auténtica. En el caso de un mensaje sencillo, como una alarma o una advertencia, la función del servicio de autenticación es asegurar al receptor que el mensaje es del emisor original. En el caso de una interacción que puede ser un inicio de conexión, el servicio asegura que las dos entidades son auténticas, es decir, que cada una es la entidad que dice ser. Además el servicio debe asegurar que la conexión no es interferida de manera que un tercer actor supuesto como uno de los dos legítimos anteriores pueda realizar transmisiones no autorizadas de envío y recepción.

- Integridad

La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado. Un servicio de integridad que trata con un flujo continuo de mensajes debe asegurar que los mensajes son recibidos como se enviaron, sin duplicaciones, inserciones, modificaciones, reordenaciones ni reenvíos. La destrucción de datos está también cubierta bajo este servicio. Además, el servicio de integridad debe manejar tanto la modificación del mensaje así como la negación del servicio. Puede hacerse una distinción entre el servicio con y sin recuperación. Debido a que el servicio de integridad hace relación a ataques activos, a menudo se relaciona más con detección que con prevención. Si una violación de la integridad es detectada, entonces el servicio puede simplemente reportar la violación, y alguna otra porción del software o la intervención humana será necesaria para recuperarse de la violación.

- Control de Acceso

Los propietarios de un sistema deben ser capaces de controlarlo en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios. En el contexto de la

seguridad de red, el control de acceso es la habilidad para limitar y controlar el acceso al sistema host y aplicaciones vía enlaces de comunicación.

2.1.1.5.2 Análisis de Riesgos[4]

El análisis de Riesgos trata sobre como minimizar los efectos de un problema de seguridad; para esto se debe tener identificado claramente qué es lo se quiere proteger, contra qué, y cómo se lo va a proteger. Se conocen dos alternativas para responder a estas inquietudes, una cuantitativa y otra cualitativa.

La cuantitativa se basa en cálculos complejos que implica la probabilidad de que un suceso ocurra y una estimación a las pérdidas en caso de que éste se dé; el llamado Costo Anual Equivalente, se obtiene del productos de estos términos, sin embargo, la inexactitud en el cálculo, a menudo hace difícil que esta alternativa sea tomada en cuenta.

El segundo método de análisis de riesgos es el cualitativo, últimamente muy difundido por las llamadas “consultoras de seguridad”, que se especializan en seguridad lógica, cortafuegos, tests de infiltración y similares. Este método toma en consideración realizar estimaciones de pérdidas potenciales, para lo cual relacionan cuatro puntos importantes:

- Las amenazas
- Las vulnerabilidades
- El impacto asociado a una amenaza
- Los controles o salvaguardas.

Con estos cuatro elementos se puede obtener un indicador cualitativo del nivel de riesgo asociado a un activo determinado dentro de la organización, visto como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

[4] , Tesis Auditoría de la Gestión de seguridad en la red de Datos del Swissôtel basada en COBIT, EPN, 2006.

2.1.1.5.3 Identificación de Recursos[5]

Donde se identifican todos los recursos cuya integridad pueda ser amenazada de cualquier forma:

- Hardware
  Procesadores, tarjetas, teclados, terminales estaciones de trabajo, computadores personales, impresoras, unidades de disco, líneas de comunicación, servidores, routers.
- Software
  Códigos fuente y objeto de aplicaciones, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicación, aplicaciones cliente – servidor.
- Información
  En ejecución, almacenada en línea, almacenada fuera de línea, en comunicación, bases de datos..
- Personas
  Usuarios, operadores, administradores.
- Accesorios
  Papel, cintas, tóners, CD´s.

2.1.1.5.4 Identificación de Amenazas y Vulnerabilidades[6]

Luego de identificados los recursos a proteger se deben identificar las vulnerabilidades y amenazas a que están expuestos. Una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

Las amenazas se catalogan en diferentes grupos según su impacto sobre los sistemas informáticos y la forma como se producen:

---

[5] Tesis Auditoría de la Gestión de seguridad en la red de Datos del Swissôtel basada en COBIT, EPN, 2006.
[6] Tesis Auditoría de la Gestión de seguridad en la red de Datos del Swissôtel basada en COBIT, EPN, 2006.

- **Desastres del Entorno**

Se refieren a problemas relacionados con la ubicación del entorno de trabajo informático o de la propia organización, así como con las personas que de una u otra forma están relacionadas con el mismo. Se toman en cuenta desastres naturales (terremotos, inundaciones, etc.), desastres producidos por elementos cercanos, como los cortes de fluido eléctrico, y peligros relacionados con operadores, programadores o usuarios del sistema.

- **Amenazas en el Sistema**

Se refieren a todas las vulnerabilidades de los equipos y su software que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, medidas de protección que éste ofrece, fallos en los programas, copias de seguridad, etc.

- **Amenazas en la Red**

Se debe tener en cuenta los aspectos relativos al cifrado de los datos que son sujetos de transmisión, protección de una red local de la Internet, sistemas de autenticación de usuarios remotos que accedan a ciertos recursos de la red.

Cabe anotar que para el análisis de las amenazas no solo se deben tomar en cuenta a los posibles atacantes externos (piratas informáticos, crakers) a la organización, sino que en la mayoría de los casos los potenciales ataques vienen desde el interior de la organización, debido principalmente a los pocos conocimientos sobre sistemas informáticos, seguridades y el trabajo en red básicamente.

Por otro lado, están también los actos accidentales, producidos por los mismos usuarios como pueden ser los borrados accidentales, fallas de programación, desconexión de cables de energía, etc.

2.1.1.5.5 Medidas de Protección [7]

Una vez identificados todos los recursos a proteger, las posibles vulnerabilidades y amenazas a que son expuestos y los posibles atacantes que pueden intentar violar la seguridad, procede el estudio de cómo proteger los sistemas.

Esto implica en primer lugar cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades de que una amenaza se pueda convertir en realidad. Este cálculo puede realizarse partiendo de hechos sucedidos con anterioridad en la organización. La clasificación de riesgos de cara a estudiar medidas de protección suele realizarse en base al nivel de importancia del daño causado y a la probabilidad aproximada de que ese daño se convierta en realidad; se trata principalmente de no gastar más dinero en una implementación para proteger un recurso de lo que vale dicho recurso o de lo que costaría recuperarse de un daño en él o de su pérdida total. Evidentemente, los recursos que presenten a la evaluación un riesgo mayor serán los que más medidas de protección deben poseer, ya que esto significa que es probable que sean atacados, y que además el ataque puede causar pérdidas importantes.

Como un riesgo, es imposible de eliminarlo completamente se lo puede minimizar, por lo que se debe planificar no solo la prevención de que una amenaza se realice (medidas proactivas), sino también aplicar el procedimiento para recuperarse del ataque si este se produce (medidas reactivas).

2.1.1.5.6 Estrategias de Respuesta[8]

Existen dos estrategias de respuesta ante un incidente de seguridad:

- Proteger y proceder.
- Perseguir y procesar.

[7] Tesis Auditoría de la Gestión de seguridad en la red de Datos del Swissôtel basada en COBIT, EPN, 2006.
[8] Tesis Auditoría de la Gestión de seguridad en la red de Datos del Swissôtel basada en COBIT, EPN, 2006.

- **Proteger y Proceder**

  Se aplica cuando la organización es muy vulnerable o el nivel de los atacantes es elevado; la filosofía es proteger de manera inmediata la red y los sistemas y restaurar su estado normal, de forma que los usuarios puedan seguir trabajando normalmente. Será necesario interferir de forma activa las acciones del intruso para evitar más accesos, y analizar el daño causado. La principal desventaja de esta estrategia es que el atacante se da cuenta rápidamente de que ha sido descubierto, y puede emprender acciones para no ser identificado, lo que incluso conduce al borrado de logs o de sistemas de ficheros completos; incluso puede cambiar su estrategia de ataque a un nuevo método, y seguir comprometiendo al sistema. Sin embargo, esta estrategia también presenta una parte positiva: el bajo nivel de conocimientos de los atacantes en sistemas habituales hace que en muchas ocasiones se limiten a abandonar su ataque.

- **Perseguir y Procesar**

  Adopta la filosofía de permitir al atacante proseguir sus actividades, pero de forma controlada y observada por los administradores, de la forma más discreta posible. Con esto, se intentan guardar pruebas para ser utilizadas en la segunda parte de la estrategia, la de acusación y procesamiento del atacante (ya sea ante la justicia o ante los responsables de la organización, si se trata de usuarios internos). Se corre el peligro de que el intruso descubra su monitorización y destruya completamente el sistema, así como que los resultados no se tengan en cuenta ante un tribunal debido a estrategias legales.

2.2 El Marco de Trabajo COBIT 4.1.

2.2.1 Historia y Evolución

El proyecto **COBIT** se emprendió por primera vez en el año 1995, con el fin de crear un mayor producto global que pudiese tener un impacto duradero sobre el campo de visión de los negocios, así como sobre los controles de los sistemas de información implantados. La primera edición del **COBIT**, fue publicada en 1996 y fue vendida en 98 países de todo el mundo. La segunda edición (tema de estudio en este informe) publicada en Abril de 1998, desarrolla y mejora lo que poseía la anterior mediante la incorporación de un mayor número de documentos de referencia fundamentales, nuevos y revisados (de forma detallada) objetivos de control de alto nivel, intensificando las líneas maestras de auditoría, introduciendo un conjunto de herramientas de implementación, así como un CD-ROM completamente organizado el cual contiene la totalidad de los contenidos de esta segunda edición.

Una temprana adición significativa visualizada para la familia de productos **COBIT**, es el desarrollo de las Guías de Gerencia que incluyen Factores Críticos de Éxito, Indicadores Clave de Desempeño y Medidas Comparativas. Los Factores Críticos de Éxito, identificarán los aspectos o acciones más importantes para la administración y poder tomar, así, dichas acciones o considerar los aspectos para lograr control sobre sus procesos de TI. Los Indicadores Clave de Desempeño proporcionarán medidas de éxito que permitirán a la gerencia conocer si un proceso de TI está alcanzando los requerimientos de negocio. La Medidas Comparativas definirán niveles de madurez que pueden ser utilizadas por la gerencia para: determinar el nivel actual de madurez de la empresa; determinar el nivel de madurez que se desea lograr, como una función de sus riesgos y objetivos; y proporcionar una base de comparación de sus prácticas de control de TI contra empresas similares o normas de la industria. Esta adición, proporcionará herramientas a la gerencia para evaluar el ambiente de TI de su organización con respecto a los 34 Objetivos de Control de alto nivel de **COBIT**.

En definitiva, la organización **ISACF** (creadora, como ya se ha comentado, de la norma) espera que el **COBIT** sea adoptado por las comunidades de auditoría y negocio como un estándar generalmente aceptado para el control de las Tecnologías de la Información.[9]

2.2.2 Misión

Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento.[10]

2.2.3 Alcance

Orientado al negocio o gerencia es el tema principal de COBIT. Está diseñado para ser utilizado no sólo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los dueños de los procesos de negocio.

- Alineado con estándares y regulaciones de hecho y de derecho.
- Basado en normas revisadas crítica y analíticamente para ser aceptadas en las tareas y actividades de TI.
- Alineado con estándares de control y auditoría (COSO, IFAC, IIA, ISACA, AICPA).
- Aplicable a las funciones de Servicios de Sistemas de Información de toda la empresa.

2.2.4 Objetivos

- Entregar a la Gerencia normas basadas en buenas prácticas para el control de TI incluyendo la seguridad informática. COBIT es la herramienta de Gobierno de TI que ayude al entendimiento y a la administración de los riesgos y las ventajas asociadas con la información y sus tecnologías relacionadas.

[9] COBIT, Estadar de TI, http://ds5-andre-ortega-5a.host56.com/historia.html
[10] © 2007 IT Governance Institute, COBIT 4.1, Pág 9

- Proporcionar a los usuarios una base confiable para la administración correcta de los recursos de TI.
- Proveer a los auditores de buenos criterios para las tareas de evaluación, control y auditoría.
- Entregar a la Gerencia, responsables de procesos de negocio y auditores, el respaldo suficiente para mejorar la administración de la T.I. COBIT está diseñado para ser utilizado por los propietarios de los procesos de negocio como una guía clara y entendible para que estos tengan total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio.

2.2.5 Estructura del Marco de Trabajo COBIT

2.2.5.1 Resumen Ejecutivo[11]

Para muchas empresas, la información y la tecnología que las soportan representan sus más valiosos activos, aunque con frecuencia son poco entendidos. Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (stakeholders). Estas empresas también entienden y administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI.

La necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados a TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del Gobierno Corporativo. El valor, el riesgo y el control constituyen la esencia del gobierno de TI.

El gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que TI en la empresa sostiene y extiende las estrategias y objetivos organizacionales.

[11] © 2007 IT Governance Institute, COBIT 4.1, Pág 5

Más aún, el Gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que TI en la empresa soporta los objetivos del negocio. De esta manera, el gobierno de TI facilita que la empresa aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas. Estos resultados requieren un marco de referencia para controlar la TI, que se ajuste y sirva como soporte a COSO[12]

Marco de Referencia Integrado – Control Interno, el marco de referencia de control ampliamente aceptado para gobierno corporativo y para la administración de riesgos, así como a marcos compatibles similares.

Las organizaciones deben satisfacer la calidad, los requerimientos fiduciarios y de seguridad de su información, así como de todos sus activos. La dirección también debe optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y personas. Para descargar estas responsabilidades, así como para lograr sus objetivos, la dirección debe entender el estatus de su arquitectura empresarial para TI y decidir qué tipo de gobierno y de control debe aplicar.

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT®) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

Para que TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

- Estableciendo un vínculo con los requerimientos del negocio.

[12] Committee Of Sponsoring Organisations Of The Treadway Commission

- Organizando las actividades de TI en un modelo de procesos generalmente aceptado.
- Identificando los principales recursos de TI a ser utilizados.
- Definiendo los objetivos de control gerenciales a ser considerados.

La orientación al negocio que enfoca COBIT consiste en alinear las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de la TI. Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

En resumen, para proporcionar la información que la empresa necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural.

Primero, la dirección requiere objetivos de control que definan la meta final de implementar políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar un aseguramiento razonable de que:

- Se alcancen los objetivos del negocio.
- Se prevengan o se detecten y corrijan los eventos no deseados.

La evaluación de la capacidad de los procesos basada en los modelos de madurez de COBIT, es una parte clave de la implementación del gobierno de TI. Después de identificar los procesos y controles críticos de TI, el modelo de madurez permite identificar y demostrar a la dirección las brechas en la capacidad. Entonces se pueden crear planes de acción para llevar estos procesos hasta el nivel objetivo de capacidad deseado.

COBIT da soporte al gobierno de TI **figura 2.1,** al brindar un marco de trabajo que garantiza que:

- TI está alineada con el negocio
- TI habilita al negocio y maximiza los beneficios
- Los recursos de TI se usan de manera responsable
- Los riesgos de TI se administran apropiadamente

Figura 2.1 – Áreas de Enfoque del Gobierno de TI[13]

Alineación Estratégica. Se enfoca en organizar la alineación entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de TI; y en alinear las operaciones de TI con las operaciones de la empresa.

Entrega de Valor. Se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.

Administración de Recursos. Se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.

Administración de Riesgos. Requiere consciencia de los riesgos por parte de los altos ejecutivos de la empresa, comprender los requerimientos de

[13] © 2007 IT Governance Institute, COBIT 4.1, Pág 6

cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

Medición del Desempeño. Rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo el balanced scorecards que traducen la estrategia en acción para lograr las metas medibles más allá del registro convencional.

Todos estos componentes de COBIT se interrelacionan, ofreciendo soporte para las necesidades de gobierno, de administración, de control y de auditoría de los distintos interesados, como se muestra en la **figura 2.2**.

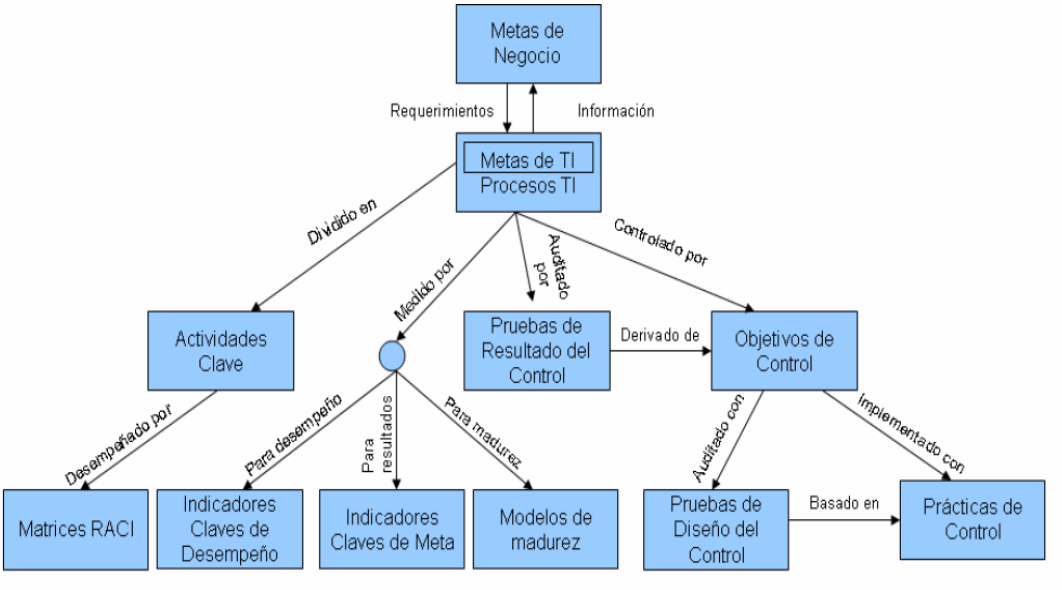


Figura 2.2 – Interrelaciones de los componentes de COBIT.[14]

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (Stakeholders).

COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y

[14] © 2007 IT Governance Institute, COBIT 4.1, Pág 8

armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma.

2.2.5.2 Marco de Trabajo COBIT

Como satisface COBIT la necesidad

Como respuesta a las necesidades descritas en la sección anterior, el marco de trabajo COBIT se creó con las características principales de ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

Orientado al negocio

La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no sólo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los dueños de los procesos de negocio.

El marco de trabajo COBIT se basa en el siguiente principio **figura 2.3:** Para proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita invertir en, y administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida.

El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.

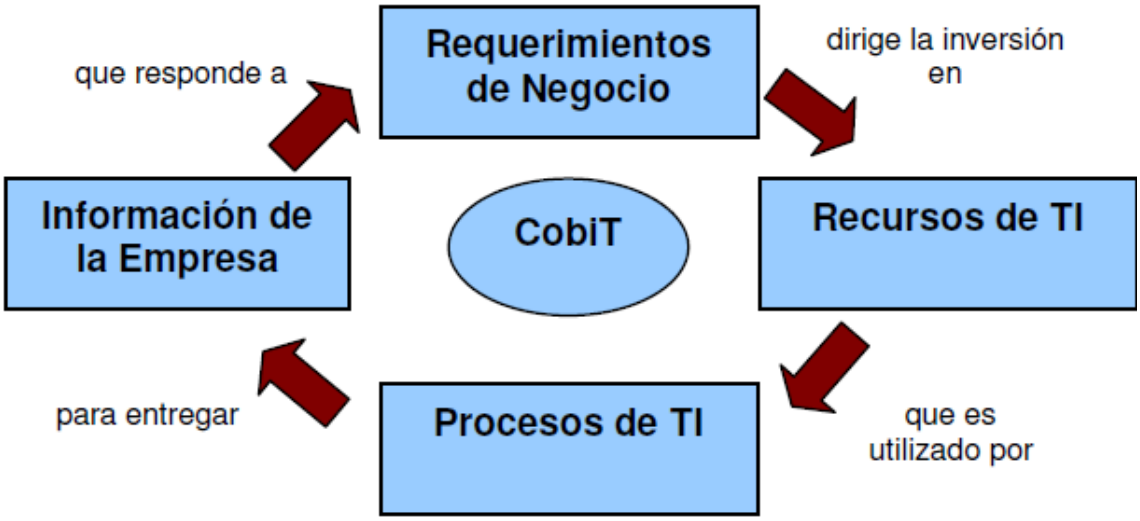


Figura 2.3 – Principio Básico de COBIT[15]

CRITERIOS DE INFORMACIÓN DE COBIT[16]

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos más amplios de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

• La **efectividad** tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.

• La **eficiencia** consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.

• La **confidencialidad** se refiere a la protección de información sensitiva contra revelación no autorizada.

[15] © 2007 IT Governance Institute, COBIT 4.1, Pág 10
[16] © 2007 IT Governance Institute, COBIT 4.1, Pág 10

• La **integridad** está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

• La **disponibilidad** se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.

• El **cumplimiento** tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

• La **confiabilidad** se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

METAS DE NEGOCIOS Y DE TI[17]

Mientras que los criterios de información proporcionan un método genérico para definir los requerimientos del negocio, la definición de un conjunto de metas genéricas de negocio y de TI ofrece una base más refinada y relacionada con el negocio para el establecimiento de requerimientos de negocio y para el desarrollo de métricas que permitan la medición con respecto a estas metas.

Toda empresa usa TI para habilitar iniciativas del negocio y estas pueden ser representadas como metas del negocio para TI. El **Anexo 1,** proporciona una matriz de metas genéricas de negocios y metas de TI y como se asocian con los criterios de la información. Estos ejemplos genéricos se pueden utilizar como guía para determinar los requerimientos, metas y métricas específicas del negocio para la empresa.

[17] © 2007 IT Governance Institute, COBIT 4.1, Pág 11

Si se pretende que TI proporcione servicios de forma exitosa para dar soporte a la estrategia de la empresa, debe existir una propiedad y una dirección clara de los requerimientos por parte del negocio (el cliente) y un claro entendimiento para TI, de cómo y qué debe entregar (el proveedor). La **figura 2.4,** ilustra como la estrategia de la empresa se debe traducir por parte del negocio en objetivos relacionados con iniciativas habilitadas por TI (Las metas de negocio para TI). Estos objetivos a su vez, deben conducir a una clara definición de los propios objetivos de TI (las metas de TI), y luego éstas a su vez definir los recursos y capacidades de TI (la arquitectura empresarial para TI) requeridos para ejecutar, de forma exitosa la parte que le corresponde a TI de la estrategia empresarial. Para que el cliente entienda las metas y los Scorecard de TI, todos estos objetivos y sus métricas asociadas se deben expresar en términos de negocio significativos para el cliente, y esto, combinado con una alineación efectiva de la jerarquía de objetivos, asegurará que el negocio pueda confirmar que TI puede, con alta probabilidad, dar soporte a las metas del negocio.

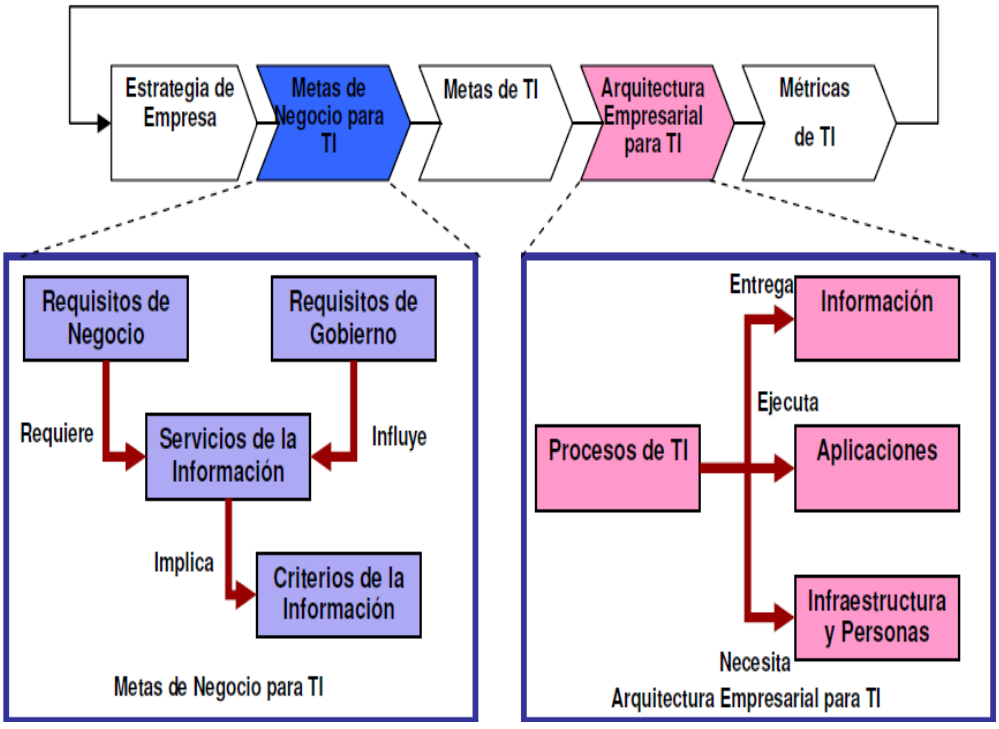


Figura 2.4 – Definir las Metas de TI y la Arquitectura Empresarial para TI[18]

[18] © 2007 IT Governance Institute, COBIT 4.1, Pág 11

Una vez que han sido definidas las metas alineadas, estás requieren ser monitoreadas para garantizar que la entrega cumple con las expectativas. Esto se logra con métricas derivadas de las metas y capturadas en el scorecard de TI.

Para que el cliente pueda entender las metas de TI y el scorecard de TI, todos estos objetivos y métricas asociadas deben expresarse en términos de negocio significativos para el cliente. Esto, combinado con un alineamiento efectivo de los objetivos jerárquicos aseguraría que el negocio puede confirmar que es probable que TI soporte los objetivos de la empresa.

RECURSOS DE TI

La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad, que utiliza las habilidades de las personas y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio. Estos recursos, junto con los procesos, constituyen una arquitectura empresarial para TI.

Para responder a los requerimientos que el negocio tiene hacia TI, la empresa debe invertir en los recursos requeridos para crear una capacidad técnica adecuada (Ej. Un sistema de planeación de recursos empresariales [ERP]) para dar soporte a la capacidad del negocio (Ej. Implementando una cadena de suministro) que genere el resultado deseado (Ej. Mayores ventas y beneficios financieros).

Los recursos de TI identificados en COBIT se pueden definir como sigue:

- Las aplicaciones incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- La información son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.

- La infraestructura es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- Las personas son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

La **figura 2.5,** resume cómo las metas de negocio para TI influencian la manera en que se manejan los recursos necesarios de TI por parte de los procesos de TI para lograr las metas de TI.

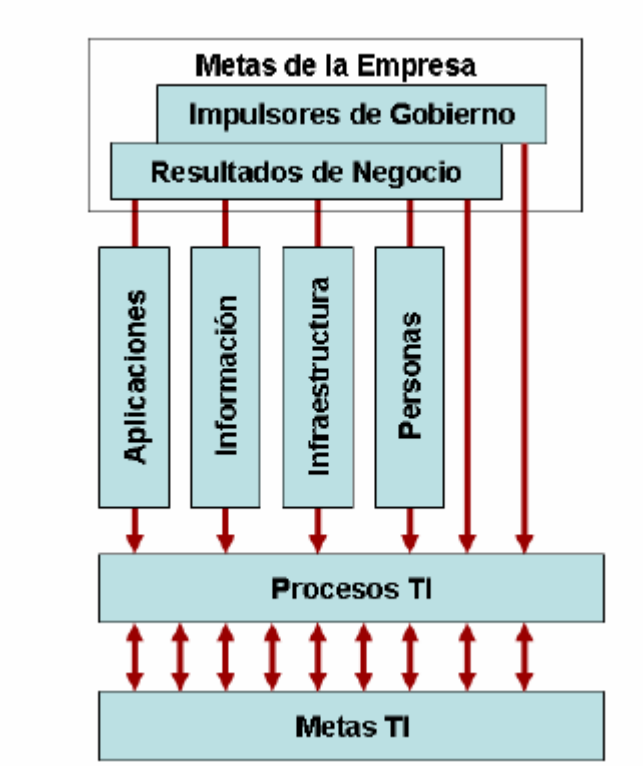


Figura 2.5 – Gestión de los Recursos de TI para entregar Metas de TI[19]

[19] © 2007 IT Governance Institute, COBIT 4.1, Pág 12

Orientado a Procesos[20]

COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que todos en la empresa visualicen y administren las actividades de TI. La incorporación de un modelo operativo y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno. También brinda un marco de trabajo para la medición y monitoreo del desempeño de TI, comunicándose con los proveedores de servicios e integrando las mejores prácticas de administración. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Normalmente se ordenan dentro de dominios de responsabilidad de plan, construir, ejecutar y Monitorear. Dentro del marco de COBIT, estos dominios, como se muestra en la **Figura 2.6**, se llaman:

- **Planear y Organizar (PO)** – Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
- **Adquirir e Implementar (AI)** – Proporciona las soluciones y las pasa para convertirlas en servicios.
- **Entregar y Dar Soporte (DS)** – Recibe las soluciones y las hace utilizables por los usuarios finales.
- **Monitorear y Evaluar (ME)** - Monitorear todos los procesos para asegurar que se sigue la dirección provista.

[20] © 2007 IT Governance Institute, COBIT 4.1, Pág 12 - 13

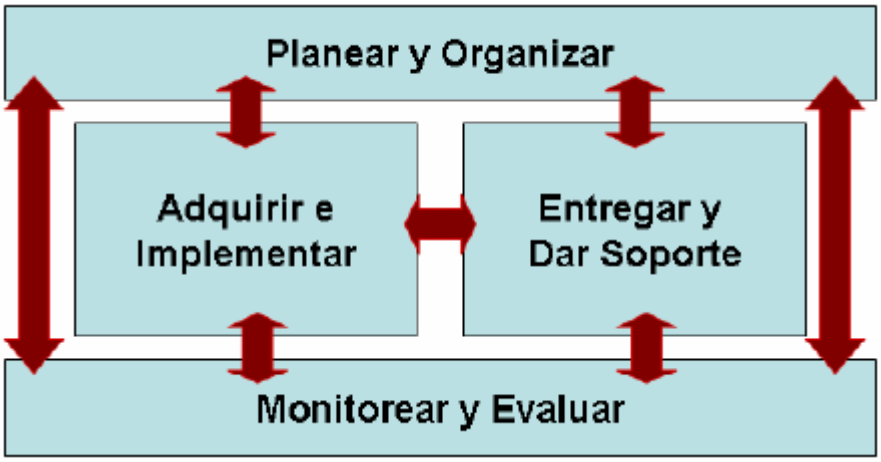


Figura 2.6 – Los Cuatro Dominios Interrelacionados de COBIT[21]

2.2.5.2.1 Planear y Organizar (PO)

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

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

2.2.5.2.2 Adquirir e Implementar (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los

[21] © 2007 IT Governance Institute, COBIT 4.1, Pág 12

sistemas existentes están, cubiertos por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:

- ¿Es probable que los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?
- ¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?
- ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
- ¿Los cambios no afectarán a las operaciones actuales del negocio?

2.2.5.2.3 Entregar y Dar soporte (DS)

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

Por lo general cubre las siguientes preguntas de la gerencia:

- ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?
- ¿Están optimizados los costos de TI?
- ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?
- ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

2.2.5.2.4 Monitorear y Evaluar (ME)

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

- ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
- ¿La Gerencia garantiza que los controles internos son efectivos y eficientes?
- ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?
- ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

A lo largo de estos cuatro dominios, COBIT ha identificado 34 procesos de TI generalmente usados. Mientras la mayoría de las empresas ha definido las responsabilidades de planear, construir, ejecutar y monitorear para TI, y la mayoría tienen los mismos procesos clave, pocas tienen la misma estructura de procesos o le aplicaran todos los 34 procesos de COBIT.

COBIT proporciona una lista completa de procesos que puede ser utilizada para verificar que se completan las actividades y responsabilidades; sin embargo, no es necesario que apliquen todas, y, aún más, se pueden combinar como se necesite por cada empresa.

Para cada uno de estos 34 procesos, tiene un enlace a las metas de negocio y TI que soporta. Información de cómo se pueden medir las metas, también se proporcionan cuáles son sus actividades clave y entregables principales, y quién es el responsable de ellas.

Modelos de Madurez[22]

Cada vez con más frecuencia, se les pide a los directivos de empresas corporativas y públicas que consideren qué tan bien se está administrando TI. Como respuesta a esto, se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información. Aunque pocos argumentarían que esto no es algo bueno, se debe considerar el equilibrio del costo beneficio y éstas preguntas relacionadas:

[22] © 2007 IT Governance Institute, COBIT 4.1, Pág 17 - 18

- ¿Qué está haciendo nuestra competencia en la industria, y cómo estamos posicionados en relación a ellos?
- ¿Cuáles son las mejores prácticas aceptables en la industria, y cómo estamos posicionados con respecto a estas prácticas?
- Con base en estas comparaciones, ¿se puede decir que estamos haciendo lo suficiente?
- ¿Cómo identificamos lo que se requiere hacer para alcanzar un nivel adecuado de administración y control sobre nuestros procesos de TI?

Puede resultar difícil proporcionar respuestas significativas a estas preguntas. La gerencia de TI está buscando constantemente herramientas de evaluación para benchmarking y herramientas de auto-evaluación como respuesta a la necesidad de saber qué hacer de manera eficiente. Comenzando con los procesos y los objetivos de control de alto nivel de COBIT, el dueño del proceso se debe poder evaluar de forma progresiva, contra los objetivos de control. Esto responde a tres necesidades:

1. Una medición relativa de dónde se encuentra la empresa
2. Una manera de decidir hacia dónde ir de forma eficiente
3. Una herramienta para medir el avance contra la meta

El modelo de madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5).

Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. El propósito no es avaluar el nivel de adherencia a los objetivos de control.

Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Con los modelos de madurez de COBIT, a diferencia de la aproximación del CMM original de SEI, no hay intención de medir los niveles de forma precisa o probar a certificar que un nivel se ha conseguido con exactitud. Una evaluación de la madurez de COBIT resultara en un perfil donde las condiciones relevantes a diferentes niveles de madurez se han conseguido, como se muestra en el ejemplo gráfico de la **figura 2.7.**

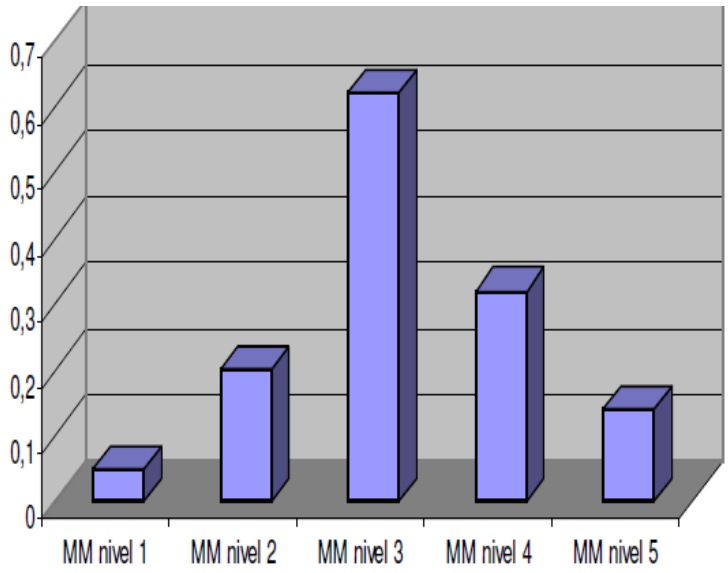


Figura 2.7 – Posible Nivel de Madurez de un Proceso de TI.[23]

Posible nivel de madurez de un proceso de TI: El ejemplo ilustra un proceso que está ampliamente en el nivel 3, pero cumple algunas acciones con menos nivel de requerimiento mientras sigue investigando en la medición del desarrollo.

Esto se debe a que cuando se emplea la evaluación de la madurez con los modelos de COBIT, a menudo algunas implementaciones estarán en diferentes niveles aunque no esté completa o suficiente. Estas fortalezas pueden apalancarse para seguir mejorando la madurez. Por ejemplo, algunas partes del proceso pueden estar bien definidas, y, aún cuando esté incompleto, sería erróneo decir que no está definido del todo.

[23] © 2007 IT Governance Institute, COBIT 4.1, Pág 18

Utilizando los modelos de madurez desarrollados para cada uno de los 34 procesos TI de COBIT, la gerencia podrá identificar:

- El desempeño real de la empresa—Dónde se encuentra la empresa hoy
- El estatus actual de la industria—La comparación
- El objetivo de mejora de la empresa—Dónde desea estar la empresa
- El crecimiento requerido entre “como es” y “como será”

Para hacer que los resultados sean utilizables con facilidad en resúmenes gerenciales, donde se presentarán como un medio para dar soporte al caso de negocio para planes futuros, se requiere contar con un método gráfico de presentación **figura 2.8.**

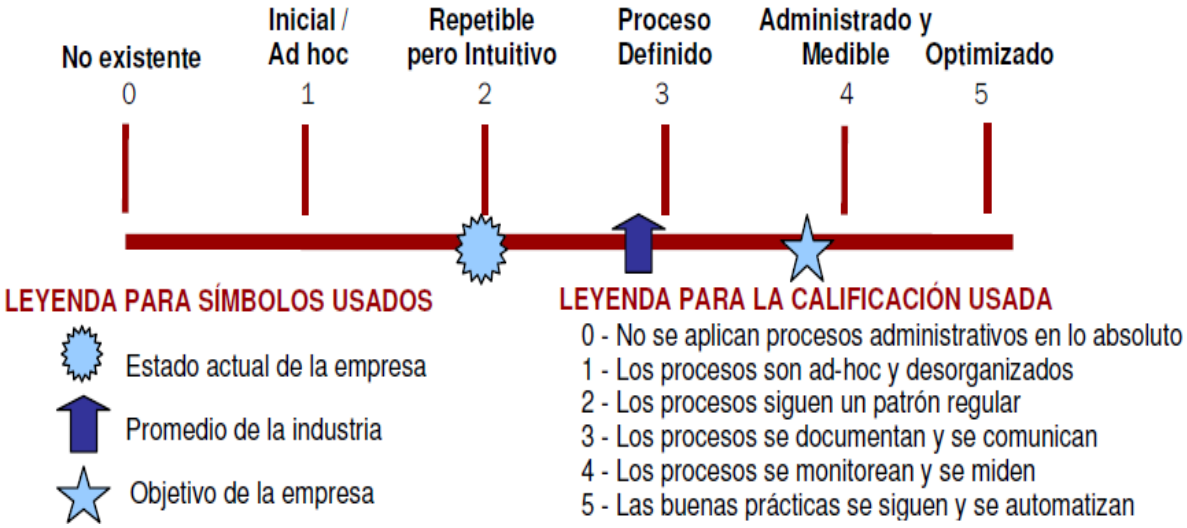


Figura 2.8 – Representación Gráfica de los Modelos de Madurez[8]

Para resumir, los recursos de TI son manejados por procesos de TI para lograr metas de TI que respondan a los requerimientos del negocio. Este es el principio básico del marco de trabajo COBIT, como se ilustra en el cubo COBIT **figura 2.9**.

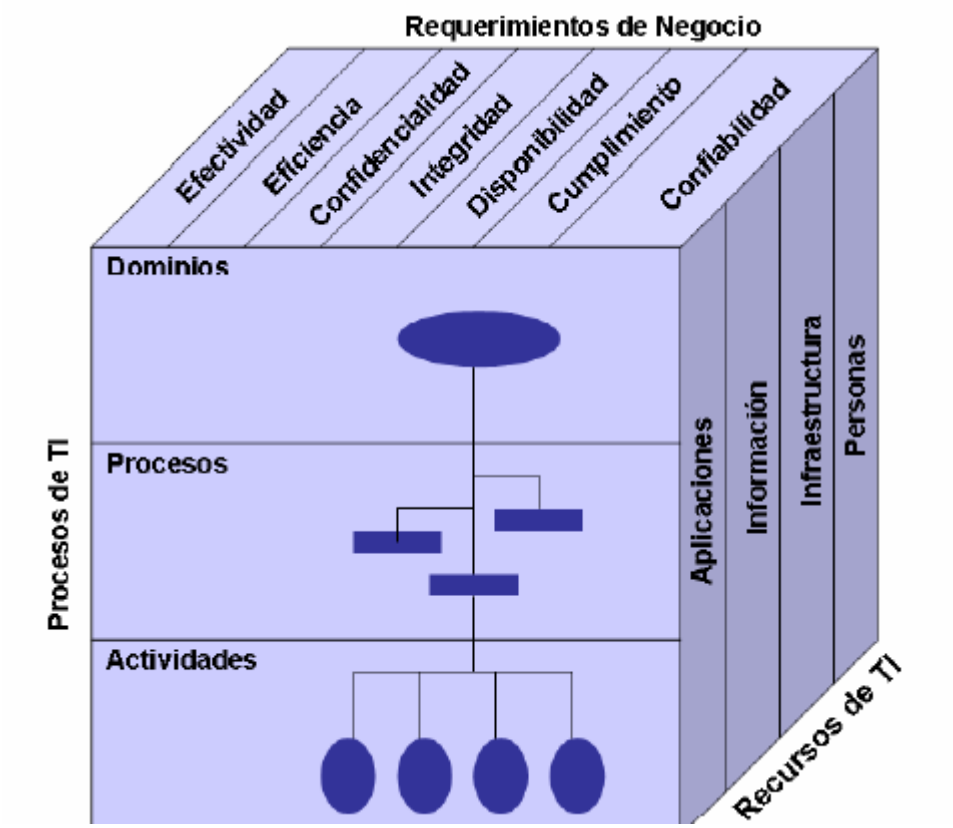


Figura 2.9 – Representación Grafica de los Modelos de Madurez[24]

Aceptabilidad General de COBIT[25]

COBIT se basa en el análisis y armonización de estándares y mejores prácticas de TI existentes y se adapta a principios de gobierno generalmente aceptados. Está posicionado a un nivel alto, impulsado por los requerimientos del negocio, cubre el rango completo de actividades de TI, y se concentra en lo que se debe lograr en lugar de como lograr un gobierno, administración y control efectivos. Por lo tanto, funciona como un integrador de prácticas de gobierno de TI y es de interés para la dirección ejecutiva; para la gerencia del negocio, para la gerencia y gobierno de TI; para los profesionales de aseguramiento y seguridad; así como para los profesionales de auditoría y control de TI. Está diseñado para ser complementario y para ser usado junto con otros estándares y mejores prácticas.

[24] © 2007 IT Governance Institute, COBIT 4.1, Pág 25
[25] © 2007 IT Governance Institute, COBIT 4.1, Pág 25

La implantación de las mejores prácticas debe ser consistente con el gobierno y el marco de control de la empresa, debe ser apropiada para la organización, y debe estar integrada con otros métodos y prácticas que se utilicen. Los estándares y las mejores prácticas no son una panacea y su efectividad depende de cómo hayan sido implementados en realidad y de cómo se mantengan actualizados. Son más útiles cuando se aplican como un conjunto de principios y como un punto de partida para adaptar procedimientos específicos. La gerencia y el equipo deben entender qué hacer, cómo hacerlo y porqué es importante hacerlo para garantizar que se utilicen las prácticas.

Para lograr la alineación de las mejores prácticas con los requerimientos del negocio, se recomienda que COBIT se utilice al más alto nivel, brindando así un marco de control general basado en un modelo de procesos de TI que debe ser aplicable en general a toda empresa. Las prácticas y los estándares específicos que cubren áreas discretas, se pueden equiparar con el marco de trabajo de COBIT, brindando así una jerarquía de materiales guía.

COBIT resulta de interés a distintos usuarios:

- **Dirección ejecutiva—** Para obtener valor de las inversiones y para balancear las inversiones en riesgo y control en un ambiente de TI con frecuencia impredecible.
- **Gerencia del negocio—** Para obtener certidumbre sobre la administración y control de los servicios de TI, proporcionados internamente o por terceros
- **Gerencia de TI—**Para proporcionar los servicios de TI que el negocio requiere para dar soporte a la estrategia del negocio de una forma controlada y administrada.
- **Auditores—**Para respaldar sus opiniones y/o para proporcionar asesoría a la gerencia sobre controles internos.-

COBIT ha sido desarrollado y es mantenido por un instituto de investigación sin ánimo de lucro, tomando la experiencia de los miembros de sus asociaciones afiliadas, de los expertos de la industria, y de los profesionales de control y seguridad. Su contenido se basa en una investigación continua sobre las

mejores prácticas de TI y se le da un mantenimiento continuo, proporcionando así un recurso objetivo y práctico para todo tipo de usuario.

COBIT está orientado a los objetivos y al alcance del gobierno de TI, asegurando que su marco de control sea integral, que esté alineado con los principios de Gobierno Corporativo y, por lo tanto, que sea aceptable para los consejos directivos, para la dirección ejecutiva, para los auditores y reguladores. En el Apéndice II, se ofrece un mapa que muestra cómo los objetivos de control detallados de COBIT se relacionan con las cinco áreas de enfoque del gobierno de TI y con las actividades de control de COSO.

El **Anexo 2,** muestra el Marco de Trabajo Completo de COBIT.

El marco de trabajo de COBIT está compuesto de los siguientes componentes esenciales, incluidos en el resto de esta publicación y organizados en los 34 procesos de TI, brindando así una visión completa de cómo controlar, administrar y medir cada proceso.

CAPITULO 3

SITUACION ACTUAL

TELECOMUNICACIONES FULLDATA CIA. LTDA. es una empresa que provee soluciones integrales para necesidades puntuales, buscando una proyección en las compañías que contratan sus servicios para poder contribuir al desarrollo de las mismas.

FULLDATA CIA. LTDA. está conformada por personal calificado, con más de veinte años de experiencia y gestores de la implementación de importantes proyectos de comunicaciones en el país. La capacitación de dicho personal es permanente, tanto en el país, así como también en el exterior y en cada una de las fábricas a las representan, razón que los mantiene al día en el vertiginoso avance de la tecnología.

Ofreciendo un amplio portafolio de productos y servicios entre los que encontramos: instalación, asesoría, mantenimiento de redes, proporcionando una solución total, ajustándonos al tamaño necesidades, desde configuraciones punto a punto hasta configuraciones estrella y mixtas, logrando así un mejor rendimiento, un control simplificado y una reducción de costos significativa.

Misión

Proveer soluciones integrales a nivel nacional en telecomunicaciones, transmisión de datos, voz y video, brindando óptima calidad tanto en servicio como en tecnología de punta, trabajando conjuntamente con nuestros clientes y proveedores como socios estratégicos; con un equipo humano altamente calificado.

Visión

Ser una empresa líder a nivel nacional, diseñando, aplicando, ejecutando tecnología de punta y sistemas en soluciones integrales de telecomunicaciones con el apoyo de alianzas estratégicas y calidad total en el servicio.

3.1 Descripción de la Organización Administrativa de FullData Cía. Ltda.

La organización de FullData Cía. Ltda. se encuentra conformada por una junta general de accionistas que consta con tres miembros, la mesa directiva consta de presidente, gerente general y gerentes por cada departamento los cuales deciden las diferentes cuestiones de la administración empresarial.

Se presenta en la **figura 3.1,** el diagrama organizacional de la empresa.

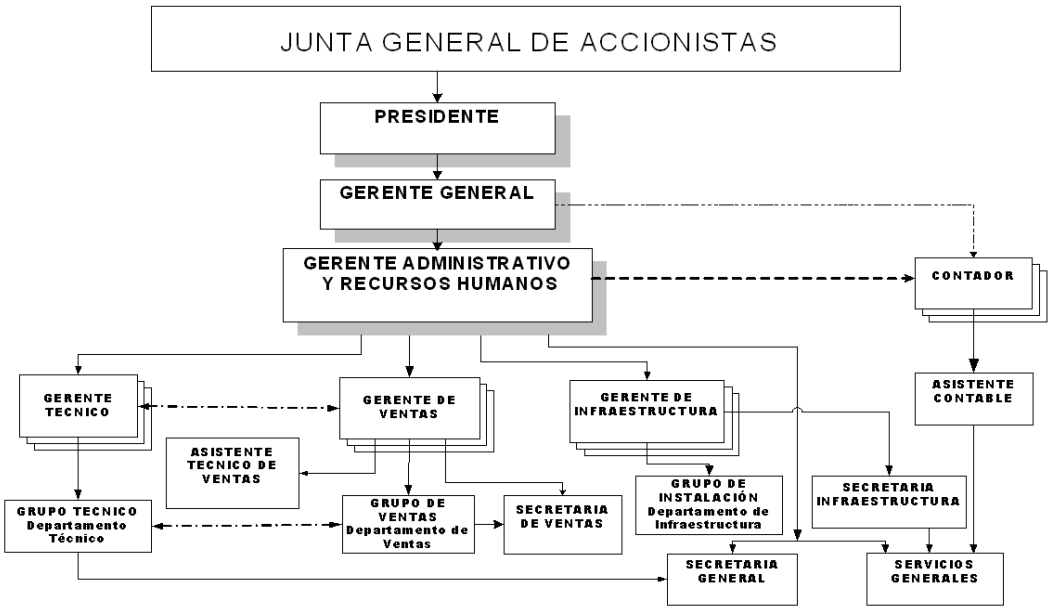


Figura 3.1 - Diagrama Organizacional de FullData Cía. Ltda.

