VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRÍA EN GERENCIA DE SISTEMAS

PROMOCIÓN XII

TESIS DE GRADO

TEMA: "AUDITORIA DE GESTIÓN DE PROCESOS EN EL DEPARTAMENTO DE TIC'S DE LA EMPRESA PÚBLICA ESTRATÉGICA HIDROELÉCTRICA COCA CODO SINCLAIR, COCASINCLAIR EP, UTILIZANDO EL MARCO DE REFERENCIA COBIT 4.1."

AUTOR: SUÁREZ, MARCO DAMIÁN

DIRECTOR: ECO. CHIRIBOGA, GABRIEL

SANGOLQUÍ, ENERO DE 2014

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

MAESTRÍA EN GERENCIA DE SISTEMAS

CERTIFICO

Que el trabajo titulado “AUDITORÍA DE GESTIÓN DE PROCESOS EN EL DEPARTAMENTO DE TIC’S DE LA EMPRESA PÚBLICA ESTRATÉGICA HIDROELÉCTRICA COCA CODO SINCLAIR, COCASINCLAIR EP, UTILIZANDO EL MARCO DE REFERENCIA COBIT 4.1”, realizado por el Ing. Marco Damián Suárez Torres, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el reglamento de estudiantes de la Escuela Politécnica del Ejército.

Sangolquí, Enero de 2014.

_____

ECO. GABRIEL E. CHIRIBOGA B. MSC.

DIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

MAESTRÍA EN GERENCIA DE SISTEMAS

DECLARACIÓN DE RESPONSABILIDAD

Yo, **SUÁREZ TORRES MARCO DAMIÁN**

DECLARO QUE:

El proyecto de grado denominado "AUDITORÍA DE GESTIÓN DE PROCESOS EN EL DEPARTAMENTO DE TIC'S DE LA EMPRESA PÚBLICA ESTRATÉGICA HIDROELÉCTRICA COCA CODO SINCLAIR, COCASINCLAIR EP, UTILIZANDO EL MARCO DE REFERENCIA COBIT 4.1", ha sido desarrollado en base a la revisión de la documentación proporcionada, respetando derechos intelectuales de terceros, conforme las citas que constan en el pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este documento es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del proyecto de grado en mención.

Sangolquí, Enero de 2014

_____

Ing. Marco Suárez Torres

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

MAESTRÍA EN GERENCIA DE SISTEMAS

AUTORIZACIÓN

Yo, **SUÁREZ TORRES MARCO DAMIÁN**

Autorizo a la Escuela Politécnica del Ejército, la publicación, en la Biblioteca Virtual de la Institución del trabajo "AUDITORÍA DE GESTIÓN DE PROCESOS EN EL DEPARTAMENTO DE TIC'S DE LA EMPRESA PÚBLICA ESTRATÉGICA HIDROELÉCTRICA COCA CODO SINCLAIR, COCASINCLAIR EP, UTILIZANDO EL MARCO DE REFERENCIA COBIT 4.1", cuyo contenido, ideas y criterio son de mi exclusiva responsabilidad y autoría.

Sangolquí, Enero de 2014

_____

Ing. Marco Suárez Torres

DEDICATORIA

Este trabajo de Tesis está dedicado a todas las personas que me han apoyado a conseguir este logro, en especial a mi esposa Alexandra y a mis hijos Mateo, Josué y Ariana, quienes que con el pasar del tiempo sabrán valorar el esfuerzo realizado para culminar con éxito esta etapa de mi vida profesional.

Marco Suárez Torres

AGRADECIMIENTO

Mi agradecimiento a Dios, por iluminarme y permitirme tomar las mejores decisiones en mi vida personal y profesional, por las personas que me rodean, la salud, el trabajo y por todos los favores recibidos diariamente.

Mi agradecimiento a mi familia, en especial a mi esposa, quién me ha apoyado constantemente para culminar los estudios de la Maestría y posteriormente este trabajo de Tesis, por su esfuerzo para suplir mi ausencia en el tiempo que duró los estudios.

A mi hermana, quién me motivó a seguir la Maestría en Gerencia de Sistemas, a mis padres y hermanos que a pesar de la distancia, siempre me han apoyado en los retos que me he planteado y en las decisiones que he tomado en la vida.

Un agradecimiento especial al Eco. Gabriel Chiriboga Barrera, por su dedicación, tiempo y apoyo al presente proyecto de tesis, ya que por su experiencia, material de investigación, consejos y lineamientos, me han permitido cumplir con el cronograma planteado y con las metas alcanzadas demostradas en este trabajo de Tesis.