En base al diagrama se detalla a continuación los cargos y sus funciones dentro de la organización.

- **Presidente:** Es la máxima autoridad de la empresa, dirige y organiza el funcionamiento de la misma, estando a cargo de la rendición de cuentas a la junta de accionistas, presidiendo juntas y consejos.
- **Gerente General:** Encargado de la dirección en general de la empresa coordinado los diferentes departamentos con el fin de tener un desarrollo eficiente de la organización.
- **Gerente Administrativo y RRHH:** Dirige y controla actividades administrativas y de recursos humanos.

- Gerente Técnico: Encargado de la dirección del departamento técnico y sus actividades.
- **Gerente de Ventas:** Dirige el departamento de ventas y las negociaciones con clientes.
- **Gerente de Infraestructura:** Dirige y controla las actividades del departamento de infraestructura.
- **Departamento Técnico:** Encargado del soporte y monitoreo de los clientes de la empresa.
- **Departamento de Ventas:** Encargado de negociaciones con clientes potenciales y asesoramiento a clientes en cuanto a mejoras en su infraestructura y servicios.
- **Secretaria de Ventas:** Encargada del apoyo en las tareas del departamento.
- **Asistente Técnico de Ventas:** Encargado de estudios de enlaces para nuevas instalaciones y mejoras para clientes.
- **Departamento de Infraestructura:** Encargado de la construcción e instalación de torres, shelters, mástiles entre otros.
- **Secretaria de Infraestructura:** Encargada del apoyo en las tareas del departamento.
- **Secretaria General:** Encargada de la recepción apoyo al departamento técnico, encargada del soporte de primer nivel.
- **Contador:** Encargado de elaborar y mantener la información financiera de la empresa de la empresa.
- **Asistente Contable:** Apoyo a la gestión del contador.

3.2 Infraestructura actual de la Red Wan de Soporte y Monitoreo

La red WAN de Soporte y Monitoreo se encuentra conformada principalmente por nueve repetidoras ubicadas estratégicamente dentro del área de Quito, teniendo conexión con la oficina principal de la empresa mediante enlaces vía microonda, en la frecuencia de 5.8 GHz, en su gran mayoría la red esta integrada con radios de la marca Mikrotik, para disminuir colisiones y mejorar la seguridad brindada a los clientes, se ha implementado VLANs creando de esta manera diferentes dominios de broadcast, para lo cual, se utiliza switchs

administrables, para el monitoreo de las repetidoras fuera de la provincia de Pichincha se utiliza la infraestructura de los clientes, los clientes a los que se brinda servicios se detallan a continuación.

- Ambacar
- Bco.PROCREDIT
- Coop. Riobamba
- Coop. 14 de Marzo
- Coop. Tulcan
- Coop. Chibuleo
- Coop. Kullkihuasi
- Casa Brasil
- La Ganga
- Expropalm
- Coop. El Sagrario
- Botrosa
- DANEC
- Energy Palm
- Autolandia
- Moyabaca
- Ecuasanitas
- Termas de Papallacta

De los cuales se tomará tres clientes exclusivamente para análisis de monitoreo, con lo que se tendrá un panorama más amplio de cómo se maneja a los usuarios y sus enlaces, se ha escogido a los usuarios por la infraestructura implementada, con enlaces distribuidos a lo largo del país.

Los clientes a los que se analizarán son:

- **ENDESA-BOTROSA**. Industria forestal ecuatoriana, constituida con la finalidad de producir tableros contrachapados de madera, alistonados,

chapas decorativas y productos afines[26], el diagrama de la empresa se encuentra en el **Anexo 3.**

- **DANEC S.A.** Empresa productora de aceites, mantecas, margarinas y jabones. Desde entonces estamos entre las primeras empresas fabricantes y proveedoras de productos derivados de grasas y aceites en Ecuador[27], el diagrama de red de la empresa se encuentra en el **Anexo 5.**
- **Cooperativa de Ahorro y Crédito Riobamba.** Entidad de intermediación financiera dedicada a la captación de recursos de sus socios y clientes a través de libretas de ahorro y certificados de depósito a plazo fijo; y el otorgamiento de créditos, fomentando el progreso y desarrollo de la comunidad[28], el diagrama de red de la empresa se encuentra en el **Anexo 7.**

Se han creado VLANs para cada uno de los enlaces microonda, estos son concentrados en un switch InterVLANs para ser monitorizados desde la oficina principal de FullData Cía. Ltda. el direccionamiento se detalla en la **tabla 3.1**:

Enlace	**Direccionamiento**
Intranet Fulldata	192.168.57.0/24
Red Monitoreo Oficina	192.168.58.0/24
Oficina – Libertad – Ilumbisi	192.168.55.0/24
Oficina – Pichincha Alto – Pilisurco	192.168.58.0/24
Oficina – Pichincha Bajo	192.168.54.0/24
Oficina – Condorcocha – Gerente General	192.168.51.0/24
Oficina – Atacazo Alto – Presidencia – Gerente Técnico	192.168.56.0/24
Atacazo Alto – Atacazo Bajo	192.168.49.0/24

Tabla 3.1 - Enlaces y direccionamiento

Para un mejor entendimiento de la Red de Soporte y Monitoreo se presenta a continuación en la **figura 3.2,** el diagrama físico de la red WAN de Soporte y Monitoreo.

[26] Página Web ENDESA-BOTROSA http://www.endesabotrosa.com/pages/1_quienes_somos.html
[27] Página Web DANEC S.A. http://www.danec.com/index.php?menu=2&option=2&idioma=1
[28] Página Web Coop. Riobamba http://www.cooprio.fin.ec/index.php/institucion/quienes-somos

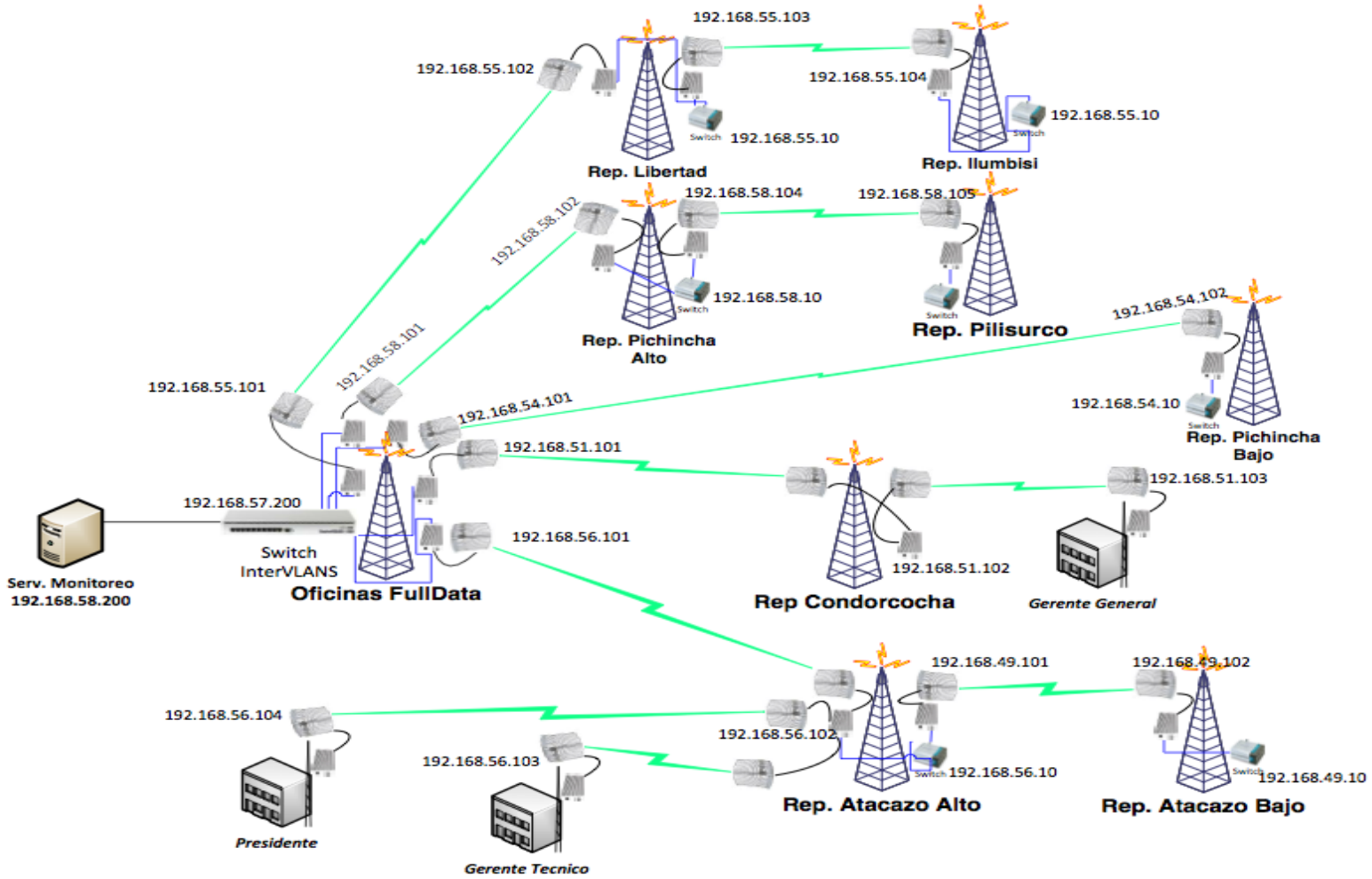


Figura 3.2 - Diagrama Físico de la Red WAN de Soporte y Monitoreo

En la **tabla 3.2**[29]**,** se detalla la distribución de las VLAN de monitoreo para cada uno de los clientes en el switch InterVLANs.

Switch de Monitoreo InterVLANs		
FULLDATA		
IP: 192.168.57.200/24		
PUERTO	**CLIENTE**	**VLAN**
1	Radio hacia Atacazo	TRUNK
	V1-V10	
2	Radio hacia Libertad	TRUNK
	V21-V25,V31	
3	Radio hacia Pichincha Alto	TRUNK
	V41-V47	
4	Radio hacia Pichincha Bajo	TRUNK
	V51-V55	
5	Coop. Riobamba	5
6	Coop. Chibuleo	6
7	Expropalm	7
8	Coop. El Sagrario	8
9	Coop. 14 de Marzo Sto. Dgo.	4
10	Botrosa	10
11	N/C	1
12	Ambacar	2
13	Bco. Procredit	3
14	Coop. 14 de Marzo Quito	21
15	Coop. Tulsan	22
16	Petrobras	23
17	AndesPetro	24
18	DANEC	25
19	Kullkihuasi	48
20	N/C	1
21	N/C	1
22	Soporte Técnico	C
23	Sala de Monitoreo	C
24	Red Fulldata	1
25	N/C	1
26	N/C	1

Tabla 3.2 - Distribución VLANs switch InterVLANs

- Los puertos resaltados con amarillos describen los puertos asignados como Trunk, siendo así tenemos conexión hacia 4 Repetidores.
- Sobre cada uno de los Trunk se asocian puertos VLAN de Acceso y de esta forma es como se le indica al switch que redes llegan o se transmiten.

Cada cliente ya tiene asignado un VLAN ID[30]. A continuación en la **figura 3.3,** se detalla la distribución de VLANs en cada uno de las repetidoras que conforman la red WAN de Soporte y Monitoreo.

[29] Manual de Administración Monitoreo FulData Cía. Ltda. página 9
[30] Manual de Administración Monitoreo, FulData Cía. Ltda., página

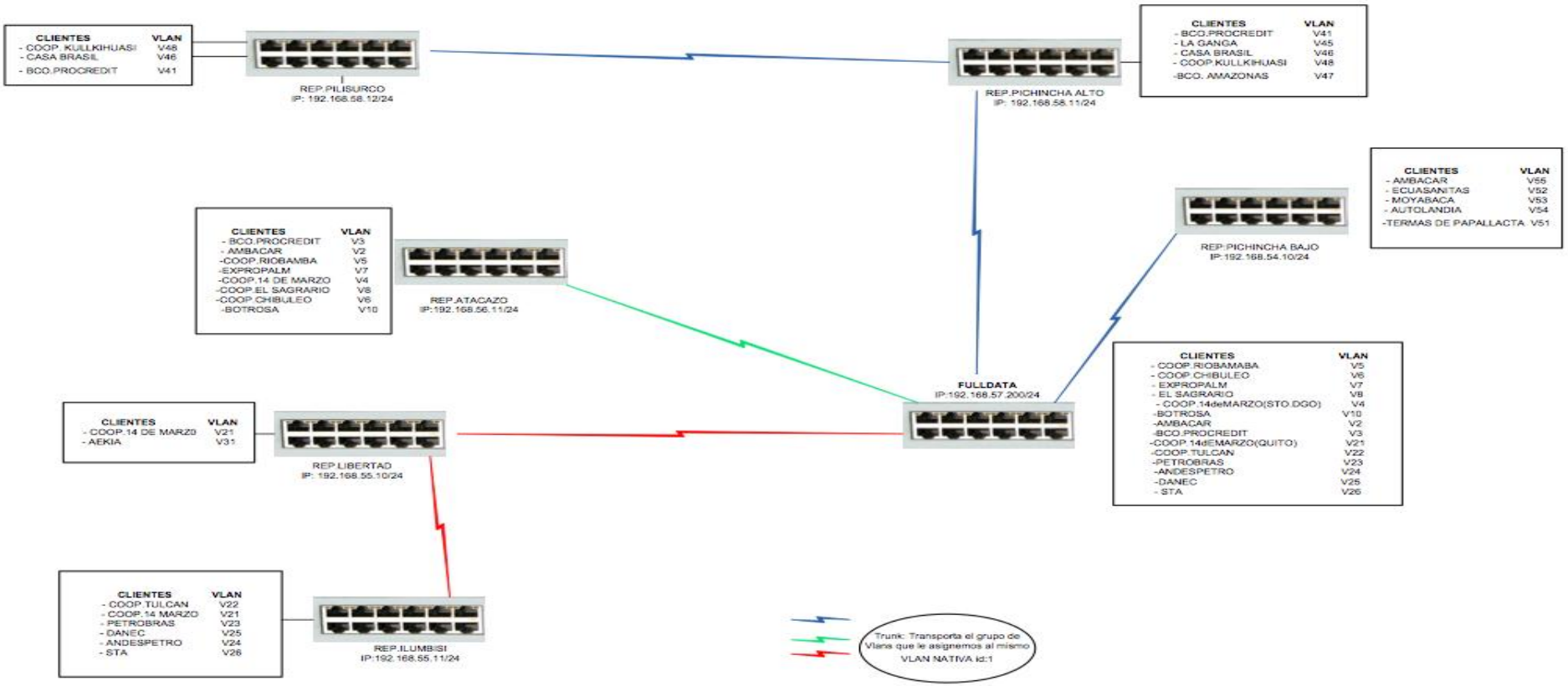


Figura 3.3 - Diagrama de VLANS

3.2.1 Monitoreo a Clientes

Mediante el uso de WhatsUp Gold programa utilizado para el monitoreo de enlaces en FullData, se ha obtenido reportes de los 3 clientes elegidos los únicos reportes disponibles y archivados son los de disponibilidad de enlaces, en base a estos reportes se busca tener un visión clara de la disponibilidad de los enlaces en un tiempo determinado, tomado los datos transcurridos en 1 mes, específicamente noviembre del 2012 pudiendo analizar enlaces que se encuentren bajo los niveles aceptados y el impacto en caso de ser enlaces principales para los clientes.

En las tablas presentadas a continuación se detallan los dispositivos en cada uno de las repetidoras o locaciones de los clientes.

3.2.1.1 Cliente ENDESA-BOTROSA

En primera instancia se revisará los enlaces de la empresa ENDESA-BOTROSA cuyo diagrama de red se encuentra en el **Anexo 3**. La infraestructura utilizada para este cliente consta de 5 repetidoras con enlaces a 5 locaciones en el país.

Repetidoras:

- Atacazo
- Santo Domingo
- La Palma
- Bijahual
- Zapallo

Oficinas:

- Quito
- Quininde
- Rio Verde
- El Vergel
- Yarayacu

En el **Anexo 4** se muestran las tablas del monitoreo realizado con la herramienta WhatsUp Gold a las repetidoras involucradas en la interconexión de ENDESA – BOTROSA, y los dispositivos que se encuentran conectados directamente a cada repetidora.

3.2.1.2 Cliente Cooperativa Riobamba

A continuación se revisará los enlaces de la Cooperativa de Ahorro y Crédito Riobamba cuyo diagrama de red se encuentra en el **Anexo 5.** La infraestructura utilizada para este cliente consta de 9 repetidoras con enlaces a 11 locaciones en el país.

Repetidoras:

- Atacazo
- Ayurco
- Santa Rosa
- Carshao
- Bueran
- Rep. Cuenca
- La Mira
- Rep. Guano
- Pilisurco

Oficinas:

- Quito
- Alausí
- Cumandá
- Chunchi
- Riobamba
- Guano
- Riobamba Sur
- Riobamba Norte

- Riobamba Condamine
- Cuenca Agencia 1
- Cuenca Agencia 2

En el **Anexo 6,** se muestran las tablas del monitoreo realizado con la herramienta WhatsUp Gold a las repetidoras involucradas en la interconexión de la Cooperativa Riobamba, y los dispositivos que se encuentran conectados directamente a cada repetidora.

3.2.1.3 Cliente DANEC

A continuación se revisará los enlaces de la empresa DANEC cuyo diagrama de red se encuentra en el **Anexo 7**. La infraestructura utilizada para este cliente consta de 6 repetidoras con enlaces a 8 locaciones en el país.

Repetidoras:

- Atacazo
- Cayambe
- Condorcocha
- Mirador
- Ilumbisi
- Zapallo

Oficinas:

- SangolquÍ
- Cole
- Shushufindi
    - Plantación
    - Extractora
- Quininde
    - Plantación
    - Extractora
- San Lorenzo

- Oficinas
- Villas

En el **Anexo 8,** se muestran las tablas del monitoreo realizado con la herramienta WhatsUp Gold a las repetidoras involucradas en la interconexión de DANEC, y los dispositivos que se encuentran conectados directamente a cada repetidora.

3.3.1 Inventario de Hardware y Software

Con la finalidad de tener una visión clara de todos los recursos tanto de hardware como de software se ha realizado un inventario en el cual se detallan los equipos con los que se maneja la red WAN de Soporte y Monitoreo, se presenta a continuación un conjunto de tablas en las que se detalla los recursos en la red.

Recursos de Hardware

En la **tabla 3.3,** se muestra los servidores que albergan servicios indispensables para el buen funcionamiento de la red.

Nombre	Marca	Modelo	Memoria	Disco Duro	S.O.	Servicios
DOMAIN	IBM	X3250 M3	2 GB	500 GB	Windows Server 2008 R1	ERP, AD
Mail Server	IBM	eServer xSeries 100	2 GB	250 GB	CentOS 5.5	Mail
Firewall	Clon	N/A	1 GB	50 GB	RouterOS	Firewall

Tabla 3.3 - Servidores

Equipos de Red

La **tabla 3.4,** contiene los radios que se utilizan para los enlaces de la red WAN.

Marca	Modelo	Firmware	IP	Ubicación	Enlace
Mikrotik	Rb711A 5Hn-MMCX	5.20	192.168.55.101	Oficina	Oficina-Libertad
Mikrotik	Rb711A 5Hn-MMCX	5.20	192.168.55.102	Rep. Libertad	Libertad-Oficina
Mikrotik	Rb711A 5Hn-MMCX	5.20	192.168.55.103	Rep. Libertad	Libertad-Ilumbisi
Mikrotik	Rb711A 5Hn-MMCX	5.20	192.168.55.104	Rep. Libertad	Ilumbisi-Libertad
Mikrotik	Rb600	5.18	192.168.56.101	Oficina	Oficina-Atacazo Alto
Mikrotik	Rb532	5.10	192.168.56.102	Atacazo Alto	Atacazo Alto-

					Oficina Atacazo Alto-Presidente Atacazo Alto-Gerente Tecnico
Ubiquity	NanoStation 5	UB-NS5	192.168.56.103	Gerencia Tecnica	Gerencia Tecnica-Atacazo
Ubiquity	NanoStation 5	UB-NS5	192.168.56.104	Presidencia	Presidencia-Atacazo
Ubiquity	NanoStation 5	UB-NS5	192.168.49.101	Atacazo Alto	Atacazo Alto-Atacazo Bajo
Mikrotik	Rb711A 5Hn-MMCX	5.20	192.168.49.102	Atacazo Bajo	Atacazo Bajo-Atacazo Alto
Mikrotik	Rb711A 5Hn-MMCX	5.20	192.168.58.101	Oficina	Oficina-Pichincha Alto
Mikrotik	Rb711A 5Hn-MMCX	5.20	192.168.58.102	Pichincha Alto	Pichincha Alto-Oficina
Mikrotik	Rb411	5.20	192.168.58.104	Pichincha Alto	Pichincha Alto-Pilisurco
Mikrotik	Rb411	5.20	192.168.58.105	Pilisurco	Pilisurco-Pichincha Alto
Orinoco	ROR1000	3.7	192.168.54.101	Oficina	Oficina-Pichincha Bajo
Orinoco	ROR1000	3.7	192.168.54.102	Pichincha Bajo	Pichincha Bajo-Oficina
Mikrotik	Rb433	5.20	192.168.51.101	Oficina	Oficina-Condorcocha
Mikrotik	Rb800	5.20	192.168.51.102	Condorcocha	Condorcocha-Gerente General
Mikrotik	Rb411AH	5.20	192.168.51.103	Gerente General	Gerente General-Condorcocha

Tabla 3.4 - Radios

La **tabla 3.5,** contiene las antenas utilizadas dependiendo las distancias de cada enlace.

Marca	**Ganacia**	**Descripcion**	**Cantidad**
RFElements	17dBi	Antena Flatpanel Integrada	8
Hyperlink	27dBi	Antena Grilla	8
RadioWAVE	34dBi	Antena Parabolica 4 pies	2
Hyperlink	29dBi	Antena Parabolica 2 pies	2
Ubiquity	14dBi	Antena integrada	2

Tabla 3.5 - Antenas

La **tabla 3.6,** contiene los diferentes switches los cuales en su totalidad son de capa 3 para manejar VLANS.

Marca	**Modelo**	**IP**	**Puertos**	**Ubicación**
3Com	Baseline 2226	192.168.55.10	24	Libertad
3Com	Baseline 2226	192.168.55.11	24	Ilumbisi

3Com	Baseline 2226	192.168.54.10	24	Pichincha Bajo
Mikrotik	1100AH PoE	192.168.56.10	13	Atacazo Alto
Mikrotik	1200	192.168.57.200	10	Oficina
Mikrotik	Rb493	192.168.49.10	8	Atacazo Bajo
AlliedTelesis	ATFS 750/24 PoE	192.168.58.10	24	Pichincha Alto

Tabla.3.6 - Switchs

Recursos de Software

En la **tabla 3.7,** se encuentran los sistemas ocupados para la administración del soporte y monitoreo de la red.

Nombre	Descripción	Ubicación	Versión
SugarCRM	Sistema CRM	DOMAIN	Cummunity Edition
Zimbra VMWare	Sistema de Correo	Mail Server	7.0.0
SFCsys	Sistema ERP	DOMAIN	

Tabla 3.7, Sistemas en red

En **la tabla 3.8,** contiene los sistemas operativos utilizados tanto para servidores como para equipos de escritorio.

Nombre	Versión	Descripción
Centos 5.5	5.5	Mail Server
Windows Server 2008	Enterprise R1	Active Directory, ERP, Antivirus
RouterOS	6.0	Firewall
Windows Xp	Service Pack 3	Sistema Operativo técnicos
Windows 7	Service Pack 1	Sistema Operativo técnicos

Tabla 3.8 - Sistemas Operativos

A continuación en la **tabla 3.9,** se recopilan EL software utilizado por el personal encargado del soporte y monitoreo de la red.

Nombre	Versión	Descripción
Kasperky Security Center	2012	Antivirus
Microsoft Office	Professional 2010	Ofimática
Microsoft Visio	2010	Diagramas
WathsUp	Gold edition	Monitoreo
The Dude (Mikrotik)	Dude v3.6	Monitoreo

Tabla 3.9 - Otro Software

3.3.2 Sistemas en Red

- **Sistema CRM[31]**

  El sistema CRM utilizado por la empresa es **SugarCRM** en su versión Sugar Community Edition, el cual permite la administración de la relación con los clientes, se utiliza este sistema para la creación de tickets de atención a clientes y seguimiento del estado de los mismos, permitiendo tener control sobre el trabajo realizado por cada técnico en base a los requerimientos atendidos.

- **Sistema de Correo Electrónico**

  El sistema de correo electrónico es empleado por el sistema CRM para asignación de requerimientos y confirmaciones de estados a cada técnico, para lo cual se utiliza el sistema Zimbra.

- **Sistema de Monitorización**

  Para la monitorización general de la red WAN se maneja el sistema de monitoreo WhatsUp Gold[32] permitiendo un monitoreo proactivo de la red, este sistema mantiene un registro mediante el cual se puede tener informes de disponibilidad de los enlaces para los clientes acorde con los eventos presentados dentro de la red de soporte y monitoreo.3.4 EVALUACIÓN DE RIESGOS DE LA GESTIÓN DE SEGURIDAD EN LA RED WAN DE SOPORTE Y MONITOREO

El análisis de riegos se realiza empleando la metodología MAGERIT[33] elaborado por el CSAE[34]. COBIT permite el uso de diferentes fuentes para la definición de su estándar por lo que se ha elegido esta metodología en específico.

[31] Customer Relationship Management
[32] Gestor de redes exequible y escalable
33 MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
[34] CSAE: Consejo Superior de Administración Electrónica

3.4.1 Metodología MAGERIT para Administración de Riesgos

"La gestión de los riesgos es una piedra angular en las guías de buen gobierno, público o privado, donde se considera un principio fundamental que las decisiones de gobierno se fundamenten en el conocimiento de los riesgos que implican"[35]

En base al método cualitativo de investigación se tomará en cuenta las siguientes tareas para una óptima evaluación de riesgos:

(MAR) Método de Análisis de Riesgo

- MAR.1 – Caracterización de los activos
  - MAR.11 – Identificación de los activos
  - MAR.12 – Dependencias entre activos
  - MAR.13 – Valoración de los activos
- MAR.2 – Caracterización de las amenazas
  - MAR.21 – Identificación de las amenazas
  - MAR.22 – Valoración de las amenazas
- MAR.3 – Caracterización de las salvaguardas
  - MAR.31 – Identificación de las salvaguardas pertinentes
  - MAR.32 – Valoración de las salvaguardas
- MAR.4 – Estimación del estado de riesgo
  - MAR.41 – Estimación del impacto
  - MAR.42 – Estimación del riesgo

3.4.2 Evaluación de Riesgos de la Gestión de la Seguridad en la Red WAN de Soporte y Monitoreo

Mediante la evaluación de riesgos se logra obtener un panorama claro de la situación en la que se encuentra la administración actual de los recursos con los que cuenta la empresa para gestionar la red de Soporte y Monitoreo, aplicando

[35] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método.

adecuadamente Magerit, se puede enfocar directamente en los datos más relevantes en la Gestión de la Seguridad.

3.4.2.1. Caracterización de los activos

Mediante la caracterización de los activos se identifican los activos relevantes, caracterizándolos por su tipo, logrando determinar relaciones entre activos, para poder valorarlos acorde al riesgo al que se encuentran expuestos.

El resultado de esta actividad es el informe denominado "modelo de valor"[36].

- **Identificación de los activos**

Se denomina a un activo como "Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos"[37].

Teniendo en cuenta el concepto de un activo previamente mencionado, Magerit ha clasificado los activos de manera que se tenga un control objetivo sobre los activos con mayor riesgo.

- **[essential] Activos esenciales**. En un sistema de información hay 2 cosas esenciales:
  - la **información** que se maneja y
  - los **servicios** que prestan.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema. Dentro de la información que se maneja, puede ser interesante considerar algunas características formales tales como si son de carácter personal, con requisitos legales, o si están sometidos a alguna

[36] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método, pag. 36
[37] Norma **UNE 71504:2008**

clasificación de seguridad.

- **[info] Información**. Información de nivel administrativo o datos de suma importancia en la organización.
    - [adm] datos de interés para la administración
    - [vr] datos vitales (registros de la organización)
- **[S]Servicios**. Toma en cuenta los servicios prestados por parte de FULLDATA Cia. Ltda. para la administración de la Red WAN de Soporte y Monitoreo.
    - [Mon] Monitoreo de red
    - [Sop] Soporte Técnico
    - [ext] a usuarios externos (bajo una relación contractual)
- **[arch] Arquitectura del sistema**. Se trata de elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.
    - [sap] punto de acceso al servicio
    - [ip] punto de interconexión
- **[D] Datos**. Son los activos más importantes dentro de la organización, pues representan el conocimiento que tiene la organización en todas las áreas dentro de la misma.
    - [int] datos de gestión interna
    - [password] credenciales por ejemplo contraseñas
    - [auth] datos de validación de credenciales
    - [log] registro de actividad
- **[K] Claves criptográficas**. Con la finalidad de proteger la información y otros activos, se utilizan claves criptográficas que permiten autenticar o mantener secretos servicios e información importante.
    - [com] protección de las comunicaciones
    - [channel] claves de cifrado del canal
    - [authentication] claves de autenticación
    - [verification] claves de verificación de autenticación

- **[SW] Software**. Se denomina software a un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora[38].
    - [sub] desarrollo a medida (subcontratado)
    - [app] servidor de aplicaciones
    - [email_client] cliente de correo electrónico
    - [email_server] servidor de correo electrónico
    - [office] ofimática
    - [av] anti virus
    - [os] sistema operativo
- **[HW] Equipamiento informático (hardware)**. Equipos, materiales y medios físicos que son utilizados en forma directa o indirecta para manejar los servicios que presta la organización.
    - [host] grandes equipos[39]
    - [mid] equipos medios[40]
    - [pc] informática personal
    - [network] soporte de la red[41]
        - [switch] conmutadores
        - [ant] antenas
        - [rad] radios
        - [router] encaminadores
- **[COM] Redes de comunicaciones**. Servicios e instalaciones que brindan comunicación dentro de una red como servicios contratados o prestados a terceros.
    - [pp] punto a punto

[38] RAE, Real Academia Española

[39] Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente gravosos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción.

[40] Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso de destrucción.

[41] equipamiento necesario para transmitir datos: routers, switchs, entre otros

    - [LAN] red local
    - [WAN] red de área amplia
    - [Internet] Internet
- **[AUX] Equipamiento auxiliar**. Equipos que no se encuetran relacionados directamente con los datos pero que forman parte importante dentro de la red.
    - [power] fuentes de alimentación
    - [ups] sistemas de alimentación ininterrumpida
    - [gen] generadores eléctricos
    - [furniture] mobiliario: armarios, etc.
- **[L] Instalaciones**. Lugares donde se encuentran equipos o información de la organización.
    - [site] recinto
    - [building] edificio
    - [bod] bodega
    - [mobile] plataformas móviles
        - [car] vehículo terrestre: automóvil.
- **[P] Personal**. El recurso humano que es utilizado para las funciones diarias de la red.
    - [op] operadores
    - [com] administradores de comunicaciones

- **Dependencias entre activos**

La dependencia entre activos supone que en el caso de que una amenaza que afecte a un activo del que dependa otro activo superior, tendrá impacto directo sobre el activo superior. Para llevar a cabo la definición de dependencias la metodología empleada propone una estructura de 5 capas, las cuales se identifican a continuación empezando por la inferior:

1. Entorno: equipamiento auxiliar, personal y edificios.
2. Sistema de información: hardware, software, comunicaciones y soportes.
3. Información: Datos.
4. Funciones de la organización: Servicios finales.
5. Otros activos: Imagen, know how.

- **Valorización de los activos**

La valorización de los activos es una parte primordial en la evaluación de riesgos de la red debido a que de esta manera se puede evaluar la importancia de un activo y el costo que representa a la administración la posible pérdida parcial o total de un activo especifico, para valorar de una manera adecuada se utilizan dimensiones, se utilizaran: [D] Disponibilidad, [I] integridad y [C] Confidencialidad.

En la dimensión de [D] Disponibilidad se tiene que un activo tiene alta valoración en el caso de no estar disponible, este ocasione consecuencias perjudiciales para la empresa, por el contrario si el activo puede no estar disponible por lagos periodos de tiempo sin afectar a la empresa ese tiene una valoración baja.

En la dimensión de [I] Integridad, un activo tiene un nivel de valoración alto en el caso de que su alteración intencional o no, ocasione consecuencias perjudiciales para la empresa, por el contrario si el activo a pesar de ser alterado no afecte el funcionamiento empresarial.

En la dimensión de [C] Confidencialidad, un activo tiene un nivel de valoración alto en el caso de que su revelación a personas no autorizadas cree consecuencias perjudiciales a la empresa, en el caso contrario el activo tendrá una valoración baja. Se tiene una escala de valoración presentada a continuación en la **tabla 10.**

Valoración	Nivel	Consecuencia
10	Muy Alto	Daño muy grave para la organización
7	Alto- Medio	Daño grave a la organización
5	Medio	Daño importante a la organización
3	Medio- Bajo	Daño menor a la organización
1	Bajo	Daño irrelevante a la organización

Tabla 3.10 - Escala de valoración de Activos

En base a estas valoraciones se tiene las siguientes tablas presentado una valoración para cada activo en cada dominio antes mencionado.

- En **la tabla 3.11,** se muestran la valoración de los activos de la información [inf].

Activo	**[D]**	**[I]**	**[C]**
[adm] datos de interés para la administración	10	10	10
[vr] datos vitales (registros de la organización)	10	10	10

Tabla 3.11 - [inf] Información

- En la **tabla 3.12,** se muestran la valoración de los activos de servicios [S].

Activo	**[D]**	**[I]**	**[C]**
[mon] Monitoreo de red	7	10	N/A
[sop] Soporte Técnico	7	N/A	N/A
[ext] a usuarios externos (bajo una relación contractual)	10	N/A	N/A

Tabla 3.12 - [S] Servicios

- En la **tabla 3.13,** se muestra la valoración de los activos de la arquitectura de red [arch]

Activo	**[D]**	**[I]**	**[C]**
[sap] punto de acceso al servicio	10	N/A	N/A
[ip] punto de interconexión	10	N/A	N/A

Tabla 3.13 - [arch] Arquitectura

- En la tabla **3.14,** se muestran la valoración de los activos en la categoría de Datos [D]

Activo	**[D]**	**[I]**	**[C]**
[int] datos de gestión interna	7	7	7
[password] credenciales por ejemplo contraseñas	7	10	10
[auth] datos de validación de credenciales	10	10	10
[log] registro de actividad	7	5	5

Tabla 3.33 - [D] Datos

- En la **tabla 3.15,** se muestran la valoración de los activos pertenecientes a claves criptográficas [K]

Activo	[D]	[I]	[C]
[com] protección de las comunicaciones	10	10	10
[channel] claves de cifrado del canal	10	7	7
[authentication] claves de autenticación	10	10	10
[verification] claves de verificación de autenticación	10	10	10

Tabla 3.15 - [K] Claves criptográficas

- En la **tabla 3.16,** se muestran la valoración de los activos dentro de la categoría de software [SW].

Activo	[D]	[I]	[C]
[sub] desarrollo a medida (subcontratado)	10	10	7
[app] servidor de aplicaciones	10	10	7
[email_client] cliente de correo electrónico	7	5	10
[email_server] servidor de correo electrónico	10	10	10
[office] ofimática	5	3	N/A
[av] anti virus	10	10	N/A
[os] sistema operativo	7	7	N/A

Tabla 3.16 - [SW] Software

- En la **tabla 3.17,** se muestran la valoración de los activos de la categoría de hardware [HW]

Activo	[D]	[I]	[C]
[host] grandes equipos	10	10	10
[mid] equipos medios	10	7	7
[pc] informática personal	10	5	N/A
[switch] conmutadores	10	10	7
[ant] antenas	10	10	N/A
[rad] radios	10	10	10
[router] encaminadores	10	10	10

Tabla 3.17 - [HW] Equipamiento informático (hardware).

- En la **tabla 3.18,** se muestran la valoración de los activos de redes de comunicaciones [COM]

Activo	[D]	[I]	[C]
[pp] punto a punto	10	10	10

[LAN] red local	10	10	7
[WAN] red de área amplia	10	10	10

Tabla 3.18 - [COM] Redes de comunicaciones

- En la **tabla 3.19,** se muestran la valoración de los activos con el equipamiento auxiliar [AUX].

Activo	**[D]**	**[I]**	**[C]**
[power] fuentes de alimentación	10	7	N/A
[ups] sistemas de alimentación ininterrumpida	10	7	N/A
[gen] generadores eléctricos	5	1	N/A

Tabla 3.19 - [AUX] Equipamiento auxiliar

- En la **tabla 3.20,** se muestran la valoración de los activos en la categoría de instalaciones [L].

Activo	**[D]**	**[I]**	**[C]**
[site] recinto	10	5	N/A
[building] edificio	10	5	N/A
[bod] bodega	7	7	N/A
[car] vehículo terrestre: carro	7	10	N/A

Tabla 3.20 - [L] Instalaciones

- En la **tabla 3.21,** se muestran la valoración de los activos del grupo de personal [P].

Activo	**[D]**	**[I]**	**[C]**
[op] operadores	10	N/A	N/A
[com] administradores de comunicaciones	10	N/A	N/A

Tabla 3.21 - [P] Personal

3.4.2.2 Caracterización de las amenazas

El objetivo de estas tareas es caracterizar el entorno al que se enfrenta el sistema, qué puede pasar, qué consecuencias se derivarían y cómo de probable es que pase. Se lo puede resumir en la expresión “conoce a tu enemigo”.

- **Identificación de las amenazas**

En base a las evaluaciones realizadas en la red WAN de Soporte y Monitoreo a continuación se presentan las amenazas que pueden atacar a los activos dentro de la metodología Magerit se tiene amenazas clasificadas de la siguiente manera:

- **[N] Desastres Naturales**

  [N.1] ***Fuego***. Posibilidad de incendios forestales en repetidoras.

  [N.2] ***Daños por agua.*** Posibilidad de inundaciones.

  [N.3] ***Fenómenos Sísmicos***. Posibilidad de pérdida de repetidoras por movimientos telúricos.

  [N.4] ***Fenómeno de origen volcánico***. Posibilidad de pérdida de equipos por erupciones volcánicas o emanaciones de ceniza.

- **[I] Amenazas Industriales**

  [I.1] ***Fuego***. Posibilidad de pérdida por incendios.

  [I.2] ***Contaminación Mecánica***. Esta amenaza esta atribuida a la acumulación de polvo o suciedad causando mal funcionamiento de equipos.

  [I.3] ***Contaminación Electromagnética***. Producida por interferencias de radio o campos electromagnéticos.

  [I.4] ***Averías de origen Físico o Lógico***. Problemas en equipos o programas, debido a fallas de fábrica.

  [I.5] ***Condiciones inadecuadas de temperatura y/o humedad***. Posibilidad de mal funcionamiento o inhibición de equipos.

  [I.6] ***Fallo de servicios de comunicaciones***. Interrupción o cese de servicios de comunicación debido a destrucción de equipos de comunicaciones o cualquier problema que cause la detención del servicio.

  [I.7] ***Degradación de los soportes de almacenamiento de la información***. Amenaza causada por la degradación de equipos y sistemas de información debido al paso del tiempo.

- **Errores y fallos no intencionados.**

  [E.1] ***Errores de los usuarios***. Hace referencia a las equivocaciones de las personas cuando hacen uso de los servicios o de los datos.

  [E.2] ***Errores del Administrador***. Hace referencia a las equivocaciones cometidas por personas con responsabilidades de instalación y de operación.

  [E.4] ***Errores de Configuración***. Introducción de datos erróneos.

  [E.7] ***Deficiencias en la organización***. Se produce cuando dentro de la organización los procesos no se encuentran asignados correctamente causando descoordinaciones y errores.

  [E.8] ***Difusión de software dañino***. Propagación de virus, gusanos, troyanos, bombas lógicas, entre otros.

  [E.14] ***Escapes de Información***. Perdida de información debido al conocimiento de personas ajenas y sin acceso a esta información sin que necesariamente sea alterada.

  [E.15] ***Alteración de la información***. Alteración accidental de la información.

  [E.16] ***Introducción de falsa información***. Introducción accidental de información incorrecta.

  [E.18] ***Destrucción de la información***. Perdida accidental de información.

  [E.19] ***Divulgación de información***. Entrega de información por parte del personal, ya sea por causas ya sea con o sin intención.

  [E.20] ***Vulnerabilidades de los programas (Software)***. Errores en los programas desarrollados como solución empresarial

  [E.21] ***Errores de mantenimiento / Actualización de programas (Software).*** Falta o desconocimiento de procedimientos de actualización y mantenimiento de software.

  [E.23] ***Errores de mantenimiento / Actualización de equipos (hardware).*** Falta de mantenimiento o de criterio para cambiar equipos que se encuentren el mal estado o hayan su vida útil.

  [E.24] ***Caída del sistema por agotamiento de recursos.*** Problemas en los sistemas a causa del mal uso, o falta de equipos para mantener la red

en cuestión.

[E.28] ***Indisponibilidad del personal***. Hace referencia a la ausencia accidental del puesto de trabajo de una persona ya sea por enfermedad o calamidad doméstica.

- **Ataques intencionados.**

  [A.4] ***Manipulación de la configuración***. La mayoría de activos dependen de una configuración la misma depende del administrador.

  [A.5] ***Suplantación de la identidad del usuario***. Cuando un atacante utiliza credenciales para hacerse pasar por un usuario autorizado utilizando sus privilegios para sus fines.

  [A.6] ***Abuso de privilegios de acceso***. Tiene que ver con el abuso por parte de un colaborador dado por su nivel de privilegios dentro de la red.

  [A.7] ***Uso no previsto.*** Manejo de recursos de la red con fines no adecuados o previstos normalmente para uso de interés personal.

  [A.8] ***Difusión de Software dañino.*** Propagación intencionada de virus, espías, gusanos, troyanos, bombas lógicas, etc.

  [A.11] ***Acceso no autorizado***. Acceso a los sistemas informáticos sin autorización comúnmente debido a fallos en el sistema de identificación y autorización.

  [A.15] ***Modificación de la información***. Causar perjuicio a la organización mediante la modificación intencional de la información.

  [A.16] ***Introducción de falsa información***. Causar perjuicio a la organización insertando información invalida.

  [A.17] ***Corrupción de la información***. Causar perjuicio a la organización mediante la manipulación intencionada de la información.

  [A.18] ***Destrucción de la información***. Supresión intencional de información.

  [A.19] ***Divulgación de la información***. Revelación de información

  [A.22] ***Manipulación de programas***. Alteración del código de un programa con la finalidad de obtener un beneficio indirecto cuando un usuario autorizado utiliza el programa.

[A.24] ***Denegación de servicio***. En estos ataques se niega el uso de recursos del sistema a usuarios legítimos.

[A.25] ***Robo de Equipos***. Sustracción de equipamiento o dispositivos que causan perdida a la organización.

[A.26] ***Ataque destructivo***. Vandalismo.

[A.28] ***Indisponibilidad del personal***. Ausencia deliberada del puesto de trabajo

[A.30] ***Ingeniería Social***. Uso de medios no técnicos para obtener accesos no autorizados

- **Valoración de las amenazas**

Las amenazas detalladas anteriormente se las relaciona adecuadamente con los activos, una vez identificadas las amenazas se procede a valorizarlas para determinar la posibilidad de que estas ocurran sobre los activos.

De igual forma que en los activos existe una tabla de escala de valoración para amenazas presentada en la **tabla 3.22.**

Valoración	Frecuencia	Significado en tiempo
100	Muy Frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Un vez al año
1/10	Poco Frecuente	Cada varios años
0	Nunca	Sin ocurrencia

Tabla 3.22 - Escala de valoración de amenazas

De la misma manera existe una escala que valora el impacto que tiene una amenaza en un activo especifico se la presenta en la **tabla 3.23.**

Valoración	Impacto	Significado
100 %	Alto	Degrada totalmente el activo
70 %	Alto-Medio	Degrada parcialmente el activo
50 %	Medio	Degrada el activo
30 %	Medio- Bajo	Posiblemente cause daño a la organización
10 %	Bajo	No causa daño a la organización

Tabla 3.23 - Escala de valoración de la degradación de activos

3.3.2.4 Estimación del estado de riesgo

Una vez realizada la valorización de los activos y de las amenazas se puede realizar una estimación tanto del impacto y el riesgo que pueden provocar las amenazas en la organización.

- **Estimación del impacto**

Para cada activo se realiza el cálculo de impacto, para el cálculo existen dos tipos de impacto:

- ***Impacto Acumulado***. Se calcula con base en el valor acumulado del activo (valor propio + valor de los activos que dependen de él) y las amenazas a las que está expuesto. Este impacto se calcula para cada activo, por cada amenaza y en cada dimensión de valoración.
- ***Impacto repercutido***. Es el impacto calculado sobre un activo teniendo en cuenta: su valor propio y las amenazas a las que están expuestos los activos de los que depende. El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración.

- **Estimación del riesgo**

Se denomina riesgo a la medida del daño probable sobre un sistema, Conociendo el impacto de las amenazas sobre los activos, es inmediato derivar el riesgo sin necesidad de tener en cuenta la frecuencia de ocurrencia. Existen 2 tipos de riesgo:

- ***Riesgo Acumulado***. Este tipo de riesgo es el calculado sobre un activo teniendo en cuenta el impacto acumulado sobre un activo debido a una amenaza y la frecuencia de la amenaza.
- ***Riesgo Repercutido***. Este tipo de riesgo es el calculado sobre un activo teniendo en cuenta el impacto repercutido sobre un activo debido a una amenaza y la frecuencia de la amenaza.

El riesgo se clasifica de acuerdo a su nivel de criticidad, lo que significa que entre más alto sea el nivel de criticidad del riesgo mayor atención requiere por parte de organización la amenaza, de tal forma que al ser gestionado con unas contramedidas su nivel disminuya y se logre de esta forma un equilibrio en el sistema. En la **tabla 3.24,** se muestra la escala de nivel de criticidad de Riesgo.

Valor numérico	Significado
5	Critico
4	Muy alto
3	Alto
2	Medio
1	Bajo
0	Despreciable

Tabla 3.24 - se muestra la escala de nivel de criticidad de Riesgo

En conclusión con los datos obtenidos se procede a crear una tabla de riesgo acumulado de activos en base a la situación actual. Permitiendo enfocarse en los activos que presenten un mayor estado de riesgo, y de esta manera emitir un criterio claro de cómo se puede optimizar la seguridad de dicho activo.

En la **tabla 3.25,** se muestra la información de riesgo acumulado tomando en cuenta los siguientes valores.

- **Activo.** Hace referencia los bienes tangibles e intangibles a valorarse.
- **Amenaza.** Hace referencia a la amenaza materializada en el activo.
- **Dimensión.** Hace referencia a la dimensión de valoración (D, I, C) en la que se materializo la amenaza. o Valor propio. Hace referencia al valor de la apreciación inicial del activo.
- **Valor propio.** Hace referencia al valor que se establece en base al impacto que causaría la pérdida total o parcial de dicho activo.
- **Degradación.** Hace referencia al nivel porcentual que perjudica una amenaza específica a los activos.
- **Impacto.** Calculo del daño del activo a causa de una posible amenaza.
- **Frecuencia.** Que tan frecuente se presenta o puede presentarse una amenaza.

- **Riesgo.** Hace referencia a la medida del daño sobre el sistema.