Marco Suárez Torres.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En la empresa COCASINCLAIR EP, se ha realizado la auditoria a los procesos de la Coordinación de Tecnologías de Información y Comunicación (TIC). Los procesos auditados han sido el resultado de aplicar los criterios de la Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad), utilizando la metodología de la matriz de riesgos y el estándar de buenas prácticas de COBIT 4.1. Esta revisión ha permitido conocer su situación y poder plantear las acciones que ayuden a mejorar el nivel de madurez de cada proceso auditado. Este proyecto de tesis, inicia describiendo a la empresa COCASINCLAIR EP, posteriormente, se presenta el marco teórico de una Auditoria, el marco de referencia COBIT 4.1, los Riesgos en TIC'S, obteniendo la matriz de riesgos priorizada con los criterios de Seguridad de la Información. Se realiza la auditoria a los seis procesos más relevantes identificados en la matriz de riesgos utilizando el marco de referencia COBIT 4.1 y aplicando el IT ASSURANCE GUIDE COBIT 4.1. Se analiza el cumplimiento de los objetivos de control, evaluando sus resultados, obteniendo los indicadores claves de rendimiento y llegando a determinar el nivel de madurez de cada proceso. Como resultado de la auditoria, se genera el Informe Detallado y el Informe Ejecutivo con sus recomendaciones. Finalmente, en el capítulo 6 se detallan las conclusiones y recomendaciones. Es importante señalar que, las recomendaciones que fueron resultado de la auditoria, se encuentran en los Informes detallados en el capítulo 5, éstas nada tienen que ver con las recomendaciones del capítulo 6 que se refieren a todo el proyecto de tesis.

PALABRAS CLAVES:

- Auditoria.
- TI (Tecnologías de Información).
- COBIT (Objetivos de Control de Tecnologías de Información).
- Instituto de Gobernabilidad de TI.
- Guía de Aseguramiento de COBIT 4.1.

ABSTRACT

In the company COCASINCLAIR EP is has audited processes Coordination of Information and Communication Technologies (ICT). Audited processes have been the result of applying the criteria of the Security of Information (Confidentiality , Integrity and Availability) , using the methodology of the risk matrix and the standard of best practice of COBIT 4.1. This has allowed to review their situation and bring actions to help improve the level of maturity of each audited process. This thesis project begins by describing the company COCASINCLAIR EP then the theoretical framework of an audit occurs, the framework COBIT 4.1, Risk ICT'S, until the risk matrix prioritized criteria Security Information . Audit at six processes most relevant identified in the risk matrix using the COBIT 4.1 framework and applying IT ASSURANCE GUIDE COBIT 4.1, analyzing the performance of the control objectives , assessing their results, with the key performance indicators and arriving is done determine the level of maturity of each process. As a result of the audit, the Detailed Report and the Executive Summary with recommendations generates. Finally, in Chapter 6 the conclusions and recommendations are detailed. Importantly, the recommendations were the result of the audit, are found in the detailed reports in Chapter 5, these have nothing to do with the recommendations of Chapter 6 concerning the whole thesis.

KEYWORDS:

- Audit
- IT (Information Technology)
- COBIT (Control Objectives for Information and related Technology)

- IT Institute Governance
- COBIT Assurance Guide.

CAPÍTULO 1

GENERALIDADES

TEMA DE INVESTIGACIÓN

Auditoría de Gestión de Procesos en el Departamento de TIC'S de la Empresa Pública Estratégica Hidroeléctrica Coca Codo Sinclair, COCASINCLAIR EP, utilizando el Marco de Referencia Cobit 4.1.

1.1 Descripción de la empresa COCASINCLAIR EP

1.1.1 Antecedentes

Mediante Decreto Ejecutivo No. 370, de 26 de mayo de 2010, de conformidad con lo establecido en el numeral 2.5 de la Disposición Transitoria Segunda, de la Ley Orgánica de Empresas Públicas, se transformó a la Compañía HIDROELÉCTRICA COCA CODO SINCLAIR S. A., en la Empresa Pública Estratégica HIDROELÉCTRICA COCA CODO SINCLAIR, COCASINCLAIR EP y es la concesionaria para la construcción del Proyecto Hidroeléctrico Coca Codo Sinclair. El aporte de generación eléctrica estará por el orden del 40% de la demanda nacional cuando la central hidroeléctrica esté en la fase de operación, esto es 1500 MW para inicios del año 2016.

En el año 2011, se aprobó el Plan Estratégico de la Empresa COCASINCLAIR EP con una vigencia hasta el 2016. A continuación se detalla la Misión y Visión del Plan:

MISIÓN

Construir la Central Hidroeléctrica Coca Codo Sinclair de 1.500 MW, en el plazo establecido, en óptimas condiciones técnicas, con Responsabilidad Social y Ambiental

VISIÓN

En el Año 2016, poner en operación la Central Hidroeléctrica Coca Codo Sinclair que aporte al Sistema Nacional Interconectado 1.500 MW, cumpliendo con los más altos estándares técnicos, contribuyendo a la preservación de los ecosistemas y con el reconocimiento de las comunidades de la zona y de todos los ecuatorianos

CULTURA ORGANIZACIONAL

Las 3´C de Coca Codo Sinclair: Compromiso, Cumplimiento y Calidad

Los principales ejes estratégicos de la Empresa son los siguientes:

- Excelente ejecución técnica y económica del proyecto.
- Responsabilidad social corporativa.
- Preservación y conservación de los ecosistemas.
- Consolidación y fortalecimiento del apoyo de las autoridades.
- Efectiva difusión y socialización del proyecto.
- Mantener una organización eficiente y ágil.

La empresa COCASINCALIR EP, cuenta con un mecanismo para el control de gestión y monitoreo, con un enfoque metodológico del Balance Score Card o Cuadro de Mando Integral. Las principales perspectivas y objetivos a alcanzar en el proyecto se resumen a continuación:

Perspectiva de la Misión / Visión

_ **M01:** Cumplir con el cronograma de plazos y costos del proyecto.