Activo	Amenaza	Dimensión	Valor Propio	Degradación (%)	Impacto	Frecuencia	Riesgo
[adm] datos de interés para la administración	E.1	I	10	100	10	1	5
[adm] datos de interés para la administración	E.2	I	10	100	10	1	5
[adm] datos de interés para la administración	E.18	D	10	100	10	1	5
[adm] datos de interés para la administración	A.6	C	10	100	10	1	3
[adm] datos de interés para la administración	A.17	I	10	80	10	1	4
[adm] datos de interés para la administración	A.18	D	10	100	10	1	5
[vr] datos vitales (registros de la organización)	E.2	D	10	50	10	1	5
[vr] datos vitales (registros de la organización)	E.18	D	10	100	10	1	4
[vr] datos vitales (registros de la organización)	A.6	C	10	100	10	1	4
[Mon] Monitoreo de red	E.2	D	10	100	7	1	3
[Mon] Monitoreo de red	E.7	D	7	70	7	1	4
[Mon] Monitoreo de red	E.20	I	7	50	10	1	4
[Mon] Monitoreo de red	E.21	D	7	50	10	10	4
[Mon] Monitoreo de red	E.23	D	7	50	7	1	4
[Mon] Monitoreo de red	E.24	D	10	50	7	1	5
[Mon] Monitoreo de red	E.28	D	10	100	7	1	3
[Mon] Monitoreo de red	A.11	C	10	100	10	1	4
[Sop] Soporte Técnico	E.21	D	10	100	7	1	3
[Sop] Soporte Técnico	E.24	D	7	100	10	1	4
[sap] punto de acceso al servicio	E.21	D	7	75	10	1	4
[sap] punto de acceso al servicio	E.23	D	10	75	7	1	4
[sap] punto de acceso al servicio	E.24	D	10	100	7	1	4
[sap] punto de acceso al servicio	E.28	D	10	100	10	1	5
[sap] punto de acceso al servicio	A.4	I	7	75	10	1	5
[sap] punto de acceso al servicio	A.7	I	10	100	10	1	4
[ip] punto de interconexión	[N]	I	7	100	10	1	5
[ip] punto de interconexión	E.21	D	7	75	7	1	5
[ip] punto de interconexión	E.23	D	7	75	7	1	5
[ip] punto de interconexión	E.24	D	5	100	7	1	4

[ip] punto de interconexión	E.28	D	10	100	7	1	4
[ip] punto de interconexión	A.4	I	10	75	7	1	5
[ip] punto de interconexión	A.25	D	5	100	10	1	4
[ip] punto de interconexión	A.26	D	10	75	10	1	4
[int] datos de gestión interna	E.8	I	10	100	7	1	5
[int] datos de gestión interna	E.14	C	10	75	7	1	4
[int] datos de gestión interna	E.15	D	10	100	10	1	4
[int] datos de gestión interna	E.16	I	7	100	10	1	4
[int] datos de gestión interna	E.18	I	5	100	10	1	5
[int] datos de gestión interna	E.19	C	5	75	10	1	4
[password] credenciales por ejemplo contraseñas	A.5	C	10	100	7	1	5
[password] credenciales por ejemplo contraseñas	A.11	C	10	100	7	1	5
[auth] datos de validación de credenciales	A.5	C	10	100	10	1	5
[auth] datos de validación de credenciales	A.6	C	10	100	10	1	5
[auth] datos de validación de credenciales	A.11	C	10	100	10	1	5
[log] registro de actividad	E.21	I	7	75	5	1	5
[com] protección de las comunicaciones	A.4	I	5	100	7	1	4
[channel] claves de cifrado del canal	A.11	C	7	100	7	1	5
[authentication] claves de autenticación	A.5	C	7	100	7	1	4
[verification] claves de verificación de autenticación	A.5	C	7	100	7	1	4
[verification] claves de verificación de autenticación	A.11	I	7	100	10	1	4
[ext] a usuarios externos (bajo una relación contractual)	E.20	D	10	100	10	1	5
[ext] a usuarios externos (bajo una relación contractual)	E.21	D	10	100	10	1	5
[sub] desarrollo a medida (subcontratado)	E.21	D	7	75	10	1	5
[app] servidor de aplicaciones	E.20	D	5	100	10	1	4
[email_client] cliente de correo electrónico	E.21	D	10	75	10	1	3
[email_server] servidor de correo electrónico	E.21	D	10	75	10	1	3
[office] ofimática	E.21	D	10	75	7	1	4
[av] antivirus	E.21	D	10	75	7	1	5
[os] sistema operativo	E.4	I	10	100	10	1	5
[os] sistema operativo	E.4	C	10	100	10	1	5
[os] sistema operativo	E.4	D	10	100	10	1	5
[os] sistema operativo	A.6	C	7	100	10	1	5

[os] sistema operativo	A.6	I	10	100	10	1	5
[host] grandes equipos	E.2	D	7	75	7	1	5
[host] grandes equipos	E.4	I	7	75	7	1	5
[host] grandes equipos	A.4	C	10	100	5	1	5
[mid] equipos medianos	E.2	D	5	75	5	1	5
[mid] equipos medianos	E.4	I	5	75	7	1	5
[mid] equipos medianos	A.4	C	5	100	7	1	5
[pc] informática personal	E.2	D	10	75	5	1	5
[pc] informática personal	E.4	I	10	75	7	1	4
[pc] informática personal	A.4	C	10	100	7	1	4
[switch] conmutadores	I.4	D	10	100	10	1	5
[switch] conmutadores	I.5	D	10	100	10	1	5
[switch] conmutadores	E.4	I	7	50	10	1	5
[ant] antenas	I.4	D	7	100	10	1	5
[ant] antenas	A.25	I	10	100	10	1	5
[ant] antenas	A.26	D	5	100	10	1	4
[rad] radios	I.2	D	5	100	10	1	5
[rad] radios	I.3	D	10	100	10	1	5
[rad] radios	I.5	D	7	50	10	1	5
[rad] radios	A.4	I	7	75	7	1	4
[rad] radios	A.26	I	10	100	7	1	4
[router] encaminadores	I.2	D	10	100	7	1	4
[router] encaminadores	I.3	D	10	100	10	1	5
[router] encaminadores	I.5	D	7	50	10	1	5
[router] encaminadores	A.4	I	7	75	7	1	5
[router] encaminadores	A.26	I	10	100	7	1	5
[pp] punto a punto	I.3	I	5	100	10	1	5
[pp] punto a punto	I.4	D	10	100	7	1	4
[pp] punto a punto	I.6	D	10	100	7	1	5
[LAN] red local	E.2	D	10	75	10	1	5
[LAN] red local	I.6	D	10	100	10	1	4
[WAN] red de área amplia	E.2	D	10	75	10	1	5
[WAN] red de área amplia	I.6	D	10	100	10	1	5

[power] fuentes de alimentación	E.23	D	7	100	10	1	5
[power] fuentes de alimentación	A.25	I	5	100	7	1	4
[ups] sistemas de alimentación ininterrumpida	E.23	D	7	75	7	1	3
[ups] sistemas de alimentación ininterrumpida	A.25	I	5	100	5	1	3
[gen] generadores eléctricos	E.23	D	7	75	7	1	4
[gen] generadores eléctricos	A.25	I	5	100	5	1	4
[site] recinto	N.1	D	10	100	5	1	5
[site] recinto	N.2	D	10	100	5	1	5
[site] recinto	N.3	D	7	100	5	1	5
[site] recinto	I.1	D	7	100	10	1	5
[building] edificio	N.1	D	10	100	10	1	5
[building] edificio	N.2	D	7	100	10	1	5
[building] edificio	N.3	D	7	100	10	1	5
[building] edificio	I.1	D	10	100	10	1	5
[car] vehículo terrestre: automóvil	A.25	D	7	100	7	1	5
[car] vehículo terrestre: automóvil	A.26	D	5	100	7	1	5
[op] operadores	E.28	D	10	100	7	1	4
[op] operadores	A.28	D	10	100	10	1	5
[com] administradores de comunicaciones	E.2	D	7	100	10	1	4
[com] administradores de comunicaciones	E.28	D	7	100	10	1	5
[com] administradores de comunicaciones	A.28	D	10	100	10	1	5

Tabla 3.44 Riesgo acumulado de situación actual

CAPÍTULO 4

PLAN DE AUDITORÍA PARA LA GESTIÓN DE SEGURIDAD DE LA RED WAN

4.1 Alcance de la Auditoría de la Gestión de la Red Wan

Para realizar el desarrollo de la auditoria determinamos los procesos COBIT involucrados dentro de la Gestión de la Red de Datos WAN, siguiendo los objetivos de control detallados en el Marco de Trabajo COBIT 4.1.

Se han seleccionado aquellos procesos que tienen relación con la gestión de la seguridad de la red WAN que sean aplicable a la naturaleza del negocio y que contribuyen a alcanzar los objetivos del negocio.

4.2 Modelo de Madurez

Los directivos y ejecutivos de la Organización deben tener una correcta administración de TI, realizando un plan de negocio para alcanzar un nivel óptimo de administración y control de TI.

Los modelos de madurez una Organización los reconocería como estados posiblemente actuales y futuros, estos modelos no están diseñados para ser limitantes, donde no se puede pasar a los niveles superiores sin haber cumplido antes los niveles antecesores, al usar los modelos de madurez para los 34 procesos de TI de COBIT.

Se ha definido un modelo de madurez para cada uno de los 34 procesos de TI, con una escala de medición creciente a partir de 0, no existente, hasta 5, optimizado, la ventaja es que es relativamente fácil para la dirección ubicarse a sí misma en una escala y de esta forma evaluar que se debe hacer si se requiere una mejora.

En la **tabla 4.1,** se muestra el modelo de madurez a usarse en esta auditoria.

Nivel de Madurez	Estado del Entorno de Control
0 No existe	No se reconoce la necesidad del control. El control no es parte de la cultura organizacional. Existe una alto riesgo de deficiencias e incidentes de control
1 Inicial /ad hoc	Se reconoce algo de la necesidad del control interno. El enfoque hacia los requerimientos de riesgo y control es inicial y desorganizado, sin comunicación o supervisión. No se identifican las deficiencias. Los empleados no están conscientes de sus responsabilidades.
2 Repetible pero . Intuitivo	Existen controles pero no están documentados. Su operación depende del conocimiento y motivación de los individuos. La efectividad no se evalúa de forma adecuada. Existen muchas debilidades de control y no se resuelven de forma apropiada; el impacto puede ser severo. Las medidas de la gerencia para resolver problemas de control no son consistentes ni tienen prioridades. Los empleados pueden no estar conscientes de sus responsabilidades.
3 Definido	Existen controles y están documentados de forma adecuada. Se evalúa la efectividad operativa de forma periódica y existe un número promedio de problemas. Sin embargo, el proceso de evaluación no está documentado. Aunque la gerencia puede manejar la mayoría de los problemas de control de forma predecible, algunas debilidades de control persisten y los impactos pueden ser severos. Los empleados están conscientes de sus responsabilidades de control.
4 Administrado y . Medible	Existe un ambiente efectivo de control interno y de administración de riesgos. La evaluación formal y documentada de los controles ocurre de forma periódica. Muchos controles están automatizados y se realizan de forma periódica. Es probable que la gerencia detecte la mayoría de los problemas de control, aunque no todos los problemas se identifican de forma rutinaria. Hay un seguimiento consistente para manejar las debilidades de control identificadas. Se aplica un uso de la tecnología táctico y limitado a los controles automatizados.
5 Optimizado	Un programa organizacional de riesgo y control proporciona la solución continua y efectiva a problemas de control y riesgo. El control interno y la administración de riesgos se integran a las prácticas empresariales, apoyadas con una supervisión en tiempo real, y una rendición de cuentas completa para la vigilancia de los controles, administración de riesgos, e implantación del cumplimiento. La evaluación del control es continua y se basa en auto-evaluaciones y en análisis de brechas y de causas raíz. Los empleados se involucran de forma pro-activa en las mejoras de control.

Tabla 4.1 – Modelo de Madurez [42]

[42] © 2007 IT Governance Institute, COBIT 4.1, Pág 175

4.3 Mapeo entre los Procesos de y las Áreas focales de Gobierno de TI, COSO, los Recursos TI y los Criterios de Información de COBIT

En la **tabla 4.2,** proporciona las equivalencias entre los procesos de TI de COBIT y las cinco áreas focales del gobierno de TI, los recursos de TI y los criterios de información. La tabla también contiene un indicador de importancia relativa (alta, media y baja), con base en la evaluación por comparación vía COBIT ONLINE. Esta matriz en una página, y a alto nivel como el marco de trabajo de COBIT resuelve los requisitos de gobierno de TI y de COSO[43], y muestra la relación entre los procesos de TI, los recursos y criterios de información de TI. La P se usa cuando hay una relación primaria y la S cuando solamente existe una relación secundaria. El hecho de que no exista una P ni una S no significa que no exista relación, sólo que es menos importante o marginal. Los valores de importancia se basan en una encuesta y en la opinión de expertos, y se incluyen sólo como una guía. Los usuarios deben considerar qué procesos son importantes dentro de sus propias organizaciones, en cambio cuando se encuentra con (X) significa que los objetivos de control tienen impacto en los recursos, y cuando se encuentra en blanco ( ), es que los objetivos de control no tienen ningún impacto con los recursos.

Para desarrollar la auditoria de la Administración de la Red de Datos WAN de soporte y monitoreo implementada por Telecomunicaciones Full Data Cía. Ltda., se basa sobre el impacto de los Objetivos de Control de COBIT 4.1 sobre los Criterios de Información y los Recursos TI, de esta manera se puede verificar el nivel de madurez auditando la gestión y control de los sistemas de Información y Tecnología, orientando a todos los sectores de una organización, es decir, administradores TI, usuarios y obviamente los auditores involucrados en el proceso, abarcando controles específicos de TI desde una perspectiva de negocios.

[43] COSO (Committee of Sponsoring Organizations)

		Gobierno TI					COSO					Recursos TI de COBIT				Criterios de Información de COBIT						
	IMPORTANCIA	Alineación estratégica	Entrega de valor	Gestión de Riesgos	Gestión de Recursos	Medición del Desempeño	Entorno de Control	Evaluación de riesgos	Actividades de control	Información	Monitoreo	Aplicación	Información	Infraestructura	Personas	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Planear y Organizar																						
PO1 Definir un Plan Estratégico de TI	A	P		S	S			P		S	S	X	X	X	X	P	S					
PO2 Definir la Arquitectura de la Información	B	P	S	P	S				P	P		X	X			S	P	S	P			
PO3 Determinar la Dirección Tecnológica	M	S	S	P	S			S	P	S		X		X		P	P					
PO4 Definir los Procesos, Organización y Relaciones de TI	B	S		P	P		P			S	S				X	P	P					S
PO5 Administrar la Inversión en TI	M	S	P	S		S		S	P			X		X	X	P	P					
PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia	M	P			P		P			P			X		X	P					S	
PO7 Administrar Recursos Humanos de TI	B	P		P	S	S	P			S					X	P	P					
PO8 Administrar la Calidad	M	P	S		S		P		P	S	P	X	X	X	X	P	P		S			S
PO9 Evaluar y Administrar los Riesgos de TI	A	P			P			P				X	X	X	X	S	S	P	P	P	S	S
PO10 Administrar Proyectos	A	P	S	S	S	S	S	S	P		S	X		X	X	P	P					
Adquirir e implementar																						
AI1 Identificar soluciones automatizadas	M	P	P	S	S				P			X		X		P	S					
AI2 Adquirir y mantener software aplicativo	M	P	P		S				P			X				P	P		S			S
AI3 Adquirir y mantener infraestructura tecnológica	B			P					P					X		S	P		S	S		
AI4 Facilitar la operación y el uso	B	S	P	S	S				P	S		X		X	X	P	P		S	S	S	S

AI5 Adquirir recursos de TI	M		S	P					P			X	X	X	X	S	P				S			
AI6 Administrar cambios	A		P	S				S	P		S	X	X	X	X	P	P		P	P		S		
AI7 Instalar y acreditar soluciones y cambios	M	S	P	S	S	S			P	S	S	X	X	X	X	P	S		S	S				
Entregar y Dar Soporte																								
DS1 Definir y administrar los niveles de servicio	M	P	P	P		P	S		P	S	S	X	X	X	X	P	P	S	S	S	S	S		
DS2 Administrar los servicios de terceros	B		P	S	P	S	P	S	P		S	X	X	X	X	P	P	S	S	S	S	S		
DS3 Administrar el desempeño y la capacidad	B	S	S	P	S	S			P		S	X		X		P	P			S				
DS4 Garantizar la continuidad del servicio	M	S	P	S	P	S	S		P	S		X	X	X	X	P	S			P				
DS5 Garantizar la seguridad de los sistemas	A				P				P	S	S	X	X	X	X			P	P	S	S	S		
DS6 Identificar y asignar costos	B		S	P		S			P			X	X	X	X		P					P		
DS7 Educar y entrenar a los usuarios	B	S	P	S	S		P			S					X	P	S							
DS8 Administrar la mesa de servicio y los incidentes	B		P			S	S			P	P	X			X	P	P							
DS9 Administrar la configuración	M		P	P	S				P			X	X	X		P	S			S		S		
DS10 Administrar los problemas	M		P		S	S			P	S	S	X	X	X	X	P	P			S				
DS11 Administrar los datos	A		P	P	P				P				X						P			P		
DS12 Administrar el ambiente físico	B			S	P			S	P					X					P	P				
DS13 Administrar las operaciones	B			P					P	S		X	X	X	X	P	P		S	S				
Monitorear y Evaluar																								
ME1 Monitorear y Evaluar el Desempeño de TI	A	S	S	S	S	P				S	P	X	X	X	X	P	P	S	S	S	S	S		
ME2 Monitorear y Evaluar el Control Interno	M		P		P							X	X	X	X						P	S		
ME3 Garantizar el Cumplimiento Regulatorio	A								P	S	S	X	X	X	X	P	P	S	S	S	S	S		
ME4 Proporcionar Gobierno de TI	A	P	P	P	P	P	P	S		S	P	X	X	X	X	P	P	S	S	S	S	S		

Tabla 4.2 – Mapeo de Procesos de TI[44]

[44] © 2007 IT Governance Institute, COBIT 4.1, Pág 173
Nota: El mapeo COSO está basado sobre el marco original COSO. El mapeo también aplica sobre el ultimo COSO Administración de Riesgos Empresarial – Marco Integrado, que expande sobre los controles internos proporcionando un enfoque más robusto y extensivo sobre el sujeto de la gestión de riesgos de la empresa.

4.4 Determinación de los Procesos COBIT aplicables a la Gestión de Seguridad

A continuación se exponen los objetivos de control por dominios que han sido escogidos para la ejecución del trabajo de auditoría de la gestión de la red WAN.

- PO1. Definir un plan estratégico de TI.
- PO2. Definir la arquitectura de la información.
- PO3. Determinar la dirección tecnológica.
- PO4. Definir procesos, organización y relaciones de TI.
- PO5. Administrar la inversión en TI.
- PO6. Comunicar las aspiraciones y la dirección la dirección de la gerencia.
- PO8. Administrar calidad.
- PO9. Evaluar y administrar riesgos de TI.
- AI1. Identificar soluciones automatizadas.
- AI2. Adquirir y mantener el software aplicativo.
- AI3. Adquirir y mantener la infraestructura tecnológica.
- AI4. Facilitar la operación y el uso.
- AI5. Adquirir recursos de TI.
- DS1. Definir y administrar niveles de servicio.
- DS2. Administrar servicios de terceros.
- DS3. Administrar desempeño y calidad.
- DS4. Garantizar la continuidad del servicio.
- DS5. Garantizar la seguridad de los sistemas.
- DS9. Administrar la configuración.
- DS10. Administrar los problemas.
- DS12. Administrar el ambiente físico.
- DS13. Administrar las operaciones.
- ME1. Monitorear y evaluar el desempeño de TI.
- ME2. Monitorear y evaluar el control interno.
- ME3. Garantizar cumplimiento regulatorio.
- ME4. Proporcionar gobierno de TI.

En la **tabla 4.3,** se muestran los Objetivos de Control seleccionados relacionados con los Criterios de Información y Recursos de Información.

Dominio	Procesos		Criterios de Información de COBIT							Recursos TI de COBIT			
			Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Aplicación	Información	Infraestructura	Personas
PLANIFICAR Y ORGANIZAR	PO1	Definir un plan estratégico de TI.	P	S						X	X	X	X
	PO2	Definir la arquitectura de la información.	S	P	S	P				X	X		
	PO3	Determinar la dirección tecnológica.	P	P						X		X	
	PO4	Definir procesos, organización y relaciones de TI.	P	P					S				X
	PO5	Administrar la inversión en TI.	P	P						X		X	X
	PO6	Comunicar las aspiraciones y la dirección la dirección de la gerencia.	P					S			X		X
	PO8	Administrar calidad.	P	P		S			S	X	X	X	X
	PO9	Evaluar y administrar riesgos de TI.	S	S	P	P	P	S	S	X	X	X	X
ADQUIRIR E IMPLEMENTAR	AI1	Identificar soluciones automatizadas.	P	S						X		X	
	AI2	Adquirir y mantener el software aplicativo.	P	P		S			S	X			
	AI3	Adquirir y mantener la infraestructura tecnológica.	S	P		S	S					X	
	AI4	Facilitar la operación y el uso.	P	P		S	S	S	S	X		X	X
	AI5	Adquirir recursos de TI.	S	P				S		X	X	X	X
ENTREGAR Y DAR SOPORTE	DS1	Definir y administrar niveles de servicio.	P	P	S	S	S	S	S	X	X	X	X
	DS2	Administrar servicios de terceros.	P	P	S	S	S	S	S	X	X	X	X
	DS3	Administrar desempeño y calidad.	P	P			S			X		X	
	DS4	Garantizar la continuidad del servicio.	P	S			P			X	X	X	X
	DS5	Garantizar la seguridad de los sistemas.			P	P	S	S	S	X	X	X	X
	DS9	Administrar la configuración.	P	S			S		S	X	X	X	
	DS10	Administrar los problemas.	P	P			S			X	X	X	X
	DS12	Administrar el ambiente físico.				P	P					X	
	DS13	Administrar las operaciones.	P	P		S	S			X	X	X	X
MONITOREAR Y EVALUAR	ME1	Monitorear y evaluar el desempeño de TI.	P	P	S	S	S	S	S	X	X	X	X
	ME2	Monitorear y evaluar el control interno.						P	S	X	X	X	X
	ME3	Garantizar cumplimiento regulatorio.	P	P	S	S	S	S	S	X	X	X	X
	ME4	Proporcionar gobierno de TI.	P	P	S	S	S	S	S	X	X	X	X

Tabla 4.3 – Objetivos de Control COBIT- Criterios y Recursos TI afectados.

4.4.1 Dominio Planificar y Organizar.

P01 Definir un Plan Estratégico de TI.

La planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. La función de TI y los interesados del negocio son responsables de asegurar que el valor óptimo se consigue desde los proyectos y el portafolio de servicios. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido. La estrategia de negocio y prioridades se reflejarán en portafolios y se ejecutarán por los planes estratégicos de TI, que especifican objetivos concisos, planes de acción y tareas que están comprendidas y aceptadas tanto por el negocio como por TI.[45]

P02. Definir la Arquitectura de la Información.

La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. Este proceso mejora la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias del negocio. Este proceso de TI también es necesario para incrementar la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de la información compartida a lo largo de las aplicaciones y de las entidades.[46]

[45] © 2007 IT Governance Institute, COBIT 4.1, Pág 29
[46] © 2007 IT Governance Institute, COBIT 4.1, Pág 33

P03. Determinar la Dirección Tecnológica.

La función de servicios de información debe determinar la dirección tecnológica para dar soporte al negocio. Esto requiere de la creación de un plan de infraestructura tecnológica y de un comité de arquitectura que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación. El plan se debe actualizar de forma regular y abarca aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias. Esto permite contar con respuestas oportunas a cambios en el ambiente competitivo, economías de escala para consecución de personal de sistemas de información e inversiones, así como una interoperabilidad mejorada de las plataformas y de las aplicaciones.[47]

P04. Definir los Procesos, Organización y Relaciones de TI.

Una organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión. La organización está embebida en un marco de trabajo de procesos de TI que asegure la transparencia y el control, así como el involucramiento de los altos ejecutivos y de la gerencia del negocio. Un comité estratégico debe garantizar la vigilancia del consejo directivo sobre TI, y uno ó más comités de dirección, en los cuales participen tanto el negocio como TI, deben determinar las prioridades de los recursos de TI alineados con las necesidades del negocio. Deben existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas y la segregación de funciones. Para garantizar el soporte oportuno de los requerimientos del negocio, TI se debe involucrar en los procesos importantes de decisión.[48]

[47] © 2007 IT Governance Institute, COBIT 4.1, Pág 37
[48] © 2007 IT Governance Institute, COBIT 4.1, Pág 41

P05. Administrar la Inversión en TI.

Establecer y mantener un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios, prioridades dentro del presupuesto, un proceso presupuestal formal y administración contra ese presupuesto. Los interesados (stakeholders) son consultados para identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, y tomar medidas correctivas según sean necesarias. El proceso fomenta la asociación entre TI y los interesados del negocio, facilita el uso efectivo y eficiente de recursos de TI, y brinda transparencia y responsabilidad dentro del costo total de la propiedad, la materialización de los beneficios del negocio y el retorno sobre las inversiones en TI.[49]

P06. Comunicar las Aspiraciones y la Dirección de la Gerencia.

La dirección debe elaborar un marco de trabajo de control empresarial para TI, y definir y comunicar las políticas. Un programa de comunicación continua se debe implementar para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc., aprobados y apoyados por la dirección. La comunicación apoya el logro de los objetivos de TI y asegura la concienciación y el entendimiento de los riesgos de negocio y de TI. El proceso debe garantizar el cumplimiento de las leyes y reglamentos relevantes.[50]

P08. Administrar la Calidad.

Se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares probados de desarrollo y de adquisición. Esto se facilita por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad, proporcionando requerimientos, procedimientos y políticas claras de calidad. Los requerimientos de calidad se deben manifestar y documentar con indicadores cuantificables y alcanzables. La mejora continua se logra por medio del constante monitoreo, corrección de desviaciones y la comunicación de los resultados a los interesados. La administración de calidad es

[49] © 2007 IT Governance Institute, COBIT 4.1, Pág 47
[50] © 2007 IT Governance Institute, COBIT 4.1, Pág 51

esencial para garantizar que TI está dando valor al negocio, mejora continua y transparencia para los interesados.[51]

P09. Evaluar y Administrar los Riesgos de TI.

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los Interesados (Stakeholders) y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia.[52]

4.4.2 Dominio Adquirir e Implementar.

AI1. Identificar Soluciones Automatizadas.

La necesidad de una nueva aplicación o función requiere de análisis antes de la compra o desarrollo para garantizar que los requisitos del negocio se satisfacen con un enfoque efectivo y eficiente. Este proceso cubre la definición de las necesidades, considera las fuentes alternativas, realiza una revisión de la factibilidad tecnológica y económica, ejecuta un análisis de riesgo y de

costo-beneficio y concluye con una decisión final de “desarrollar” o “comprar”. Todos estos pasos permiten a las organizaciones minimizar el costo para Adquirir e Implementar soluciones, mientras que al mismo tiempo facilitan el logro de los objetivos del negocio.[53]

[51] © 2007 IT Governance Institute, COBIT 4.1, Pág 59
[52] © 2007 IT Governance Institute, COBIT 4.1, Pág 63
[53] © 2007 IT Governance Institute, COBIT 4.1, Pág 73

AI2. Adquirir y Mantener Software Aplicativo.

Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y la configuración en sí de acuerdo a los estándares. Esto permite a las organizaciones apoyar la operatividad del negocio de forma apropiada con las aplicaciones automatizadas correctas.[54]

AI3. Adquirir y Mantener Infraestructura Tecnológica.

Las organizaciones deben contar con procesos para adquirir, Implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.[55]

AI4. Facilitar la Operación y el Uso.

El conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar el uso y la operación correctos de las aplicaciones y la infraestructura.[56]

AI5. Adquirir Recursos de TI.

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

[54] © 2007 IT Governance Institute, COBIT 4.1, Pág 77
[55] © 2007 IT Governance Institute, COBIT 4.1, Pág 81
[56] © 2007 IT Governance Institute, COBIT 4.1, Pág 85

adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable.[57]

4.4.3 Dominio Entrega y Soporte.

DS1. Definir y Administrar los Niveles de Servicio.

Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los Interesados (Stakeholders) sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.[58]

DS2. Administrar los Servicios de Terceros.

La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.[59]

DS3. Administrar el Desempeño y la Capacidad.

La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI. Este proceso incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso brinda la seguridad de que los

[57] © 2007 IT Governance Institute, COBIT 4.1, Pág 89
[58] © 2007 IT Governance Institute, COBIT 4.1, Pág 101
[59] © 2007 IT Governance Institute, COBIT 4.1, Pág 105

recursos de información que soportan los requerimientos del negocio están disponibles de manera continua.[60]

DS4. Garantizar la Continuidad del Servicio.

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.[61]

DS5. Garantizar la Seguridad de los Sistemas.

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.[62]

DS9. Administrar la Configuración.

Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conforme se necesite. Una efectiva administración de la configuración facilita una mayor

[60] © 2007 IT Governance Institute, COBIT 4.1, Pág 109
[61] © 2007 IT Governance Institute, COBIT 4.1, Pág 113
[62] © 2007 IT Governance Institute, COBIT 4.1, Pág 117

disponibilidad, minimiza los problemas de producción y resuelve los problemas más rápido.[63]

DS10. Administración de Problemas.

Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de problemas mejora los niveles de servicio, reduce costos y mejora la conveniencia y satisfacción del usuario.[64]

DS12. Administración del Ambiente Físico.

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.[65]

DS13. Administración de Operaciones.

Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la

[63] © 2007 IT Governance Institute, COBIT 4.1, Pág 133
[64] © 2007 IT Governance Institute, COBIT 4.1, Pág 137
[65] © 2007 IT Governance Institute, COBIT 4.1, Pág 145

integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI.[66]

4.4.4 Dominio Monitorear y Evaluar.

ME1. Monitorear y Evaluar el Desempeño de TI.

Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas.[67]

ME2. Monitorear y Evaluar el Control Interno.

Establecer un programa de control interno efectivo para TI requiere un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.[68]

ME3. Garantizar el Cumplimiento con Requerimientos Externos.

Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento, optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio.[69]

---

[66] © 2007 IT Governance Institute, COBIT 4.1, Pág 149
[67] © 2007 IT Governance Institute, COBIT 4.1, Pág 153
[68] © 2007 IT Governance Institute, COBIT 4.1, Pág 157
[69] © 2007 IT Governance Institute, COBIT 4.1, Pág 161

ME4 Proporcionar Gobierno de TI

El establecimiento de un marco de trabajo de gobierno efectivo, incluye la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales para garantizar así que las inversiones empresariales en TI estén alineadas y de acuerdo con las estrategias y objetivos empresariales.[70]

4.5 Herramientas Aplicables al Desarrollo de la Auditoría.

Para desarrollar la auditoría primero se obtuvo toda la información requerida y se recolectó toda la documentación disponible, además se tomó como guías los siguientes documentos:

COBIT 4.1

ITGI diseñó y creó esta publicación titulada COBIT ® 4.1, principalmente como recurso educativo para los directores de informática CIOs, altos directivos de TI, gestión y control de los profesionales. El propietario no pretende que el uso de cualquiera de los trabajos asegure un resultado exitoso. Para determinar la conveniencia de cualquier información, procedimiento o prueba, los CIO, la alta gerencia, TI profesionales de la gestión y el control deben aplicar su propio juicio profesional a las circunstancias específicas presentadas por los sistemas o el medio ambiente de TI.

MAGERIT v3

La Metodología MAGERIT, servirá como método formal para el análisis de riesgos e identificación de amenazas y vulnerabilidades que existen en la Administración de la Red de Datos WAN.

[70] © 2007 IT Governance Institute, COBIT 4.1, Pág 165

4.6 Plan de Auditoría

Las principales actividades para desarrollar la Auditoría a la Administración de la Red de Datos WAN:

1. Descripción de la Situación Actual de la Empresa
    - Organización Administrativa
    - Infraestructura Actual de la Red WAN de Soporte y Monitoreo
    - Evaluación de Riesgos de la Gestión de la Red WAN de Soporte y Monitoreo.
2. Elaboración del Plan de Auditoría
    - Definición del alcance de la Auditoría
    - Selección de los Procesos COBIT aplicables a la Auditoría
3. Ejecutar el Plan de Auditoría
    - Elaborar los Modelos de Madurez de los procesos
    - Calcular el impacto de los Criterios de Información.
    - Resumen de Análisis por Dominio
4. Elaboración del Informe Técnico
5. Elaboración del Informe Ejecutivo

Las personas responsables de la realización de la auditoría son:

Carlos Andrés Alvear Niacata

Leonardo Patricio Yánez Cáceres.

CAPÍTULO 5

EJECUCIÓN DEL PLAN DE AUDITORÍA [1]

Todos los conceptos y definiciones de los niveles de madurez de cada uno de los procesos se obtienen del Marco de Trabajo COBIT 4.1.[71]

5.1 Procesos del Dominio Planear y Organizar

DOMINIO: PLANEAR Y ORGANIZAR				
PO1: Definir el Plan Estratégico de Tecnología de la Información				
NIVEL DE MADUREZ		cumple	no cumple	Observaciones
Nivel 0	No se lleva a cabo la planeación estratégica de TI. No existe conciencia por parte de la gerencia de que la planeación estratégica de TI es requerida para dar soporte a las metas del negocio.		√	**GRADO DE MADUREZ** El proceso Definir el Plan Estratégico de Tecnología Información se encuentra en nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** - La existencia de un plan estratégico de TI correctamente elaborado. - Realizar planes a largo plazo de TI, haciendo solo actualizaciones debido a los avances tecnológicos.
Nivel 1	La planeación estratégica de TI se discute de forma ocasional en las reuniones de la gerencia de TI. La alineación de los requerimientos de las aplicaciones y tecnología del negocio se lleva a cabo de modo reactivo en lugar de hacerlo por medio de una estrategia organizacional. La posición de riesgo estratégico se identifica de manera informal.	√		
Nivel 2	La actualización de los planes de TI ocurre como respuesta a las solicitudes de la dirección. Las decisiones estratégicas se toman proyecto por proyecto, sin ser consistentes con una estrategia global de la organización. Los riesgos y beneficios al usuario, resultado de decisiones estratégicas importantes se reconocen de forma intuitiva.	√		
Nivel 3	TI. La planeación estratégica de TI sigue un enfoque estructurado, el cual se documenta y se da a conocer a todo el equipo. El proceso de planeación de TI es razonablemente sólido y garantiza que es factible realizar una planeación adecuada. Sin embargo, se otorga discrecionalidad a gerentes individuales específicos con respecto a la implantación del proceso, y no existen procedimientos para analizar el proceso. La estrategia general de TI incluye una definición consistente de los riesgos que la organización está dispuesta a tomar como innovador o como seguidor.		√	

[71] © 2007 IT Governance Institute, COBIT 4.1, Págs 29 - 168

Nivel 4	La dirección puede monitorear el proceso estratégico de TI, tomar decisiones informadas con base en el plan y medir su efectividad. La estrategia de TI y la estrategia organizacional se vuelven cada vez más coordinadas al abordar procesos de negocio y capacidades de valor agregado y al apalancar el uso de aplicaciones y tecnologías por medio de la re-ingeniería de procesos de negocio. Existen procesos bien definidos para determinar e uso de recursos internos y externos requeridos en el desarrollo y las operaciones de los sistemas.		√	
Nivel 5	La planeación estratégica de TI es un proceso documentado y vivo, que cada vez más se toma en cuenta en el establecimiento de las metas del negocio y da como resultado un valor observable de negocios por medio de las inversiones en TI. Se desarrollan planes realistas a largo plazo de TI y se actualizan de manera constante para reflejar los cambiantes avances tecnológicos y el progreso relacionado al negocio. Se realizan evaluaciones por comparación contra normas industriales bien entendidas y confiables y se integran con el proceso de formulación de la estrategia.		√	

RECOMENDACIONES

Para el proceso PO1 de COBIT estable los siguientes objetivos de control:
- Planes a largo plazo de TI.
- Tomar decisiones estratégicas.
- Definir los recursos internos y externos necesarios.

Para pasar al nivel de madurez 3, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Realizar una evaluación de los planes existentes, así como de los sistemas de información y su impacto de los objetivos del Servicio al Cliente.

Largo Plazo:

- Crear planes tácticos de TI a futuro en la Administración y soporte de la red WAN, estos planes deben ser bien detallados para realizar la definición de planes proyectados.

DOMINIO: PLANEAR Y ORGANIZAR				
PO2: Definir la Arquitectura de la Información				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	No existe conciencia de la importancia de la arquitectura de la información para la organización. El conocimiento, la experiencia y las responsabilidades necesarias para desarrollar esta arquitectura no existen en la organización.		√	**GRADO DE MADUREZ** El proceso Definir la Arquitectura de la Información se encuentra en nivel de madurez 2.

Nivel 1	La gerencia reconoce la necesidad de una arquitectura de información. Las definiciones abarcan datos en lugar de información, y son impulsadas por ofertas de proveedores de software aplicativo. Existe una comunicación esporádica e inconsistente de la necesidad de una arquitectura de información.	√		**OBJETIVOS NO CUMPLIDOS** - Resolver las necesidades futuras del negocio realizando el proceso de la arquitectura de la información. - Aprovechar las habilidades personales para la construcción de la arquitectura de la información.
Nivel 2	Surge un proceso de arquitectura de información y existen procedimientos similares, aunque intuitivos e informales, que se siguen por distintos individuos dentro de la organización. Las personas obtienen sus habilidades al construir la arquitectura de información por medio de experiencia práctica y la aplicación repetida de técnicas.	√		
Nivel 3	La importancia de la arquitectura de la información se entiende y se acepta, y la responsabilidad de su aplicación se asigna y se comunica de forma clara. Se han desarrollado políticas básicas de arquitectura de información, incluyendo algunos requerimientos estratégicos, aunque el cumplimiento de políticas, estándares y herramientas no se refuerza de manera consistente. Existe una función de administración de datos definida formalmente, que establece estándares para toda la organización, y empieza a reportar sobre la aplicación y uso de la arquitectura de la información.		√	
Nivel 4	Se da soporte completo al desarrollo e implantación de la arquitectura de información por medio de métodos y técnicas formales. La responsabilidad sobre el desempeño del proceso de desarrollo de la arquitectura se refuerza y se mide el éxito de la arquitectura de información. Las herramientas automatizadas de soporte están ampliamente generalizadas, pero todavía no están integradas. Se han identificado métricas básicas y existe un sistema de medición. El proceso de definición de la arquitectura de información es proactivo y se enfoca en resolver necesidades futuras del negocio.		√	
Nivel 5	El valor de la arquitectura de la información para el negocio se enfatiza de forma continua. El personal de TI cuenta con la experiencia y las habilidades necesarias para desarrollar y dar mantenimiento a una arquitectura de información robusta y sensible que refleje todos los requerimientos del negocio. La información provista por la arquitectura se aplica de modo consistente y amplio. Se hace un uso amplio de las mejores prácticas de la industria en el desarrollo y mantenimiento de la arquitectura de información incluyendo un proceso de mejora continua.		√	

RECOMENDACIONES
Para el proceso PO2 de COBIT estable los siguientes objetivos de control:
- Definir claramente la definición del proceso de la arquitectura de la información.
- Definir los recursos internos y externos necesarios.
- Desarrollar y mantener la arquitectura de la información.

Para pasar al nivel de madurez 3, se debe adoptar las siguientes estrategias:
Corto Plazo:
- Establecer y mantener un modelo de arquitectura de la información para facilitar el desarrollo de aplicaciones y actividades de soporte a la toma de decisiones, este modelo será útil para la creación, uso y compartición óptimas de la información vital.

Largo Plazo:
- Definir e implementar procedimientos para brindar integridad y consistencia de todos los datos que se encuentran almacenado en forma digital, como bases de datos, archivos.

DOMINIO: PLANEAR Y ORGANIZAR				
PO3: Determinar la Dirección Tecnológica.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	No existe conciencia sobre la importancia de la planeación de la infraestructura tecnológica para la entidad. El conocimiento y la experiencia necesarios para desarrollar dicho plan de infraestructura tecnológica no existen.		√	**GRADO DE MADUREZ** El proceso Determinar la Dirección Tecnológica se encuentra en nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** - Desarrollar las habilidades para la elaboración del plan de la infraestructura tecnológica. - Elaborar correctamente plan de infraestructura tecnológica de acuerdo a la necesidad de la empresa.
Nivel 1	La gerencia reconoce la necesidad de planear la infraestructura tecnológica. El desarrollo de componentes tecnológicos y la implementación de tecnologías emergentes son ad hoc y aisladas. Existe un enfoque reactivo y con foco operativo hacia la planeación de la infraestructura.	√		
Nivel 2	La planeación es táctica y se enfoca en generar soluciones técnicas a problemas técnicos, en lugar de usar la tecnología para satisfacer las necesidades del negocio. La evaluación de los cambios tecnológicos se delega a individuos que siguen procesos intuitivos, aunque similares.	√		
Nivel 3	La gerencia está consciente de la importancia del plan de infraestructura tecnológica. El proceso para el plan de infraestructura tecnológica es razonablemente sólido y está alineado con el plan estratégico de TI. Existe un plan de infraestructura tecnológica definido, documentado y bien difundido, aunque se aplica de forma inconsistente. La orientación de la infraestructura tecnológica incluye el entendimiento de dónde la empresa desea ser líder y dónde desea rezagarse respecto al uso de tecnología, con base en los riesgos y en la alineación con la estrategia organizacional.		√	

Nivel 4	La dirección garantiza el desarrollo del plan de infraestructura tecnológica. El equipo de TI cuenta con la experiencia y las habilidades necesarias para desarrollar un plan de infraestructura tecnológica. El impacto potencial de las tecnologías cambiantes y emergentes se toma en cuenta. La dirección puede identificar las desviaciones respecto al plan y anticipar los problemas. La responsabilidad del desarrollo y mantenimiento del plan de infraestructura tecnológica ha sido asignada. El proceso para desarrollar el plan de infraestructura tecnológica es sofisticado y sensible a los cambios. Se han incluido buenas prácticas internas en el proceso. Los planes de migración para la introducción de nuevas tecnologías están definidos.		**√**	
Nivel 5	Existe una función de investigación que revisa las tecnologías emergentes y evolutivas y para evaluar la organización por comparación contra las normas industriales. La dirección del plan de infraestructura tecnológica está impulsada por los estándares y avances industriales e internacionales, en lugar de estar orientada por los proveedores de tecnología. El impacto potencial de los cambios tecnológicos sobre el negocio se revisa al nivel de la alta dirección. Existe un proceso continuo y reforzado para mejorar el plan de infraestructura tecnológica.		**√**	

RECOMENDACIONES

Para el proceso PO3 de COBIT estable los siguientes objetivos de control:
- Desarrollar un plan adecuado de infraestructura tecnológica.
- Promover la orientación de la infraestructura tecnológica con los proveedores.
- Asignar los cambios tecnológicos a personas que tienen la debida experiencia.

Para pasar al nivel de madurez 3. se debe adoptar las siguientes estrategias:

Corto Plazo:

- Analizar las tecnologías existentes y emergentes, para determinar cuál dirección tecnológica es apropiada para cumplir con las estrategias de TI, y la arquitectura de sistemas del negocio.

Largo Plazo:

- Implementar un proceso de monitoreo de tendencias tecnológicas, estableciendo un foro para brindar mejor dirección tecnológica.

DOMINIO: PLANEAR Y ORGANIZAR				
PO4: Definir Procesos, Organización y Relaciones de TI.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	La organización de TI no está establecida de forma efectiva para enfocarse en el logro de los objetivos del negocio.		**√**	**GRADO DE MADUREZ** El proceso Definir Procesos, Organización y Relaciones de TI se encuentran en el

Nivel 1	Las actividades y funciones de TI son reactivas y se implantan de forma inconsistente. TI se involucra en los proyectos solamente en las etapas finales. La función de TI se considera como una función de soporte, sin una perspectiva organizacional general. Existe un entendimiento explícito de la necesidad de una organización.	√		nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** - Establecer las relaciones con terceros para TI. - Satisfacer los requerimientos del negocio para tener una correcta alineación.
Nivel 2	La función de TI está organizada para responder de forma táctica aunque de forma inconsistente, a las necesidades de los clientes y a las relaciones con los proveedores. La necesidad de contar con una organización estructurada y una administración de proveedores se comunica, pero las decisiones todavía dependen del conocimiento y habilidades de individuos clave.	√		
Nivel 3	Existen roles y responsabilidades definidos para la organización de TI y para terceros. La organización de TI se desarrolla, documenta, comunica y se alinea con la estrategia de TI. Se define el ambiente de control interno. Se formulan las relaciones con terceros, incluyendo los comités de dirección, auditoría interna y administración de proveedores. La organización de TI está funcionalmente completa. Existen definiciones de las funciones a ser realizadas por parte del personal de TI y las que deben realizar los usuarios.		√	
Nivel 4	La organización de TI responde de forma proactiva al cambio e incluye todos los roles necesarios para satisfacer los requerimientos del negocio. La administración, la propiedad de procesos, la delegación y la responsabilidad de TI están definidas y balanceadas. Se han aplicado buenas prácticas internas en la organización de las funciones de TI. La gerencia de TI cuenta con la experiencia y habilidades apropiadas para definir, implementar y monitorear la organización deseada y las relaciones. Las métricas medibles para dar soporte a los objetivos del negocio y los factores críticos de éxito definidos por el usuario siguen un estándar. Existen inventarios de habilidades para apoyar al personal de los proyectos y el desarrollo profesional.		√	
Nivel 5	La estructura organizacional de TI es flexible y adaptable. Se ponen en funcionamiento las mejores prácticas de la industria. Existe un uso amplio de la tecnología para monitorear el desempeño de la organización y de los procesos de TI. La tecnología se aprovecha para apoyar la complejidad y distribución geográfica de la organización. Un proceso de mejora continua existe y está implantado.		√	

RECOMENDACIONES

Para el proceso PO4 de COBIT estable los siguientes objetivos de control:

- Tener flexibilidad para adoptar la estructura organizacional de TI en la empresa.
- Responder inmediatamente de forma actica los requerimientos del negocio.
- Realizar auditoría interna para formular relaciones con terceros.

Para pasar al nivel de madurez 3, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Realizar una capacitación y evaluación permanente al personal, para asignar correctamente las funciones existentes.

Largo Plazo:

- Supervisar las funciones de TI mediante metodologías existentes como ITIL o la ISO 27000 para garantizar que los roles y responsabilidades se ejerzan correctamente.

DOMINIO: PLANEAR Y ORGANIZAR				
PO5: Administrar la Inversión en TI.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	No existe conciencia de la importancia de la selección y presupuesto de las inversiones en TI. No existe seguimiento o monitoreo de las inversiones y gastos de TI.		√	**GRADO DE MADUREZ** El proceso Administrar la Inversión en TI se encuentra en nivel de madurez 3. **OBJETIVOS NO CUMPLIDOS** - Determinar correctamente las relaciones de terceros con la empresa. - Identificar estándares de inversión para garantizar el funcionamiento de TI.
Nivel 1	La organización reconoce la necesidad de administrar la inversión en TI, aunque esta necesidad se comunica de manera inconsistente. La asignación de responsabilidades de selección de inversiones en TI y de desarrollo de presupuestos se hace de una forma ad hoc. Existen implantaciones aisladas de selección y presupuesto de inversiones en TI, con documentación informal.		√	
Nivel 2	Existe un entendimiento implícito de la necesidad de seleccionar y presupuestar las inversiones en TI. La necesidad de un proceso de selección y presupuesto se comunica. El cumplimiento depende de la iniciativa de individuos dentro de la organización. Surgen técnicas comunes para desarrollar componentes del presupuesto de TI. Se toman decisiones presupuestales reactivas y tácticas.	√		
Nivel 3	Las políticas y los procesos para inversiones y presupuestos están definidas, documentadas y comunicadas y cubren temas clave de negocio y de tecnología. El presupuesto de TI está alineado con los planes estratégicos de TI y con los planes del negocio. Los procesos de selección de inversiones en TI y de presupuestos están formalizados, documentados y comunicados. Surge el entrenamiento formal aunque todavía se basa de modo principal en iniciativas individuales. Ocurre la aprobación formal de la selección de inversiones en TI y presupuestos.	√		

Nivel 4	La responsabilidad y la rendición de cuentas por la selección y presupuestos de inversiones se asignan a un individuo específico. Las diferencias en el presupuesto se identifican y se resuelven. Se realizan análisis formales de costos que cubren los costos directos e indirectos de las operaciones existentes, así como propuestas de inversiones, considerando todos los costos a lo largo del ciclo completo de vida. Se usa un proceso de presupuestos proactivo y estándar. El impacto en los costos operativos y de desarrollo debidos a cambios en hardware y software, hasta cambios en integración de sistemas y recursos humanos de TI, se reconoce en los planes de inversión.		**√**	
Nivel 5	Se utilizan las buenas prácticas de la industria para evaluar los costos por comparación e identificar la efectividad de las inversiones. Se utiliza el análisis de los avances tecnológicos en el proceso de selección y presupuesto de inversiones. El proceso de administración de inversiones se mejora de forma continua con base en las lecciones aprendidas provenientes del análisis del desempeño real de las inversiones. Las decisiones de inversiones incluyen las tendencias de mejora de precio/desempeño. Existe la identificación proactiva de varianzas. Se incluye un análisis de los costos y beneficios a largo plazo del ciclo de vida total en la toma de decisiones de inversión.		**√**	

RECOMENDACIONES

Para el proceso PO5 de COBIT estable los siguientes objetivos de control:

- Reconocer la necesidad de perfeccionar la forma de administrar la inversión en TI.
- Utilizar las mejores prácticas para la evaluación de costos de inversión.
- Documentar adecuadamente y formalizar el presupuesto en TI.

Para pasar al nivel de madurez 4, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Realizar un análisis de costos y beneficios a mediano y largo plazo para determinar el ciclo de vida de los Recursos de TI.

Largo Plazo:

- Mejorar continuamente la administración de inversiones en base a estándares y lecciones aprendidas del análisis del desempeño de inversiones.

DOMINIO: PLANEAR Y ORGANIZAR				
PO6: Comunicar las Aspiraciones y la Dirección a la Gerencia.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	La gerencia no ha establecido un ambiente positivo de control de información. No hay reconocimiento de la necesidad de establecer un conjunto de políticas, procedimientos, estándares y procesos de cumplimiento.		**√**	**GRADO DE MADUREZ** El proceso Comunicar las Aspiraciones y la Dirección a la Gerencia se encuentra en

Nivel 1	La gerencia es reactiva al resolver los requerimientos del ambiente de control de información. Las políticas, procedimientos y estándares se elaboran y comunican de forma ad hoc de acuerdo a los temas. Los procesos de elaboración, comunicación y cumplimiento son informales e inconsistentes.	√		nivel de madurez 1. **OBJETIVOS NO CUMPLIDOS** - Elaborar un ambiente completo de administración de calidad y control de TI. - Adoptar las mejores prácticas para el sector al que pertenece la empresa.
Nivel 2	La gerencia tiene un entendimiento implícito de las necesidades y de los requerimientos de un ambiente de control de información efectivo, aunque las prácticas son en su mayoría informales. La gerencia ha comunicado la necesidad de políticas, procedimientos y estándares de control, pero la elaboración se delega a la discreción de gerentes y áreas de negocio individuales. La calidad se reconoce como una filosofía deseable a seguir, pero las prácticas se dejan a discreción de gerentes individuales.		√	
Nivel 3	La gerencia ha elaborado, documentado y comunicado un ambiente completo de administración de calidad y control de la información, que incluye un marco para las políticas, procedimientos y estándares. El proceso de elaboración de políticas es estructurado, mantenido y conocido por el personal, y las políticas, procedimientos y estándares existentes son razonablemente sólidos y cubren temas clave. La gerencia ha reconocido la importancia de la conciencia de la seguridad de TI y ha iniciado programas de concienciación. El entrenamiento formal está disponible para apoyar al ambiente de control de información, aunque no se aplica de forma rigurosa.		√	
Nivel 4	La gerencia asume la responsabilidad de comunicar las políticas de control interno y delega la responsabilidad y asigna suficientes recursos para mantener el ambiente en línea con los cambios significativos. Se ha establecido un ambiente de control de información positivo y proactivo. Se ha establecido un juego completo de políticas, procedimientos y estándares, los cuales se mantienen y comunican, y forman un componente de buenas prácticas internas.		√	
Nivel 5	El ambiente de control de la información está alineado con el marco administrativo estratégico y con la visión, y con frecuencia se revisa, actualiza y mejora. Se asignan expertos internos y externos para garantizar que se adoptan las mejores prácticas de la industria, con respecto a las guías de control y a las técnicas de comunicación. El monitoreo, la auto-evaluación y las verificaciones de cumplimiento están extendidas en la organización. La tecnología se usa para mantener bases de conocimiento de políticas y de concienciación y para optimizar la comunicación, usando herramientas de automatización de oficina y de entrenamiento basado en computadora.		√	

RECOMENDACIONES
Para el proceso PO6 de COBIT estable los siguientes objetivos de control:
- Estructurar correctamente las políticas.
- La Gerencia debe comunicar políticas de control interno y delegar responsabilidades.

Para pasar al nivel de madurez 2, se debe adoptar las siguientes estrategias:
Corto Plazo:
- Comunicar la necesidad de un estándar de políticas y procedimientos de control.

Largo Plazo:
- Elaborar y documentar las políticas de control para garantizar la calidad y control de la Información.

DOMINIO: PLANEAR Y ORGANIZAR				
PO8: Administrar la Calidad.				
NIVEL DE MADUREZ		cumple	no cumple	Observaciones
Nivel 0	La organización carece de un sistema de un proceso de planeación de QMS[72] y de una metodología de ciclo de vida de desarrollo de sistemas. La alta dirección y el equipo de TI no reconocen que un programa de calidad es necesario. Nunca se revisa la calidad de los proyectos y las operaciones.	√		**GRADO DE MADUREZ** El proceso Administrar la Calidad se encuentra en un nivel de madurez 1. **OBJETIVOS NO CUMPLIDOS** - El QMS es entendido y utilizado correctamente para la planeación de controles de calidad. -Realizar una comparación externa de acuerdo a estándares establecidos.
Nivel 1	Existe conciencia por parte de la dirección de la necesidad de un QMS. El QMS es impulsado por individuos cuando éste ocurre. La dirección realiza juicios informales sobre la calidad.	√		
Nivel 2	Se establece un programa para definir y monitorear las actividades de QMS dentro de TI. Las actividades de QMS que ocurren están enfocadas en iniciativas orientadas a procesos y proyectos, no a procesos de toda la organización.		√	
Nivel 3	La dirección ha comunicado un proceso definido de QMS e involucra a TI y a la gerencia del usuario final. Un programa de educación y entrenamiento está surgiendo para instruir a todos los niveles de la organización sobre el tema de la calidad. Se han definido expectativas básicas de calidad y éstas se comparten dentro de los proyectos y la organización de TI. Están surgiendo herramientas y prácticas comunes para administrar la calidad.		√	
Nivel 4	El QMS está incluido en todos los procesos, incluyendo aquellos que dependen de terceros. Se está estableciendo una base de conocimiento estandarizada para las métricas de calidad. Se usan métodos de análisis de costo/beneficio para justificar las iniciativas de QMS, Surge el uso de benchmarking contra la industria y con los competidores. Se ha institucionalizado un programa de educación y entrenamiento para educar a todos los niveles de la organización en el		√	

[72] *Quality Management Systems*

	tema de la calidad. Se están estandarizando herramientas y prácticas y el análisis de causas raíz se aplica de forma periódica. Se conducen encuestas de satisfacción de calidad de manera consistente.			
Nivel 5	El QMS está integrado y se aplica a todas las actividades de TI. Los procesos de QMS son flexibles y adaptables a los cambios en el ambiente de TI. Se mejora la base de conocimientos para métricas de calidad con las mejores prácticas externas. Se realiza benchmarking contra estándares externos rutinariamente. Las encuestas de satisfacción de la calidad constituyen un proceso constante y conducen al análisis de causas raíz y a medidas de mejora.		**√**	

RECOMENDACIONES

Para el proceso PO1 de COBIT estable los siguientes objetivos de control:

- Planes a largo plazo de TI.
- Tomar decisiones estratégicas.
- Definir los recursos internos y externos necesarios.

Para pasar al nivel de madurez 2, se debe adoptar las siguientes estrategias:

En el Corto Plazo:

- Realizar una evaluación de los planes existentes, así como de los sistemas de información y su impacto de los objetivos del Servicio al Cliente.

En el Largo Plazo:

- Del plan estratégico de TI, crear planes tácticos a futuro debidamente detallados para realizar la definición de proyectos establecidos.

DOMINIO: PLANEAR Y ORGANIZAR				
PO9: Evaluar y Administrar Riesgos de TI.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	La evaluación de riesgos para los procesos y las decisiones de negocio no ocurre. La organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI.	**√**		**GRADO DE MADUREZ** El proceso Evaluar y Administrar Riesgos de TI se encuentra en nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** - Realizar constantemente evaluación e identificación de riesgos para administrar adecuadamente. - Aplicar mejores prácticas en toda la organización para alinear TI con el negocio.
Nivel 1	Los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine cada proyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos pero se asignan rara vez a gerentes específicos. Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto. Los riesgos relativos a TI que afectan las operaciones del día a día, son rara vez discutidas en reuniones gerenciales.	**√**		

Nivel 2	Existe un enfoque de evaluación de riesgos en desarrollo y se implementa a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están empezando a ser implementados donde se identifican riesgos.	√	
Nivel 3	Una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos. La administración de riesgos sigue un proceso definido, el cual está documentado. El entrenamiento sobre administración de riesgos está disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se deja a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves para el negocio sean identificados.		√
Nivel 4	La evaluación y administración de riesgos son procedimientos estándar. Las excepciones al proceso de administración de riesgos se reportan a la gerencia de TI. La administración de riesgos de TI es una responsabilidad de alto nivel. Los riesgos se evalúan y se mitigan a nivel de proyecto individual y también por lo regular se hace con respecto a la operación global de TI. La gerencia recibe notificación sobre los cambios en el ambiente de negocios y de TI que pudieran afectar de manera significativa los escenarios de riesgo relacionados con TI.		√
Nivel 5	La administración de riesgos ha evolucionado al nivel en que un proceso estructurado está implantado en toda la organización y es bien administrado. Las buenas prácticas se aplican en toda la organización. La captura, análisis y reporte de los datos de administración de riesgos están altamente automatizados. La orientación se toma de los líderes en el campo y la organización de TI participa en grupos de interés para intercambiar experiencias. La administración de riesgos está altamente integrada en todo el negocio y en las operaciones de TI, está bien aceptada, y abarca a los usuarios de servicios de TI.		√

RECOMENDACIONES

Para el proceso PO9 de COBIT estable los siguientes objetivos de control:

- Administrar los riesgos en un alto nivel en respuesta a los problemas.
- Definir un proceso de evaluación de riesgos previamente documentado.

–Definir procesos para mitigar los riesgos.

Para pasar al nivel de madurez 3, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Definir la evaluación y administración de riesgos como procedimientos estándares, reportando a Gerencia.

Largo Plazo:

- Automatizar la captura, análisis y reportes de la administración de riesgos para evaluar estrategias de mitigación de forma continua.

5.2 Procesos del Dominio Adquirir e Implementar

<table>
<tr><th colspan="5">DOMINIO: ADQUIRIR E IMPLEMENTAR</th></tr>
<tr><th colspan="5">AI1: Identificar Soluciones Automatizadas.</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>cumple</th><th>no cumple</th><th>Observaciones</th></tr>
<tr><td>Nivel 0</td><td>Las técnicas de administración de proyectos no se usan y la organización no toma en cuenta los impactos al negocio asociados con la mala administración de los proyectos y con las fallas de desarrollo en el proyecto.</td><td>√</td><td></td><td rowspan="6">GRADO DE MADUREZ

El proceso Identificar Soluciones Automatizadas se encuentra en nivel de madurez 1.

OBJETIVOS NO CUMPLIDOS

- Determinar los procesos para la solución de TI, de acuerdo al requerimiento del negocio.

- Documentar correctamente los proyectos realizados.</td></tr>
<tr><td>Nivel 1</td><td>El uso de técnicas y enfoques de administración de proyectos dentro de TI es una decisión individual que se deja a los gerentes de TI.
Existe una carencia de compromiso por parte de la gerencia hacia la propiedad de proyectos y hacia la administración de proyectos.
Las decisiones críticas sobre administración de proyectos se realizan sin la intervención de la gerencia usuaria ni del cliente. Hay poca
o nula participación del cliente y del usuario para definir los proyectos de TI.</td><td>√</td><td></td></tr>
<tr><td>Nivel 2</td><td>La alta dirección ha obtenido y comunicado la conciencia de la necesidad de la administración de los proyectos de TI. La organización está en proceso de desarrollar y utilizar algunas técnicas y métodos proyecto por proyecto. Los proyectos de TI han definido objetivos técnicos y de negocio de manera informal. Hay participación limitada de los interesados en la administración de los proyectos de TI. Las directrices iniciales se han elaborado para muchos aspectos de la administración de proyectos.</td><td></td><td>√</td></tr>
<tr><td>Nivel 3</td><td>El proceso y la metodología de administración de proyectos de TI han sido establecidos y comunicados. Los proyectos de TI se definen con los objetivos técnicos y de negocio adecuados. La alta dirección del negocio y de TI, empiezan a comprometerse y a participar en la administración de los proyectos de TI. Se ha establecido una oficina de administración de proyectos dentro de TI, con roles y responsabilidades iniciales definidas. Los proyectos de TI se monitorean, con puntos clave, cronogramas y mediciones de presupuesto y desempeño definidos y actualizados. Existe entrenamiento para la administración de proyectos. El entrenamiento en administración de proyectos es un resultado principalmente de las iniciativas individuales del equipo.</td><td></td><td>√</td></tr>
<tr><td>Nivel 4</td><td>La gerencia requiere que se revisen métricas y lecciones aprendidas estandarizadas y formales después de terminar cada proyecto.
La administración de proyectos se mide y evalúa a través de la organización y no sólo en TI. Las mejoras al proceso de administración de proyectos se formalizan y comunican y los miembros del equipo reciben entrenamiento sobre estas mejoras. La gerencia de TI implementa una estructura organizacional de proyectos con roles,</td><td></td><td>√</td></tr>
</table>

	responsabilidades y criterios de desempeño documentados. Los criterios para evaluar el éxito en cada punto clave se han establecido. El valor y el riesgo se miden y se administran, antes, durante y al final de los proyectos. Cada vez más, los proyectos abordan las metas organizacionales, en lugar de abordar solamente las específicas a TI.			
Nivel 5	Se encuentra implantada una metodología comprobada de ciclo de vida de proyectos, la cual se refuerza y se integra en la cultura de la organización completa. Se ha implantado una iniciativa continua para identificar e institucionalizar las mejores prácticas de administración de proyectos. Se ha definido e implantado una estrategia de TI para contratar el desarrollo y los proyectos operativos. Una oficina de administración de proyectos integrada es responsable de los proyectos y programas desde su concepción hasta su post-implantación.		**√**	

RECOMENDACIONES

Para el proceso AI1 de COBIT estable los siguientes objetivos de control:

- Las Bases de Datos deben soportar la metodología establecida para TI.
- Identificar y desarrollar los procesos para las soluciones de TI.
- Aprovechar la experiencia de los trabajadores para tomar decisiones correctas.

Para pasar al nivel de madurez 2, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Priorizar el desempeño, costo, confiabilidad, compatibilidad, auditoria, seguridad, disponibilidad y continuidad de los requerimientos funcionales y técnicos específicos.

Largo Plazo:

- Alinear las estrategias de las empresa con los objetivos de TI.

DOMINIO: ADQUIRIR E IMPLEMENTAR				
AI2: Adquirir y Mantener el Software Aplicativo.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	La organización no requiere de la identificación de los requerimientos funcionales y operativos para el desarrollo, implantación o modificación de soluciones, tales como sistemas, servicios, infraestructura y datos. La organización no está consciente de las soluciones tecnológicas disponibles que son potencialmente relevantes para su negocio.		**√**	**GRADO DE MADUREZ** El proceso Adquirir y Mantener el Software Aplicativo se encuentra en nivel de madurez 3. **OBJETIVOS NO CUMPLIDOS** - Informar el proceso de adquisición y mantenimiento del Sistema de Información y aplicaciones. - Determinar la metodología estándar para la documentación del software en uso.
Nivel 1	Existe conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas. Grupos individuales se reúnen para analizar las necesidades de manera informal y los requerimientos se documentan algunas veces. Los individuos identifican soluciones con base en una conciencia limitada de mercado o como respuesta a ofertas de proveedores. Existe una investigación o análisis estructurado mínimo de la tecnología disponible.	**√**		

Nivel 2	Existen algunos enfoques intuitivos para identificar que existen soluciones de TI y éstos varían a lo largo del negocio. Las soluciones se identifican de manera informal con base en la experiencia interna y en el conocimiento de la función de TI. El éxito de cada proyecto depende de la experiencia de unos cuantos individuos clave. La calidad de la documentación y de la toma de decisiones varía de forma considerable.	√		
Nivel 3	Existen enfoques claros y estructurados para determinar las soluciones de TI. El enfoque para la determinación de las soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del negocio o del usuario, las oportunidades tecnológicas, la factibilidad económica, las evaluaciones de riesgo y otros factores. El proceso para determinar las soluciones de TI se aplica para algunos proyectos con base en factores tales como las decisiones tomadas por el personal involucrado, la cantidad de tiempo administrativo dedicado, y el tamaño y prioridad del requerimiento de negocio original.	√		
Nivel 4	Existe una metodología establecida para la identificación y la evaluación de las soluciones de TI y se usa para la mayoría de los proyectos. La documentación de los proyectos es de buena calidad y cada etapa se aprueba adecuadamente. Los requerimientos están bien articulados y de acuerdo con las estructuras predefinidas. Se consideran soluciones alternativas, incluyendo el análisis de costos y beneficios. La metodología es clara, definida, generalmente entendida y medible.		√	
Nivel 5	La metodología para la identificación y evaluación de las soluciones de TI está sujeta a una mejora continua. La metodología de adquisición e implantación tiene la flexibilidad para proyectos de grande y de pequeña escala. La metodología está soportada en bases de datos de conocimiento internas y externas que contienen material de referencia sobre soluciones tecnológicas. La metodología en sí misma genera documentación en una estructura predefinida que hace que la producción y el mantenimiento sean eficientes. Con frecuencia, se identifican nuevas oportunidades de uso de la tecnología para ganar una ventaja competitiva, ejercer influencia en la re-ingeniería de los procesos de negocio y mejorar la eficiencia en general.		√	

RECOMENDACIONES

Para el proceso AI2 de COBIT estable los siguientes objetivos de control:

- Asegura la calidad del software adquirido.
- Elaborar un diseño detallado, y los requerimientos técnicos del software implementado.
- Identificar los objetivos del negocio para adquirir o desarrollar el software.

Para pasar al nivel de madurez 4, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Elaborar estrategias y planes de mantenimiento para el software aplicativo.

Largo Plazo:

- El software aplicativo debe estar sujeto a la mejora continua con soporte a las bases de datos internas y externas.

DOMINIO: ADQUIRIR E IMPLEMENTAR				
AI3: Adquirir y Mantener la Infraestructura Tecnológica.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	No se reconoce la administración de la infraestructura de tecnología como un asunto importante al cual deba ser resuelto.		√	**GRADO DE MADUREZ** El proceso Adquirir y Mantener la Infraestructura Tecnológica se encuentra en nivel de madurez 3. **OBJETIVOS NO CUMPLIDOS** - Definir una óptima estrategia para la adquisición y mantenimiento de toda la infraestructura. - Organizar y prevenir el proceso de adquisición y mantenimiento de la infraestructura tecnológica.
Nivel 1	Se realizan cambios a la infraestructura para cada nueva aplicación, sin ningún plan en conjunto. Aunque se tiene la percepción de que la infraestructura de TI es importante, no existe un enfoque general consistente. La actividad de mantenimiento reacciona a necesidades de corto plazo. El ambiente de producción es el ambiente de prueba.	√		
Nivel 2	La adquisición y mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que se deben respaldar. Se tiene la noción de que la infraestructura de TI es importante, que se apoya en algunas prácticas formales. Algunos mantenimientos se programan, pero no se programa ni se coordina en su totalidad. Para algunos ambientes, existe un ambiente de prueba por separado.	√		
Nivel 3	Existe un claro, definido y generalmente entendido proceso para adquirir y dar mantenimiento a la infraestructura TI. El proceso respalda las necesidades de las aplicaciones críticas del negocio y concuerda con la estrategia de negocio de TI, pero no se aplica en forma consistente. Se planea, programa y coordina el mantenimiento. Existen ambientes separados para prueba y producción.	√		
Nivel 4	Se desarrolla el proceso de adquisición y mantenimiento de la infraestructura de tecnología a tal punto que funciona bien para la mayoría de las situaciones, se le da un seguimiento consistente y un enfoque hacia la reutilización. La infraestructura de TI soporta adecuadamente las aplicaciones del negocio. El proceso está bien organizado y es preventivo.		√	
Nivel 5	El proceso de adquisición y mantenimiento de la infraestructura de tecnología es preventivo y está estrechamente en línea con las aplicaciones críticas del negocio y con la arquitectura de la tecnología. Se siguen buenas prácticas respecto a las soluciones de tecnología, y la organización tiene conciencia de las últimas plataformas desarrolladas y herramientas de administración. Se reducen costos al racionalizar y estandarizar los componentes de la infraestructura y con el uso de la automatización.		√	

RECOMENDACIONES
Para el proceso AI3 de COBIT estable los siguientes objetivos de control:
- Identificar el mejor plan para la adquisición de infraestructura tecnológica.
- Garantizar la disponibilidad de la infraestructura tecnológica.
- Conocer las necesidades de infraestructura tecnológica para nuevas adquisiciones.

Para pasar al nivel de madurez 4, se debe adoptar las siguientes estrategias:
Corto Plazo:
- Reestructurar y mejorar el plan existente para la adquisición de infraestructura tecnológica.

Largo Plazo:
- Proteger la infraestructura tecnológica mediante medidas de control interno, seguridad y documentar la configuración, integración y mantenimiento de hardware y software de la infraestructura tecnológica.

DOMINIO: ADQUIRIR E IMPLEMENTAR				
AI4: Facilitar la Operación y el Uso.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	No existe el proceso con respecto a la producción de documentación de usuario, manuales de operación y material de entrenamiento. Los únicos materiales existentes son aquellos que se suministran con los productos que se adquieren.		√	**GRADO DE MADUREZ** El proceso Facilitar la Operación y el Uso se encuentra en nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** -Generar los materiales de entretenimiento que cuenten con el soporte de la administración. - Garantizar a la empresa buenas prácticas para el desarrollo de proceso.
Nivel 1	La documentación se genera ocasionalmente y se distribuye en forma desigual a grupos limitados. Mucha de la documentación y muchos de los procedimientos ya caducaron. Los materiales de entrenamiento tienden a ser esquemas únicos con calidad variable. Virtualmente no existen procedimientos de integración a través de los diferentes sistemas y unidades de negocio. No hay aportes de las unidades de negocio en el diseño de programas de entrenamiento.	√		
Nivel 2	No hay un enfoque uniforme para el desarrollo de procedimientos de usuario y de operación. Individuos o equipos de proyecto generan los materiales de entrenamiento, y la calidad depende de los individuos que se involucran. Los procedimientos y la calidad del soporte al usuario van desde pobre a muy buena, con una consistencia e integración muy pequeña a lo largo de la organización. Se proporcionan o facilitan programas de entrenamiento para el negocio y los usuarios, pero no hay un plan general para ofrecer o dar entrenamiento.	√		
Nivel 3	Se guardan y se mantienen los procedimientos en una biblioteca formal y cualquiera que necesite saber tiene acceso a ella. Las correcciones a la documentación y a los procedimientos se realizan por reacción. Los procedimientos se encuentran disponibles fuera de línea y se pueden acceder y mantener en caso de desastre. Existe un proceso que		√	

	especifica las actualizaciones de procedimientos y los materiales de entrenamiento para que sea un entregable explícito de un proyecto de cambio. A pesar de la existencia de enfoques definidos, el contenido actual varía debido a que no hay un control para reforzar el cumplimiento de estándares. Los usuarios se involucran en los procesos informalmente. Cada vez se utilizan más herramientas automatizadas en la generación y distribución de procedimientos.			
Nivel 4	Existe un esquema definido para los procedimientos de mantenimiento y para los materiales de entrenamiento que cuentan con el soporte de la administración de TI. Existen controles para garantizar que se adhieren los estándares y que se desarrollan y mantienen procedimientos para todos los procesos. El desarrollo automatizado de procedimientos se integra cada vez más con el desarrollo de sistemas aplicativos, facilitando la consistencia y el acceso al usuario. El entrenamiento de negocio y usuario es sensible a las necesidades del negocio. La administración de TI está desarrollando medidas para el desarrollo y la entrega de documentación, materiales y programas de entrenamiento.		√	
Nivel 5	El proceso para la documentación de usuario y de operación se mejora constantemente con la adopción de nuevas herramientas o métodos. Los materiales de procedimiento y de entrenamiento se tratan como una base de conocimiento en evolución constante que se mantiene en forma electrónica, con el uso de administración de conocimiento actualizada, flujo de trabajo y tecnologías de distribución, que los hacen accesibles y fáciles de mantener.		√	

RECOMENDACIONES

Para el proceso AI4 de COBIT estable los siguientes objetivos de control:

- Garantizar el control en los estándares para el mantenimiento de los procesos.
- Desarrollar un plan para realizar soluciones de operación el cual sirva para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos.

Para pasar al nivel de madurez 3, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Transferir los conocimiento a la parte gerencial lo cual permitirá que estos tomen posesión del sistema y la información.

Largo Plazo:

- Transferir los conocimientos a los usuarios finales para lograr que usen los sistemas con efectividad y eficiencia para el apoyo a los procesos de la Organización.

DOMINIO: ADQUIRIR E IMPLEMENTAR				
AI5: Adquirir Recursos de TI.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	No existe un proceso definido de adquisición de recursos de TI. La organización no reconoce la necesidad de tener políticas y procedimientos claros de adquisición para garantizar que todos los recursos de TI se encuentren disponibles y de forma oportuna y rentable.		√	**GRADO DE MADUREZ** El proceso Adquirir Recursos de TI se encuentra en nivel de madurez 3. **OBJETIVOS NO CUMPLIDOS** - Utilizar estándares para la adquisición de Recursos de TI en todos los procesos. - Establecer buenas relaciones con todos los proveedores de forma estratégica.
Nivel 1	La organización ha reconocido la necesidad de tener políticas y procedimientos documentados que enlacen la adquisición de TI con el proceso general de adquisiciones de la organización. Los contratos para la adquisición de recursos de TI son elaborados y administrados por gerentes de proyecto y otras personas que ejercen su juicio profesional más que seguir resultados de procedimientos y políticas formales. Sólo existe un relación ad hoc entre los procesos de administración de adquisiciones y contratos corporativos y TI.	√		
Nivel 2	Las políticas y procedimientos se integran parcialmente con el proceso general de adquisición de la organización del negocio. Los procesos de adquisición se utilizan principalmente en proyectos mayores y bastante visibles. Se determinan responsabilidades y rendición de cuentas para la administración de adquisición y contrato de TI según la experiencia particular del gerente de contrato. Se reconoce la importancia de administrar proveedores y las relaciones con ellos, pero se manejan con base en la iniciativa individual. Los procesos de contrato se utilizan principalmente en proyectos mayores o muy visibles.	√		
Nivel 3	Las políticas y procedimientos toman como guía el proceso general de adquisición de la organización. La adquisición de TI se integra en gran parte con los sistemas generales de adquisición del negocio. Existen estándares de TI para la adquisición de recursos de TI. Los proveedores de recursos de TI se integran dentro de los mecanismos de administración de proyectos de la organización desde una perspectiva de administración de contratos. La administración de TI comunica la necesidad de contar con una administración adecuada de adquisiciones y contratos en toda la función de TI.	√		
Nivel 4	Se utilizan los estándares para la adquisición de recursos de TI en todos los procesos de adquisición. Se toman medidas para la administración de contratos y adquisiciones relevantes para los casos de negocio que requieran la adquisición de TI. Se dispone de reportes que sustentan los objetivos de negocio. La administración está consciente por lo general, de las excepciones a las políticas y procedimientos para la adquisición de TI. Se está desarrollando una administración		√	

	estratégica de relaciones. La administración de TI implanta el uso de procesos de administración para adquisición y contratos en todas las adquisiciones mediante la revisión de medición al desempeño.			
Nivel 5	La administración impulsa el cumplimiento de las políticas y procedimientos de adquisición de TI. Se toman las medidas en la administración de contratos y adquisiciones, relevantes en casos de negocio para adquisición de TI. Se establecen buenas relaciones con el tiempo con la mayoría de los proveedores y socios, y se mide y vigila la calidad de estas relaciones. Se manejan las relaciones en forma estratégica. Los estándares, políticas y procedimientos de TI para la adquisición de recursos TI se manejan estratégicamente y responden a la medición del proceso. La administración de TI comunica la importancia estratégica de tener una administración apropiada de adquisiciones y contratos, a través de la función TI.		**√**	

RECOMENDACIONES

Para el proceso AI5 de COBIT estable los siguientes objetivos de control:

- Elaborar un buen plan de control en la administración de contratos y adquisiciones.
- Establecer y mantener buenas relaciones con los proveedores y socios.

Para pasar al nivel de madurez 4, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Establecer y manejar estratégicamente los estándares, políticas y procedimientos de TI para adquirir los recursos de TI.

Largo Plazo:

- Impulsar los derechos y obligaciones, tanto de la empresa y los proveedores en los términos contractuales.

5.3 Procesos del Dominio Entregar y dar Soporte

<table>
<tr><th colspan="5">DOMINIO: ENTREGAR Y DAR SOPORTE</th></tr>
<tr><th colspan="5">DS1: Definir y Administrar Niveles de Servicio.</th></tr>
<tr><th colspan="2">NIVEL DE MADUREZ</th><th>cumple</th><th>no cumple</th><th>Observaciones</th></tr>
<tr><td>Nivel 0</td><td>La gerencia no reconoce la necesidad de un proceso para definir los niveles de servicio. La responsabilidad y la rendición de cuentas sobre el monitoreo no está asignada.</td><td></td><td>√</td><td rowspan="6">GRADO DE MADUREZ

El proceso Definir y Administrar Niveles de Servicio se encuentra en nivel de madurez 2.

OBJETIVOS NO CUMPLIDOS

- Ordenar los procesos de desarrollo de acuerdo a los niveles de servicio.

- Realizar reportes de servicio de forma completa y relevante.</td></tr>
<tr><td>Nivel 1</td><td>Hay conciencia de la necesidad de administrar los niveles de servicio, pero el proceso es informal y reactivo. La responsabilidad y la rendición de cuentas sobre para la definición y la administración de servicios no está definida. Si existen las medidas para medir el desempeño son solamente cualitativas con metas definidas de forma imprecisa.</td><td>√</td><td></td></tr>
<tr><td>Nivel 2</td><td>Los niveles de servicio están acordados pero son informales y no están revisados. Los reportes de los niveles de servicio están incompletos y pueden ser irrelevantes o engañosos para los clientes. Los reportes de los niveles de servicio dependen, en forma individual, de las habilidades y la iniciativa de los administradores. Está designado un coordinador de niveles de servicio con responsabilidades definidas, pero con autoridad limitada.</td><td>√</td><td></td></tr>
<tr><td>Nivel 3</td><td>El proceso de desarrollo del acuerdo de niveles de servicio está en orden y cuenta con puntos de control para revalorar los niveles de servicio y la satisfacción de cliente. Los servicios y los niveles de servicio están definidos, documentados y se ha acordado utilizar un proceso estándar. Las deficiencias en los niveles de servicio están identificadas pero los procedimientos para resolver las deficiencias son informales. Hay un claro vínculo entre el cumplimiento del nivel de servicio esperado y el presupuesto contemplado.</td><td></td><td>√</td></tr>
<tr><td>Nivel 4</td><td>La satisfacción del cliente es medida y valorada de forma rutinaria. Las medidas de desempeño reflejan las necesidades del cliente, en lugar de las metas de TI. Las medidas para la valoración de los niveles de servicio se vuelven estandarizadas y reflejan los estándares de la industria. Los criterios para la definición de los niveles de servicio están basados en la criticidad del negocio e incluyen consideraciones de disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, soporte al usuario, planeación de continuidad y seguridad. Cuando no se cumplen los niveles de servicio, se llevan a cabos análisis causa-raíz de manera rutinaria.</td><td></td><td>√</td></tr>
</table>

Nivel 5	Los niveles de servicio son continuamente reevaluados para asegurar la alineación de TI y los objetivos del negocio, mientras se toma ventaja de la tecnología incluyendo le relación costo-beneficio. Todos los procesos de administración de niveles de servicio están sujetos a mejora continua. Los niveles de satisfacción del cliente son administrados y monitoreados de manera continua. Los niveles de servicio esperados reflejan metas estratégicas de las unidades de negocio y son evaluadas contra las normas de la industria. La administración de TI tiene los recursos y la asignación de responsabilidades necesarias para cumplir con los objetivos de niveles de servicio y la compensación está estructurada para brindar incentivos por cumplir con dichos objetivos.		**√**	

RECOMENDACIONES

Para el proceso DS1 de COBIT estable los siguientes objetivos de control:

- Definir acuerdos de niveles de servicio según estándares establecidos.
-Asegurar que los niveles de servicio respondan las necesidades del negocio

Para pasar al nivel de madurez 3 se debe adoptar las siguientes estrategias:

Corto Plazo:

- Revisar continuamente los acuerdos de niveles de servicio con los proveedores internos y externos.

Largo Plazo:

- Monitorizar y reportar el cumplimiento de los niveles de servicio, estos reportes deben mantener un formato aceptable por parte de los interesados.

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS2: Administrar Servicios de Terceros.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	No hay políticas y procedimientos formales respecto a la contratación con terceros. Los servicios de terceros no son ni aprobados ni revisados por la gerencia. No hay actividades de medición y los terceros no reportan. A falta de una obligación contractual de reportar, la alta gerencia no está al tanto de la calidad del servicio prestado.	**√**		**GRADO DE MADUREZ** El proceso Administrar Servicios de Terceros se encuentra en nivel de madurez 3. **OBJETIVOS NO CUMPLIDOS** - Revisar de forma continúa las capacidades del proveedor. -Revisar en forma periódica los contratos firmados con terceros.
Nivel 1	La gerencia está consciente de la importancia de la necesidad de tener políticas y procedimientos documentados para la administración de los servicios de terceros, incluyendo la firma de contratos. No hay condiciones estandarizadas para los convenios con los prestadores de servicios. La medición de los servicios prestados es informal y reactiva. Las prácticas dependen de la experiencia de los individuos y del proveedor (por ejemplo, por demanda).	**√**		

Nivel 2	El proceso de supervisión de los proveedores de servicios de terceros, de los riesgos asociados y de la prestación de servicios es informal. Se utiliza un contrato pro-forma con términos y condiciones estándares del proveedor (por ejemplo, la descripción de servicios que se prestarán). Los reportes sobre los servicios existen, pero no apoyan los objetivos del negocio.		√	
Nivel 3	Hay procedimientos bien documentados para controlar los servicios de terceros con procesos claros para tratar y negociar con los proveedores. Cuando se hace un acuerdo de prestación de servicios, la relación con el tercero es meramente contractual. La naturaleza de los servicios a prestar se detalla en el contrato e incluye requerimientos legales, operativos y de control. Se asigna la responsabilidad de supervisar los servicios de terceros.		√	
Nivel 4	Se establecen criterios formales y estandarizados para definir los términos de un acuerdo, incluyendo alcance del trabajo, servicios/entregables a suministrar, suposiciones, cronograma, costos, acuerdos de facturación y responsabilidades. Se asignan las responsabilidades para la administración del contrato y del proveedor. Las aptitudes, capacidades y riesgos del proveedor son verificadas de forma continua. Los requerimientos del servicio están definidos y alineados con los objetivos del negocio. Existe un proceso para comparar el desempeño contra los términos contractuales, lo cual proporciona información para evaluar los servicios actuales y futuros del tercero. Se utilizan modelos de fijación de precios de transferencia en el proceso de adquisición.		√	
Nivel 5	Los contratos firmados con los terceros son revisados de forma periódica en intervalos predefinidos. La responsabilidad de administrar a los proveedores y la calidad de los servicios prestados está asignada. Se monitorea el cumplimiento de las condiciones operativas, legales y de control y se implantan acciones correctivas. El tercero está sujeto a revisiones periódicas independientes y se le retroalimenta sobre su desempeño para mejorar la prestación del servicio. Las mediciones varían como respuesta a los cambios en las condiciones del negocio. Las mediciones ayudan a la detección temprana de problemas potenciales con los servicios de terceros. La notificación completa y bien definida del cumplimiento de los niveles de servicio, está asociada con la compensación del tercero. La gerencia ajusta el proceso de adquisición y monitoreo de servicios de terceros.		√	

RECOMENDACIONES

Para el proceso DS2 de COBIT estable los siguientes objetivos de control:

- Administrar los riesgos del proveedor, asegurando los contratos legalmente.
- Monitorear el desempeño del proveedor e implementar acciones correctivas.

Para pasar al nivel de madurez 4, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Definir criterios formales y estandarizados para identificar los términos del acuerdo.

Largo Plazo:

- Mantener acuerdos de confidencialidad con los proveedores y mantener revisiones periódicas.

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS3: Administrar el Desempeño y la Capacidad.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	La gerencia no reconoce que los procesos clave del negocio pueden requerir altos niveles de desempeño de TI o que el total de los requerimientos de servicios de TI del negocio pueden exceder la capacidad. No se lleva cabo un proceso de planeación de la capacidad.		√	**GRADO DE MADUREZ** El proceso Administrar el Desempeño y la Capacidad se encuentra en nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** -Realizar evaluaciones de la infraestructura de TI logrando una capacidad óptima. -Monitorear continuamente el desempeño y la capacidad de los Recursos TI.
Nivel 1	Los usuarios, con frecuencia, tienen que llevar acabo soluciones alternas para resolver las limitaciones de desempeño y capacidad. Los responsables de los procesos del negocio valoran poco la necesidad de llevar a cabo una planeación de la capacidad y del desempeño. Las acciones para administrar el desempeño y la capacidad son típicamente reactivas. El proceso de planeación de la capacidad y el desempeño es informal. El entendimiento sobre la capacidad y el desempeño de TI, actual y futuro, es limitado	√		
Nivel 2	Los responsables del negocio y la gerencia de TI están conscientes del impacto de no administrar el desempeño y la capacidad. Las necesidades de desempeño se logran por lo general con base en evaluaciones de sistemas individuales y el conocimiento y soporte de equipos de proyecto. Algunas herramientas individuales pueden utilizarse para diagnosticar problemas de desempeño y de capacidad, pero la consistencia de los resultados depende de la experiencia de individuos clave. No hay una evaluación general de la capacidad de desempeño de TI o consideración sobre situaciones de carga pico y peor-escenario.	√		
Nivel 3	Los requerimientos de desempeño y capacidad están definidos a lo largo del ciclo de vida del sistema. Hay métricas y requerimientos de niveles de servicio bien definidos, que pueden utilizarse para medir el desempeño operacional. Los pronósticos de la capacidad y el desempeño se modelan por medio de un proceso definido. Los reportes se generan con estadísticas de desempeño. Los problemas relacionados al desempeño y a la capacidad siguen siendo		√	

	susceptibles a ocurrir y su resolución sigue consumiendo tiempo.			
Nivel 4	Hay procesos y herramientas disponibles para medir el uso del sistema, el desempeño y la capacidad, y los resultados se comparan con metas definidas. Hay información actualizada disponible, brindando estadísticas de desempeño estandarizadas y alertando sobre incidentes causados por falta de desempeño o de capacidad. Los problemas de falta de desempeño y de capacidad se enfrentan de acuerdo con procedimientos definidos y estandarizados. Se utilizan herramientas automatizadas para monitorear recursos específicos tales como espacios en disco, redes, servidores y compuertas de red. Las estadísticas de desempeño y capacidad son reportadas en términos de los procesos de negocio, de forma que los usuarios y los clientes comprendan los niveles de servicio de TI.		**√**	
Nivel 5	Los planes de desempeño y capacidad están completamente sincronizados con las proyecciones de demanda del negocio. La infraestructura de TI y la demanda del negocio están sujetas a revisiones regulares para asegurar que se logre una capacidad óptima con el menor costo posible. Las herramientas para monitorear recursos críticos de TI han sido estandarizadas y usadas a través de diferentes plataformas y vinculadas a un sistema de administración de incidentes a lo largo de toda la organización. Las herramientas de monitoreo detectan y pueden corregir automáticamente problemas relacionados con la capacidad y el desempeño. Se llevan a cabo análisis de tendencias, los cuales muestran problemas de desempeño inminentes causados por incrementos en los volúmenes de negocio, lo que permite planear y evitar problemas inesperados.		**√**	

RECOMENDACIONES

Para el proceso DS3 de COBIT estable los siguientes objetivos de control:

- Establecer en la empresa métrica de desempeño y evaluación de la capacidad.
- Revisar periódicamente la demanda del negocio con menor costo.

Para pasar al nivel de madurez 3, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Realizar pronósticos de la capacidad y el desempeño futuros de los recursos de TI en intervalos regulares.

Largo Plazo:

- Realizar un monitoreo continuo del desempeño y la capacidad de los recursos de TI, reportando la disponibilidad hacia el negocio del servicio prestado.

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS4: Garantizar la Continuidad del Servicio.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	No hay entendimiento de los riesgos, vulnerabilidades y amenazas a las operaciones de TI o del impacto en el negocio por la pérdida de los servicios de TI. No se considera que la continuidad en los servicios deba tener atención de la gerencia.		**√**	**GRADO DE MADUREZ** El proceso Garantizar la Continuidad del Servicio se encuentra en nivel de madurez 3. **OBJETIVOS NO CUMPLIDOS** - Cumplir estándares para garantizar la continuidad del servicio -Integrar los procesos de servicios para mejores prácticas externas.
Nivel 1	Las responsabilidades sobre la continuidad de los servicios son informales y la autoridad para ejecutar responsabilidades es limitada. La gerencia comienza a darse cuenta de los riesgos relacionados y de la necesidad de mantener continuidad en los servicios. El enfoque de la gerencia sobre la continuidad del servicio radica en los recursos de infraestructura, en vez de radicar en los servicios de TI. Los usuarios utilizan soluciones alternas como respuesta a la interrupción de los servicios. La respuesta de TI a las interrupciones mayores es reactiva y sin preparación.	**√**		
Nivel 2	Los enfoques para asegurar la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en el negocio. No hay un plan de continuidad de TI documentado, aunque hay compromiso para mantener disponible la continuidad del servicio y sus principios más importantes se conocen. Existe un inventario de sistemas y componentes críticos, pero puede no ser confiable. Las prácticas de continuidad en los servicios emergen, pero el éxito depende de los individuos.	**√**		
Nivel 3	Las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas. El plan de continuidad de TI está documentado y basado en la criticidad de los sistemas y el impacto al negocio. Hay reportes periódicos de las pruebas de continuidad. Los individuos toman la iniciativa para seguir estándares y recibir entrenamiento para enfrentarse con incidentes mayores o desastres. La gerencia comunica de forma regular la necesidad de planear el aseguramiento de la continuidad del servicio. Se han aplicado componentes de alta disponibilidad y redundancia. Se mantiene un inventario de sistemas y componentes críticos.	**√**		
Nivel 4	Se asigna la responsabilidad de mantener un plan de continuidad de servicios. Las actividades de mantenimiento están basadas en los resultados de las pruebas de continuidad, en las buenas prácticas internas y en los cambios en el ambiente del negocio y de TI. Se recopila, analiza y reporta documentación estructurada sobre la continuidad en los servicios y se actúa en consecuencia. Se brinda entrenamiento formal y obligatorio sobre los procesos de		**√**	

	continuidad. Se implementan regularmente buenas prácticas de disponibilidad de los sistemas. Las prácticas de disponibilidad y la planeación de la continuidad de los servicios tienen influencia una sobre la otra. Se clasifican los incidentes de discontinuidad y la ruta de escalamiento es bien conocida por todos los involucrados.			
Nivel 5	El plan de continuidad de TI está integrado con los planes de continuidad del negocio y se le da mantenimiento de manera rutinaria. El requerimiento para asegurar continuidad es garantizado por los proveedores y principales distribuidores. Se realizan pruebas globales de continuidad del servicio, y los resultados de las pruebas se utilizan para actualizar el plan. La recopilación y el análisis de datos se utilizan para mejorar continuamente el proceso. Las prácticas de disponibilidad y la continua planeación de la continuidad están totalmente alineadas. La gerencia asegura que un desastre o un incidente mayor no ocurrirán como resultado de un punto único de falla. Las prácticas de escalamiento se entienden y se hacen cumplir a fondo. Los KGIs y KPIs sobre el cumplimiento de la continuidad de los servicios se miden de manera sistemática.		**√**	

RECOMENDACIONES

Para el proceso DS4 de COBIT estable los siguientes objetivos de control:

- Desarrollar y tomar muy en cuenta planes de continuidad.
- Tener respaldos y documentación importante fuera de la empresa

Para pasar al nivel de madurez 4, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Realizar pruebas continuidad para garantizar que los sistemas puedan ser recuperados efectivamente.

Largo Plazo:

- Tener sitios de activación de respaldos para realizar procedimientos de reanudación.

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS5: Garantizar la Seguridad de los Sistema.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	La organización no reconoce la necesidad de la seguridad para TI. Las responsabilidades y la rendición de cuentas no están asignadas para garantizar la seguridad. Las medidas para soportar la administrar la seguridad de TI no están implementadas. No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI. Hay una total falta de procesos reconocibles de administración de seguridad de sistemas.		**√**	**GRADO DE MADUREZ** El proceso Garantizar la Seguridad de los Sistemas se encuentra en nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** - Concientizar a todos los interesados el valor de la seguridad de la información. - Elaborar un plan de seguridad de TI, basado en estándares aceptables.
Nivel 1	La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan	**√**		

	respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.			
Nivel 2	Las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. La conciencia sobre la necesidad de la seguridad esta fraccionada y limitada. Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza. Los servicios de terceros pueden no cumplir con los requerimientos específicos de seguridad de la empresa. Las políticas de seguridad se han estado desarrollando, pero las herramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables. La entrenamiento sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo.	**√**		
Nivel 3	Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis de riesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe entrenamiento en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.		**√**	
Nivel 4	Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada. La certificación en seguridad es buscada por parte del personal que es responsable de la auditoría y la administración de la seguridad. Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización. Los reportes de seguridad están ligados con los objetivos del negocio. La entrenamiento sobre seguridad se imparte tanto para TI como para el negocio.		**√**	
Nivel 5	La seguridad en TI es una responsabilidad conjunta del negocio y de la gerencia de TI y está integrada con los objetivos de seguridad del negocio en la corporación. Los requerimientos de seguridad de TI están definidos de forma clara, optimizados e incluidos en un plan de seguridad aprobado. Los usuarios y los clientes se responsabilizan cada vez más de definir requerimientos de seguridad, y las funciones de seguridad están		**√**	

	integradas con las aplicaciones en la fase de diseño. Los incidentes de seguridad son atendidos de forma inmediata con procedimientos formales de respuesta soportados por herramientas automatizadas. Se llevan a cabo valoraciones de seguridad de forma periódica para evaluar la efectividad de la implementación del plan de seguridad. La información sobre amenazas y vulnerabilidades se recolecta y analiza de manera sistemática. Se recolectan e implementan de forma oportuna controles adecuados para mitigar riesgos. Se llevan a cabo pruebas de seguridad, análisis de causa-efecto e identificación pro-activa de riesgos para la mejora continua de procesos. Los procesos de seguridad y la tecnología están integrados a lo largo de toda la organización.			

RECOMENDACIONES

Para el proceso DS5 de COBIT estable los siguientes objetivos de control:

- Elaborar un plan de administración de la seguridad de TI.
- Garantizar que la tecnología relacionada con la seguridad sea resistente a sabotajes.

Para pasar al nivel de madurez 3, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Implementar seguridad en la red como por ejemplo firewalls, dispositivos de seguridad, detección de intrusos.

Largo Plazo:

- Monitorizar y realizar pruebas periódicas para garantizar la Seguridad de los sistemas TI.