_ **M02:** Impulsar el desarrollo de las comunidades en la zona de influencia.

_ **M03:** Preservar el ambiente.

_ **V01:** Alcanzar un nivel de conocimiento y aceptación del proyecto por parte de la Sociedad ecuatoriana.

Perspectiva de Stakeholders

_ **AU01:** Informar de forma oportuna acerca del avance del proyecto.

_ **C01:** Mejorar la participación de las comunidades en el proyecto.

_ **C02:** Mantener buenas relaciones con las comunidades.

Perspectiva de Procesos

_ **P01:** Garantizar una planificación y ejecución de la empresa.

_ **P02:** Ejecutar el control de fiscalización del proyecto.

_ **P03:** Cumplimiento de los hitos y objetivos del proyecto.

_ **P04:** Cumplir con los proyectos de desarrollo de las comunidades.

_ **P05:** Minimizar el Impacto ambiental del proyecto.

Perspectiva de Aprendizaje & Crecimiento

_ **AC01:** Mejorar el nivel de competencias de todo el personal.

_ **AC03:** Crear un clima organizacional satisfactorio basado en la cultura de las 3 C´s (Calidad, Cumplimiento y Compromiso).

Perspectiva de Recursos / Infraestructura

_ **R01:** Disponer oportunamente de los recursos económicos.

Adicionalmente, la empresa COCASINCLAIR EP, se encuentra en proceso de certificación del Sistema Integrado de Gestión, basadas en las normas ISO 9001:2008 Gestión de la Calidad, ISO 14001:2004 Gestión Ambiental y la Norma OHSAS 18001:2007 Gestión de la Seguridad y Salud en el Trabajo; consecuentemente, la Coordinación de TIC'S de la Empresa cumplirá un rol importante proporcionando mecanismos de seguimiento a lo requerido en las tres normas antes señaladas.

Por su estructura orgánica, COCASINCLAIR EP remite información técnica, operativa y financiera a diferentes Instituciones del Estado, como ejemplo el Ministerio de Electricidad y Energía Renovable, Ministerio de Sectores Estratégicos, Secretaría Nacional de Planificación, entre otras.

A continuación, se muestra el mapa de procesos de la Empresa.

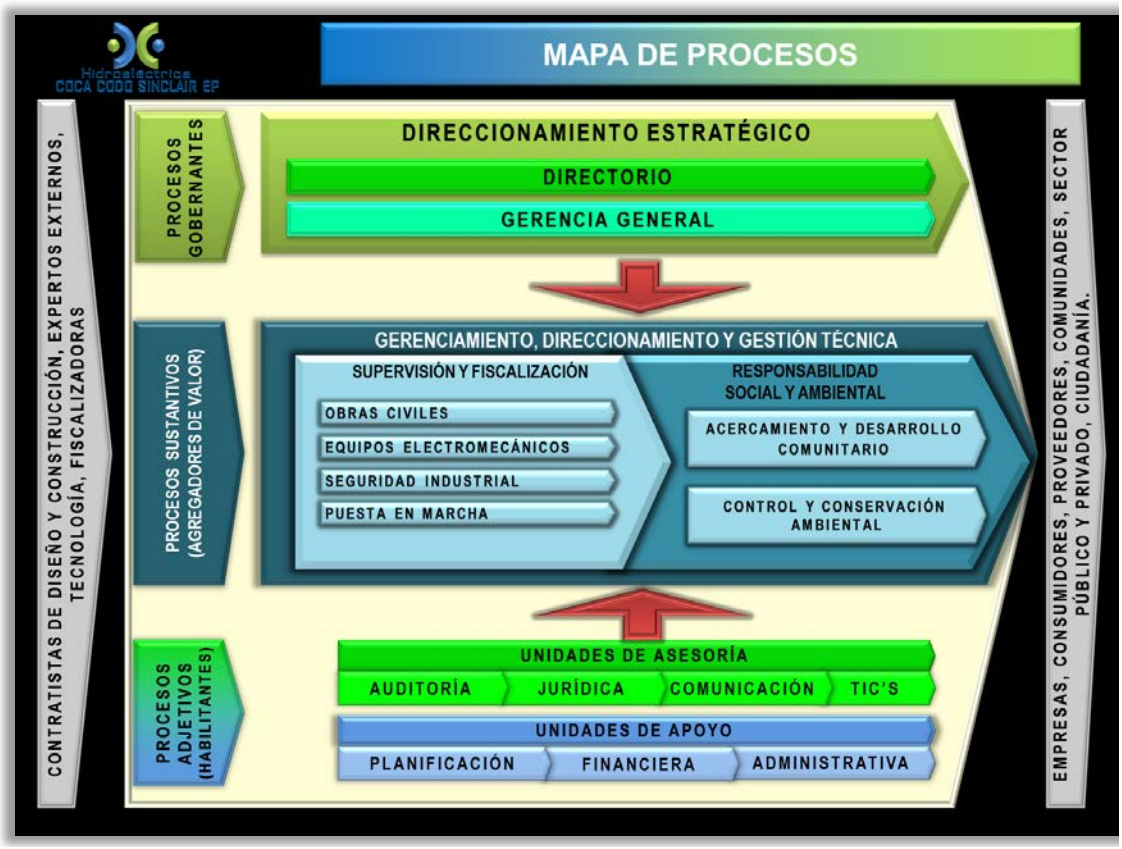


Figura No.1-1 Cadena de Valor de la empresa COCASINCLAIR EP.