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS9: Administrar la Configuración.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	La gerencia no valora los beneficios de tener un proceso implementado que sea capaz de reportar y administrar las configuraciones de la infraestructura de TI, tanto para configuraciones de hardware como de software.		**√**	**GRADO DE MADUREZ** El proceso Administrar la Configuración se encuentra en nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** - Identificar los elementos de configuración para un adecuado mantenimiento. - Verificar la integridad de los elementos configurados, teniendo un histórico.
Nivel 1	Se reconoce la necesidad de contar con una administración de configuración. Se llevan a cabo tareas básicas de administración de configuraciones, tales como mantener inventarios de hardware y software pero de manera individual. No están definidas prácticas estandarizadas.	**√**		
Nivel 2	La gerencia está consciente de la necesidad de controlar la configuración de TI y entiende los beneficios de mantener información completa y precisa sobre las configuraciones, pero hay una dependencia implícita del conocimiento y experiencia del personal técnico. Las herramientas para la administración de configuraciones se utilizan hasta cierto grado, pero difieren entre plataformas. Además no se han definido prácticas estandarizadas de trabajo. El contenido de la información de la configuración es limitado y no lo utilizan los procesos interrelacionados, tales	**√**		

	como administración de cambios y administración de problemas.		
Nivel 3	Los procedimientos y las prácticas de trabajo se han documentado, estandarizado y comunicado, pero la entrenamiento y la aplicación de estándares dependen del individuo. Además se han implementado herramientas similares de administración de configuración entre plataformas. Es poco probable detectar las desviaciones de los procedimientos y las verificaciones físicas se realizan de manera inconsistente. Se lleva a cabo algún tipo de automatización para ayudar a rastrear cambios en el software o en el hardware. La información de la configuración es utilizada por los procesos interrelacionados.		√
Nivel 4	En todos los niveles de la organización se reconoce la necesidad de administrar la configuración y las buenas prácticas siguen evolucionando. Los procedimientos y los estándares se comunican e incorporan a la entrenamiento y las desviaciones son monitoreadas, rastreadas y reportadas. Se utilizan herramientas automatizadas para fomentar el uso de estándares y mejorar la estabilidad. Los sistemas de administración de configuraciones cubren la mayoría de los activos de TI y permiten una adecuada administración de liberaciones y control de distribución.		√
Nivel 5	Todos los activos de TI se administran en un sistema central de configuraciones que contiene toda la información necesaria acerca de los componentes, sus interrelaciones y eventos. La información de las configuraciones está alineada con los catálogos de los proveedores. Hay una completa integración de los procesos interrelacionados, y estos utilizan y actualizan la información de la configuración de manera automática. Los reportes de auditoría de los puntos de referencia, brindan información esencial sobre el software y hardware con respecto a reparaciones, servicios, garantías, actualizaciones y evaluaciones técnicas de cada unidad individual. Se fomentan las reglas para limitar la instalación de software no autorizado. La gerencia proyecta las reparaciones y las actualizaciones utilizando reportes de análisis que proporcionan funciones de programación de actualizaciones y de renovación de tecnología.		√

RECOMENDACIONES

Para el proceso DS9 de COBIT estable los siguientes objetivos de control:

- Establecer herramientas de soporte y repositorio central.
- Dar un adecuado mantenimiento a los elementos de configuración identificados.

Para pasar al nivel de madurez 3, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Tener un repositorio central que contenga la información relevante sobre los elementos de configuración.

Largo Plazo:

- Integrar los procedimientos de configuración con la gestión de cambios, incidentes y problemas.

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS10: Administración de Problemas.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	No hay conciencia sobre la necesidad de administrar problemas, y no hay diferencia entre problemas e incidentes. Por lo tanto, no se han hecho intentos por identificar la causa raíz de los incidentes.		**√**	**GRADO DE MADUREZ** El proceso Administración de Problemas se encuentra en nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** - Clasificar adecuadamente los problemas identificados. - Mantener pistas de auditoria para rastrear, analizar y determinar las causas del problema.
Nivel 1	Los individuos reconocen la necesidad de administrar los problemas y de revolver las causas de fondo. Algunos individuos expertos clave brindan asesoría sobre problemas relacionados a su área de experiencia, pero no está asignada la responsabilidad para la administración de problemas. La información no se comparte, resultando en la creación de nuevos problemas y la pérdida de tiempo productivo mientras se buscan respuestas.	**√**		
Nivel 2	Hay una amplia conciencia sobre la necesidad y los beneficios de administrar los problemas relacionados con TI, tanto dentro de las áreas de negocio como en la función de servicios de información. El proceso de resolución ha evolucionado un punto en el que unos cuantos individuos clave son responsables de identificar y resolver los problemas. La información se comparte entre el personal de manera informal y reactiva.	**√**		
Nivel 3	Se acepta la necesidad de un sistema integrado de administración de problemas y se evidencia con el apoyo de la gerencia y la asignación de presupuesto para personal y entrenamiento. Se estandarizan los procesos de escalamiento y resolución de problemas. El registro y rastreo de problemas y de sus soluciones se dividen dentro del equipo de respuesta, utilizando las herramientas disponibles sin centralizar. Es poco probable detectar las desviaciones de los estándares y de las normas establecidas. La información se comparte entre el personal de manera formal y proactiva. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.		**√**	
Nivel 4	El proceso de administración de problemas se entiende a todos los niveles de la organización. Las responsabilidades y la propiedad de los problemas están claramente establecidas. Los métodos y los procedimientos son documentados, comunicados y medidos para evaluar su efectividad. La mayoría de los problemas están identificados, registrados y reportados, y su solución ha iniciado. El conocimiento y la experiencia se cultivan, mantienen y desarrollan hacia un nivel más alto a medida que la función es vista como un activo y una gran contribución al logro de las metas de TI y a la mejora de los servicios de TI.		**√**	

Nivel 5	El proceso de administración de problemas ha evolucionado a un proceso proactivo y preventivo, que contribuye con los objetivos de TI. Los problemas se anticipan y previenen. El conocimiento respecto a patrones de problemas pasados y futuros se mantiene a través de contactos regulares con proveedores y expertos. El registro, reporte y análisis de problemas y soluciones está integrado por completo con la administración de datos de configuración. Los KPIs y KGIs son medidos de manera consistente. La mayoría de los sistemas están equipados con mecanismos automáticos de advertencia y detección, los cuales son rastreados y evaluados de manera continua.		**√**	

RECOMENDACIONES

Para el proceso DS10 de COBIT estable los siguientes objetivos de control:

- Implementar procesos para reportar y clasificar los problemas.
- Implementar un seguimiento a las tendencias de los problemas.

Para pasar al nivel de madurez 3 se debe adoptar las siguientes estrategias:

Corto Plazo:

- Realizar auditorías para rastrear, analizar y determinar causas de los problemas reportados.

Largo Plazo:

- Elaborar un procedimiento para cerrar registros de problemas una vez confirmada la eliminación del error.

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS12: Administración del Ambiente Físico.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	No hay conciencia sobre la necesidad de proteger las instalaciones o la inversión en recursos de cómputo. Los factores ambientales tales como protección contra fuego, polvo, tierra y exceso de calor y humedad no se controlan ni se monitorean.		**√**	**GRADO DE MADUREZ** El proceso Administración del Ambiente Físico se encuentra en nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** - Implementar medidas de seguridad físicas alineadas con los objetivos del negocio. - Implementar medidas de protección contra factores ambientales, mediante equipos de monitoreo.
Nivel 1	La organización reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre. La administración de instalaciones y de equipo depende de las habilidades de individuos clave. El personal se puede mover dentro de las instalaciones sin restricción. La gerencia no monitorea los controles ambientales de las instalaciones o el movimiento del personal.	**√**		
Nivel 2	La seguridad física es un proceso informal, realizado por un pequeño grupo de empleados con alto nivel de preocupación por asegurar las instalaciones físicas. Los procedimientos de mantenimiento de instalaciones no están bien documentados y dependen de las buenas prácticas de unos cuantos individuos. Las metas de seguridad física no se basan en estándares formales y la gerencia no se asegura de que se cumplan los objetivos de seguridad.	**√**		

Nivel 3	Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad. Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro.		√	
Nivel 4	Se asignan las responsabilidades para la administración del contrato y del proveedor. Las aptitudes, capacidades y riesgos del proveedor son verificadas de forma continua. Los requerimientos del servicio están definidos y alineados con los objetivos del negocio. Existe un proceso para comparar el desempeño contra los términos contractuales, lo cual proporciona información para evaluar los servicios actuales y futuros del tercero. Se utilizan modelos de fijación de precios de transferencia en el proceso de adquisición. Todas las partes involucradas tienen conocimiento de las expectativas del servicio, de los costos y de las etapas. Se acordaron los KPIs y KGIs para la supervisión del servicio.		√	
Nivel 5	Los estándares están definidos para todas las instalaciones, incluyendo la selección del centro de cómputo, construcción, vigilancia, seguridad personal, sistemas eléctricos y mecánicos, protección contra factores ambientales (por ejemplo, fuego, rayos, inundaciones, etc.). Se clasifican y se hacen inventarios de todas las instalaciones de acuerdo con el proceso continuo de administración de riesgos de la organización. El acceso es monitoreado continuamente y controlado estrictamente con base en las necesidades del trabajo, los visitantes son acompañados en todo momento. El ambiente se monitorea y controla por medio de equipo especializado y las salas de equipo funcionan sin operadores humanos. Los KPIs y KGIs se miden regularmente. Los programas de mantenimiento preventivo fomentan un estricto apego a los horarios y se aplican pruebas regulares a los equipos sensibles. Las estrategias de instalaciones y de estándares están alineadas con las metas de disponibilidad de los servicios de TI y están integradas con la administración de crisis y con la planeación de continuidad del negocio.		√	

RECOMENDACIONES

Para el proceso DS12 de COBIT estable los siguientes objetivos de control:

- Establecer responsabilidades sobre el monitoreo y procedimientos de reportes.
-Tener una correcta administración de las instalaciones física y equipos.

Para pasar al nivel de madurez 3, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Implementar mayores medidas de seguridad física, en acceso a servidores, repetidoras.

Largo Plazo:

- Determinar todas las amenazas internas y externas en la administración del ambiente físico.

DOMINIO: ENTREGAR Y DAR SOPORTE				
DS13: Administración de Operaciones.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	La organización no dedica tiempo y recursos al establecimiento de soporte básico de TI y a actividades operativas.	**√**		**GRADO DE MADUREZ** El proceso Administración de Operaciones se encuentra en nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** - Organizar la programación de trabajos, procesos y tareas en secuencias eficientes. - Implementar procedimientos para monitorear la infraestructura de TI y eventos relacionados.
Nivel 1	Se establecen algunos procedimientos estándar y las actividades de operaciones son de naturaleza reactiva. La mayoría de los procesos de operación son programados de manera informal y el procesamiento de peticiones se acepta sin validación previa. Las computadoras, sistemas y aplicaciones que soportan los procesos del negocio con frecuencia no están disponibles, se interrumpen o retrasan. Se pierde tiempo mientras los empleados esperan recursos. Los medios de salida aparecen ocasionalmente en lugares inesperados o no aparecen.	**√**		
Nivel 2	La organización está consciente del rol clave que las actividades de operaciones de TI juegan en brindar funciones de soporte de TI. Se asignan presupuestos para herramientas con un criterio de caso por caso. Las operaciones de soporte de TI son informales e intuitivas. Hay una alta dependencia sobre las habilidades de los individuos. Las instrucciones de qué hacer, cuándo y en qué orden no están documentadas. Existe algo de entrenamiento para el operador y hay algunos estándares de operación formales.	**√**		
Nivel 3	Se han asignado recursos y se lleva a cabo algún entrenamiento durante el trabajo. Las funciones repetitivas están definidas, estandarizadas, documentadas y comunicadas de manera formal. Los resultados de las tareas completadas y de los eventos se registran, con reportes limitados hacia la gerencia. Se introduce el uso de herramientas de programación automatizadas y de otras herramientas para limitar la intervención del operador. Se introducen controles para colocar nuevos trabajos en operación. Se desarrolla una política formal para reducir el número de eventos no programados. Los acuerdos de servicio y mantenimiento con proveedores siguen siendo de naturaleza informal.		**√**	
Nivel 4	Las operaciones de cómputo y las responsabilidades de soporte están definidas de forma clara y la propiedad está asignada. Las operaciones se soportan a través de presupuestos de recursos para gastos de capital y de recursos humanos. La entrenamiento se formaliza y está en proceso. Existe un esfuerzo permanente para incrementar el nivel de automatización de procesos como un medio de mejora continua. Se establecen convenios formales de mantenimiento y servicio con los		**√**	

	proveedores. Hay una completa alineación con los procesos de administración de problemas, capacidad y disponibilidad, soportados por un análisis de causas de errores y fallas.			
Nivel 5	Las operaciones de soporte de TI son efectivas, eficientes y suficientemente flexibles para cumplir con las necesidades de niveles de servicio con una pérdida de productividad mínima. Los procesos automatizados que soportan los sistemas contribuyen a un ambiente estable. Todos los problemas y fallas se analizan para identificar la causa que los originó. Las reuniones periódicas con los responsables de administración del cambio garantizan la inclusión oportuna de cambios en las programaciones de producción. En colaboración con los proveedores, el equipo se analiza respecto a posibles síntomas de obsolescencia y fallas, y el mantenimiento es principalmente de naturaleza preventiva.		**√**	

RECOMENDACIONES

Para el proceso DS13 de COBIT estable los siguientes objetivos de control:

- Mantener procedimientos estándares para garantizar que el personal tengan procedimientos establecidos.
- Organizar correctamente las tareas estableciendo procedimientos de monitoreo.

Para pasar al nivel de madurez 3, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Establecer adecuadamente los procedimientos de operación para cubrir todos los procesos.

Largo Plazo:

- Garantizar que el registro de operación almacene suficiente información para la reconstrucción, revisión y análisis de las actividades.

5.4 Procesos del Dominio Monitorear y Evaluar.

DOMINIO: MONITOREAR Y EVALUAR				
ME1: Monitorear y Evaluar el Desempeño de TI.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	La organización no cuenta con un proceso implantado de monitoreo. TI no lleva a cabo monitoreo de proyectos o procesos de forma independiente. No se cuenta con reportes útiles, oportunos y precisos. La necesidad de entender de forma clara los objetivos de los procesos no se reconoce.		**√**	**GRADO DE MADUREZ** El proceso Monitorear y Evaluar el Desempeño de TI se encuentra en nivel de madurez 1.
Nivel 1	No se han identificado procesos estándar de recolección y evaluación. El monitoreo se implanta y las métricas se seleccionan de acuerdo a cada caso, de acuerdo a las necesidades de proyectos y procesos de TI específicos. El monitoreo por lo general se implanta de forma reactiva a algún incidente que ha ocasionado alguna perdida o vergüenza a la organización. La función de contabilidad	**√**		**OBJETIVOS NO CUMPLIDOS** - Identificar los procesos con estándares internacionales de evaluación. - Integrar todos los procesos y proyectos de TI.

	monitorea mediciones financieras básicas para TI.		
Nivel 2	Los métodos y las técnicas de recolección y evaluación existen, pero los procesos no se han adoptado en toda la organización. La interpretación de los resultados del monitoreo se basa en la experiencia de individuos clave. Herramientas limitadas son seleccionadas y se implantan para recolectar información, pero esta recolección no se basa en un enfoque planeado.		√
Nivel 3	Se han implantado programas educacionales y de entrenamiento para el monitoreo. Se ha desarrollado una base de conocimiento formalizada del desempeño histórico. Las evaluaciones todavía se realizan al nivel de procesos y proyectos individuales de TI y no están integradas a través de todos los procesos. Se han definido herramientas para monitorear los procesos y los niveles de servicio de TI. Las mediciones de la contribución de la función de servicios de información al desempeño de la organización se han definido, usando criterios financieros y operativos tradicionales. Las mediciones del desempeño específicas de TI, las mediciones no financieras, las estratégicas, las de satisfacción del cliente y los niveles de servicio están definidas.		√
Nivel 4	Los reportes de los resultados del monitoreo están en proceso de estandarizarse y normalizarse. Hay una integración de métricas a lo largo de todos los proyectos y procesos de TI. Los sistemas de reporte de la administración de TI están formalizados. Las herramientas automatizadas están integradas y se aprovechan en toda la organización para recolectar y monitorear la información operativa de las aplicaciones, sistemas y procesos. La gerencia puede evaluar el desempeño con base en criterios acordados y aprobados por las terceras partes interesadas.		√
Nivel 5	Un proceso de mejora continua de la calidad se ha desarrollado para actualizar los estándares y las políticas de monitoreo a nivel organizacional incorporando mejores prácticas de la industria. Todos los procesos de monitoreo están optimizados y dan soporte a los objetivos de toda la organización. Las métricas impulsadas por el negocio se usan de forma rutinaria para medir el desempeño, y están integradas en los marcos de trabajo estratégicos. El monitoreo de los procesos y el rediseño continuo son consistentes con los planes de mejora de los procesos de negocio en toda la organización.		√

RECOMENDACIONES

Para el proceso ME1 de COBIT estable los siguientes objetivos de control:

- Definir un método de monitoreo como Balance Scorecard.
- Comparar periódicamente las metas para evaluar el desempeño de TI con el negocio.

Para pasar al nivel de madurez 2, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Implementar métodos de recolección y avaluación en la empresa, para garantizar la continuidad del negocio.

Largo Plazo:

- Establecer un proceso estándar para el monitoreo e identificar e iniciar medidas correctivas sobre el desempeño de TI.

DOMINIO: MONITOREAR Y EVALUAR				
ME2: Monitorear y Evaluar el Control Interno.				
NIVEL DE MADUREZ		cumple	no cumple	Observaciones
Nivel 0	La organización carece de procedimientos para monitorear la efectividad de los controles internos. Los métodos de reporte de control interno gerenciales no existen. Existe una falta generalizada de conciencia sobre la seguridad operativa y el aseguramiento del control interno de TI. La gerencia y los empleados no tienen conciencia general sobre el control interno.		√	**GRADO DE MADUREZ** El proceso Monitorear y Evaluar el Control Interno se encuentra en nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** -Establecer los procesos para la evaluación y aseguramiento del control interno. -Implementar herramientas integradas para la detección del control interno de TI.
Nivel 1	La experiencia individual para evaluar la suficiencia del control interno se aplica de forma ad hoc. La gerencia de TI no ha asignado de manera formal las responsabilidades para monitorear la efectividad de los controles internos. Las evaluaciones de control interno de TI se realizan como parte de las auditorías financieras tradicionales, con metodologías y habilidades que no reflejan las necesidades de la función de los servicios de información.	√		
Nivel 2	La evaluación del control interno depende de las habilidades de individuos clave. La organización tiene una mayor conciencia sobre el monitoreo de los controles internos. La gerencia de servicios de información realiza monitoreo periódico sobre la efectividad de lo que considera controles internos críticos. Se están empezando a usar metodologías y herramientas para monitorear los controles internos, aunque no se basan en un plan. Los factores de riesgo específicos del ambiente de TI se identifican con base en las habilidades de individuos.	√		
Nivel 3	Se han desarrollado políticas y procedimientos para evaluar y reportar las actividades de monitoreo del control interno. Se ha definido un programa de educación y entrenamiento para el monitoreo del control interno. Se ha definido también un proceso para auto-evaluaciones y revisiones de aseguramiento del control interno, con roles definidos para los responsables de la administración del negocio y de TI. Se usan herramientas, aunque no necesariamente están integradas en todos los procesos. Las políticas de evaluación de riesgos de los procesos de TI se utilizan dentro de los marcos de trabajo desarrollados de manera específica para la función de TI.		√	
Nivel 4	La organización ha establecido niveles de tolerancia para el proceso de monitoreo del control interno. Se han implantado herramientas para estandarizar evaluaciones y para detectar de forma automática las excepciones de control. Se ha establecido una función formal para el control interno de TI, con profesionales especializados y certificados que utilizan un marco de trabajo de control formal avalado por la alta dirección. Un		√	

	equipo calificado de TI participa de forma rutinaria en las evaluaciones de control interno. Se ha establecido una base de datos de métricas para información histórica sobre el monitoreo del control interno.			
Nivel 5	La organización ha establecido niveles de tolerancia para el proceso de monitoreo del control interno. Se han implantado herramientas para estandarizar evaluaciones y para detectar de forma automática las excepciones de control. Se ha establecido una función formal para el control interno de TI, con profesionales especializados y certificados que utilizan un marco de trabajo de control formal avalado por la alta dirección. Un equipo calificado de TI participa de forma rutinaria en las evaluaciones de control interno. Se ha establecido una base de datos de métricas para información histórica sobre el monitoreo del control interno.		**√**	

RECOMENDACIONES

Para el proceso ME2 de COBIT estable los siguientes objetivos de control:

- Monitorear el marco de trabajo de control interno de forma continua.
- Realizar revisiones de auditoría para evaluar la eficiencia y efectividad de los controles internos sobre las TI.

- **Para pasar al nivel de madurez 3, se debe adoptar las siguientes estrategias:**

Corto Plazo:

- Realizar una auto-evaluación del control interno de la administración de procesos, políticas y contratos de TI.

Largo Plazo:

- Implementar herramientas para estandarizar evaluaciones y detectar automáticamente las excepciones de control.

DOMINIO: MONITOREAR Y EVALUAR				
ME3: Garantizar el Cumplimiento con Requerimientos Externos.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	Existe poca conciencia respecto a los requerimientos externos que afectan a TI, sin procesos referentes al cumplimiento de requisitos regulatorios, legales y contractuales.		**√**	**GRADO DE MADUREZ** El proceso Garantizar el Cumplimiento con Requerimientos Externos se encuentra en nivel de madurez 1. **OBJETIVOS NO CUMPLIDOS** - Capacitar al personal sobre requisitos legales y regulatorios externos. - Confirmar el cumplimiento de políticas, estándares, procedimientos y metodologías de TI.
Nivel 1	Existe conciencia de los requisitos de cumplimiento regulatorio, contractual y legal que tienen impacto en la organización. Se siguen procesos informales para mantener el cumplimiento, pero solo si la necesidad surge en nuevos proyectos o como respuesta a auditorías o revisiones.	**√**		
Nivel 2	En los casos en que el cumplimiento se ha convertido en un requerimiento recurrente, como en los requerimientos financieros o en la legislación de privacidad, se han desarrollado procedimientos individuales de cumplimiento y se siguen año a año. No existe, sin embargo, un enfoque estándar. Hay mucha confianza en el conocimiento y responsabilidad de los individuos, y los errores son posibles. Se brinda entrenamiento informal respecto a los requerimientos externos y a los temas de		**√**	

	cumplimiento.			
Nivel 3	Se han desarrollado, documentado y comunicado políticas, procedimientos y procesos, para garantizar el cumplimiento de los reglamentos y de las obligaciones contractuales y legales, pero algunas quizá no se sigan y algunas quizá estén desactualizadas o sean poco prácticas de implementar. Se realiza poco monitoreo y existen requisitos de cumplimiento que no han sido resueltos. Se brinda entrenamiento sobre requisitos legales y regulatorios externos que afectan a la organización y se instruye respecto a los procesos de cumplimiento definidos.		√	
Nivel 4	Existe un entendimiento completo de los eventos y de la exposición a requerimientos externos, y la necesidad de asegurar el cumplimiento a todos los niveles. Las responsabilidades son claras y se entiende el empoderamiento de los procesos. El proceso incluye una revisión del entorno para identificar requerimientos externos y cambios recurrentes. Existe un mecanismo implantado para monitorear el no cumplimiento de los requisitos externos, reforzar las prácticas internas e implementar acciones correctivas. Los eventos de no cumplimiento se analizan de forma estándar en busca de las causas raíz, con el objetivo de identificar soluciones sostenibles. Buenas prácticas internas estandarizadas se usan para necesidades específicas tales como reglamentos vigentes y contratos recurrentes de servicio.		√	
Nivel 5	Existe un proceso bien organizado, eficiente e implantado para cumplir con los requerimientos externos, basado en una sola función central que brinda orientación y coordinación a toda la organización. La organización participa en discusiones externas con grupos regulatorios y de la industria para entender e influenciar los requerimientos externos que la puedan afectar. Se han desarrollado mejores prácticas que aseguran el cumplimiento de los requisitos externos, y esto ocasiona que haya muy pocos casos de excepciones de cumplimiento. El estilo y la cultura administrativa de la organización referente al cumplimiento es suficientemente fuerte, y se elaboran los procesos suficientemente bien para que el entrenamiento se limite al nuevo personal y siempre que ocurra un cambio significativo.		√	

RECOMENDACIONES

Para el proceso ME3 de COBIT estable los siguientes objetivos de control:

- Integrar los reporte de TI sobre el cumplimiento regulatorio.
- Garantizar la identificación de requerimientos locales e internacionales legales, contractuales de políticas, y regulatorios.

Para pasar al nivel de madurez 2, se debe adoptar las siguientes estrategias:

Corto Plazo:

- Garantizar el cumplimiento de los reglamentos y de las obligaciones contractuales y legales.

Largo Plazo:

- Definir los contratos y procesos legales estándar para minimizar riesgos asociados.

DOMINIO: MONITOREAR Y EVALUAR				
ME4: Proporcionar Gobierno de TI.				
NIVEL DE MADUREZ		**cumple**	**no cumple**	**Observaciones**
Nivel 0	Existe una carencia completa de cualquier proceso reconocible de gobierno de TI. La organización ni siquiera ha reconocido que existe un problema a resolver; por lo tanto, no existe comunicación respecto al tema.		√	**GRADO DE MADUREZ** El proceso Proporcionar Gobierno de TI se encuentra en nivel de madurez 2. **OBJETIVOS NO CUMPLIDOS** - Establecer y alinear el marco de gobierno de TI con la visión completa de la empresa. -Definir el nivel de riesgo de TI aceptable por la empresa.
Nivel 1	Existen enfoques ad hoc aplicados individualmente o caso por caso. El enfoque de la gerencia es reactivo y solamente existe una comunicación esporádica e inconsistente sobre los temas y los enfoques para resolverlos. La gerencia solo cuenta con una indicación aproximada de cómo TI contribuye al desempeño del negocio. La gerencia solo responde de forma reactiva a los incidentes que hayan causado pérdidas o vergüenza a la organización.	√		
Nivel 2	Las actividades y los indicadores de desempeño del gobierno de TI, los cuales incluyen procesos planeación, entrega y supervisión de TI, están en desarrollo. Los procesos de TI seleccionados se identifican para ser mejorados con base en decisiones individuales. La gerencia ha identificado mediciones básicas para el gobierno de TI, así como métodos de evaluación y técnicas; sin embargo, el proceso no ha sido adoptado a lo largo de la organización. Los procesos, herramientas y métricas para medir el gobierno de TI están limitadas y pueden no usarse a toda su capacidad debido a la falta de experiencia en su funcionalidad.	√		
Nivel 3	Un conjunto de indicadores base de gobierno de TI se elaboran donde se definen y documentan los vínculos entre las mediciones de resultados y los impulsores del desempeño. Los procedimientos se han estandarizado y documentado. La gerencia ha comunicado los procedimientos estandarizados y el entrenamiento está establecido. Puede ser que se monitoreen los procesos sin embargo la mayoría de desviaciones, se resuelven con iniciativa individual y es poco probable que se detecten por parte de la gerencia.		√	
Nivel 4	Existe un entendimiento completo de los eventos y de la exposición a requerimientos externos, y la necesidad de asegurar el cumplimiento a todos los niveles. Las responsabilidades son claras y se entiende el empoderamiento de los procesos. El proceso incluye una revisión del entorno para identificar requerimientos externos y cambios recurrentes. Existe un mecanismo implantado para monitorear el no cumplimiento de los requisitos externos, reforzar las prácticas internas e implementar acciones correctivas. Los eventos de no cumplimiento se analizan de forma estándar en busca de las causas raíz, con el objetivo de identificar soluciones sostenibles. Buenas prácticas internas estandarizadas se usan para necesidades específicas tales como reglamentos		√	

	vigentes y contratos recurrentes de servicio.			
Nivel 5	Hay un entendimiento claro de quién es el cliente y se definen y supervisan las responsabilidades por medio de acuerdos de niveles de servicio. Las responsabilidades son claras y la propiedad de procesos está establecida. Los procesos de TI y el gobierno de TI están alineados e integrados con la estrategia corporativa de TI. La mejora de los procesos de TI se basa principalmente en un entendimiento cuantitativo y es posible monitorear y medir el cumplimiento con procedimientos y métricas de procesos. El gobierno de TI ha sido integrado a los procesos de planeación estratégica y operativa, así como a los procesos de monitoreo. Los indicadores de desempeño de todas las actividades de gobierno de TI se registran y siguen, y esto lidera mejoras a nivel de toda la empresa. La rendición general de cuentas del desempeño de los procesos clave es clara, y la gerencia recibe recompensas con base en las mediciones clave de desempeño.		**√**	

RECOMENDACIONES

Para el proceso ME4 de COBIT estable los siguientes objetivos de control:
- Asegurar el cumplimento de marco de trabajo con las leyes y regulaciones.
- Garantizar el entendimiento de temas estratégicos de TI al concejo directivo.
- Garantizar un entendimiento compartido entre el negocio y la función de TI.

Para pasar al nivel de madurez 3, se debe adoptar las siguientes estrategias:

Corto Plazo:
- Establecer un marco de gobierno para garantizar la alineación de TI con el negocio.

Largo Plazo:
- Alinear correctamente las estrategias de TI para garantizar la entrega de valor, administrando los programas de inversión, activos y servicios con TI.

5.5 Reporte General de Grados de Madurez

En la **Tabla 5.1,** se muestra el resumen de los niveles de madurez obtenidos.

DOMINIO	PROCESOS		NIVEL DE MADUREZ
PLANEAR Y ORGANIZAR	PO1	Definir un Plan Estratégico de TI	2
	PO2	Definir la Arquitectura de la Información	2
	PO3	Determinar la Dirección Tecnológica	2
	PO4	Definir los Procesos, Organización y Relaciones de TI	2
	PO5	Administrar la Inversión en TI	3
	PO6	Comunicar las Aspiraciones y la Dirección de la Gerencia	1
	PO8	Administrar la Calidad	1
	PO9	Evaluar y Administrar los Riesgos de TI	2
ADQUIRIR E IMPLEMENTAR	AI1	Identificar soluciones automatizadas	1
	AI2	Adquirir y mantener software aplicativo	3
	AI3	Adquirir y mantener infraestructura tecnológica	3
	AI4	Facilitar la operación y el uso	2

	AI5	Adquirir recursos de TI	3
ENTREGAR Y DAR SOPORTE	DS1	Definir y administrar los niveles de servicio	2
	DS2	Administrar los servicios de terceros	3
	DS3	Administrar el desempeño y la capacidad	2
	DS4	Garantizar la continuidad del servicio	3
	DS5	Garantizar la seguridad de los sistemas	2
	DS9	Administrar la configuración	2
	DS10	Administrar los problemas	2
	DS12	Administrar el ambiente físico	2
	DS13	Administrar las operaciones	2
MONITOREAR Y EVALUAR	ME1	Monitorear y Evaluar el Desempeño de TI	1
	ME2	Monitorear y Evaluar el Control Interno	2
	ME3	Garantizar el Cumplimiento Regulatorio	1
	ME4	Proporcionar Gobierno de TI	2

Tabla 5.1 – Niveles de Madurez Obtenidos.

5.6 Resumen de Procesos y Criterios de Información por Impacto [3]

En la **tabla 5.2,** se muestra los Criterios de Información donde el grado de impacto Primario se asigna 86%, cuyo impacto es alto, para el grado de impacto Secundario se asigna 63%, cuyo impacto es medio y para el caso que la casilla se encuentre vacío, no se asignará ningún valor ya que no tiene ningún impacto a los Criterios de Información, según lo que especifica El Marco de Trabajo COBIT[73].

	Criterios de Información de COBIT						
	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Planear y Organizar							
PO1 Definir un Plan Estratégico de TI	0,86	0,63					
PO2 Definir la Arquitectura de la Información	0,63	0,86	0,63	0,86			
PO3 Determinar la Dirección Tecnológica	0,86	0,86					
PO4 Definir los Procesos, Organización y Relaciones de TI	0,86	0,86					0,63
PO5 Administrar la Inversión en TI	0,86	0,86					
PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia	0,86					0,63	
PO7 Administrar Recursos Humanos de TI	0,86	0,86					
PO8 Administrar la Calidad	0,86	0,86		0,63			0,63

[73] © 2007 IT Governance Institute, COBIT 4.1 Pág. 173

PO9 Evaluar y Administrar los Riesgos de TI	0,63	0,63	0,86	0,86	0,86	0,63	0,63
PO10 Administrar Proyectos	0,86	0,86					
Adquirir e implementar							
AI1 Identificar soluciones automatizadas	0,86	0,63					
AI2 Adquirir y mantener software aplicativo	0,86	0,86		0,63			0,63
AI3 Adquirir y mantener infraestructura tecnológica	0,63	0,86		0,63	0,63		
AI4 Facilitar la operación y el uso	0,86	0,86		0,63	0,63	0,63	0,63
AI5 Adquirir recursos de TI	0,63	0,86				0,63	
AI6 Administrar cambios	0,86	0,86		0,86	0,86		0,63
AI7 Instalar y acreditar soluciones y cambios	0,86	0,63		0,63	0,63		
Entregar y Dar Soporte							
DS1 Definir y administrar los niveles de servicio	0,86	0,86	0,63	0,63	0,63	0,63	0,63
DS2 Administrar los servicios de terceros	0,86	0,86	0,63	0,63	0,63	0,63	0,63
DS3 Administrar el desempeño y la capacidad	0,86	0,86			0,63		
DS4 Garantizar la continuidad del servicio	0,86	0,63			0,86		
DS5 Garantizar la seguridad de los sistemas			0,86	0,86	0,63	0,63	0,63
DS6 Identificar y asignar costos		0,86					0,86
DS7 Educar y entrenar a los usuarios	0,86	0,63					
DS8 Administrar la mesa de servicio y los incidentes	0,86	0,86					
DS9 Administrar la configuración	0,86	0,63			0,63		0,63
DS10 Administrar los problemas	0,86	0,86			0,63		
DS11 Administrar los datos				0,86			0,86
DS12 Administrar el ambiente físico				0,86	0,86		
DS13 Administrar las operaciones	0,86	0,86		0,63	0,63		
Monitorear y Evaluar							
ME1 Monitorear y Evaluar el Desempeño de TI	0,86	0,86	0,63	0,63	0,63	0,63	0,63
ME2 Monitorear y Evaluar el Control Interno						0,86	0,63
ME3 Garantizar el Cumplimiento Regulatorio	0,86	0,86	0,63	0,63	0,63	0,63	0,63
ME4 Proporcionar Gobierno de TI	0,86	0,86	0,63	0,63	0,63	0,63	0,63

Tabla 5.2 –Procesos y Criterios de Información por Impacto

5.7 Resultados Finales del Impacto sobre los Criterios de Información [3]

Se procede a multiplicar el nivel de madurez obtenido en la auditoria de cada proceso por sus respectivos valores de cada criterio de información COBIT. Después de culminar con cada multiplicación se realiza una sumatoria de la columna efectividad y se compara con el total ideal de dicho criterio de información si se hubiera tenido que multiplicar con los grados de madurez óptimos (5) de cada criterio de información y se realiza el mismo procedimiento

para cada columna de los Criterios de Información. Entonces el proceso de sumas totales se realiza por cada columna de los Criterios de Información obteniendo como resultado los totales reales e ideales de cada impacto del criterio de información. Po último se procede a realizar el cálculo del porcentaje obtenido mediante la división o comparación del total real para el total ideal para posteriormente multiplicarle por 100% y así obtenemos el porcentaje del impacto de los Criterios de Información que se muestra en la **tabla 5.3**.

PROCESOS	NIVEL DE MADUREZ	Criterios de Información de COBIT							PROMEDIO CRITERIOS TI
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	
Planear y Organizar									
PO1	2	1,72	1,26						
PO2	2	1,26	1,72	1,26	1,72				
PO3	2	1,72	1,72						
PO4	2	1,72	1,72					1,26	
PO5	3	2,58	2,58						
PO6	1	0,86					0,63		
PO8	1	0,86	0,86		0,63			0,63	
PO9	2	1,26	1,26	1,72	1,72	1,72	1,26	1,26	
Adquirir e implementar									
AI1	1	0,86	0,63						
AI2	3	2,58	2,58		1,89			1,89	
AI3	3	1,89	2,58		1,89	1,89			
AI4	2	1,72	1,72		1,26	1,26	1,26	1,26	
AI5	3	1,89	2,58				1,89		
Entregar y Dar Soporte									
DS1	2	1,72	1,72	1,26	1,26	1,26	1,26	1,26	
DS2	3	2,58	2,58	1,89	1,89	1,89	1,89	1,89	
DS3	2	1,72	1,72			1,26			
DS4	3	2,58	1,89			2,58			
DS5	2			1,72	1,72	1,26	1,26	1,26	
DS9	2	1,72	1,26			1,26		1,26	
DS10	2	1,72	1,72			1,26			
DS12	2				1,72	1,72			
DS13	2	1,72	1,72		1,26	1,26			
Monitorear y Evaluar									

ME1	1	0,86	0,86	0,63	0,63	0,63	0,63	0,63	
ME2	2						1,72	1,26	
ME3	1	0,86	0,86	0,63	0,63	0,63	0,63	0,63	
ME4	2	1,72	1,72	1,26	1,26	1,26	1,26	1,26	

TOTAL REAL	38,12	26,08	10,37	19,48	21,14	13,69	15,75	20,66
TOTAL IDEAL	94,3	88,85	27,5	48,7	50,7	35,8	40,95	55,26
PORCENTAJE	40,42%	29,35%	37,71%	40%	41,70%	38,24%	38,46%	37,98%

Tabla 5.3 – Resultados del Impacto sobre los Procesos y Criterios de Información.

En la **figura 5.1,** se muestra gráficamente el Impacto de los Criterios de Información obtenidos.

5.8 Resumen de Análisis por Dominio

5.8.1 Dominio: Planear y Organizar (PO)

No existe una óptima estructura organizacional y tecnológica, por tanto las estrategias de TI y del negocio no están alineadas correctamente en la "Administración de la Red de Datos WAN denominada Soporte y Monitoreo de la Plataforma Clientes", ya que no todas las personas en la organización entienden los Objetivos de TI, no se alcanza el uso óptimo de todos los recursos y no se entiende y administra de forma adecuada los riesgos para alcanzar una apropiada calidad de los sistemas de TI para las necesidades del negocio.

5.8.2 Dominio: Adquirir e Implementar (AI)

Para cumplir esta estrategia de TI, las soluciones no se están identificando, desarrollando, adquiriendo ni implementando e integrando correctamente en los procesos del negocio, y además el cambio y mantenimiento de los sistemas existentes deberán garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

5.8.3 Dominio: Entrega y Dar Soporte (DS)

La entrega de los servicios requeridos y la prestación del servicio no cumplen una óptima aceptación, también existe falencias en la administración de la seguridad y

continuidad en la entrega de los servicios de TI de acuerdo con las prioridades del negocio para mejorar los costos de TI manteniendo una buena administración de los datos e instalaciones operativas.

5.8.4 Dominio: Monitorear y Evaluar (ME)

No se están evaluando de forma regular los procesos de TI en la "Administración de la Red de Datos WAN denominada Soporte y Monitoreo de la Plataforma Clientes", para lograr mantener la calidad y cumplimiento de los requerimientos de control. La gerencia no administra correctamente el desempeño, el monitoreo del control interno y la aplicación de un buen gobierno de TI, por lo que no se logra vincular lo realizado con las metas del negocio y detectar con anticipación los problemas.

No existe una medición óptima de riesgos y reporte de estos, así como el cumplimiento, desempeño y control.

5.9 Informes de la Auditoría

5.9.1 Informe Técnico

Alcance

Mediante la Auditoría a la Administración de la Red de Datos WAN de soporte y monitoreo, se pretende evaluar su estado actual determinando el nivel de madurez de cada proceso y de esta manera brindar a Full Data Cía. Ltda. sus respectivas conclusiones y recomendaciones a los Objetivos de Control evaluados en cada dominio según la metodología COBIT 4.1. para contribuir al alcance de los objetivos del negocio.

Objetivos

Objetivo General

Realizar una Auditoria a la Administración de la Red de Datos WAN de Soporte y Monitoreo, utilizando el Marco de Trabajo COBIT 4.1, con el fin de presentar las actividades de control en una estructura manejable y lógica, alineando TI con los objetivos del negocio de Telecomunicaciones FullData Cía. Ltda.

Objetivos Específicos

- Analizar y diagnosticar la situación actual de la Administración de la Red de Datos WAN que brinda soporte y monitoreo.
- Plantear mejores prácticas para la Administración de la Red de Datos WAN de soporte y monitoreo.

A continuación, se detalla los resultados de la evaluación de cada uno de los procesos seleccionados divididos en sus respectivos dominios (Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte, Monitorear y Evaluar.), basados en los niveles de madurez, los cuales van desde el grado 0 (no existente) al grado máximo 5 (administrado).

DOMINIO PLANEAR Y ORAGANIZAR

PO1. DEFINIR UNPLAN ESTARTEGICO.

CONCLUSIÓN.

Este proceso se encuentra en el nivel de madurez 2 ya que la empresa no cuenta con un plan estratégico bien definido.

RECOMENDACIONES COBIT

- Alinear las estrategias de TI con las del negocio, la gerencia debe informar a los jefes de departamento sobre el estado actual de las tecnológicas

actuales y las capacidades a futuro, para determinar las oportunidades que prestan las TI y mejorar el desempeño de las labores diarias.

- Del Plan Estratégico crear planes tácticos de TI para describir las iniciativas y los requerimientos de los Recursos de TI, estos planes deben ser bien detallados para realizar la definición de planes proyectados a largo plazo.

PO2. DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN.

CONCLUSIÓN.

Este proceso se encuentra en el nivel de madurez 2, ya que se reconoce tener una arquitectura de información, pero no se elabora correctamente.

RECOMENDACIONES COBIT

- Implantar un diseño de clasificación de datos que aplique a todo la Red de Datos WAN, basado en la información crítica y sensible.
- Establecer e implementar procedimientos para lograr integridad y consistencia de todos los datos que se encuentran almacenados digitalmente, como bases de datos, archivos, reportes, inventarios.

PO3. DETERMINAR LA DIRECCIÓN TECNOLÓGICA.

CONCLUSIÓN.

Este proceso se encuentra en el nivel de madurez 2, ya que el desarrollo de componentes tecnológicos y la implantación de tecnologías emergentes es repetible pero intuitiva.

RECOMENDACIONES COBIT

- Analizar las tecnologías existentes y emergentes, para determinar qué dirección tecnológica es apropiada para cumplir con las estrategias de TI, y la arquitectura de sistemas del negocio.

- Desarrollar un plan de infraestructura tecnológica que cumpla con los planes estratégicos y tácticos de TI.

PO4. DEFINIR LOS PROCESOS LA ORGANIZACIÓN Y LAS RELACIONES DE TI.

CONCLUSIÓN.

Este proceso se encuentra en el nivel de madurez 2 ya que las necesidades de los usuarios y relaciones con proveedores se responden de forma táctica aunque inconsistentemente.

RECOMENDACIONES COBIT

- Definir un marco de trabajo y realizar una capacitación y evaluación permanente al personal, para asignar correctamente las funciones existentes.
- Establecer un comité estratégico de TI a nivel del consejo directivo, para garantizar que el gobierno de TI se maneje de forma efectiva.

PO5. ADMINISTRAR LA INVERSIÓN DE TI.

CONCLUSIÓN.

La selección de presupuestos y responsabilidades de inversiones son asignadas a personas específicas por lo que se encuentra en nivel de madurez 3.

RECOMENDACIONES COBIT

- Mejorar continuamente la administración de inversiones en base a estándares y lecciones aprendidas del análisis del desempeño de inversiones.
- Realizar un análisis de costos y beneficios a mediano y largo plazo para determinar el ciclo de vida de los Recursos de TI.

PO6: COMUNICAR LAS ASPIRACIONES Y LA DIRECCIÓN A LA GERENCIA.

CONCLUSIÓN.

La elaboración de un ambiente completo de administración de calidad y control de TI se encuentra en estado Ad Hoc porque las mejores prácticas no son comunicadas a gerencia encontrándose en un nivel de madurez 1.

RECOMENDACIONES COBIT

- Comunicar la necesidad de un estándar de políticas y procedimientos de control.
- Elaborar y documentar las políticas de control para garantizar la calidad y control de la Información.

PO8: ADMINISTRAR LA CALIDAD.

CONCLUSIÓN.

El QMS no es entendido y utilizado correctamente para la planeación de controles de calidad, por lo que se encuentran en un estado Ad Hoc para realizar una comparación externa de acuerdo a estándares establecidos encontrándose en un nivel de madurez 1.

RECOMENDACIONES COBIT

- Realizar una evaluación de los planes existentes, así como de los sistemas de información y su impacto de los objetivos del Servicio al Cliente.
- Crear planes táctico de TI a futuro, que resulten del plan estratégico de TI, estos planes deben ser bien detallados para realizar la definición de planes proyectados.

PO9: EVALUAR Y ADMINISTRAR RIESGOS DE TI.

CONCLUSIÓN.

La evaluación e identificación de riesgos no se realiza constantemente, de esta manera las mejores prácticas no se utilizan adecuadamente en toda la organización para alinear TI con el negocio, por lo que se encuentra en un nivel de madurez 2

RECOMENDACIONES COBIT

- Definir la evaluación y administración de riesgos como procedimientos estándares, reportando a Gerencia.
- Automatizar la captura, análisis y reportes de la administración de riesgos para evaluar estrategias de mitigación de forma continua.

DOMINIO ADQUIRIR E IMPLEMENTAR

AI1. IDENTIFICAR SOLUCIONES AUTOMATIZADAS

CONCLUSIÓN.

Existe la conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas, las necesidades son analizadas de manera informal y por ciertos individuos por lo que se encuentra en nivel de madurez 1.

RECOMENDACIONES COBIT

- Resaltar, priorizar, especificar los requerimientos funcionales y técnicos de la Administración de la Red WAN, priorizando el desempeño, el costo, la confiabilidad, la compatibilidad, la auditoría, la seguridad, la disponibilidad, y continuidad.
- Identificar, documentar y analizar los riesgos relacionados con los procesos del negocio para el desarrollo de los requerimientos.

AI2. ADQUIRIR Y MANTENER SOFTWARE APLICATIVO.

CONCLUSIÓN.

Existen procesos de adquisición y mantenimiento de software aplicativo en base a la experiencia de TI, el mantenimiento a menudo es complicado por lo que se encuentra en nivel de madurez 3.

RECOMENDACIONES COBIT

- Realizar un diseño detallado, y los requerimientos técnicos del software, garantizando la integridad de la información, control de acceso, respaldo y pistas de auditoría.
- El software aplicativo debe estar sujeto a la mejora continua con soporte a las bases de datos internas y externas

AI3. ADQUIRIR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA.

CONCLUSIÓN.

Full Data Cía. Ltda. cuenta con un plan de adquisición de tecnología definido, por lo tanto se controlan los procesos de adquirir, implantar y actualizar infraestructura tecnológica, por lo que se encuentran en nivel de madurez 3.

RECOMENDACIONES COBIT

- Proteger la infraestructura tecnológica mediante medidas de control interno, seguridad y documentar la configuración, integración y mantenimiento de hardware y software de la infraestructura tecnológica.
- Desarrollar un plan de mantenimiento de la infraestructura y garantizar el control de cambios de esta.

AI4. FACILITAR LA OPERACIÓN Y EL USO.

CONCLUSIÓN.

Existe una generación repetible e intuitiva de documentación y políticas de generación de manuales, pero se tiene la conciencia de que esto es necesario, por lo que se encuentra en un nivel de madurez 2.

RECOMENDACIONES COBIT

- Realizar una transferencia de conocimiento a la parte gerencial lo cual permitirá que estos tomen posesión del sistema y los datos.
- Transferir los conocimientos a los usuarios finales para lograr que usen los sistemas con efectividad y eficiencia para el apoyo a los procesos de la Organización.

AI5. ADQUIRIR RECURSOS DE TI.

CONCLUSIÓN.

La adquisición de TI está definida totalmente con los sistemas generales del gobierno de TI, por lo que se encuentra en nivel de madurez 3.

RECOMENDACIONES COBIT

- Establecer buenas relaciones con la mayoría de proveedores para adquisición de recursos y socios existentes en la empresa.
- Manejar estratégicamente los estándares, políticas y procedimientos de TI para adquirir los recursos de TI.

DOMINIO ESTREGAR Y DAR SOPORTE.

DS1. DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO.

CONCLUSIÓN.

Los procesos de desarrollo de acuerdo a los niveles de servicio no se ordenan por lo que la administración es de forma repetible e intuitiva, por lo que se encuentra en nivel de madurez 2.

RECOMENDACIONES COBIT

- Definir un marco de trabajo para la administración de los niveles de servicio.
- Monitorizar y reportar el cumplimiento de los niveles de servicio, estos reportes deben mantener un formato aceptable por parte de los interesados.

DS2. ADMINISTRAR LOS SERVICIOS DE TERCEROS.

CONCLUSIÓN.

La Revisión de las capacidades de los proveedores no se realiza de forma continua y cierta parte de la revisión periódica de los contratos firmados está definida por lo que se encuentra en nivel de madurez 3.

RECOMENDACIONES COBIT

- Definir criterios formales y estandarizados para identificar los términos del acuerdo para evitar inconvenientes futuros.
- Mantener acuerdos de confidencialidad con los proveedores y mantener revisiones periódicas.

DS3. ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD.

CONCLUSIÓN.

El Monitoreo del desempeño y la capacidad de los recursos de TI no es continuo y no se evalúa la infraestructura de TI por lo que se encuentra en nivel de madurez 2.

RECOMENDACIONES COBIT

- Realizar pronósticos de la capacidad y el desempeño futuros de los recursos de TI en intervalos regulares.
- Realizar un monitoreo continuo del desempeño y la capacidad de los recursos de TI, reportando la disponibilidad hacia el negocio del servicio prestado.

DS4. GARANTIZAR LA CONTINUIDAD DEL SERVICIO.

CONCLUSIÓN.

Se cumplen ciertos estándares para garantizar la continuidad del servicio pero no se integran definidamente los procesos de servicios para obtener mejores prácticas externas por lo que se encuentra en nivel de madurez 3.

RECOMENDACIONES COBIT

- Se debe realizar pruebas de continuidad para garantizar que los sistemas puedan ser recuperados efectivamente.
- Tener sitios de activación de respaldos para realizar procedimientos de reanudación inmediata.

DS5. GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS.

CONCLUSIÓN.

No se ha elaborado un buen plan de seguridad de TI siente repetible pero intuitivo y no se ha concientizado a los interesados el valor del aseguramiento de la información por lo que se encuentra en nivel de madurez 2.

RECOMENDACIONES COBIT

- Implementar seguridad en la red como por ejemplo firewalls, dispositivos de seguridad, detección de intrusos.

- Monitorizar y realizar pruebas periódicas para garantizar la seguridad de los sistemas TI.

DS9: ADMINISTRAR LA CONFIGURACIÓN.

CONCLUSIÓN.

Los elementos de configuración están identificados pero no se da un adecuado mantenimiento y la verificación de la integridad de los elementos configurados se realiza de forma intuitiva sin tener un histórico por lo que se encuentra en nivel de madurez 2

RECOMENDACIONES COBIT

- Tener un repositorio central que contenga la información relevante sobre los elementos de configuración.
- Integrar los procedimientos de configuración con la gestión de cambios, incidentes y problemas.

DS10: ADMINISTRACIÓN DE PROBLEMAS.

CONCLUSIÓN.

Los problemas identificados no se clasifican adecuadamente y no existen pistas de auditoria para rastrear, analizar y determinar las causas del problema por lo que se encuentra en nivel de madurez 2.

RECOMENDACIONES COBIT

- Realizar auditorías para rastrear, analizar y determinar causas de los problemas reportados.
- Elaborar un procedimiento para cerrar registros de problemas una vez confirmada la eliminación del error.

DS12: ADMINISTRACIÓN DEL AMBIENTE FÍSICO.

CONCLUSIÓN.

Las medidas de seguridad físicas no son óptimas y no se elaborar adecuadas medidas de protección contra factores ambientales, mediante equipos de monitoreo por lo que se encuentra en nivel de madurez 2.

RECOMENDACIONES COBIT

- Determinar todas las amenazas internas y externas en la administración del ambiente físico
- Elaborar un plan para implementar mayores medidas de seguridad física.

DS13: ADMINISTRACIÓN DE OPERACIONES.

CONCLUSIÓN.

La programación de trabajos, procesos y tareas no se organiza en secuencias eficientes y no existen procedimientos para monitorear la infraestructura de TI y eventos relacionados por lo que se encuentra en nivel de madurez 2.

RECOMENDACIONES COBIT

- Establecer adecuadamente los procedimientos de operación para cubrir todos los procesos.
- Garantizar que el registro de operación almacene suficiente información para la reconstrucción, revisión y análisis de las actividades.

DOMINIO MONITOREAR Y EVALUAR

ME1: MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI.

CONCLUSIÓN.

Los procesos no se identifican con estándares internacionales de evaluación y no se integran todos los procesos con los proyectos de TI por lo que se encuentra en un nivel de madurez 1.

RECOMENDACIONES COBIT

- Implementar métodos y técnicas de recolección y avaluación en la empresa.
- Establecer un proceso estándar para el monitoreo e identificación del desempeño de TI, para iniciar medidas correctivas dentro de la empresa.

ME2: MONITOREAR Y EVALUAR EL CONTROL INTERNO.

CONCLUSIÓN.

Los procesos para la evaluación y aseguramiento del control interno se manejan de manera intuitiva y no se utilizan herramientas integradas para la detección del control interno de TI por lo que se encuentra en nivel de madurez 2.

RECOMENDACIONES COBIT

- Realizar una auto-evaluación del control interno de la administración de procesos, políticas y contratos de TI.
- Implementar herramientas integradas para estandarizar evaluaciones y detectar automáticamente las excepciones de control.

ME3: GARANTIZAR EL CUMPLIMIENTO CON REQUERIMIENTOS EXTERNOS.

CONCLUSIÓN.

El cumplimiento de políticas, estándares, procedimientos y metodologías de TI se encuentra en un estado Ad Hoc y no se ha capacitado al personal sobre requisitos legales y regulatorios externos por lo que se encuentra en nivel de madurez 1.

RECOMENDACIONES COBIT

- Garantizar el cumplimiento de los reglamentos y de las obligaciones contractuales y legales.
- Definir los contratos y procesos legales estándar para minimizar riesgos asociados.

ME4: PROPORCIONAR GOBIERNO DE TI.

CONCLUSIÓN.

El Marco de Gobierno de TI se establece y alinear de forma intuitiva con la visión completa de la empresa y no se definen el nivel de riesgo de TI aceptable por lo que se encuentra en nivel de madurez 2.

RECOMENDACIONES COBIT

- Establecer un marco de gobierno para garantizar la alineación de TI con el negocio.
- Alinear correctamente las estrategias de TI para garantizar la entrega de valor, administrando los programas de inversión, activos y servicios con TI.

5.9.2 Informe Ejecutivo

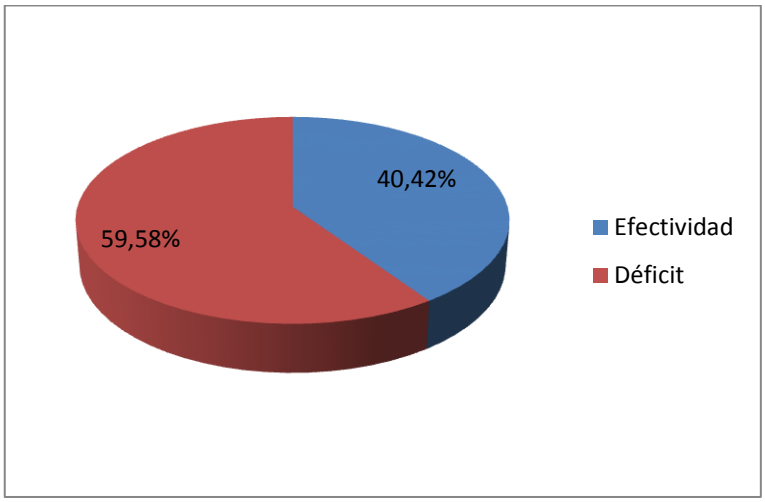
Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos más amplios de calidad, fiduciarios y de seguridad.[74]

A continuación se detallan los resultados de la evaluación a cada uno de los procesos seleccionados del Marco de Trabajo COBIT 4.1 siendo evaluado “La Administración de la Red de Datos WAN de Soporte y Monitoreo” de Full Data Cía. Ltda.

Los criterios de información se encuentran en el siguiente porcentaje todos sobre el 100%.

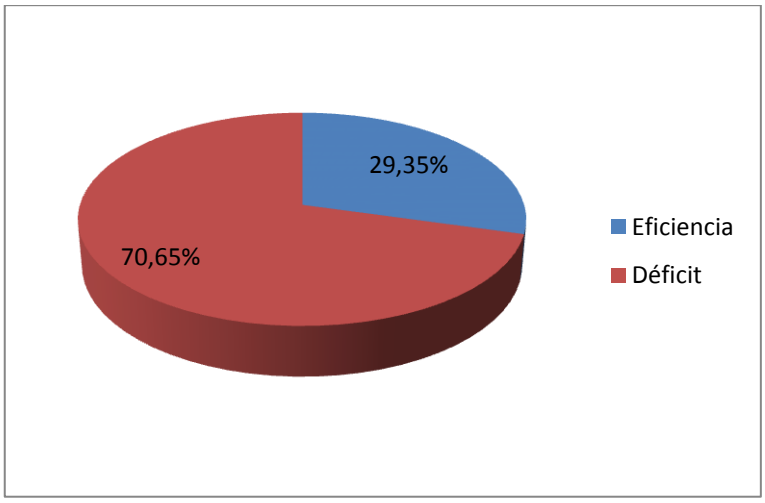
[74] © 2007 IT Governance Institute, COBIT 4.1, Pág 10

Criterio de Información: Efectividad



La efectividad tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable[75], obtuvo el 40.42%

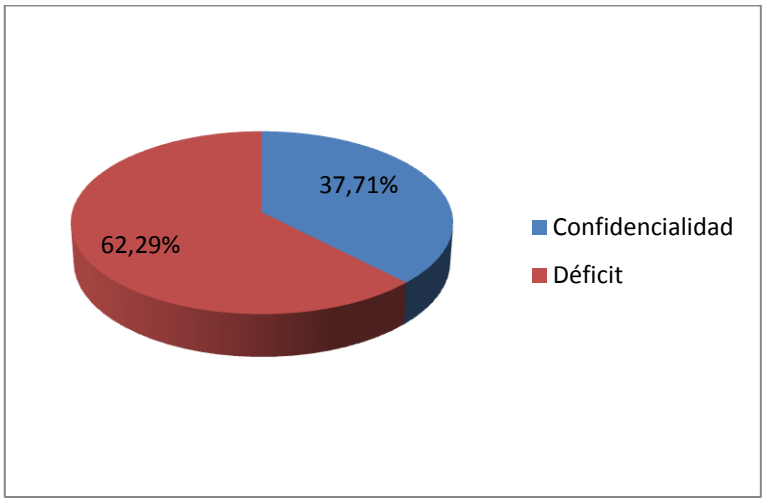
Criterio de Información: Eficiencia



La eficiencia consiste en que la información sea generada de forma más productiva y económica con el uso de los recursos[76], obtuvo el 29.35 %

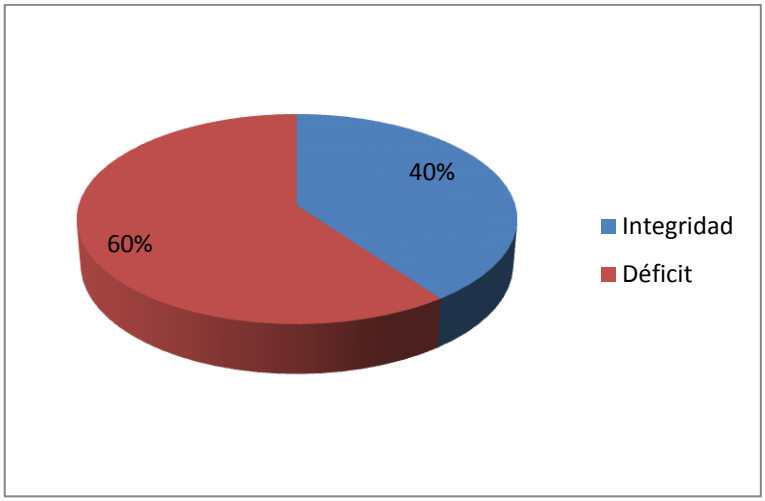
[75] © 2007 IT Governance Institute, COBIT 4.1, Pág 10

Criterio de Información: Confidencialidad



La confidencialidad se refiere a la protección de información sensitiva contra revelación no autorizada[77], obtuvo el 37.71%

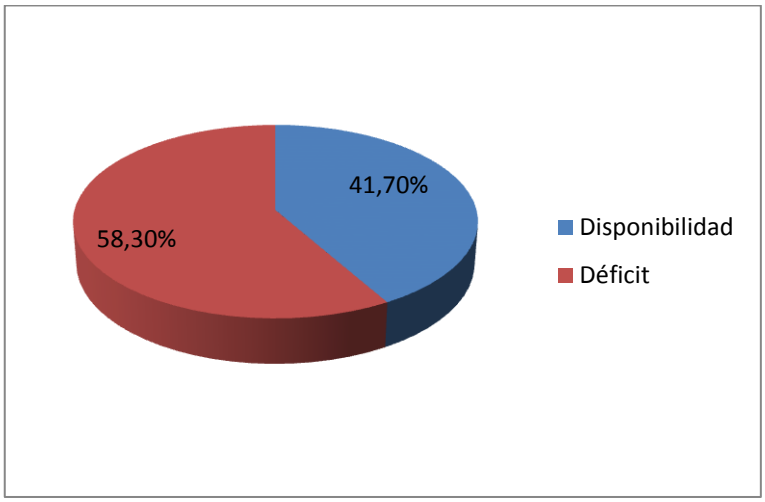
Criterio de Información: Integridad



La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio[78], obtuvo el 40%.

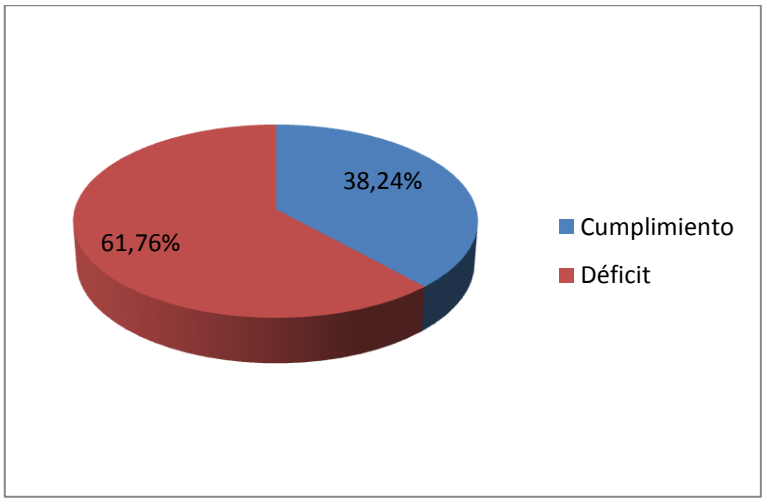
[76] © 2007 IT Governance Institute, COBIT 4.1, Pág 10
[77] © 2007 IT Governance Institute, COBIT 4.1, Pág 10

Criterio de Información: Disponibilidad



La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas[79], obtuvo el 41.70%.

Criterio de Información: Cumplimiento

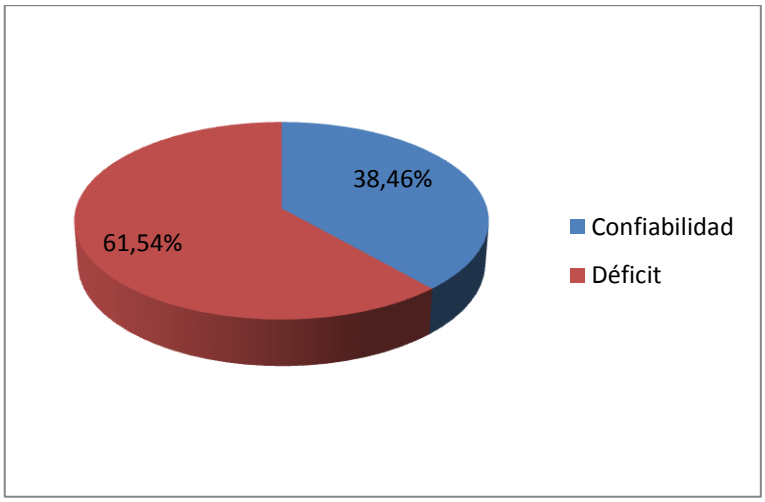


El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios

[78] © 2007 IT Governance Institute, COBIT 4.1, Pág 11
[79] © 2007 IT Governance Institute, COBIT 4.1, Pág 11

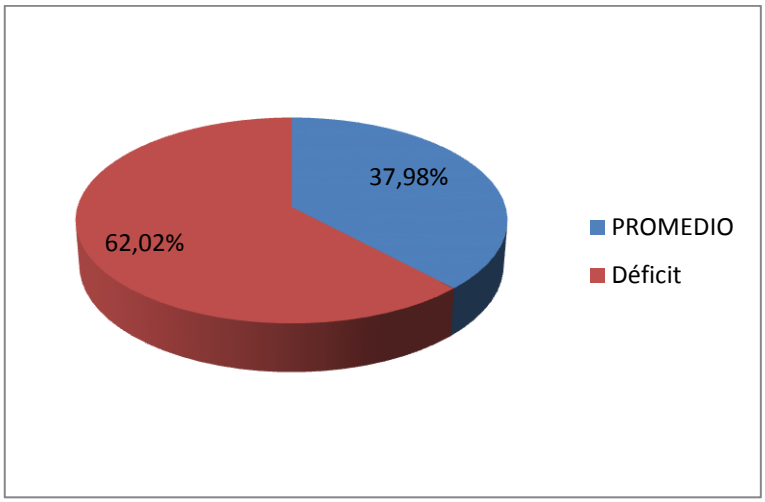
de negocios impuestos externamente, así como políticas internas[80], obtuvo el 38.24%

Criterio de Información: Confiabilidad



La confiabilidad se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno[81], obtuvo el 38.46%

Resultado promedio de Criterios de Información



[80] © 2007 IT Governance Institute, COBIT 4.1, Pág 11
[81] © 2007 IT Governance Institute, COBIT 4.1, Pág 11

Finalmente se obtuvo como promedio total del impacto de los Criterios de Información el 37.98%, lo cual se verifica que en comparación al 100% es moderadamente bajo en su impacto a la efectividad, eficiencia, confidencialidad, disponibilidad, integridad, confiabilidad, cumplimiento.

CAPITULO 6

CONCLUSIONES Y RECOMENDACIONES

En base a la auditoría realizada, las entrevistas, observaciones a la Administración de la Red de Datos WAN de Soporte y Monitoreo se ha determinado las siguientes conclusiones y recomendaciones.

6.1 Conclusiones

- En FullData Cía. Ltda. los estándares internacionales no se entiende ni se aplica óptimamente para alinear los objetivos de TI con los del negocio, como auditorias informáticas, análisis de riesgos e identificación de amenazas y vulnerabilidades, gestión de seguridad, ya que el Gobierno de TI se lleva de manera repetida e intuitiva, por lo que se presentan falencias, siendo necesario la revisión continua de los procesos aplicados.
- Con el Marco de Trabajo COBIT se puede definir los niveles madurez de cada proceso siendo aplicables a cualquier organización empresarial, siendo tan flexible se puede aprovechar metodologías para gestión de riesgos, en esta auditoria se aplicó MAGERIT la cual se acoplo de la mejor manera definiendo claramente los riesgos que pueden afectar al funcionamiento integral de la red de Soporte y Monitoreo y a los recursos empleados para la misma.
- Los informes de servicios y controles de acceso a repetidoras y vehículos empresariales utilizados en el área de TI tienen un nivel básico porque se lleva de forma manual, siendo factible la alteración de la información.
- Los procesos aplicados a bodega en lo referente a manejo de equipos y materiales para el área de TI, el sistema encargado presenta problemas de inventarios, cuadre de materiales y equipos, siendo necesario ajustes constantes de software por parte del desarrollador.

6.2 Recomendaciones

- Se recomienda a Full Data Cía. Ltda. aplicar las sugerencias emitidas por el Marco de Trabajo COBIT 4.1., obteniendo la información que la empresa necesita para lograr sus objetivos, la empresa deberá invertir, administrar y controlar los recursos de TI usando un conjunto estructurado de procesos.
- Implementar políticas dentro de la empresa que permitan crear lineamientos para la toma de decisiones y normar funciones garantizando el buen Gobierno de TI.
- Mejora el servidor de monitoreo debido al criticidad de este elemento dentro del sistema de soporte de clientes y a los problemas ocasionados debido al bajo rendimiento de este servidor.
- Respaldar y guardar en una ubicación segura dentro de Fileserver y fuera de la empresa configuraciones de radios y equipos en general de comunicaciones, con el fin de recuperar de una manera eficaz y rápida configuraciones en casos de daño de equipos o desconfiguración de los mismos.
- Habilitar SNMP en todos los equipos de comunicaciones que se monitorean con el fin de tener reportes dentro de Whatsup Gold que permitan al personal de soporte tener información más amplia de cada enlace o equipo al que se brinda servicio ya que actualmente solo se tiene información de disponibilidad mediante ICMP y aprovechar de mejor manera la aplicación de monitoreo.
- Estructurar los procesos de las áreas dentro de la organización mediante diagramas funcionales que permitan conocer de mejor manera a cada uno de los implicados en procesos que deberían ser de conocimiento general para un manejo adecuado de recursos.
- Implementar una base de conocimientos que ayude a los técnicos con las preguntas más frecuentes FAQ mejorando tiempos de respuesta en requerimientos o problemas comunes.
- Revisar la posibilidad de obtener un nuevo sistema que permita la manipulación de información como reportes, requerimientos entre otros, de

manera digital, teniendo un acceso y almacenamiento confiable de la información ya que actualmente se tiene archivada esta información de manera física.

REFERENCIAS BIBLIOGRÁFICAS

Tesis.

[1] Ramírez, Huamán y Angello, Luis, (2011). Proyecto de Auditoría Informática en la Organización DATA CENTER E.I.R.L aplicando la Metodología COBIT 4.1.. Proyecto en Auditoría y Seguridad Informática, UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO, Perú.

[2] Matute Macías, María del Carmen y Quispe Cando, Transito del Rosario, (2006). Auditoría de la Gestión de Seguridad en la red de Datos del Swissôtel basada en COBIT. Tesis en Auditoría y Seguridad Informática, ESCUELA POLITÉCNICA NACIONAL, Ecuador.

[3] Ernesto Álvarez Simba, Humberto Serrano, (2004). Diseño de un manual de mejora de procesos de tecnologías de Información para el departamento de TI de Oil Power utilizando el Marco de referencia COBIT. Tesis en Auditoría y Seguridad Informática, UNIVERSIDAD SAN FRANCISCO DE QUITO, Ecuador.

[4] Molina Sánchez Lina, (2008). Modelo de seguridad para el procedimiento no.19 del manual de procesos y procedimientos de la alcaldía de candelaria "legalización pago y contabilización de cuentas y contratos". Tesis en Auditoría y Seguridad Informática. UNIVERSIDAD AUTONOMA DE OCCIDENTE, Santiago de Cali, Colombia.

Fuente Bibliográfica

- IT Governance Institute, (2007). COBIT 4.1. EE.UU: ISACA
- IT Governance Institute, (2008). Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002. EE.UU: ISACA
- Ministerio de Hacienda y Administraciones Públicas, (2012). MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los Sistemas Libro I: Método. España: Subdirección General de Edición

- Ministerio de Hacienda y Administraciones Públicas, (2012). MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los Sistemas Libro II: Catálogo de Elementos. España: Subdirección General de Edición

- Ministerio de Hacienda y Administraciones Públicas, (2012). MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los Sistemas Libro III: Guía de Técnicas. España: Subdirección General de Edición

Internet

- PEDERIVA, ANDREA. *"The COBIT Maturity Model in a Vendor Evaluation Case"*. ISACA, Information Systems Audit and Control Association. www.isaca.org (20 de Marzo de 2004)

- Introducción a la Gestión de Redes, http://lacnic.net/documentos/lacnicx/Intro_Gestion_Redes.pdf

- Ramón Jesús Millan Tejedor, Gestión de Redes, Consultoría Estratégica en Tecnologías de la Información, http://www.ramonmillan.com/tutoriales/gestionred.php

- Procedimientos e Impulso de la Administración Electrónica de la Secretaría de Estado de Administraciones Públicas del Ministerio de Hacienda y Administraciones Públicas, MAGERIT versión 3, http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

.

GLOSARIO

Actividad—Las medidas principales tomadas para operar el proceso COBIT.

Administración de la configuración—El control de cambios realizados a un conjunto de componentes de la configuración a lo largo del ciclo de vida del sistema.

Administración del desempeño—La capacidad de administrar cualquier tipo de medición incluyendo mediciones de empleados, equipo, proceso, operativas o financieras. El término denota un control de ciclo cerrado y la vigilancia periódica de la medición.

Arquitectura de TI—Un marco integrado para evolucionar o dar mantenimiento a TI existente y adquirir nueva TI para alcanzar las metas estratégicas y de negocio de la empresa.

Arquitectura empresarial para TI—Respuesta en la entrega de TI, provista por procesos claramente definidos usando sus recursos (aplicaciones, información, infraestructura y personas).

Arquitectura empresarial—Mapa de rutas tecnológicas orientada al negocio para el logro de las metas y objetivos de negocio.

Atención al usuario—El único punto de contacto dentro de la organización de TI para los usuarios de los servicios prestados por TI.

Autenticación—El acto de verificar la identidad de un usuario y su elegibilidad para acceder a la información computarizada. La autenticación está diseñada para proteger contra conexiones de acceso fraudulentas.

Balcanced Scorecard—Un método para medir las actividades de una empresa en términos de su visión y estrategias, proporcionando una vista rápida e integral del desempeño del negocio a la gerencia. Es una herramienta administrativa cuyo fin es medir un negocio desde las siguientes perspectivas: financiera, del cliente, del negocio y del aprendizaje (Robert S. Kaplan y David Norton, 1992).

Capacidad—Contar con los atributos necesarios para realizar o lograr.

CEO—Director ejecutivo.

CFO—Director financiero.

CIO—Director de información [algunas veces Director de Tecnología (CTO, por sus siglas en inglés)].

Cliente—Una persona o una entidad externa o interna que recibe los servicios empresariales de TI.

Comité estratégico de TI—Comité al nivel del Consejo Directivo para garantizar que el consejo participe en las principales decisiones del tema de TI.

Componente de la configuración (CI) — Componente de una infraestructura—o un artículo, como una solicitud de cambio, asociado con una infraestructura—la cual está (o estará) bajo el control de la administración de configuraciones. Los CIs pueden variar ampliamente en complejidad, tamaño y tipo, desde un sistema completo (incluyendo todo el hardware, software y documentación) hasta un solo módulo o un componente menor de hardware.

Continuidad—Prevenir, mitigar y recuperarse de una interrupción. Los términos “planear la reanudación del negocio”, “planear la recuperación después de un desastre” y “planear contingencias” también se pueden usar en este contexto; todos se concentran en los aspectos de recuperación de la continuidad.

Control aplicativo—Un conjunto de controles integrados dentro de las soluciones automatizadas (aplicaciones).

Control de accesos —El proceso que limita y controla el acceso a los recursos de un sistema computacional; un control lógico o físico diseñado para brindar protección contra la entrada o el uso no autorizados.

Control de detección—Un control que se usa para identificar eventos (indeseables o deseados), errores u otras ocurrencias con efecto material sobre un proceso o producto final, de acuerdo a lo definido por la empresa.

Control general—También control general de TI. Un control que se aplica al funcionamiento general de los sistemas de TI de la organización y a un conjunto amplio de soluciones automatizadas (aplicaciones).

Control Interno —Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una garantía razonable de que los objetivos del negocio se alcanzarán y de que los eventos indeseables serán prevenidos o detectados y corregidos.

Control preventivo—Un control interno que se usa para prevenir eventos indeseables, errores u otras ocurrencias que pudieran tener un efecto material negativo sobre un proceso o producto final, de acuerdo a la organización.

Control—Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proporcionar una garantía razonable de que los objetivos del negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados.

COSO—Comité de organizaciones patrocinadoras de la comisión Treadway. Estándar aceptado a nivel internacional para el gobierno corporativo. Ver www.coso.org.

CSF—Factor crítico de éxito (FCE).

DCO—Objetivos de control detallados. Los DCOs son componentes de un objetivo de control en particular.

Declaración de auditoría—Documento que define el propósito, la autoridad y la responsabilidad de la actividad de auditoría interna, aprobado por el consejo.

Desempeño—La implantación real o el logro de un proceso.

Diccionario de datos empresarial—El nombre, tipo, rango de valores, fuente, sistema de registro, y autorización de acceso para cada elemento de datos utilizado en la empresa. Indica cuáles programas aplicativos usan esos datos, de

tal forma que cuando se contemple una estructura de datos, se pueda generar una lista de los programas afectados. Ver PO2.2.

Diccionario de datos—Un conjunto de meta-datos que contiene definiciones y representaciones de elementos de datos.

Directriz—La descripción de un modo particular de lograr algo, la cual es menos prescriptiva que un procedimiento.

Dominio—Agrupación de objetivos de control en etapas lógicas en el ciclo de vida de inversión en TI.

Dueños de datos—Individuos, por lo general gerentes o directores, que tienen la responsabilidad de la integridad, el uso y el reporte preciso de los datos computarizados.

Empresa—Un grupo de individuos que trabajan juntos para un fin común, por lo general dentro del contexto de una forma organizacional, como una corporación agencia pública, entidad de caridad o fondo.

Esquema de clasificación de datos—Un esquema empresarial para clasificar los datos por factores tales como criticidad, sensibilidad y propiedad.

Estándar—Una práctica de negocio o producto tecnológico que es una práctica aceptada, avalada por la empresa o por el equipo gerencial de TI. Los estándares se pueden Implementar para dar soporte a una política o a un proceso, o como respuesta a una necesidad operativa. Así como las políticas, los estándares deben incluir una descripción de la forma en que se detectará el incumplimiento.

Evaluación por comparación (Benchmarking) —Un proceso utilizado en administración, en particular en la administración estratégica, en el cual las compañías evalúan varios aspectos de sus procesos de negocio con respecto a las mejores prácticas, por lo general dentro de su propia industria.

Gobierno—El método por medio del cual una organización es dirigida, administrada o controlada.

Incidente—Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o una reducción de la calidad de ese servicio (alineado a ITIL).

Infraestructura—La tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones.

ISO 17799—Código de práctica para la administración de la seguridad de la información de la Organización Internacional para la Estandarización (ISO).

ISO 27001—Gestión de Seguridad de la Información- Especificación con guía para su uso; la sustituta a la BS7799-2. Ideada para proporcionar los fundamentos en auditoria a terceros e armonización con otros estándares, tales como ISO/IEC 9001 y 14001.

ISO 9001:2000—Código de práctica para la administración de la calidad de la Organización internacional para la Estandarización (ISO). El ISO 9001:2000 especifica los requisitos para un sistema de administración de calidad para cualquier organización que necesite demostrar su habilidad para ofrecer productos de manera consistente que satisfagan al cliente, a los requisitos regulatorios aplicables y que desee aumentar la satisfacción del cliente.

ITIL—Librería de Infraestructura de TI de la Oficina de Gobierno Gubernamental del Reino Unido (OGC).Un conjunto de lineamientos sobre la administración y procuración de servicios operativos de TI.

KGI—Indicador clave de meta.

KPI—Indicador clave de desempeño.

Madurez—Indica el grado de confiabilidad o dependencia que el negocio puede tener en un proceso, al alcanzar las metas y objetivos deseados.

Marco de control—Una herramienta para los dueños de los procesos de negocio que facilita la descarga de sus responsabilidades a través de la procuración de un modelo de control de soporte.

Marco de trabajo—Ver Marco de control.

Matriz RACI—Ilustra quién es responsable, quién debe rendir cuentas, a quién se debe consultar e informar dentro de un marco de trabajo organizacional estándar.

Métrica—Un estándar para medir el desempeño contra la meta.

Modelo de madurez de la capacidad (CMM) —El modelo de madurez de la capacidad para software (CMM), del Instituto de Ingeniería de Software (SEI), es un modelo utilizado por muchas organizaciones para identificar las mejores prácticas, las cuales son convenientes para ayudarles a evaluar y mejorarla madurez de su proceso de desarrollo de software.

Objetivo de control—Una declaración del resultado o propósito que se desea alcanzar al Implementar procedimientos de control en un proceso en particular.

OLA—Acuerdo a nivel operativo. Un acuerdo interno que cubre la prestación de servicios que da soporte a la organización de TI en su prestación de servicios.

Organización—La manera en que una empresa está estructurada.

Plan de infraestructura tecnológica—Un plan para el mantenimiento y desarrollo de la infraestructura tecnológica.

Plan estratégico de TI—Un plan a largo plazo, Ej., con un horizonte de tres a cinco años, en el cual la gerencia del negocio y de TI describen de forma cooperativa cómo los recursos de TI contribuirán a los objetivos estratégicos empresariales (metas)

Plan táctico de TI—Un plan a mediano plazo, Ej., con un horizonte de seis a dieciocho meses, que traduzca la dirección del plan estratégico de TI en las iniciativas requeridas, requisitos de recursos y formas en las que los recursos y los beneficios serán supervisados y administrados.

PMBOK—Cuerpo de conocimiento de administración de proyectos, un estándar para administración de proyectos desarrollado por el Instituto de Administración de Proyectos (PMI).

PMO—Director de administración de proyectos.

Política—Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por los equipos gerenciales de la empresa. Además del contenido de la política, esta debe describir las consecuencias de la falta de cumplimiento de la misma, el mecanismo para manejo de excepciones y la manera en que se verificará y medirá el cumplimiento de la política.

Portafolio —Una agrupación de programas, proyectos, servicios o activos seleccionados, administrados y vigilados para optimizar el retorno sobre la inversión.

Práctica de control—Mecanismo clave de control que apoya el logro de los objetivos de control por medio del uso responsable de recursos, la administración apropiada de los riesgos y la alineación de TI con el negocio.

Prácticas de administración clave—Las principales prácticas de administración que el dueño del proceso debe realizar para alcanzar las metas del proceso.

PRINCE2—Proyectos en un ambiente controlado, un método de administración de proyectos que cubre la administración, el control y la organización de un proyecto.

Problema—Causa subyacente desconocida de uno o más incidentes.

Procedimiento—Una descripción de una manera particular de lograr algo; una forma establecida de hacer las cosas; una serie de pasos que se siguen en un orden regular definido, garantizando un enfoque consistente y repetitivo hacia las actividades.

Proceso de negocio—Ver Proceso.

Proceso—Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toma las entradas provenientes de

un número de fuentes, incluyendo otros procesos, manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, dueños responsables, roles claros y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño.

Programa aplicativo—Un programa que procesa los datos del negocio a lo largo de las actividades, tales como la captura, actualización o consulta de datos. Contrasta con los programas de sistemas, tales como un sistema operativo o un programa de control de redes, y con los programas utilitarios, tales como copiar (copy) o clasificar (sort).

Programa—Una agrupación estructurada de proyectos independientes que incluye el alcance completo del negocio, del proceso, de
las personas, de la tecnología y las actividades organizacionales que se requieren (tanto necesarias como suficientes) para lograr un resultado de negocios claramente especificado.

Proveedor de servicios—Organización externa que presta servicios a la organización.

Proyecto—Un conjunto estructurado de actividades relacionadas con la entrega de una capacidad definida a la organización (la cual es necesaria, aunque no suficiente para lograr un resultado de negocios requerido) con base en un cronograma y presupuesto acordado.

QMS—Sistema de administración de la calidad. Un sistema que describe las políticas y procedimientos necesarios para mejorar y controlar los distintos procesos que al final conducirán a un desempeño mejorado del negocio.

Resistencia—La capacidad de un sistema o red para recuperarse de forma automática de una interrupción, por lo general con un efecto reconocible mínimo.

Riesgo—El potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo

general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia.

SDLC—Ciclo de vida del desarrollo de sistemas. Las fases utilizadas en el desarrollo o adquisición de un sistema de software. Las fases típicas incluyen al estudio de factibilidad, el estudio de los requerimientos, la definición de requerimientos, el diseño detallado, la programación, las pruebas, la instalación y la revisión post-implantación.

Segregación/separación de tareas—Un control interno básico que previene y detecta errores o irregularidades por medio de la asignación a individuos diferentes, de la responsabilidad de iniciar y registrar las transacciones y la custodia de los activos.

SLA—Acuerdo de nivel de servicio. Acuerdo por escrito entre un proveedor de servicios y los usuarios del cliente, el cual documenta los niveles de servicio acordados para un servicio prestado.

TI—Tecnología de información.

Usuario—Una persona que utiliza los sistemas empresariales.

ANEXOS

ANEXO 1

TABLA DE ENLACES ENTRE METAS Y PROCEDIMIENTOS.

Esta tabla brinda una visión global de cómo se relacionan las metas genéricas del negocio con las metas de TI con los procesos de TI y con los criterios de información. Se proporcionan tres tablas:

1. La primera tabla muestra las equivalencias de las metas del negocio, de acuerdo al balanced scorecard, con las metas de TI y con los criterios de información[82]. Esto ayuda a mostrar, para una meta genérica de negocios determinada, las metas de TI que por lo general dan soporte a esta meta, y los criterios de información de COBIT que se relacionan con la meta del negocio.

2. La segunda tabla muestra las equivalencias de las metas de TI con los procesos de TI de COBIT, así como los criterios de información sobre los cuales se basa la meta de TI[83].

3. La tercera tabla proporciona un mapeo inverso que muestra para cada proceso de TI, las metas de TI que son soportadas.

Las tablas ayudan a demostrar el alcance de COBIT y la relación general de negocio entre COBIT y los impulsores del negocio, permitiendo así establecer la equivalencia entre las metas típicas de negocio, por medio de las metas de TI, y los procesos de TI requeridos para darles soporte. Las tablas se basan en metas orgánicas y, por lo tanto, se deben usar como guía y adaptarse a la empresa determinada.

Para proporcionar una liga hacia los criterios de información usados para los requisitos de negocio de la 3ª edición de COBIT, las tablas también contienen una

[82] Los criterios de información contenidos en la gráfica de metas de negocio se basan en un agregado de los criterios para las metas de TI relacionadas y en una evaluación subjetiva de aquellos que son más relevantes para la meta del negocio. No se hizo el intento para indicar si son primarios o secundarios. Estos son tan solo indicativos y los usuarios pueden seguir un proceso similar al evaluar sus propias metas de negocio.

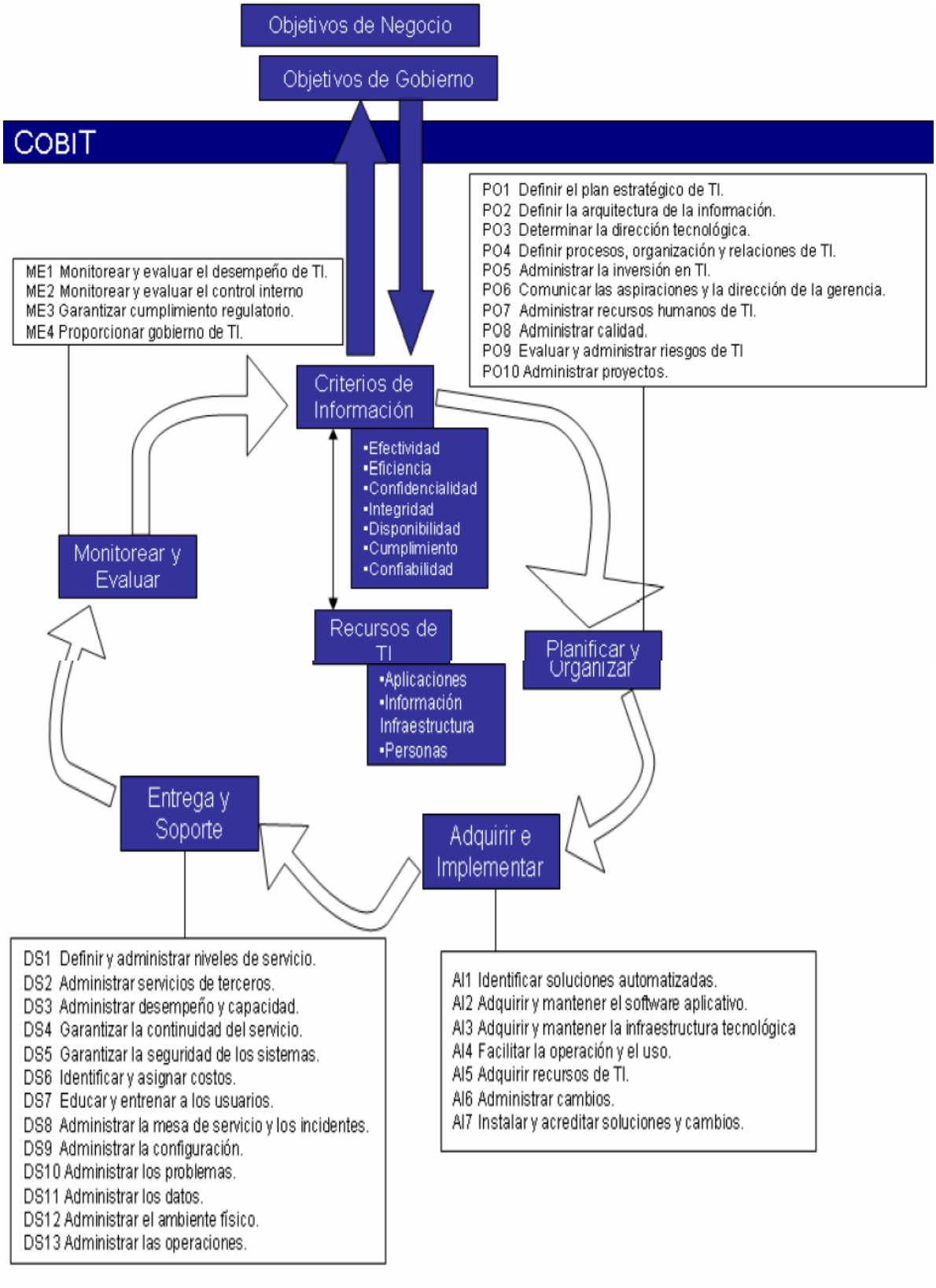
[83] Las referencias primarias y secundarias de los criterios de información en la gráfica de metas de TI se basan en un agregado de los criterios para cada proceso de TI y en una evaluación subjetiva de qué es primario y qué es secundario para la meta de TI., debido a que algunos procesos tienen mayor impacto en la meta de TI que otros. Estos son tan solo indicativos y los usuarios pueden seguir un proceso similar al evaluar sus propias metas de TI.

indicación de los criterios de información más importantes soportados por el negocio y por las metas de TI.

		Metas de Negocio	Metas de TI								*Efectividad*	*Eficiencia*	*Confidencialidad*	*Integridad*	*Disponibilidad*	*Cumplimiento*	*Confiabilidad*
Perspectiva Financiera	**1**	Proporcionar un buen entorno de inversión de TI permitiendo inversión en negocio	24	28								▯					
	2	Gestionar los riesgos de TI que afecten a negocio	2	14	17	18	19	20	21	22			▯	▯	▯		
	3	Mejorar gobierno corporativo y transparencia	2	18													▯
Perspectiva del cliente	**4**	Mejorar la orientación y servicio al cliente	3	23							▯						
	5	Ofrecer productos y servicios competitivos	5	24							▯	▯					
	6	Establecer continuidad y disponibilidad de servicios	10	16	22	23					▯				▯		
	7	Crear agilidad en la respuesta a los cambios de los requerimientos de negocio	1	5	25						▯	▯					
	8	Lograr optimización de costes de la entrega de servicios	7	8	20	24						▯					
	9	Obtener información fiable y útil para tomar decisiones estratégicas	2	4	12	20	26				▯			▯			▯
Perspectiva Interna	**10**	Mejorar y mantener funcionalidad de procesos de negocio	6	7	11						▯	▯					
	11	Reducir el coste de los procesos	7	8	13	15	24					▯					
	12	Proporcionar cumplimiento con leyes externas, regulaciones y contratos	2	19	20	21	22	26	27				▯			▯	
	13	Proporcionar cumplimiento con políticas internas	2	13									▯			▯	
	14	Gestionar cambios de negocio	1	5	6	11	28				▯	▯					
	15	Mejorar y mantener productividad operacional y de personal	7	8	11	13					▯	▯					
Perspectiva de Aprendizaje y Crecimiento	**16**	Gestionar productos e innovación de negocio	5	25	28						▯	▯					
	17	Adquirir y mantener personal cualificado y motivado	9								▯	▯					

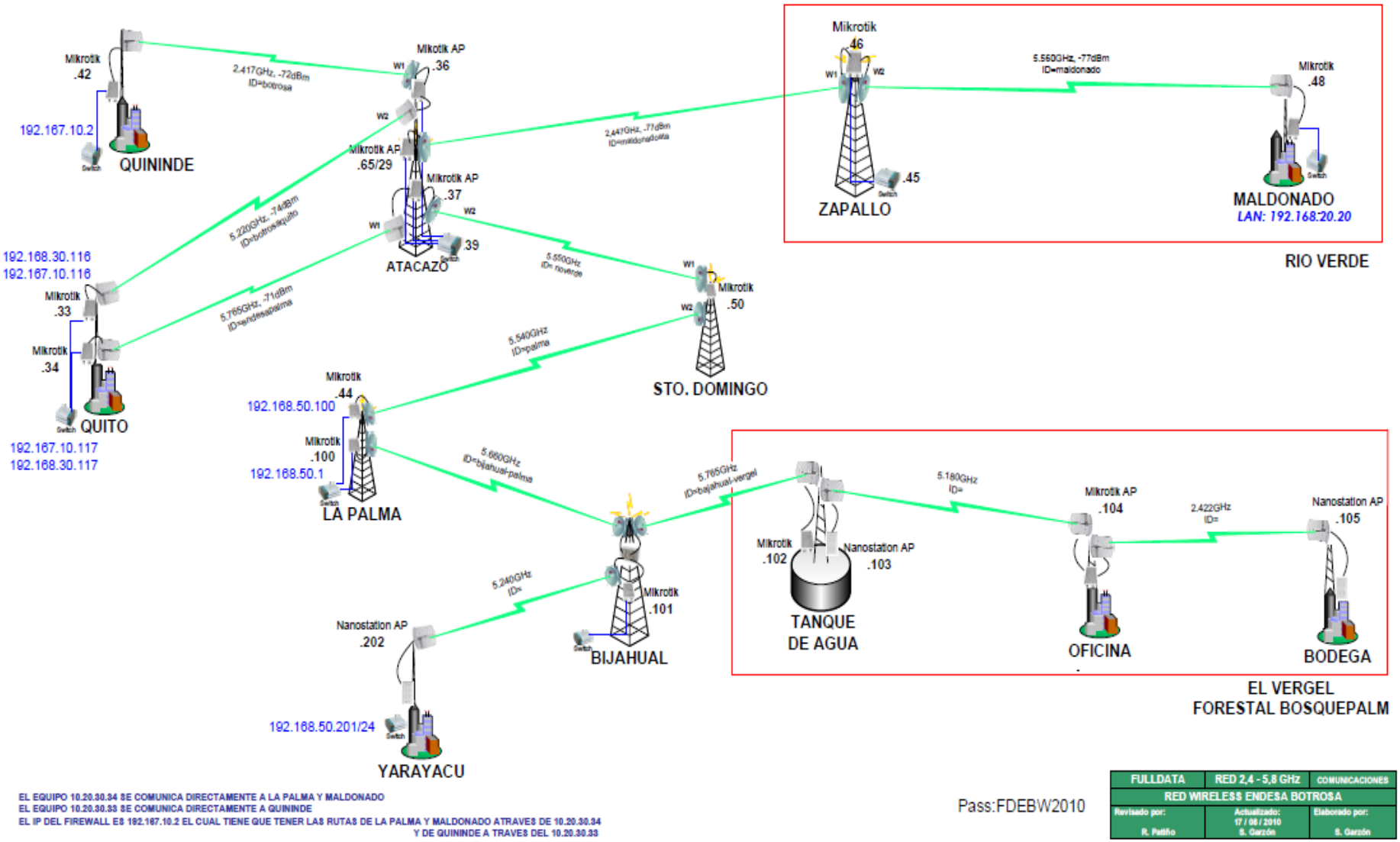
ANEXO 2

MARCO DE TRABAJO COMPLETO DE COBIT


Objetivos de Negocio
Objetivos de Gobierno
COBIT
PO1 Definir el plan estratégico de TI.
PO2 Definir la arquitectura de la información.
PO3 Determinar la dirección tecnológica.
PO4 Definir procesos, organización y relaciones de TI.
PO5 Administrar la inversión en TI.
PO6 Comunicar las aspiraciones y la dirección de la gerencia.
PO7 Administrar recursos humanos de TI.
PO8 Administrar calidad.
PO9 Evaluar y administrar riesgos de TI
PO10 Administrar proyectos.
ME1 Monitorear y evaluar el desempeño de TI.
ME2 Monitorear y evaluar el control interno
ME3 Garantizar cumplimiento regulatorio.
ME4 Proporcionar gobierno de TI.
Criterios de Información
•Efectividad
•Eficiencia
•Confidencialidad
•Integridad
•Disponibilidad
•Cumplimiento
•Confiabilidad
Monitorear y Evaluar
Recursos de TI
•Aplicaciones
•Información
Infraestructura
•Personas
Planificar y Organizar
Entrega y Soporte
Adquirir e Implementar
DS1 Definir y administrar niveles de servicio.
DS2 Administrar servicios de terceros.
DS3 Administrar desempeño y capacidad.
DS4 Garantizar la continuidad del servicio.
DS5 Garantizar la seguridad de los sistemas.
DS6 Identificar y asignar costos.
DS7 Educar y entrenar a los usuarios.
DS8 Administrar la mesa de servicio y los incidentes.
DS9 Administrar la configuración.
DS10 Administrar los problemas.
DS11 Administrar los datos.
DS12 Administrar el ambiente físico.
DS13 Administrar las operaciones.
AI1 Identificar soluciones automatizadas.
AI2 Adquirir y mantener el software aplicativo.
AI3 Adquirir y mantener la infraestructura tecnológica
AI4 Facilitar la operación y el uso.
AI5 Adquirir recursos de TI.
AI6 Administrar cambios.
AI7 Instalar y acreditar soluciones y cambios.