1.1.2 Principales productos y/o servicios

El producto final de la empresa COCASINCLAIR EP, es entregar al país la Central Hidroeléctrica Coca Codo Sinclair lista para entrar en operación en febrero del 2016, ésta generará 1500 MW para el Sistema Nacional Interconectado y va a satisfacer aproximadamente el 40 % de la demanda nacional de energía eléctrica.

El Proyecto Hidroeléctrico Coca Codo Sinclair, utiliza las aguas de los ríos Quijos y Salado, que posteriormente forman el Río Coca en una zona donde este río describe una enorme curva que produce un desnivel bruto de 620 metros, aprovechable para la generación hidroeléctrica.

La empresa contratista encargada de la construcción del proyecto hidroeléctrico es Sinohydro, y, quien realiza la fiscalización del proyecto es la Asociación CFE-PYPSA-CVA-ICA. En ocasiones, la Asociación solicita a COCASINCLAIR EP requerimientos de comunicación o interfaces con sus sistemas informáticos para que el personal de la Empresa pueda supervisar el avance de la construcción del proyecto.

Al encontrase el proyecto Hidroeléctrico Coca Codo Sinclair en la fase de construcción, la empresa COCASINCLAIR EP está enfocada en ejecutar proyectos o programas de desarrollo social en la zona de influencia que se verían afectadas directa e indirectamente por el proyecto hidroeléctrico. Entre los principales programas o proyectos de carácter social y de infraestructura para el año 2012 están:

- **Alcantarillado Sanitario en el área de influencia del Proyecto.**

  Ubicación: Cascabel. Santa Rosa, Cabecera Parroquial Linares, San Carlos.

- **Ampliación y Sectorización de la Red de Distribución de Agua Potable.**

Ubicación: San Carlos, San Luis y Gonzalo Díaz de Pineda

- **Construcción Casa Comunal Taller.**

  Ubicación: San Luis

- **Construcción de Bloque de Aulas en las Escuelas Daniel González, México, Marañón y Fray Vacas Galindo**

  Ubicación: Cantón El Chaco

- **Construcción de la Planta de Tratamiento de Agua Potable para El Chaco - Santa Rosa.**

  Ubicación: Cabecera Parroquial El Chaco.

- **Construcción del Sistema de Agua Potable (Captación-Conducción-Planta de Tratamiento- Red de Distribución).**

  Ubicación: Cascabel - Santa Rosa

- **Equipamiento del Subcentro de Salud.**

  Ubicación: Cabecera Parroquial Santa Rosa, Las Palmas, Simón Bolívar.

- **Financiamiento de un Bus para el Traslado de Estudiantes desde la Parroquia El Reventador hacia la ciudad de Lumbaqui y Bus Colegio Técnico El Chaco.**

  Ubicación: Cantones Gonzalo Pizarro y El Chaco.

- **Seguimiento Convenio INIAP a parcelas instaladas, Investigación, Capacitación y Transferencia de Tecnologías, Insumos, Semillas y Materiales SENPLADES - MAGAP.**

  Ubicación: Cantones Gonzalo Pizarro y El Chaco.

- **Equipamiento de Computadoras, Impresoras, Proyectores, Pantallas Digitales Interactivas y otros, para los Establecimientos Educativos del Área de Influencia del Proyecto.**

  Ubicación: Cantones Gonzalo Pizarro y El Chaco.

- **Internet para Establecimientos Educativos en el Área de Influencia del Proyecto según Convenio MINTEL y COCASINCLAIR EP.**

  Ubicación: Cantones Gonzalo Pizarro y El Chaco.

- **Construcción Campamento en frentes de Obra**

  Ubicación: Cantón Gonzalo Pizarro – Vía a Casa de Máquinas.

- **Construcción Campamento en frente de Obra Embalse Compensador.**

  Ubicación: Cantón Gonzalo Pizarro – Vía al Embalse.

1.1.3 Principales Mercados y Clientes

La empresa COCASINCLAIR EP, cumple sus actividades en función de las políticas y objetivos establecidos en el Plan Estratégico de la empresa

y alineados al Plan del Buen Vivir del Gobierno Central, principalmente, en cambiar la matriz energética, asignándolo cómo proyecto estratégico la Central Hidroeléctrica Coca Codo Sinclair.

Dentro de los principales mercados y/o clientes están las siguientes:

1.1.3.1 Comunidades

Se considera a las Comunidades, como las diferentes poblaciones y grupos sociales cuyo hábitat natural se ve afectado por las obras de implementación del Proyecto Hidroeléctrico.