ANEXO 3

DIAGRAMA ENDESA-BOTROSA



RED DE COMUNICACIONES "ENDESA-BOTROSA". IP: WAN 10.20.30.XX / 27 – LAN 192.168.30.XX / 24

ANEXO No. 4

Tablas de Monitoreo de **ENDESA – BOTROSA**

En la **tabla 1,** se detallan los enlaces de la repetidora Atacazo, específicamente los dispositivos que se encuentran conectados directamente a esta repetidora.

Atacazo

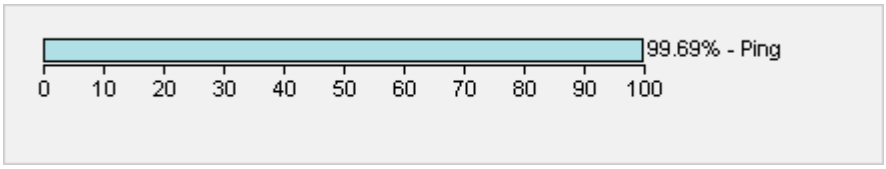
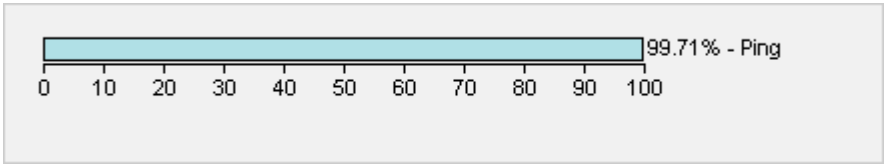
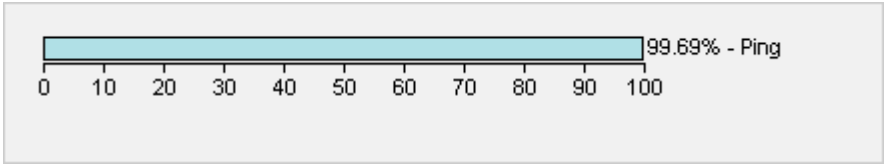
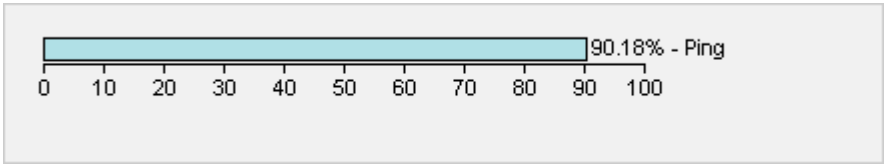
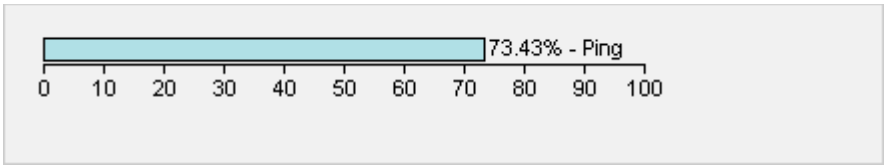
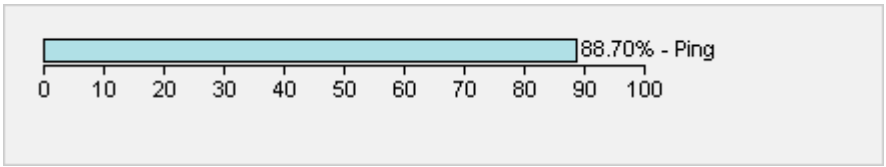
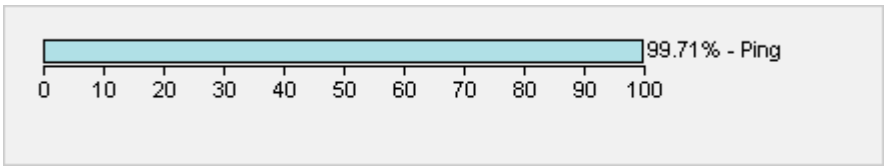
Dispositivo	Detalles
Atacazo Quito (Botrosa Atacazo Quito(Botrosa) : 10.20.30.36)	
Enlace Monitoreo Botrosa(Caseta BOTROSA) (Monitoreo Botrosa Atacazo(Caseta Botrosa) : 192.168.49.102)	
Atacazo Sto.Domingo (Botrosa Atacazo - StoDomingo : 10.20.30.37)	
Enlace Monitoreo Botrosa(Caseta FULLDATA) (Monitoreo Botrosa Atacazo (Caseta Fulldata) : 192.168.49.101)	
Equipo VLAN Atacazo (Fulldata Equipo VLAN Atacazo : 10.20.30.39)	
Atacazo Quininde (Botrosa Atacazo-Quininde : 10.20.30.38)	
Atacazo Quito(La Palma&Maldonado) (Botrosa Atacazo- Quito(La Palma&Maldonado) : 10.20.30.35)	

Tabla 1 - Dispositivos conectados a Atacazo

En la **tabla 2,** se detallan los enlaces de la repetidora La Palma, específicamente los dispositivos que se encuentran conectados directamente a esta repetidora.

La Palma

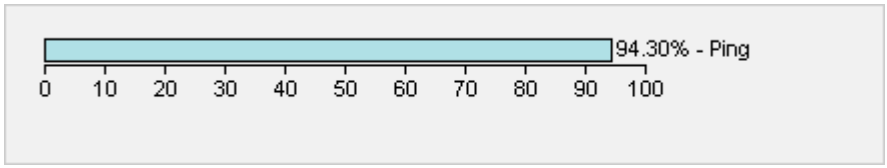
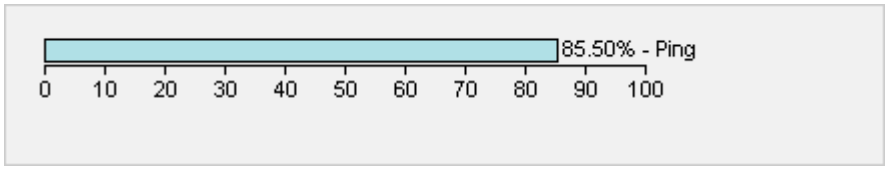
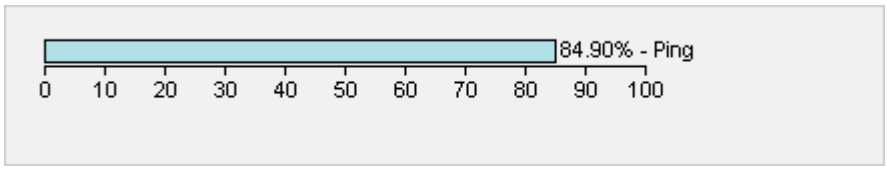
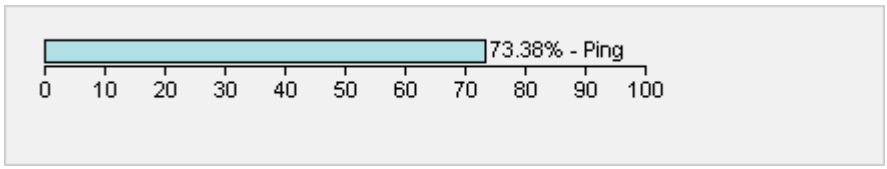
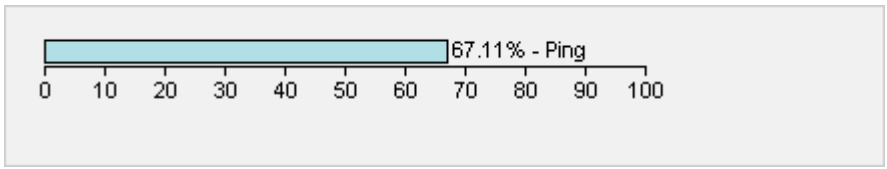
Dispositivo	Detalles
La Palma (Botrosa La Palma : 10.20.30.45)	
La Palma-Bijahual (Botrosa La Palma-Bijahual : 192.168.90.100)	
Bijahual-La Palma (Botrosa Bijahual-La Palma : 192.168.90.101)	
Bijahaul - El Vergel (Botrosa Bijahual - El Vergel : 192.168.90.102)	
El Vergel -Bijahual (Botrosa El Vergel-Bijahual:192.168.90.103)	

Tabla 2 - Dispositivos conectados a La Palma

En la **tabla 3,** se detallan los enlaces de la planta de extracción Quininde, específicamente los dispositivos que se encuentran conectados directamente a esta locación.

Quininde

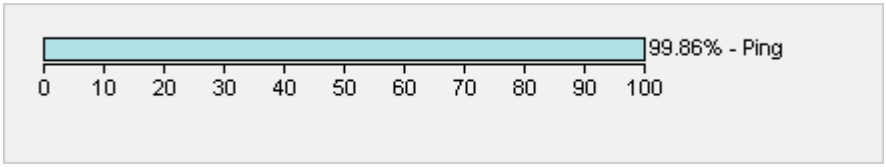
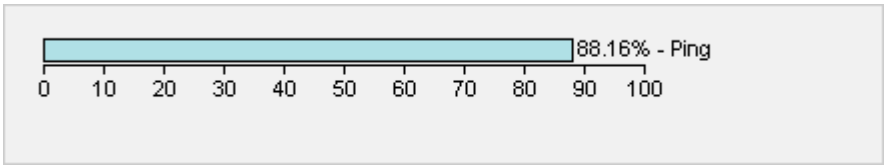
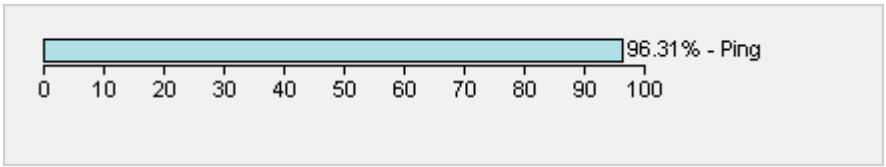
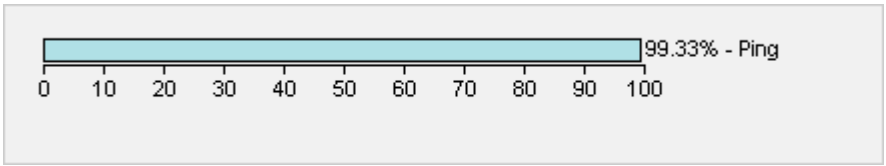
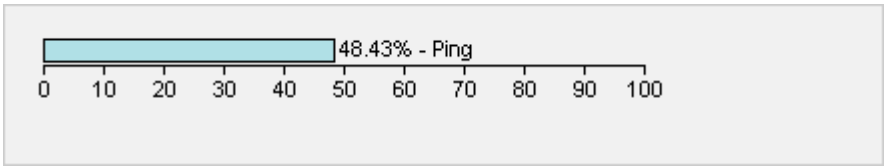
Dispositivo	Detalles
Quininde (Botrosa Quininde : 10.20.30.42)	
AP Principal WIFI (Botrosa Quininde Principal WIFI : 192.168.13.10)	
Producción Beta 2 - Principal (Botrosa Quinide WIFI Producción : 192.168.13.12)	
Producto Terminado - Principal (Botrosa Quininde WIFI Producto Terminado : 192.168.13.13)	
RRHH - Principal (Botrosa Quininde WIFI RRHH : 192.168.13.11)	

Tabla 3 - Dispositivos conectados a Quininde

En la **tabla 4,** se detallan los enlaces de la oficina y planta de procesamiento principal en Quito, específicamente los dispositivos que se encuentran conectados a esta locación.

Quito

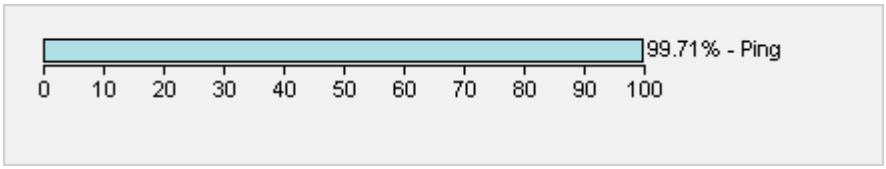
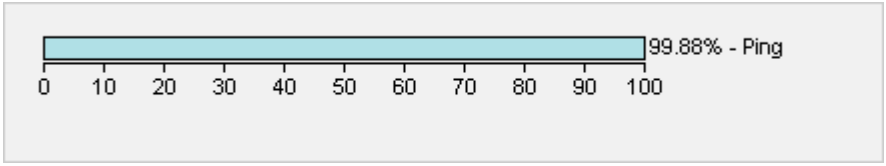
Dispositivo	Detalles
Quito Atacazo(Quininde) (Botrosa Quito-Atacazo (Quininde) : 10.20.30.33)	
Quito Atacazo(La Palma_Maldonado) (Botrosa Quito- Atacazo (La Palma) : 10.20.30.34)	

Tabla 4 - Dispositivos conectados a Quito

En la **tabla 5,** se detallan los enlaces de la repetidora Zapallo, específicamente los dispositivos que se encuentran conectados directamente a esta repetidora.

Zapallo

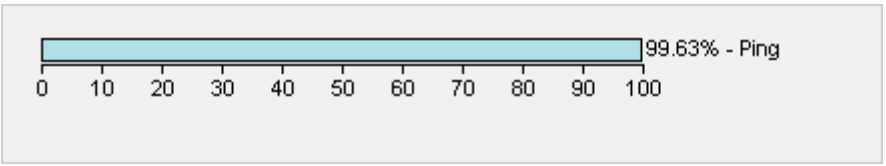
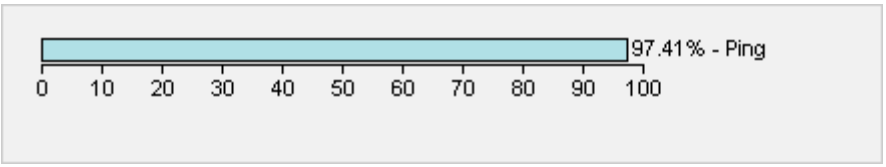
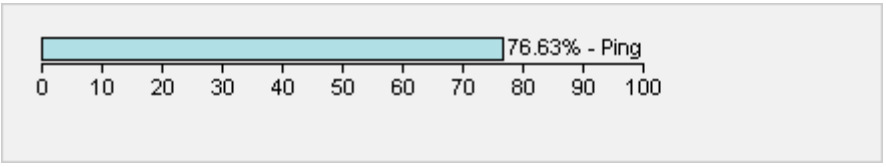
Dispositivo	Detalles
Equipo VLAN Zapallo (Fulldata Equipo VLAN Zapallo : 10.20.30.48)	
Zapallo (Botrosa Zapallo : 10.20.30.46)	
Maldonado (Botrosa Maldonado : 10.20.30.49)	

Tabla 5 - Dispositivos conectados a Zapallo

En la **tabla 6,** se detallan los enlaces de la repetidora Santo Domingo, específicamente los dispositivos que se encuentran conectados directamente a esta repetidora.

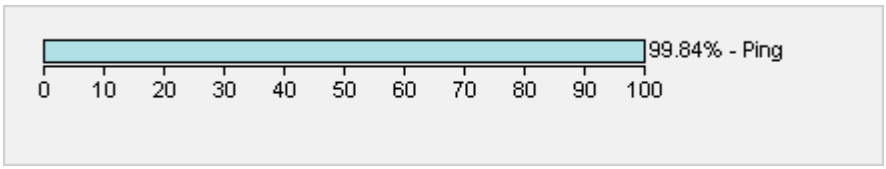
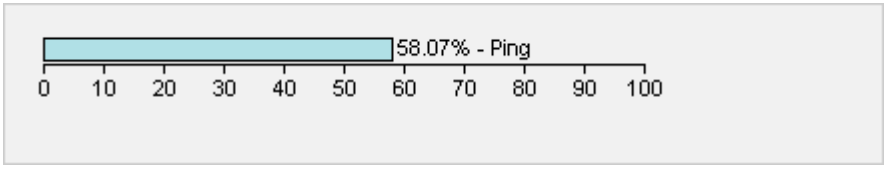
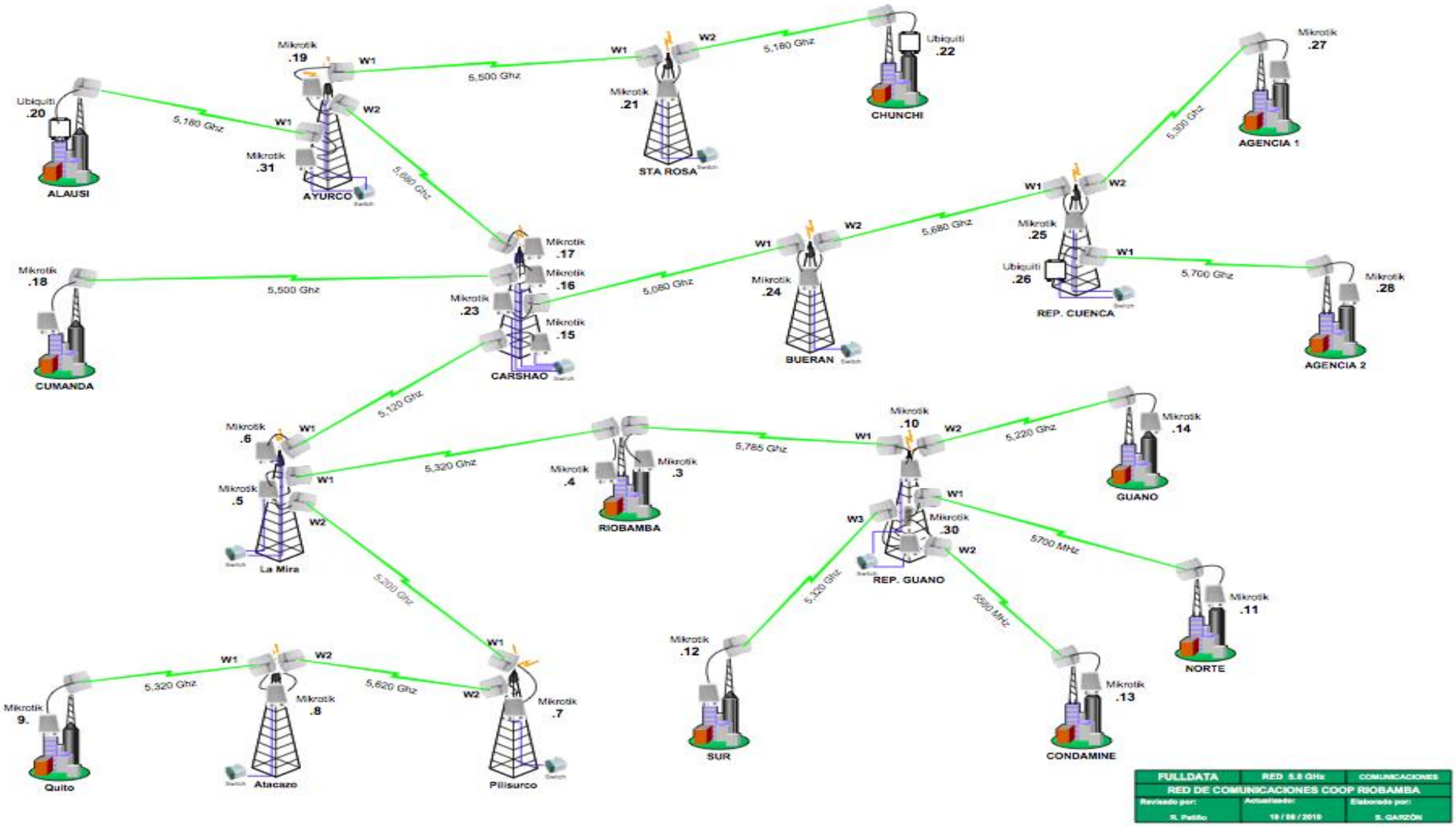
Sto.Domingo	
Dispositivo	**Detalles**
Sto. Domingo Atacazo (Botrosa Sto. Domingo-Atacazo): 10.20.30.43)	
Sto. Domingo La Palma (Botrosa Sto.Domingo-La Palma : 10.20.30.44)	

Tabla 6 - Dispositivos conectados a Santo Domingo

ANEXO No . 5

DIAGRAMA **COOPERATIVA RIOBAMBA LTDA.**



RED DE COMUNICACIONES DE LA COOPERATIVA RIOBAMBA 192.168.100.XX / 24

ANEXO No . 6

Tablas de Monitoreo de la **COOPERATIVA RIOBAMBA LTDA.**

En la **tabla 1,** se detallan los enlaces de la agencia ubicada en Alausi, específicamente los dispositivos que se encuentran conectados directamente a esta agencia.

Alausi

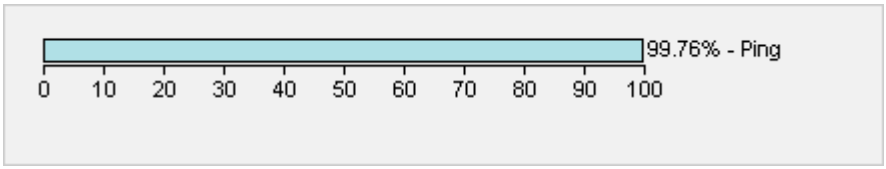
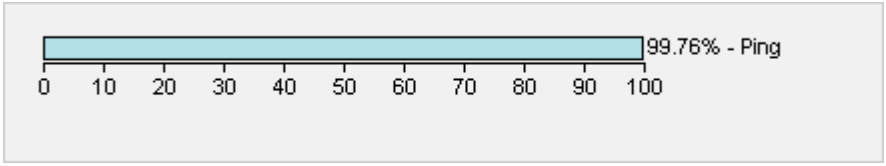
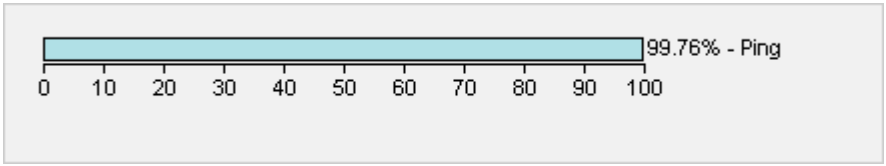
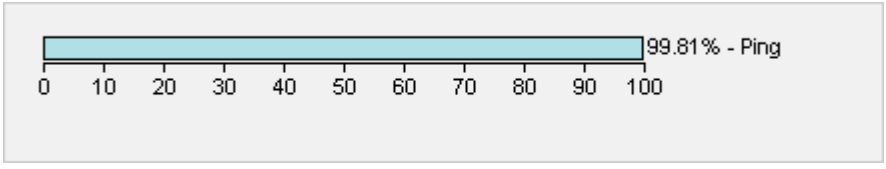
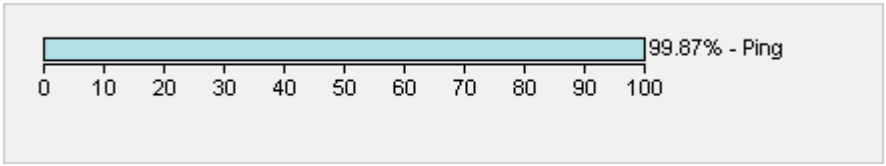
Dispositivo	Detalles
Rep. Ayurco - Rep. Sta. Rosa & Rep. Carzhao (Coop.Riobamba Rep.Ayurco1 : 192.168.100.19)	
Agencia Alausi (Coop. Riobamba Agencia Alausi : 192.168.100.20)	
Rep.Ayurco-Agencia Alausi (Coop.Riobamba Rep.Ayurco2 : 192.168.100.31)	

Tabla 1 - Dispositivos conectados a Alausi

En la **tabla 2,** se detallan los enlaces de la repetidora Carshao, específicamente los dispositivos que se encuentran conectados directamente a esta repetidora.

Carzhao

Dispositivo	Detalles
Rep.Carzhao-Rep.Lamira (Coop.Riobamba Rep.Carzhao1 : 192.168.100.15)	
Rep.Carzho-Agencia Cumanda (Coop.Riobamba Rep.Carzho2 : 192.168.100.16)	

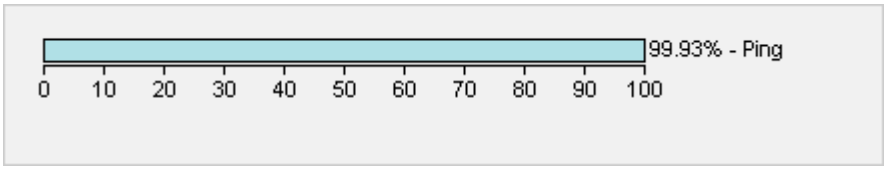
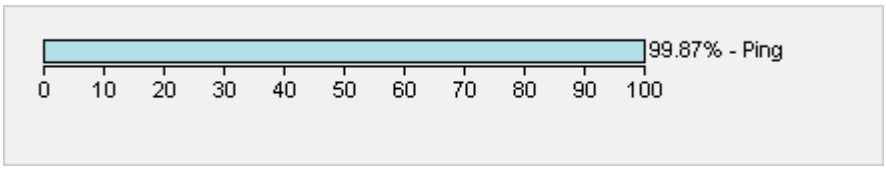
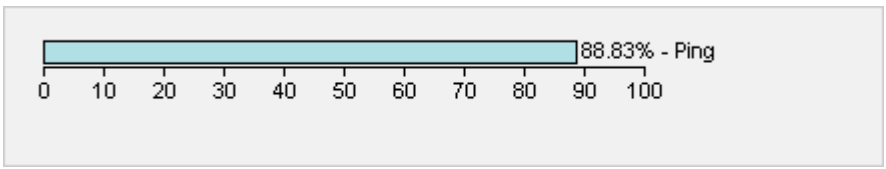
Rep.Carzhao-Rep.Ayurco (Coop.Riobamba Rep.Carzhao3 : 192.168.100.17)	
Rep.Carzhao-Rep.Bueran (Coop.Riobamba : 192.168.100.23)	
Agencia Cumanda (Coop.Riobamba.Ag.Cumanda : 192.168.100.18)	

Tabla 2 - Dispositivos conectados a la Repetidora Carshao

En la **tabla 3,** se detallan los enlaces de la agencia ubicada en Chunchi, específicamente los dispositivos que se encuentran conectados directamente a esta agencia.

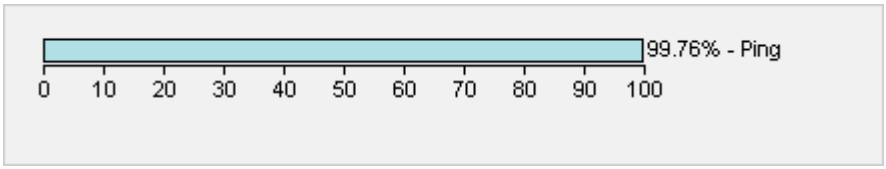
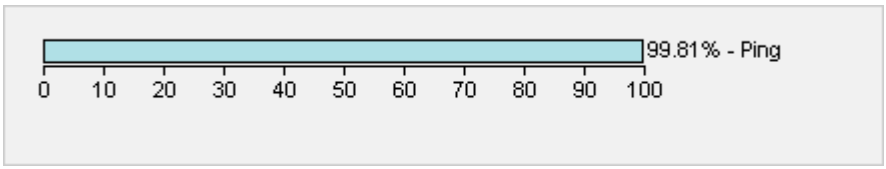
Chunchi	
Dispositivo	**Detalles**
Rep.SantaRosa (Coop.Riobamba Rep.SantaRosa : 192.168.100.21)	
Agencia Chunchi (Coop.Riobamba Agencia Chunchi : 192.168.100.22)	

Tabla 3 - Dispositivos conectados a Chunchi

En la **tabla 4,** se detallan los enlaces de la repetidora Cuenca, específicamente los dispositivos que se encuentran conectados directamente a esta agencia.

Cuenca

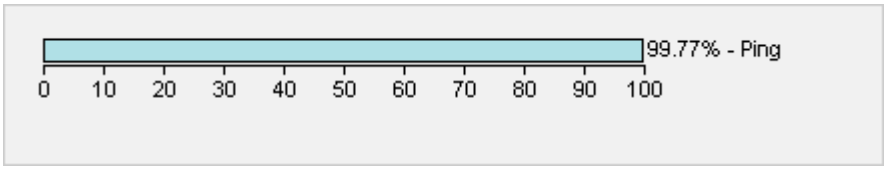
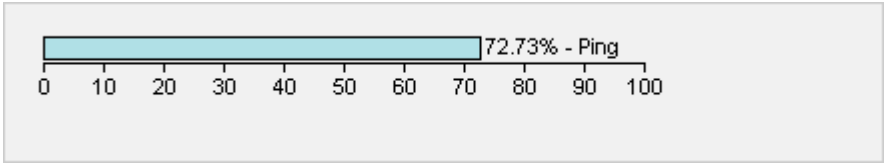
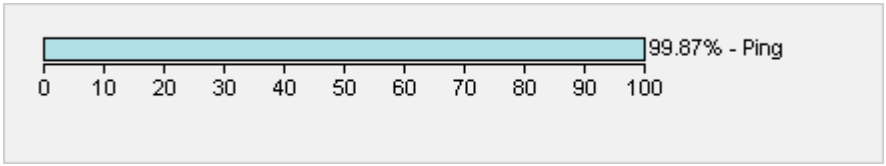
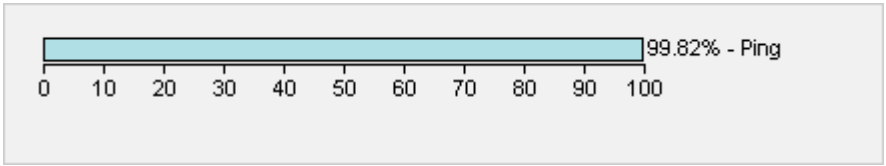
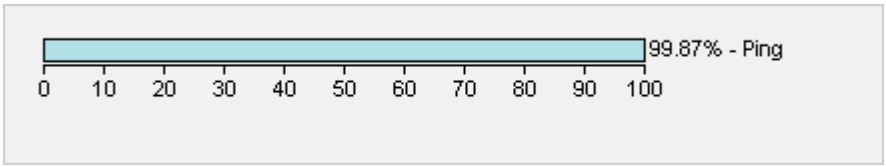
Dispositivo	Detalles
Cuenca Agencia El Arenal (Coop.Riobamba Agencia Cuenca El Arenal : 192.168.100.27)	
Cuenca Agencia Centro (Coop.Riobamba Agencia Centro : 192.168.100.28)	
Rep.Cuenca-AgenciaArenal&Rep.Bueran (Coop.Riobamba Rep.Cuenca#1 : 192.168.100.25)	
Rep.Cuenca-Agencia Centro (Coop.Riobamba Rep.Cuenca#2 : 192.168.100.26)	
Rep.Bueran (Coop.Riobamba Rep.Bueran : 192.168.100.24)	

Tabla 4 - Dispositivos conectados a la repetidora Cuenca

En la **tabla 5,** se detallan los enlaces de la agencia ubicada en Quito, específicamente los dispositivos que se encuentran conectados directamente a esta agencia.

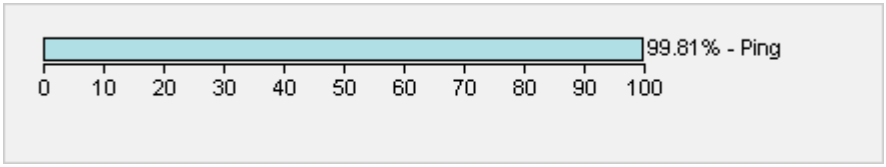
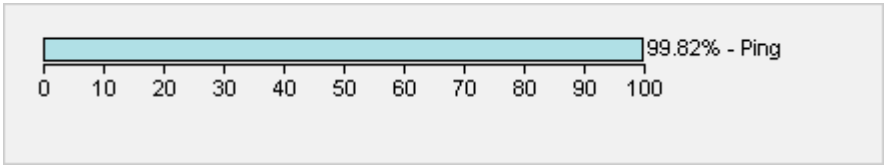
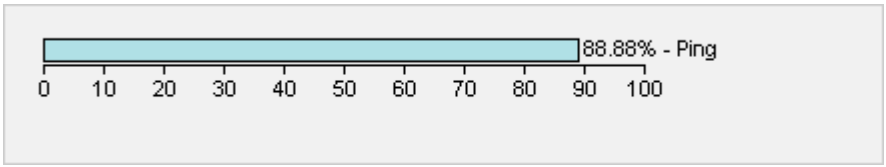
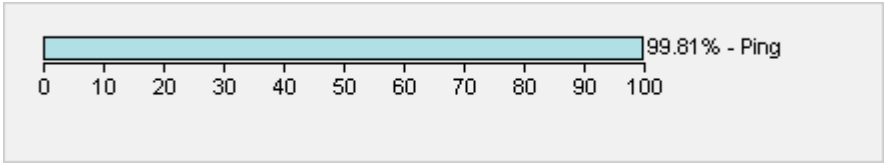
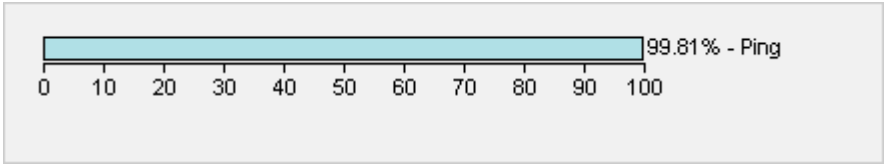
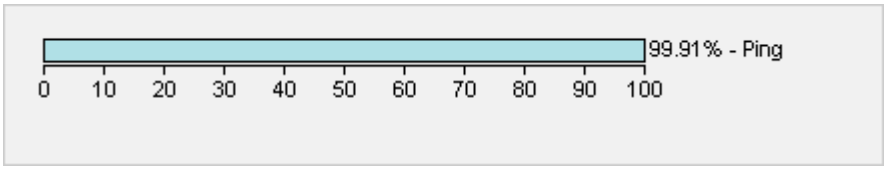
Quito	
Dispositivo	**Detalles**
Agencia Quito (Coop.Riobamba Agencia Quito : 192.168.100.9)	
Rep.Atacazo (Coop.Riobamba Rep.Atacazo : 192.168.100.8)	
Rep.Pilisurco (Coop.Riobamba Rep.Pilisurco : 192.168.100.7)	

Tabla 5 - Dispositivos conectados a la agencia Quito

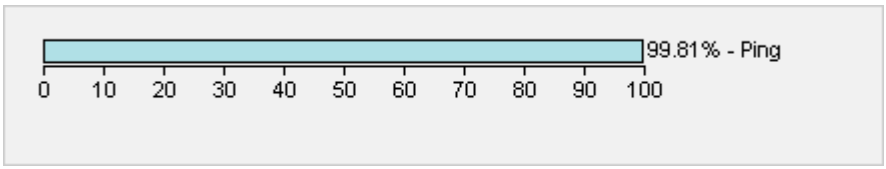
En la **tabla 6,** se detallan los enlaces de la ciudad de Riobamba, específicamente los dispositivos que se encuentran conectados en cada punto de esta ciudad.

Riobamba	
Dispositivo	**Detalles**
Rep.Guano-Matriz&Agencia.Guano (Coop.Riobamba_Rep Guano1 : 192.168.100.10)	
Matriz-Guano (Coop.Riobamba Matriz2 : 192.168.100.3)	

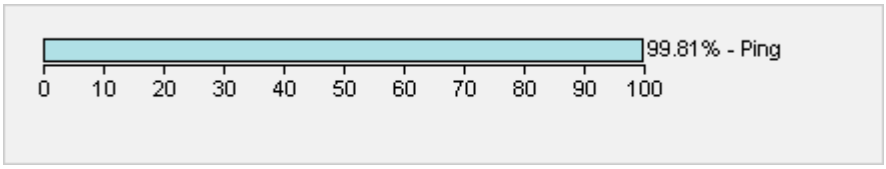
Agencia Norte (Coop.Riobamba Agencia Norte : 192.168.100.11)



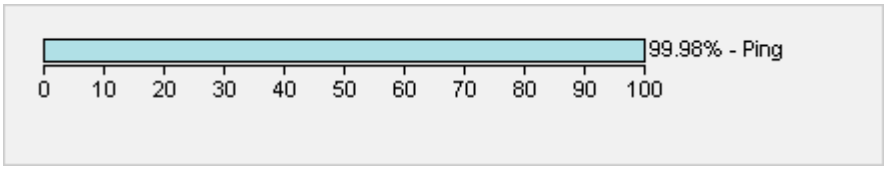
Agencia Sur (Coop.Riobamba Agencia Sur : 192.168.100.12)



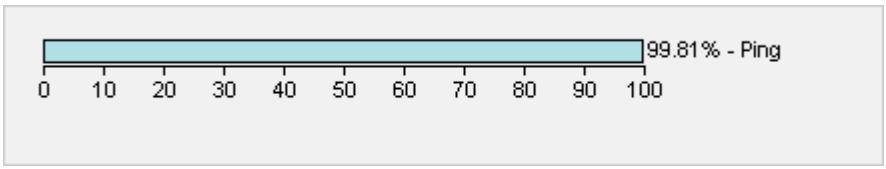
Agencia Condamine (Coop.Riobamba Agencia Condamine : 192.168.100.13)



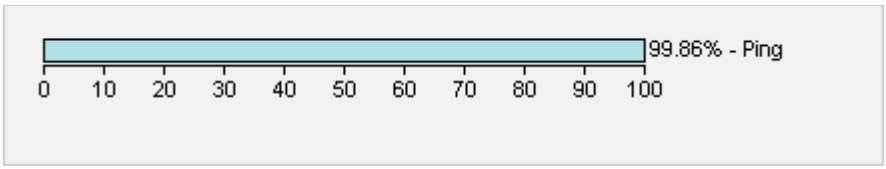
Agencia Guano (Coop.Riobamba Agencia Guano : 192.168.100.14)



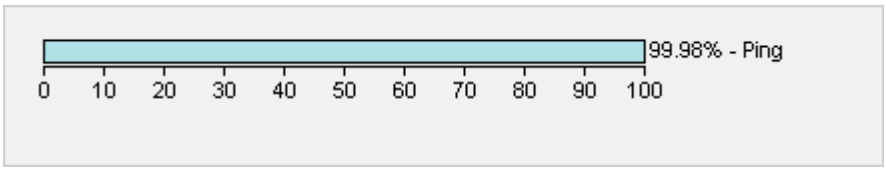
Rep.Guano-Sur&Condamine (Coop.Riobamba Rep.Guano2 : 192.168.100.30)



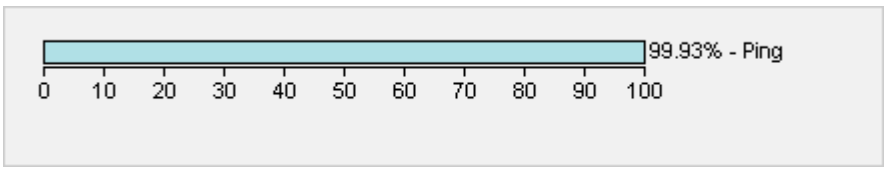
Matriz-La Mira (Coop.Riobamba Matriz1 : 192.168.100.4)



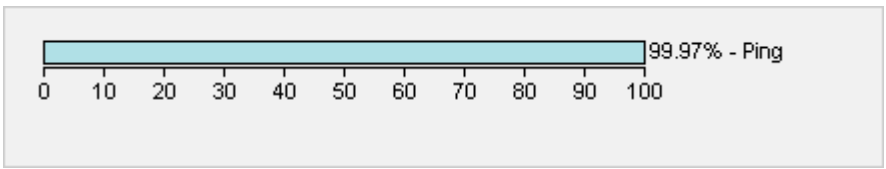
Rep.LaMira-Matriz&Pilisurco (Coop.Riobamba Rep.LaMira1 : 192.168.100.5)



Rep.LaMira-Carzhao (Coop.Riobamba Rep.LaMira2 : 192.168.100.6)



Rep.Guano-Agencia Norte (Coop.Riobamba_Rep.Guano3 : 192.168.100.29)



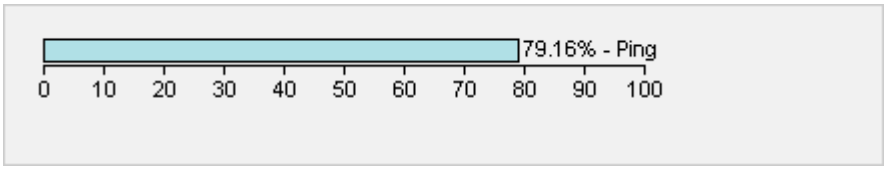
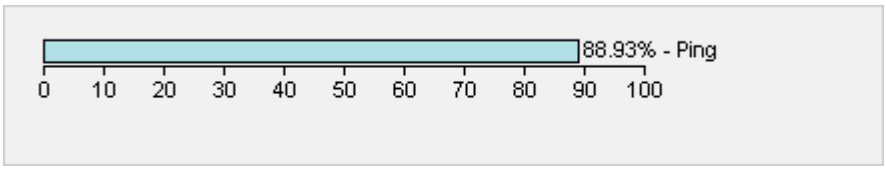
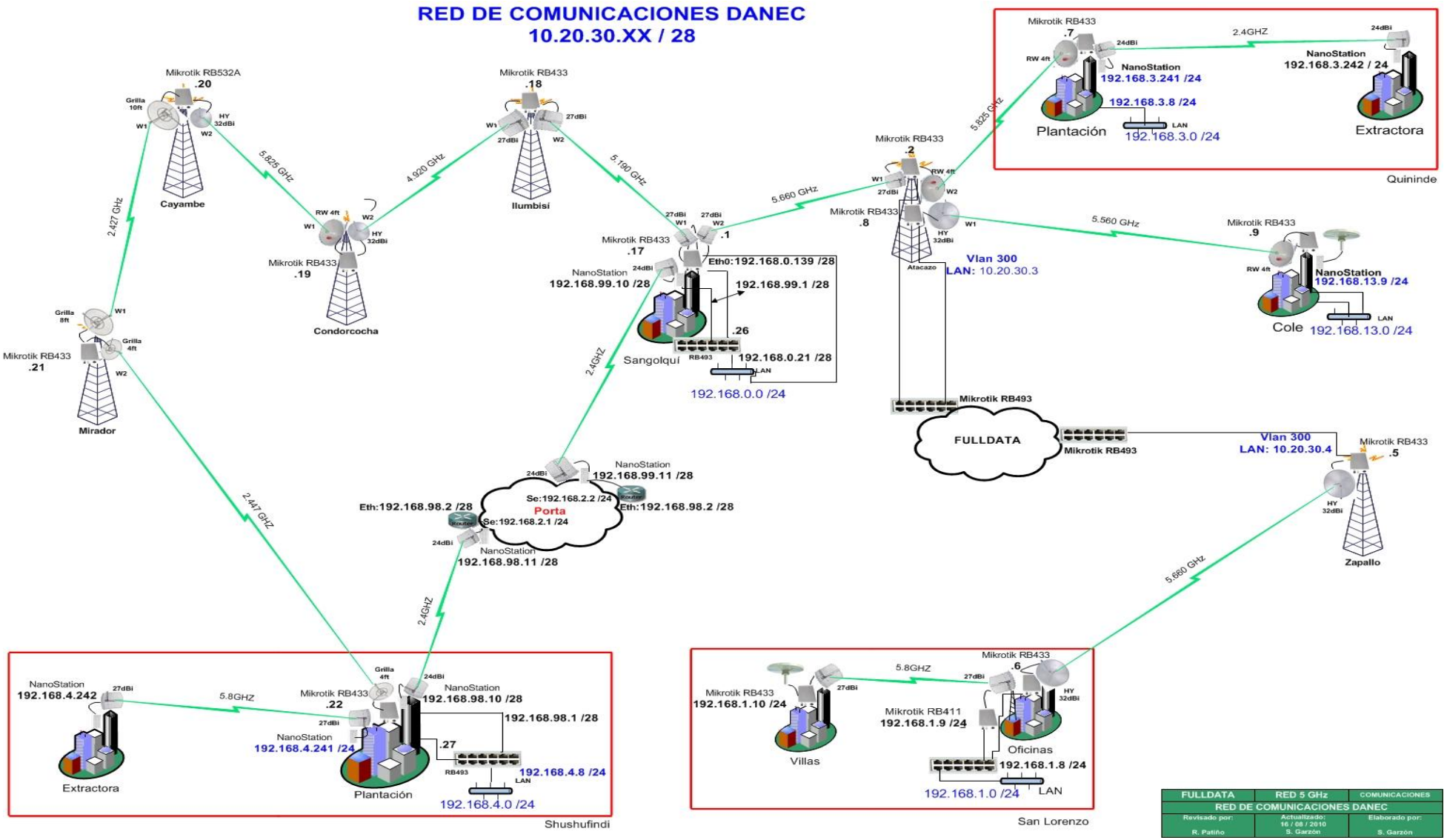
Agencia Davalos (Coop.Riobamba Agencia Davalos : 192.168.100.32)	
Matriz-Agencia Davalos (Coop.Riobamba Matriz3 : 192.168.100.33)	

Tabla 6 - Dispositivos conectados en Riobamba

ANEXO No. 7

DIAGRAMA **DANEC S.A.**



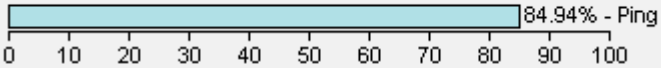
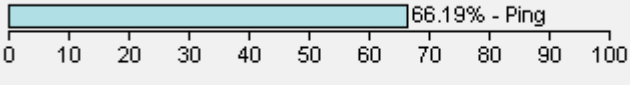
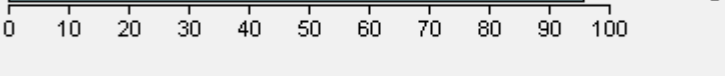
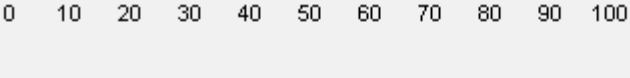
RED DE COMUNICACIONES DANEC 10.20.30.XX /24

ANEXO No. 8

Tablas de Monitoreo **DANEC S.A.**

En la **tabla 1,** se detallan los enlaces Backup de la región costa, específicamente los dispositivos que se encuentran en esta área.