¿POR QUÉ SON IMPORTANTES?	¿QUÉ ESPERAN DEL PROYECTO?
Porque son los socios estratégicos del proyecto, convirtiéndose en veedores de la ejecución y defensores de la obra	Que COCASINCLAIR EP monitoree que la constructora genere fuentes de trabajo de acuerdo a las expectativas del Estado
	Qué se los vincule con el proyecto como prestadores de servicios
	Que se impulse el desarrollo integral de la zona en coordinación con las correspondientes instituciones del Estado
	Que exista un real cuidado y respeto al ecosistema y al ambiente

1.1.3.2 Equipo Gerencial o Administradores

Son considerados como equipo gerencial o administradores, a todo el personal de la empresa, tales como el Gerente General, Subgerentes y Jefes departamentales.

En general, este grupo de interés muestra un alto nivel de satisfacción, lo cual es una gran fortaleza para impulsar los procesos de cambio requeridos por la nueva estrategia empresarial.

¿POR QUÉ SON IMPORTANTES?	¿QUÉ ESPERAN DEL PROYECTO?
Porque garantizan el Cumplimiento de la Gestión administrativa y operativa de la empresa	Que se desarrolle el capital humano y las competencias
	Que sus jefes y autoridades muestren liderazgo y tengan políticas de Comunicación de “puertas abiertas”.
	Que se les brinde reconocimiento a sus labores
	Que exista actividades de integración familia - empresa
	Que existan mecanismos que estimulen un alto desempeño laboral
	Que se les permita participar en la toma de decisiones

1.1.3.3 Servidores y Trabajadores

Son todos los colaboradores de la empresa que están subordinados a una Coordinación o subgerencia.

¿POR QUÉ SON IMPORTANTES?	¿QUÉ ESPERAN DEL PROYECTO?
Porque son la base Fundamental para la ejecución del trabajo físico de la obra	Que se genere fuentes de trabajo de acuerdo a las necesidades del Proyecto
	Que se les dé un salario justo de acuerdo a las normativas salariales existentes
	Que se les dé un trato digno y con respeto
	Que la constructora garantice un entorno de trabajo adecuado
	Que se brinde capacitación para mejorar su desempeño actual y futuro
	Que exista transferencia de conocimiento y tecnología

1.1.3.4 Equipo directivo o administradores del Proyecto

¿POR QUÉ SON IMPORTANTES?	¿QUÉ ESPERAN DEL PROYECTO?
Porque son los que ejercen el liderazgo con eficiencia y eficacia para alcanzar las metas y objetivos	Que la organización a su cargo trabaje para garantizar una adecuada consecución de las metas
	Que se les involucre en los procesos de toma de decisiones
	Que existan mecanismos que estimulen un alto desempeño laboral
	Que se les de reconocimiento por la gestión realizada
	Que exista un sistema de evaluación equitativa y que fomente el alto desempeño
	Que existan un excelente ambiente laboral y de trabajo en equipo

1.1.3.5 Gobierno, Entidades de Control, Ministerios Coordinadores y Ejecutores

¿POR QUÉ SON IMPORTANTES?	¿QUÉ ESPERAN DEL PROYECTO?
Porque son quienes siguen y controlan el buen desarrollo del proyecto y contribuyen en la implementación de programas y proyectos ambientales y sociales	Que el Proyecto se desarrolle con éxito y sin contratiempos, cumpliendo con las especificaciones técnicas, legales y ambientales
	Que el Proyecto se enmarquen en el PNVB y la Política Sectorial Eléctrico
	Que se les dé Información oportuna, veraz y continua
	Que se fomente el desarrollo de las zonas por medio de las relaciones Inter Institucionales destacando el rol de Gobierno como el principal benefactor
	Que los administradores gestionen y resuelva eficazmente los problemas
	Que la comunidades avalen el éxito del proyecto y se mejore la imagen del País a través del éxito del proyecto

1.1.3.6 Proveedores

¿POR QUÉ SON IMPORTANTES?	¿QUÉ ESPERAN DEL PROYECTO?
Porque suministran los bienes y servicios necesarios para la adecuada gestión de la empresa	Que los procesos de compra sean transparentes y estar informados de los nuevos procesos de adquisición
	Que los pagos sean oportunos y se resuelvan rápidos los problemas
	Que se les dé Información oportuna, veraz y continua

1.1.3.7 Expertos Externo y Gremios

¿POR QUÉ SON IMPORTANTES?	¿QUÉ ESPERAN DEL PROYECTO?
Porque son una guía para orientar en la adecuada toma de decisiones	Que sus opiniones sean tomados en cuenta en la toma de decisiones sobre proyecto
	Que sus miembros afiliados (cámaras y gremios profesionales) sean considerados como proveedores del proyecto

1.1.4 Tamaño de la Empresa

La empresa COCASINCLAIR EP, cuenta con un presupuesto operativo anual para el año 2012 de USD 563’383.190,00, en este se contempla los pagos que se deben realizar a la empresa constructora Shinohydro, así como a la fiscalizadora - la Asociación CFE-PYPSA-CVA-ICA -, las inversiones en proyectos de desarrollo comunitarios y gastos corrientes.

Las oficinas de la empresa se encuentran en Quito en la Av. 6 de Diciembre N31-110 y Whymper, edificio Torres Tenerife; y en el Campamento San Rafael, ubicado en el km. 150 vía a Lago Agrio, parroquia El Reventador, Cantón Gonzalo Pizarro, Provincia de Sucumbíos.

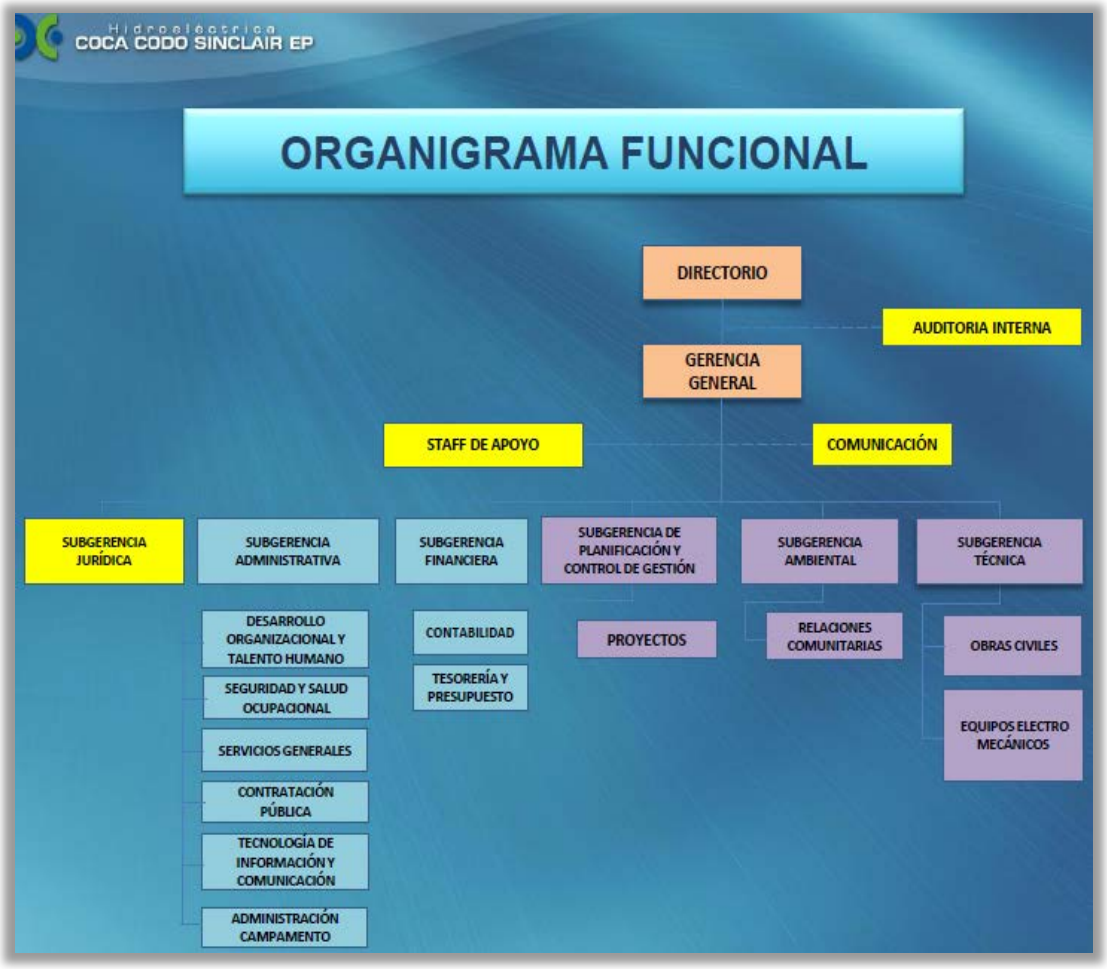


Figura No.1-2 Organigrama funcional de la empresa COCASINCLAIR EP

Orgánicamente, en Quito funcionan todas las áreas de la Empresa, apoyadas en el Campamento por personal en las áreas Administrativa, Técnica y de Relaciones Comunitarias. El personal con el que cuenta la Empresa entre ejecutivos, administrativos y trabajadores está alrededor de 170 personas.

1.1.5 Estructura y organización de TIC'S

La Coordinación de TIC'S de la empresa COCASINCLAIR EP, implementa herramientas informáticas que apoyan al control de la construcción del proyecto hidroeléctrico, a la gestión interna, así como brinda el soporte técnico al personal que labora en las oficinas matriz en Quito y en el Campamento San Rafael.

1.1.5.1 Misión.

Asesorar, proponer e implementar soluciones tecnológicas que apoyen y respalden la gestión, a través de la tecnología y redes de comunicaciones integradas a los sistemas de información de la Empresa.

1.1.5.2 Atribuciones y Responsabilidades.

Son atribuciones y responsabilidades de la Coordinación de TIC'S, las siguientes:

a) Diseñar y ejecutar el Plan Informático de acuerdo con los lineamientos del Plan Estratégico de COCASINCLAIR EP;
b) Administrar y proveer seguridad, estabilidad y alta disponibilidad de los servicios de red;

c) Emitir políticas y procedimientos para normar el uso y los servicios de los recursos informáticos;
d) Consolidar y administrar el inventario de hardware y software;
e) Determinar los recursos informáticos y de comunicaciones necesarios para el funcionamiento de la Empresa;
f) Administrar los proyectos tecnológicos;
g) Dar soporte y asesoramiento informático a todas las áreas de la Empresa;
h) Dar el soporte técnico necesario a los procesos de adquisiciones de equipos o servicios relacionados con hardware, software y comunicaciones, y;
i) Las demás que le sean asignadas por la Gerencia General y/o la Subgerencia Administrativa, en el ámbito de su competencia.