BACKUP-DANEC COSTA

Dispositivo	Detalles
Puengasi (Danec BackUp Rep.Puengasi : 192.168.101.17)	
Condorcocha (Danec BackUp Rep.Condorcocha : 192.168.101.16)	
Sangolqui(Danec) (Danec BackUp Sangolqui : 192.168.101.18)	
Zapallo Juanita (Danec BackUp Rep.Zapallo-Rep.Juanita : 192.168.101.20)	
Juanita Zapallo (Danec BackUp Rep.Juanita-Rep.Zapallo : 192.168.101.19)	
Switch Rep.Juanita (Danec BackUp Switch Capa 3 Rep.Juanita : 192.168.101.1)	
Monitoreo Energia Juanita (Danec BackUp Monitoreo Energia Rep.Juanita : 192.168.101.50)	

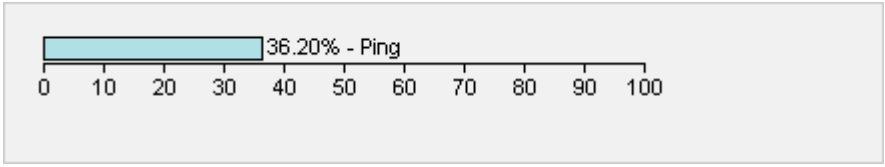
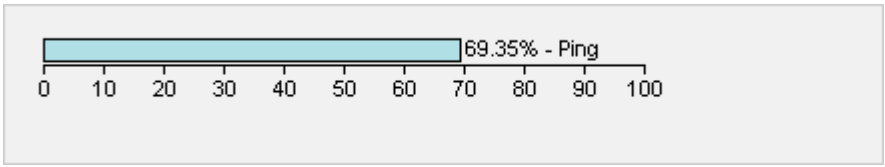
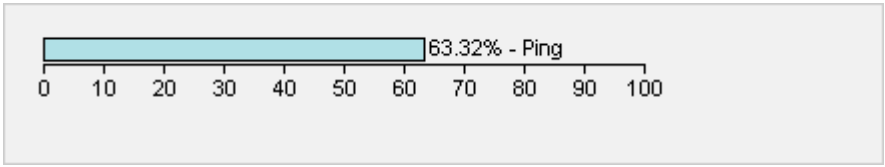
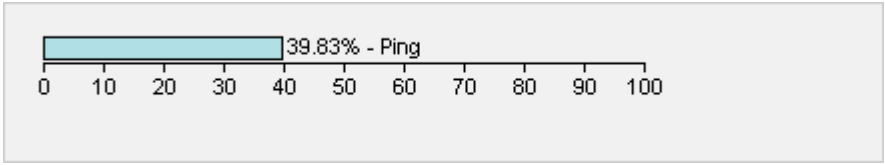
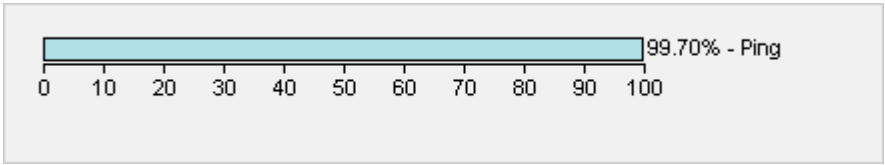
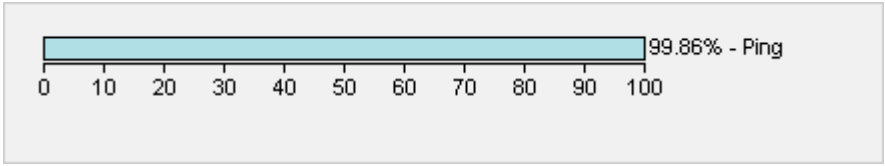
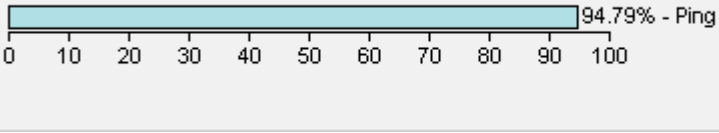
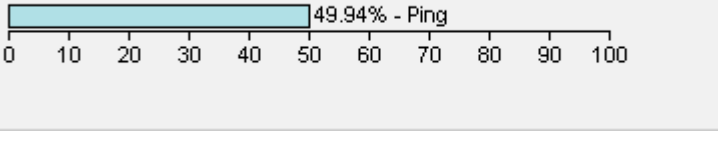
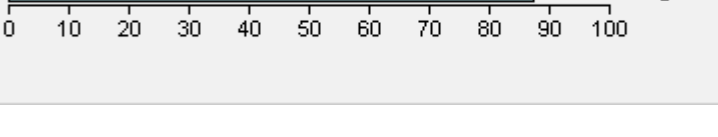
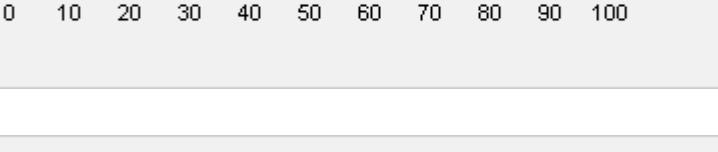
Rep.Juanita Enlaces Quininde (Danec BackUp Rep.Juanita-Plantacion/Extractora : 192.168.101.11)	
Rep.Juanita Rep.Condorcocha (Danec BackUp Rep.Juanita-Rep.Condorcocha : 192.168.101.10)	
Cole Rep.Juanita (Danec BackUp Cole hacia Rep.Juanita : 192.168.101.15)	
Rep.Juanita Cole (Danec BackUp Rep.Juanita hacia Cole : 192.168.101.14)	
Extractora-Juanita (Danec BackUp Extractora Rep.Juanita : 192.168.102.4)	
Plantacion-Juanita (Danec BackUp Plantacion-Rep.Juanita : 192.168.101.13)	

Tabla 1 - Dispositivos conectados a Región Costa

En la **tabla 2,** se detallan los enlaces principales de la región costa, específicamente los dispositivos que se encuentran en esta área.

Costa

Dispositivo	Detalles
Sangolqui - Atacazo (DANEC Sangolqui : 10.20.30.12)	
Atacazo Sangolqui (DANEC Atacazo : 10.20.30.2)	
Zapallo (DANEC Zapallo : 192.168.1.247)	
Quininde (DANEC Quininde : 10.20.30.11)	
Monitoreo Energia Zapallo (10.20.30.14)	
Atacazo-Cole (Danec Atacazo-Cole : 10.20.30.8)	
Atacazo-Quininde (DANEC Atacazo-Sangolqui : 10.20.30.10)	

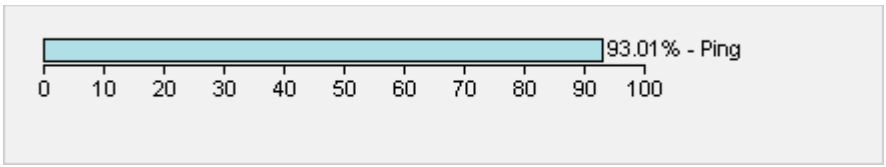
Monitoreo energia Atacazo Norte (Danec - Cole : 10.20.30.13)	

Tabla 2 - Dispositivos conectados a la Región Costa

En la **tabla 3,** se detallan los enlaces en Quininde, específicamente los dispositivos que se encuentran conectados en esta locación.

Quininde

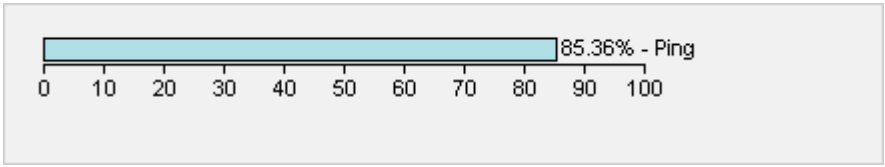
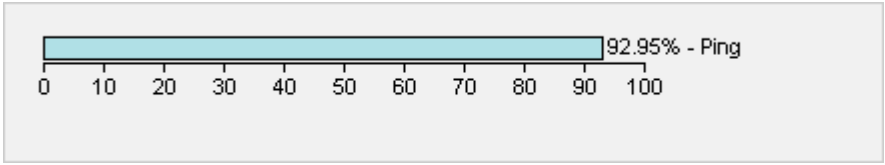
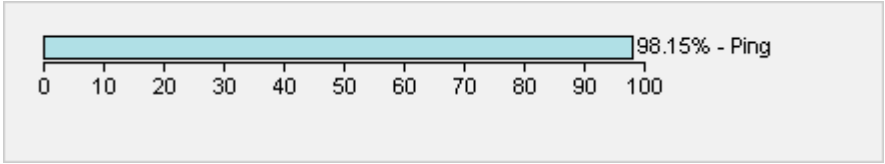
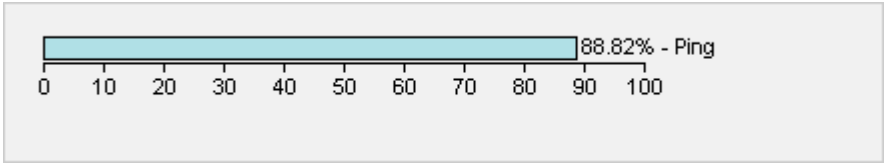
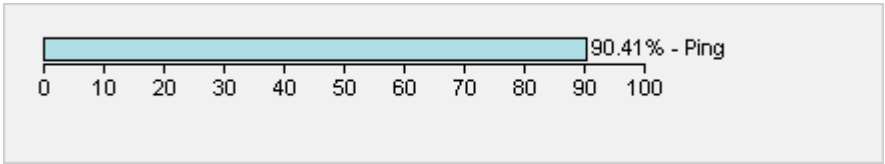
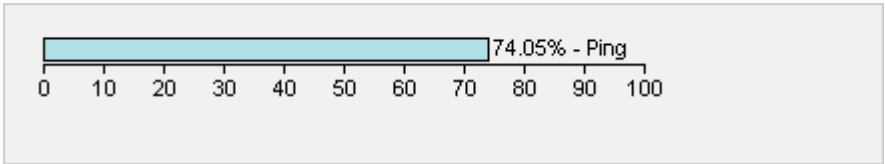
Dispositivo	Detalles
Base_Extractora (DANEC Extractora : 192.168.3.180)	
Quinta Semillero (DANEC Quinta Semillero : 192.168.3.181)	
Quinta Muleria (DANEC Quinta Muleria : 192.168.3.182)	
Sexta Muleria (DANEC Sexta Muleria : 192.168.3.183)	
Plantación (DANEC Plantación : 10.20.30.138)	
Extractora (DANEC Extractora : 10.20.30.139)	

Tabla 3 - Dispositivos conectados a Quininde

En la **tabla 4,** se detallan los enlaces en San Lorenzo, específicamente los dispositivos que se encuentran conectados en cada punto de esta locación

San Lorenzo

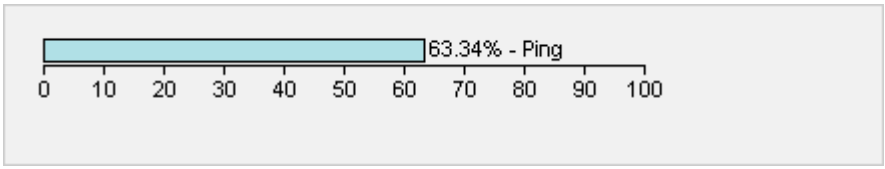
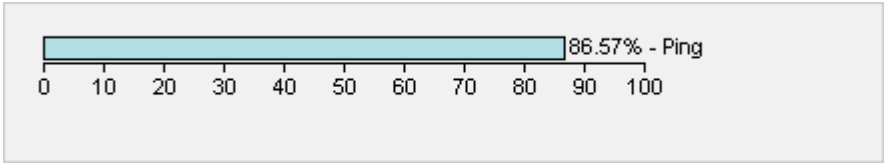
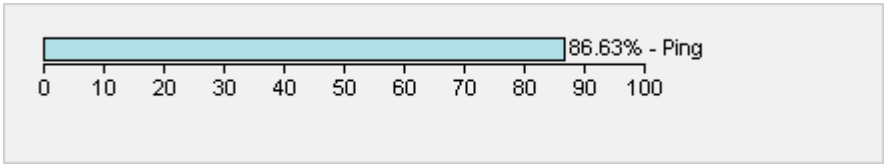
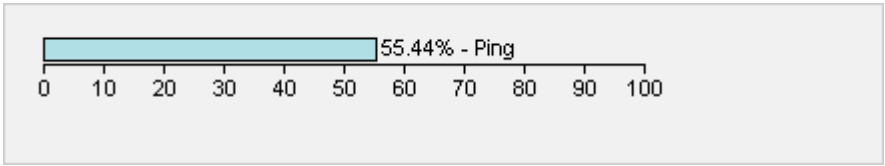
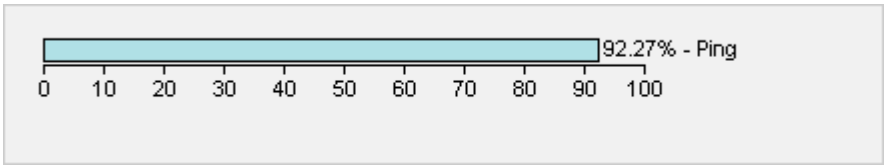
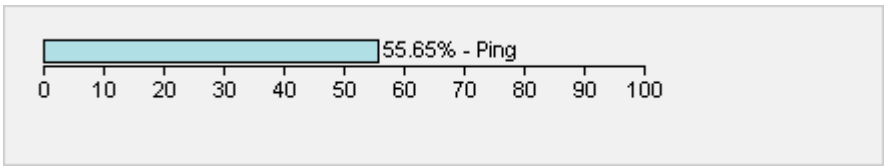
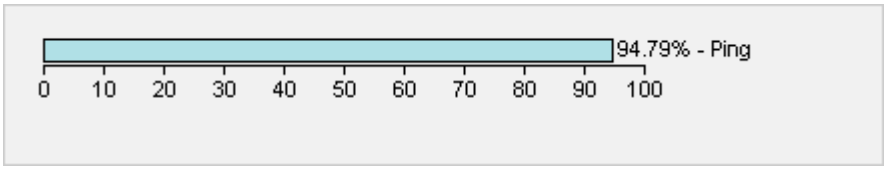
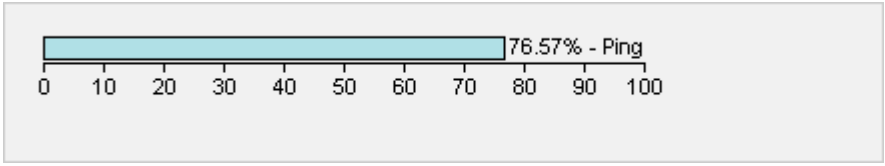
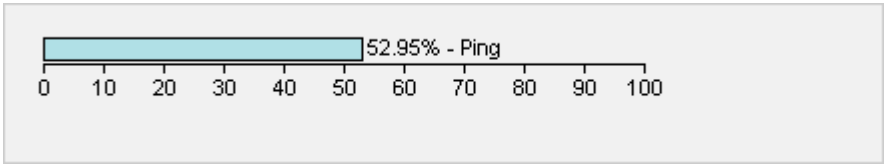
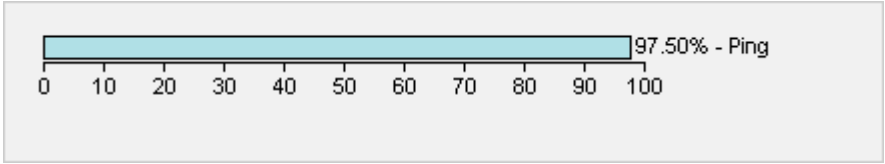
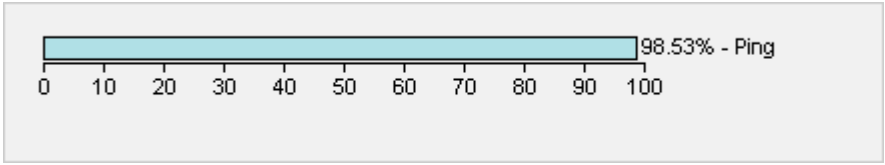
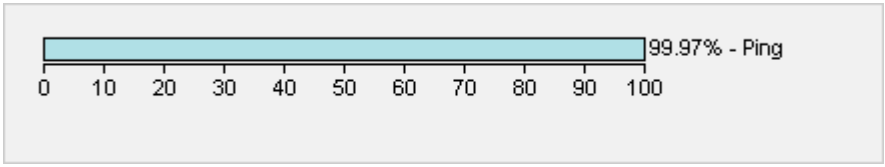
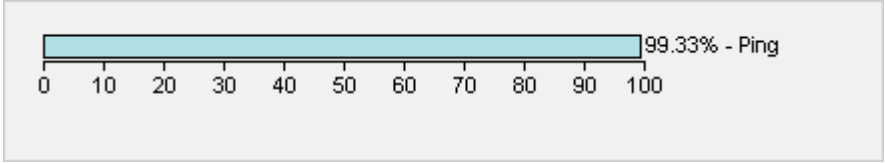
Dispositivo	Detalles
San Lorenzo (DANEC San Lorenzo : 192.168.1.246)	
Base Enlaces a relojes biometricos (Danec AP relojes Biometricos : 192.168.1.225)	
Chanul (Danec San Lorenzo Chanul : 192.168.1.226)	
Najurungo Garita (Danec San Lorenzo_Najurungo Garita : 192.168.1.227)	
Najurungo Campamento (Danec Najurungo Campamento : 192.168.1.228)	
Ecuafinca (Danec Ecuafinca : 192.168.1.229)	

Tabla 4 - Dispositivos conectados a San Lorenzo

En la **tabla 5,** se detallan los enlaces de la Región del Oriente, específicamente los dispositivos que se encuentran conectados en cada punto de esta región

Oriente

Dispositivo	Detalles
Sangolqui - Atacazo (DANEC Sangolqui : 10.20.30.12)	
Ilumbisi - Sangolqui - Condorcocha (DANEC Ilumbisi : 10.20.30.18)	
Condorcocha - Cayambe - Ilumbisi (DANEC Condorcocha : 10.20.30.19)	
Mirador -Cayambe (DANEC Mirador : 10.20.30.21)	
Shushufindi - Mirador (DANEC Shushufindi : 10.20.30.22)	
Cayambe-Mirador (DANEC Cayambe-Mirador : 10.20.30.20)	
Cayambe Energia (Monitoreo Energia Cayambe : 10.20.30.29)	

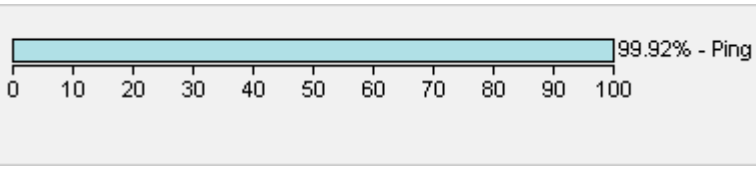
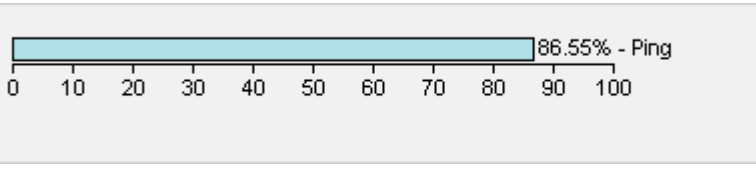
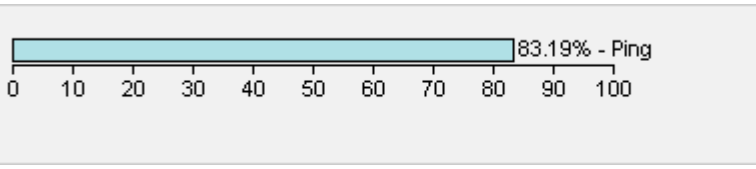
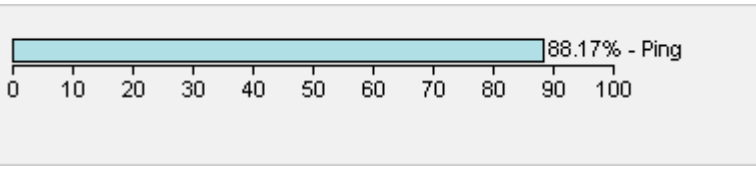
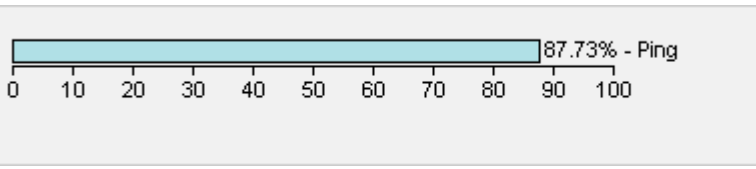
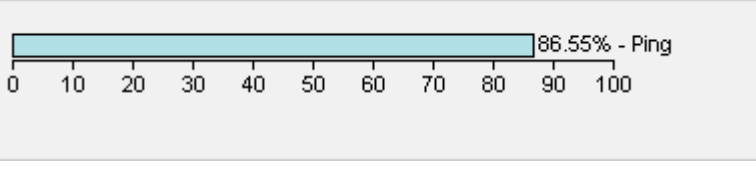
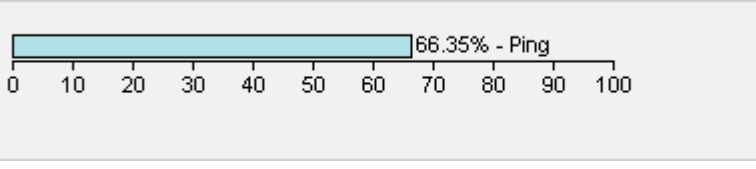
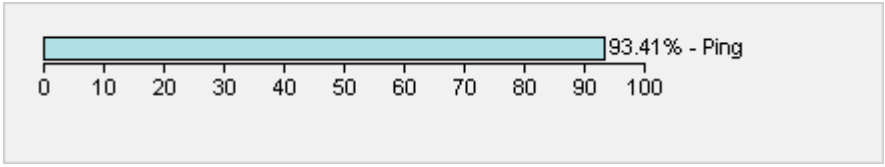
Switcheo Autom.Quito (Bonding Quito : 10.20.30.26)	
Switcheo Autom.Shushufindi (Bonding Shushufindi : 10.20.30.27)	
Mirador - Shushufindi (DANEC Mirador-Shushufindi : 10.20.30.28)	
Cayambe - Condorcocha (DANEC Cayambe-Condorcocha : 10.20.30.23)	
Sangolqui-Ilumbisi (Danec - Sangolqui-Ilumbisi : 10.20.30.17)	

Tabla 5 - Dispositivos conectados hacia el Oriente

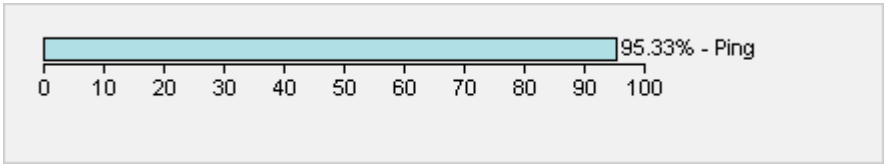
En la **tabla 6,** se detallan los enlaces de Shushufindi, específicamente los dispositivos que se encuentran conectados en cada punto de esta locación.

Shushufindi	
Dispositivo	**Detalles**
Switcheo Autom.Shushufindi (Bonding Shushufindi : 10.20.30.27)	
Muleria 6 (Danec Muleria 6 : 192.168.4.218)	

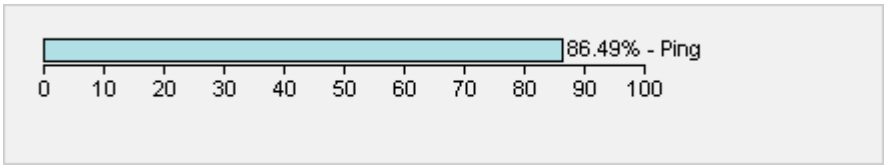
Extractora -Oficinas (Danec Extractora-Oficinas : 192.168.4.242)



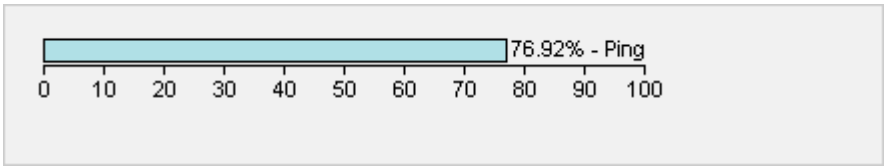
Extractora-Muleria 6 (Danec Extractora-Muleria6 : 192.168.4.217)



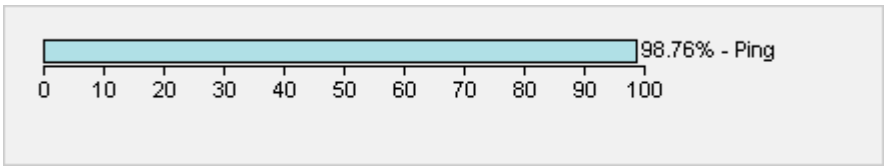
Oficinas -Villas & Muleria 12 (Danec Oficinas hacia Villas & Muleria12 : 192.168.4.176)



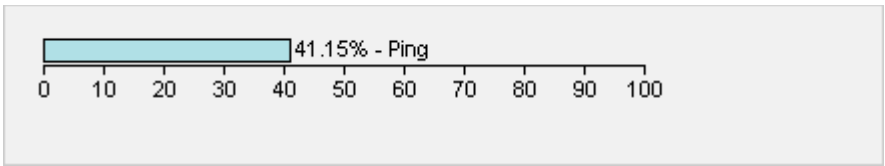
Muleria 12- Muleria 8 & Oficinas (Danec Muleria12 hacia Muleria 8& Oficinas : 192.168.4.203)



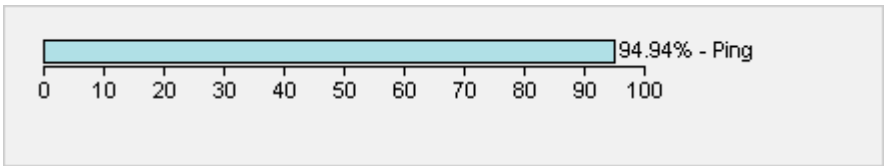
Muleria 12 - Aceipa (Danec Muleria 12 hacia Aceipa : 192.168.4.219)



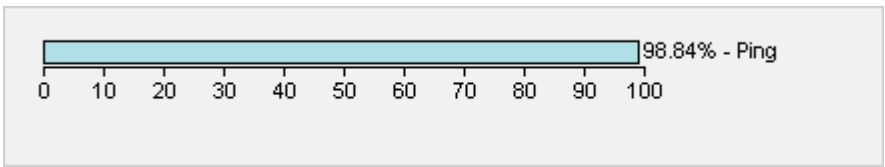
Aceipa (Danec Aceipa : 192.168.4.216)



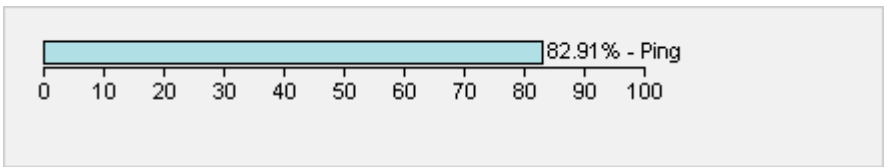
Muleria 8 (Danec Muleria 8 : 192.168.4.214)



Vivero (Danec Vivero : 192.168.4.215)



Villas-Oficinas (Danec Villas hacia Oficinas : 192.168.4.177)



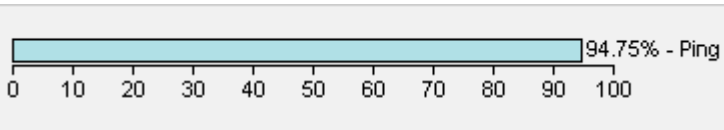
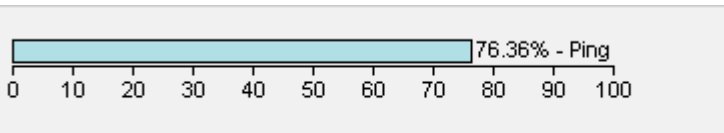
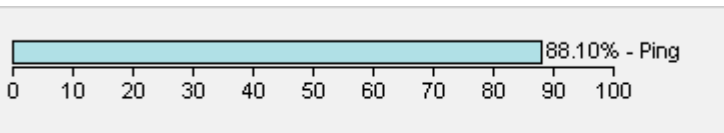
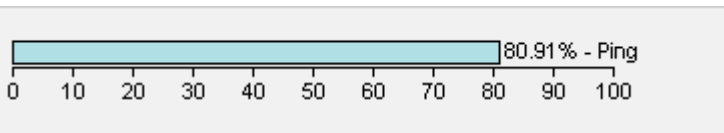
Villas - Muleria2&Muleria5 (Danec Villas hacia Muleria 2 & Muleria 5 : 192.168.4.210)	
Muleria 2 (Danec Muleria 2 : 192.168.4.211)	
Oficinas - Extractora (Danec Oficinas - Extractora : 192.168.4.241)	
Muleria 5 (Danec Shushufindi Muleria 5 : 192.168.4.202)	

Tabla 6 - Dispositivos conectados a Shushufindi

En la **tabla 7,** se detallan los enlaces de la ciudad de Quito en sus oficinas principales, específicamente los dispositivos que se encuentran conectados en cada punto de esta ciudad.

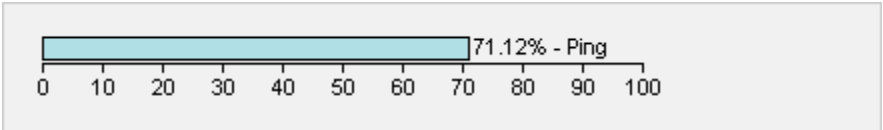
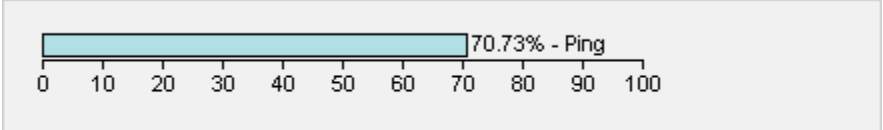
QUITO	
Dispositivo	**Detalles**
Rep.Ilumbisi -Casa William Tito (DANEC Ilumbisi-Casa William Tito: 10.20.32.10)	
Casa William Tito (DANEC William Tito: 10.20.32.11)	

Tabla 7 - Dispositivos conectados a Quito

ANEXO No . 9

REVISIÓN DE FUNCIONES A EMPLEADOS DE FULLDATA CIA. LTDA.

DESCRIPCIÓN DE FUNCIONES

NOMBRE: LINDA VALDIVIESO	**FECHA:** 02/08/12
CARGO: SECRETARIA RECEPCIONISTA Y ASISTENTE DEL DEPARTAMENTO TÉCNICO	
AREA: ADMINISTRATIVA	**REVISADO POR:**

SECCIÓN 1

Objetivo del cargo

(Resumen en un párrafo el propósito o papel de su cargo, describiendo el aporte fundamental del cargo en términos de que hace y para qué lo hace).

Apoyo Administrativo (todos los Departamentos) en cuestión comunicación (llamadas) y documentación para mejor coordinación de la empresa y desempeño de todos.

SECCIÓN 2

Descripción de funciones

(Describa, cómo sabe lo que hizo, el tiempo que emplea en hacerlo y la frecuencia)

Funciones principales (¿Qué hace?)	Forma de medir el logro (¿Cómo se sabe que lo hizo?)	Tiempo empleado	Frecuencia
Recepción y elaboración de llamadas	Se comunica a la persona que solicita o se receptan mensajes	de 5 a 15 min	Todos los días
Manejo del archivo de toda la empresa (facturas y contratos de clientes, informes técnicos, carpetas del personal, contratos repetidoras, documentos originales de la empresa como RUC, patente, nombramiento, etc)	Bandeja de entrada y salida vacías (documentos en carpetas)	1 a 2 h diarias	Todos los días
Control de llamadas de reportes de daños de clientes (CRM)	Se registra y se reporta al DT para atención inmediata	5 minutos	Todos los días

Elaboración y control de informes técnicos (sistema y excel)	Informes registrados y entregados deben ser devueltos y archivados (carpetas clientes)	1 a 2 h diarias	Todos los días
Comunicación por handy con personal técnico	Se comunica con personal para informar al cliente de los avances o novedades	Depende	Depende
Control de llaves de repetidoras	Registro (entrega y recepción de las mismas)	5 minutos	Depende
Reserva de vuelos para el personal	se envía orden se servicio por fax, se confirma y se archiva	Depende	Depende
Reserva de hoteles para el personal con convenio (Italia, Casa Alianza)	Envío de solicitud por fax se confirma y se archiva	15 minutos	Depende
Elaboración de: cartas, memos, comunicados, cronogramas, proformas, solicitudes, avisos, etc (clientes, personal, proveedores)	Se mantiene una copia con la firma de recepción para el archivo y constancia de los mismos o para seguimiento	1 a 2 h diarias	Todos los días
Elaboración de facturación (servicio técnico, venta de equipos por parte del DT, nuevos enlaces y mantenimientos por parte del DT, senatel)	Control en excel, control en archivos de contabilidad y carpeta de clientes	1 hora	4 a 6 veces al mes
Actualización de documentos legales de la empresa (certificado Super de Bcos, Super de Cia, CCQ, CCA)	Carpeta de documentos originales al día para uso de (Ventas y Contabilidad)	1 a 3 días	1 a 2 veces al mes
Elaboración de acta y seguimiento de la misma (reunión semanal y actividades programadas del DT)	Carpeta (Reunión todos los lunes) DT	1 hora	Depende
Manejo de caja chica (año 2012 un arqueo)	Se crea en el sistema y se imprime	5 minutos	Todos los días
Pago a proveedores (solo entrega de cheques elaborados en contabilidad)	Entrega de cheques y retenciones (facturas firmadas)	Tarde	Ocasionalmente
Compra y control de suministros (año 2012 kardex)	Registro (recepción-facturación y entrega de los mismos)	1 hora	1 a 2 veces al mes
Actualización de números telefónicos y mail de clientes	Registro en directorio telefónico y sistema	5 minutos	Esporádico
Control de Liquidaciones (de acuerdo a la fecha de entrega al departamento de contabilidad)	Recepción y aprobación (Gerente General) entrega (Contabilidad)	5 a 10 minutos	Depende
Coordinación trámites (senatel), solicitud y seguimiento de documentos (Clientes)	Cuadro de Registro (Facturación)	1 hora	Depende
Recepción de documentos, (sobres, cartas, facturas y varios documentos)	Archivo carpetas (clientes) # de ingreso a la Senatel	varias semanas	Depende

Funciones Adicionales (¿Qué hace?)	**Forma de medir el logro (¿Cómo se sabe que lo hizo?)**	**Tiempo empleado**	**Frecuencia**

Con Bodega (Entrega de equipos dañados a clientes)	Coordinación con bodega para envío de equipos dañados y factura respectiva a clientes	1 a 2 horas	Esporádico
Con Departamento de Ventas	Impresión de facturas, sobres y guías para envío a provincias (courier) y dentro de la ciudad	1 a 2 horas	1 vez al mes
Con Departamento de Contabilidad	Elaboración de factura reembolso suministro (Iseyco) (Nelson Hidalgo) CNT impresión de formularios décimos, utilidades y notas de crédito, envío de retenciones por fax o mail	5 minutos	1 vez al mes
Con Departamento de Contabilidad y Ventas (en las vacaciones de Ximena se ha encargado hacer la gestión de seguimientos tanto con el Dpto de Ventas como con la aseguradora colseguros) proyectos OCP	Elaboración de Pólizas y Pagares	20 minutos	Depende

SECCIÓN 3

Mecanismos adicionales

¿Qué mecanismos adicionales requeriría usted para desempeñarse mejor en su trabajo?. Ponga resumidamente su justificación.

Requerimientos	Justificación
Ayuda y colaboración del DT para agilitar trabajos.	Entrega de Informes Técnicos a tiempo claros y completos.

SECCIÓN 4

Facultad para tomar decisiones

Describa las decisiones que toma que se deriven de la realización de sus funciones y de las atribuciones otorgadas a su cargo.

Decisiones tomadas por si mismo	Decisiones que se toman consultando la superior
Asignación de clientes a técnicos	Envío de técnicos para atenciones a clientes (agencias, repetidores, etc)
	Compra de suministros

SECCIÓN 5

Relación de Trabajo

(Describa los contactos más frecuentes que usted mantiene en razón de su cargo, tanto internos como externos con personas, organizaciones, entidades, etc. Y describa en forma breve el propósito de los mismos).

Relaciones dentro de la Empresa (¿Con quién?)	Naturaleza o propósito (¿Para qué?)
Departamento Técnico	Asistente del DT
Departamento de Ventas	Pedido de información (costos movilización terrestre y aérea)
Departamento de Contabilidad	Envío de facturas y pago a proveedores
Bodega	Aviso de entrega y salida de mercadería
Gerencia General	Aprobaciones (suministros, liquidaciones)
Mensajería	Envío o retiro de documentos varios (facturas, cartas, certificados, ordenes de compra, etc)
Relaciones fuera de la empresa (¿Con quién?)	**Naturaleza o propósito (¿Para qué?)**
Clientes	Llamadas (varios departamentos, reportes de daños, proformas, confirmaciones de soluciones, varios)
Cobradores/Proveedores	Pagos o recepción (facturas, retenciones)
Mensajeros	Recepción de documentos varios (sobres, cartas)

SECCIÓN 6

Perfil Personal

Formación Académica
Primaria: Escuela "República de Venezuela"

Secundaria: Colegio Nacional Experimental Simón Bolívar
Título: Bachiller en Comercio y Administración "Secretaria en Español"
Cursos Adicionales
Grupo Portal "Asistente de Gerencia"
Corfore "Secretaria Ejecutiva"
Secap "Auxiliar Técnico en Computación"
Boehringer Infelheim "Marketing de Servicios"
Instituto Tecnológico Corporativo Latino "Técnicas Secretariales Modernas"

Experiencia Previa antes del Cargo Actual	Tiempo
Secretaria de Gerencia y Ventas	6 años

ANEXO No . 10

EVALUACIÓN DE ACTITUDES-APTITUDES, PRODUCTIVIDAD Y DESEMPEÑO DE FULLDATA CIA. LTDA.

PROCESO DE EVALUACION DE ACTITUDES- APTITUDES, PRODUCTIVIDAD Y DESEMPEÑO

DEPENDENCIA EVALUADA: DEPARTAMENTO TECNICO

INSTRUCTIVO:

En primera instancia se realizará un análisis, evaluando actitudes, identificando cuales son los puntos fuertes o FORTALEZAS, y los puntos débiles o DEBILIDADES., una vez consciente en estos dos puntos, se reflexiona sobre aquellos aspectos de formación académica y conocimientos que considere que pueden representar una ventaja o un punto fuerte:

INSTRUMENTO PARA EVALUAR ACTITUDES

Nombre del empleado: _____

Gerencia o coordinación: _____

Puesto que desempeña: _____

Período que se evalúa: de _____ a _____
(fecha) (fecha)

CUADRO DE ACTITUDES

CONCEPTOS A EVALUAR	0	1	2	3	4	5	6	7
Trabaja por objetivos								
Trabaja bajo presión con agrado								
Valora la seguridad y estabilidad que le brinda la compañía								
Acepta retos en solitario								
Tiene poder de decisión en el trabajo								
Es entusiasta en lo que realiza								
Acepta responsabilidades y acepta cuando comete errores								
No le agrada trabajar sólo								
Total Evaluación: Calificación sobre 40								

CUADRO DE APTITUDE

CONCEPTOS A EVALUAR	0	1	2	3	4	5	6	7
Identificación de problemas								
Nuevas aproximaciones a problemas								
Facilidad para investigar								
Capacidad de liderazgo								
Trabajo en equipo								

Planificación de tareas								
Organización efectiva del Tiempo								
Trabajo Individual								
Seguimiento de Instrucciones								
Proyectos a largo plazo								
Total Evaluación: Calificación sobre 50								

PRODUCTIVIDAD

#	CONCEPTOS A EVALUAR	0	1	2	3	4	5	6	7
1	Preparación de infraestructura e instalaciones eléctricas								
2	Instalación de equipos, y antenas								
3	Configuración de equipos y pruebas								
4	Proyecto entregado a tiempo y sin errores								
45	El empleado propuso la solución de algún problema importante								
6	El empleado no demostró preocupación por resolver ningún problema								
7	No ideó nada nuevo								
8	El empleado ideó una nueva forma para hacer alguna actividad								
9	El empleado falló a citas o a la entrega de los resultados de su trabajo								
10	Las tareas encomendadas se cumplieron íntegra y puntualmente								
11	Participó de manera entusiasta y decidida en los esfuerzos del equipo para corregir y prevenir errores y para mejorar.								
12	Realizó sus actividades sin interés. No puso la atención adecuada a los errores y esto pareció no importarle.								
13	Aplicó las sugerencias convenientes para mejorar su trabajo.								
14	Investigó y apoyó a otras áreas con el objeto de que su trabajo saliera lo mejor posible.								
15	El empleado mostró poca disposición para compartir o solicitar información.								
16	Desempeñó un papel fundamental para la solución de conflictos interpersonales								
17	Fue extremamente reservado y esto llegó a obstaculizar el trabajo.								
18	Solicitó retroalimentación durante la realización de su trabajo con el propósito de evitar errores								
19	Investigó y apoyó a otras áreas con el objeto de que su trabajo saliera lo mejor posible								

20	Cumplió las tareas con la clara intención de que estuvieran bien hechas								
Total Evaluación: Calificación sobre 70									
Observaciones:									

1 mínimo y 5 máximo

ANEXO 11

INFORME DE LABORATORIO

FULLDATA CIA. LTDA.

INFORME DE LABORATORIO N° 301

Informe técnico: 8707 | Fecha: 02/01/2013 | Hora: 11:40:07

Cliente: TECPECUADOR S. A.
Dirección: LABORATORIO FULLDATA
Opción: EGR ENTREGA A LABORATORIO BAD NO USAR
Telf: 2986240

Atención solicitada por: BYRON DUQUE
Técnico responsable: SAMANIEGO WAGNER RAUL GUILLERMO

SERIE	EQUIPO	MODELO	MARCA	LOCAL	STATUS

N° EQ: ______ Fecha inicial: ________ Fecha final: ________ Status: ______
Diagnóstico:
Trabajo realizado:
Observaciones:

N° EQ: ______ Fecha inicial: ________ Fecha final: ________ Status: ______
Diagnóstico:
Trabajo realizado:
Observaciones:

N° EQ: ______ Fecha inicial: ________ Fecha final: ________ Status: ______
Diagnóstico:
Trabajo realizado:
Observaciones:

N° EQ: ______ Fecha inicial: ________ Fecha final: ________ Status: ______
Diagnóstico:
Trabajo realizado:
Observaciones:

N° EQ: ______ Fecha inicial: ________ Fecha final: ________ Status: ______
Diagnóstico:
Trabajo realizado:
Observaciones:

Comprobantes de Bodega: Ingreso a Bod ________ Egreso a Lab ________ Reingreso a Bod ________

Técnico que hizo la revisión____________

Fecha de reingreso a Bodega D M A

Recibí conforme (Técnico)

Firma del bodeguero:

ANEXO 12

INFORME TÉCNICO

FULLDATA CIA LTDA.

INFORME TECNICO Nº 8748

Tipo de atención: Telefónica ● En sitio — Cód.llamada: 1020
Cliente: ENERGY & PALMA ENERGYPALMA S.A
Solicitada por: LUIS ASPIAZU
Dirección: REP. ZAPALLO
Fecha: 17/01/2013 Hora: 08:00
Opción: EGR EQUIPO RENTA
Fecha fin: 00/00/0000
Tècnico: TACO YANEZ JOSE LUIS
Telf: 062725003

RED: SSID: Código:

EQUIPO	MARCA	MODELO	SERIE	LUGAR	FRECUENCIA Tx/Pol	Rx/Pol	IP	SNR	ALT	NIVEL	STATUS	Fd/Cl

Falla reportada o razón de la visita:
REVISION DE ENLACE HACIA SAN LORENZO

Fecha: Hora de llegada:
Trabajo realizado código: Hora inicial: Hora final:
Diagnóstico:

Observaciones:

Fecha: Hora de llegada:
Trabajo realizado código: Hora inicial: Hora final:
Diagnóstico:

Observaciones:

REEMPLAZOS Y/O REPUESTOS

Comprobantes: Requerimiento y Bodega:
Problema solucionado: Si ○ No ○ Parcial ○
Causas:

CALIFICACION DEL SERVICIO
Excelente ○ Bueno ○ Malo ○

Firma del técnico:
Firma del cliente:
Cargo que ocupa:

ANEXO 13

REGISTRO LLAVES REPETIDORAS

REGISTRO LLAVES REPETIDORAS

LLAVE No	PERSONA	REPETIDORA	FECHA	FIRMA	ENTREGADO

ANEXO 14

CONTROL UTILIZACIÓN AUTOMOVIL

CONTROL UTILIZACION MAZDA (BLANCO)

FECHA	LUGAR	CLIENTE	HORA		TOTAL	KMTS			TOTAL	ENTREGADO POR	NOMBRE Y FIRMA DEL RESPONSABLE
			RECIBE	ENTREGA		COMBUSTIBLE	RECIBE	ENTREGA			

ANEXO 15

CUESTIONARIO APLICADO AL PERSONAL DE T.I.

Administración de T.I.

1. Existe una definición clara de las responsabilidades operacionales, y de instalación de los equipos?

   SI *NO*

2. Están todos los recursos asignados a un usuario específico y es su responsabilidad especificar el nivel de protección de los mismos?

   Si, Con especificación
   Si, Sin especificación
   No

3. El nuevo personal es informado de las políticas/estándares de seguridad y de su responsabilidad en relación a estas?

   SI *NO*

4. Están los usuarios consientes de la importancia de mantener sus passwords confidenciales y que será el responsable de cualquier divulgación?

   No
   Solo Confidencial
   Confidencial y Responsable
   No Aplica

5. Los técnicos saben que no deben dejar una terminal ingresada (login) y desatendida?

   SI *NO*

6. Están los datos fuentes (información, manuales, procedimientos) diseñados a un nivel de seguridad o debidamente identificados (para restringir el acceso y/o identificar su sensibilidad)?

   No
   Algunos Datos
   Todos los datos

7. Los equipos mantiene un log de los accesos e intentos de acceso?

   SI
   NO
   Solo violaciones

8. Que tan a menudo se producen y son revisados los logs por violaciones?

   Diario o más frecuente
   Un día si otro no
   Semanalmente
   Cuando se sospecha violación
   Nunca
   No aplica

9. Es posible que un técnico monitoree la actividad de un cliente específico?

SI *NO*

10. Están todos los técnicos instruidos para chequear esto y reportar cualquier discrepancia?
    SI *NO*

11. Las políticas de seguridad están detalladas y completamente documentadas?
    Si
    Si, pero no documentada
    No

12. Las auditorías de seguridad son detalladas y conducidas en periodos regulares?
    No
    Si, por este departamento
    Si, por un Dep. Independiente
    Si, por consultores externos

13. Existe un especialista a cargo de la tarea de coordinar la seguridad y asegurarar que las políticas sean comunicadas apropiadamente?
    No
    Solo coordinación
    Solo comunicación
    Ambos

14. Los gerentes saben de su responsabilidad sobre la seguridad dentro de sus dominios?
    SI *NO*

15. Existe un programa en proceso para incrementar la conciencia de seguridad (posiblemente incluya cartas y seminarios/cursos)?
    SI *NO*

16. Hay un nivel de seguridad asignado a todos los usuarios?
    SI *NO*

CONTINGENCIAS

1. Está la frecuencia de la copia de configuraciones (por back-up) parcial o completamente determinada por las capacidades de recuperación de la aplicación?
   No
   Parcial
   Completa
   No Back-Up de datos

2. Existe un mecanismo en las repetidoras, como un punto de chequeo y restart, para ayuda en caso de fallas en la interconexión?
   SI *NO*
3. Se realizan copias de back-up regularmente y donde se mantienen?
   No
   Si – En el sitio

Si – Fuera del sitio
Si - Dentro y fuera del sitio

4. Se mantienen copias de la documentación e instrucciones de operación?
   No
   Si – En el sitio
   Si – Fuera del sitio
   Si – Dentro y fuera del sitio
   No aplica

5. Los backup en el sitio, de archivos, programas, documentación e instrucciones de operación están almacenados para prevenir el acceso no autorizado y riesgo de daño (fuego, etc.)?
   Solo acceso no autorizado
   Solo riesgo de daño
   Ambos acceso y daño
   Ni acceso ni daño

6. Se han asignado responsabilidades individuales para la implementación de cada componente del plan de recuperación y se ha nombrado un coordinador de la recuperación?
   Si
   No
   Solo un Coordinador
   Solo para cada componente

7. Los detalles para el remplazo de equipos han sido formulados, incluyendo costos (unitario y total) y el tiempo de remplazo de la unidad?
   Si
   No
   No incluye costos
   No incluye tiempo

HARDWARE

1. Cuándo tiempo de servicio fue perdido el último año por fallas de hardware?
   0% - 1%
   1% - 3%
   4% - 5%
   Más de 5%

2. Existen procedimientos en el sitio para asegurar la restauración después de una falla de hardware crítica detectada?
   SI *NO*

3. El mantenimiento preventivo se lleva a cabo regularmente y en fechas predeterminadas?
   SI *NO*

4. Todo el trabajo de mantenimiento es documentado y supervisado?
   SI *NO*

RIESGOS

1. Qué tan frecuente se realizan trabajos en las repetidoras o se dan o se alteraciones en las torres?
   A menudo
   Algunas veces
   Rara vez
   Nunca

2. Ha existido una falla de energía en la instalaciones en los últimos 3 meses?
   SI *NO*

3. Existe un UPS (Uninterrumpible Power Supply) de energía y un sistema de monitoreo instalado en cada punto de la red?
   SI *NO*

4. Se realiza un mantenimiento preventivo al equipo de UPS y soporte?
   Regularmente/a la marcha
   Periódicamente
   Rara vez
   Nunca

5. Cuál de las siguientes amenazas podría afectar más seriamente a la instalación o el área en general?
   Vientos extremos
   Hundimiento
   Inundaciones
   Tormentas Eléctricas
   Daño de hielo (granizo)
   Terremotos

6. Qué de lo siguiente no ha sido definido en la red WAN?
   Enlaces críticos
   Equipos críticos
   Software crítico