1.1.5.3 Productos y Servicios de la Coordinación de TIC'S.

Cómo principales productos se detallan los siguientes:

a) Plan Integral Informático;
b) Informes de ejecución de plan informático;
c) Plan de mantenimiento de hardware y software;
d) Plan de Gestión de Seguridad de la Información;
e) Administración de Soluciones ERP, BSC, ECM;
f) Informes de ejecución de mantenimiento de hardware y software de la Empresa;

g) Registros e informes de soporte técnico;

h) Informes de seguridad;

i) Administración del portal web; y,

j) Los demás que le sean solicitados por la Gerencia General y/o la Subgerencia Administrativa, en el ámbito de su competencia.

A continuación se detalla los servicios principales implementados:

- Correo Institucional. El correo institucional proporciona servicios de comunicaciones electrónicas a 120 usuarios, este servicio abarca al personal de las oficinas en Quito como al Campamento San Rafael.

- Portal Web de la empresa. El portal Web es administrado por la Coordinación de Comunicaciones, actualmente se encuentra en el dominio www.ccs.gob.ec, el mismo que es utilizado para informar a la comunidad las noticias, links de interés, información de consultas y mantiene una sección de avance de construcción del proyecto hidroeléctrico, así como la documentación que formó parte del proceso precontractual para la contratación de la empresa que construiría la Central Hidroeléctrica.

- Videoconferencia. Se dispone de un enlace dedicado con el Campamento San Rafael que permite realizar reuniones entre áreas o con proveedores a través de videoconferencias. Además, en casos particulares se realizan videoconferencias con México (matriz de la

empresa Fiscalizadora), Estados Unidos e Inglaterra (estudios jurídicos de apoyo para resolver controversias del contrato Engineering Procurement Construction – EPC).

- Internet. Se tiene dos enlaces redundantes para la salida al Internet para balanceo de carga. Permanentemente se realiza el monitoreo del servicio y se administra el tráfico a través de los equipos de seguridad ubicados en el perímetro de la red LAN.

- Sistema de Gestión Documental. Dentro de las organizaciones es importante optimizar procesos y recursos, la empresa COCASINCLAIR EP ha implementado un Gestor Documental para automatizar el proceso de Compras Públicas con el propósito de dar seguimiento a los procesos de adquisiciones y contratación que realizan las áreas de la Empresa.

- Mantenimientos preventivos / correctivos. Para el correcto funcionamiento de los sistemas informáticos, es necesario realizar mantenimientos de los equipos computacionales y de comunicaciones de la Empresa, se cuenta con empresas especializadas que brindan este servicio.

- Soporte técnico y asistencia a usuarios. Una de las actividades que más se realiza en la Coordinación de TIC'S es el soporte técnico, actualmente se están implementando indicadores que muestren la

eficiencia y eficacia de este servicio, se espera tener en poco tiempo una consultoría de ITIL para estructurar de mejora manera el servicio y la entrega del soporte técnico. También se realizan instalaciones de hardware y software, se ayuda a los usuarios solventando sus dudas o problemas en el uso de las herramientas informáticas que dispone la Empresa.

1.1.5.4 Políticas de la Gestión de la Información y Comunicación:

a) Producir y difundir información veraz, transparente y oportuna acerca de los beneficios y avances del Proyecto, de los programas de compensación social y comunitaria; así como, de la gestión empresarial, aplicando criterios de CONFIDENCIALIDAD, INTEGRIDAD Y OPORTUNIDAD.

b) Mantener la confidencialidad en la información técnica, empresarial y en general, con aquella información, considerada por el Directorio de COCASINCLAIR EP como estratégica y sensible a los intereses de ésta.

1.1.5.5 Infraestructura en hardware

La infraestructura informática de la Empresa, en forma general se encuentra de la siguiente manera:

- Firewall: Dos equipos de seguridad, ubicado en los dos sitios en los que funciona la empresa COCASINLACIR EP.

- Enlaces: Dos enlaces para internet con balanceo de carga, un enlace de datos entre el Campamento San Rafael y las oficinas en Quito.

- Impresoras Multifunción: 8 impresoras multifunción de gran capacidad para todas las Subgerencias, Coordinaciones y la Gerencia General.

- Servidores: Se dispone de 20 servidores entre virtualizados y físicos, ubicados la mayoría en Quito. Se cuenta con servidores de correo, de bases de datos, de archivos, web, controladores de dominio, de frontera, de aplicaciones (financiero, legal y de control de asistencias), de actualización de parches de seguridad de Microsoft y de seguridad, entre otros.

- Almacenamiento: Se cuenta con unidades de almacenamiento con arreglos de discos duros de 2.7 y 3.6 terabytes de espacio para los servidores antes mencionados.

- Equipos de computación: Entre equipos portátiles y de escritorio, se dispone de 150 computadoras aproximadamente.

- Equipos de Comunicación: Se refiere a los equipos que se encuentran en el data center y principalmente son switches capa 2 y 3, ruteadores, central telefónica, módems, entre otros.

- Equipos de soporte: estos son los UPS, aire acondicionado, sistema de extinción de incendios, alarmas, etc.

- Equipos de videoconferencia: Se encuentran localizados uno en Quito y el otro en el Campamento de San Rafael.

- La topología de la red tanto para datos como para voz es tipo anillo con cableado categoría 7A.

1.1.5.6 Número de personas en la Coordinación de TIC'S

En la Coordinación de TIC'S trabajan actualmente 5 personas, distribuidas de la siguiente manera:

- **Quito**:
    - Jefe de TIC'S (E)
    - Profesional de Sistemas
    - Ingeniero de Soporte
- **Campamento San Rafael:**
    - Asistente de soporte
    - Asistente de soporte

1.2 Planteamiento del problema

Desde cuando la Empresa inició sus funciones, la Coordinación de TIC'S ha entregado sus productos o servicios con poco o nada de procedimientos y sin la documentación que respalde su gestión. Dentro del Plan Estratégico de la Empresa, se señalan cuáles son las atribuciones y responsabilidades de la Coordinación de TIC'S, sin embargo no se tiene claro cómo apoya esta área a las políticas de la Empresa, cómo están sus procesos internos, el nivel de servicios referente al soporte técnico, la seguridad de la plataforma informática implementada y la seguridad de la información que es tratada internamente, entre otros aspectos.

La falta de documentación de soporte relacionada a requerimientos en la Coordinación de TIC'S, hace difícil llevar un control de la infraestructura tecnológica, esto ha provocado desperdicios de recursos tanto de técnicos como de tiempo.

La falta de procesos claros para las diferentes actividades que se realizan en la Coordinación de TIC'S, no ha permitido llevar un mejor control y evaluar los productos o servicios que brinda esta Coordinación.

Los presupuestos financieros que se administran en la Coordinación de TIC'S para cada año, se ven reflejados en la ejecución de proyectos informáticos y de comunicaciones, que apuntan a un objetivo, ser una área

de apoyo para la Empresa de forma eficiente y eficaz, alineados a los objetivos de COCASINCLAIR EP.

Se podría optimizar los recursos a través del uso de un estándar o mejores prácticas, que permita alinear los objetivos de la Coordinación de TIC'S a los objetivos del negocio desde la planificación, operación, control y finalmente al seguimiento de sus procesos. Al ser COCASINCLAIR EP una empresa pública, mucha de esta información servirá a otras empresas que realizan actividades similares, como por ejemplo, los proyectos hidroeléctricos Sopladora en el Austro del país, Toachi Pilatón, entre otros.

Es probable que luego de la construcción del proyecto Hidroeléctrico Coca Codo Sinclair, en la fase de operación y generación de energía eléctrica, lo realice la misma empresa COCASINCLAIR EP, por lo que ya se podría contar con procesos estables en la Coordinación de TIC'S; y de no ser así, toda la infraestructura tecnológica lo podría utilizar otra empresa o institución que realice esta función, razón por la que iniciar desde hoy con el uso de un marco de referencia o estándares para administrar TI alineadas con las estrategias de negocio, servirán para que se sigan implementado el resto de procesos en forma progresiva y llegar a un nivel de madurez superior.

1.3 Objetivos

1.3.1 General

Analizar, evaluar y documentar los seis procesos más relevantes, así como los controles implementados de estos procesos en la Coordinación de TIC'S de la empresa COCASINCLAIR EP, utilizando el marco de referencia COBIT 4.1 y proponer a la Gerencia General las recomendaciones para mejorarlos.

1.3.2 Específicos

- Elaborar una matriz de riesgos de la Coordinación de TIC'S, que permita identificar los seis procesos más relevantes del área, priorizándolos con los criterios de Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad)
- Recopilar la documentación de soporte de cada proceso a analizar de la Coordinación de TIC'S en la empresa COCASINCLAIR EP.
- Auditar cada proceso identificado, usando el marco de referencia COBIT 4.1
- Determinar el nivel de madurez de cada proceso analizado.
- Documentar los procesos analizados y proponer que sean mejorados siguiendo lo recomendado por COBIT 4.1.

- Presentar un informe ejecutivo a la Gerencia General de la empresa COCASINCLAIR EP, con las recomendaciones resultantes de la auditoría realizada.

1.4 Alcance de la Auditoría

Partiendo de la elaboración de la matriz de riesgos, se determinarán los seis procesos más relevantes de la Coordinación de TIC'S, el alcance de este proyecto de tesis, es justamente realizar una auditoría a estos procesos en la Coordinación de TIC'S de la empresa COCASINCLAIR EP, utilizando el marco de referencia COBIT 4.1.

De la revisión de estos procesos, se determinará el nivel de madurez y se presentarán las recomendaciones a la Gerencia General COCASINCLAIR EP, apegados a lo señalado en el marco de referencia COBIT 4.1.

Finalmente, se cumplirá con los objetivos específicos del proyecto y se presentará un informe ejecutivo a la Gerencia General de la empresa COCASINCLAIR EP con los resultados y recomendaciones para mejorar la administración de TIC'S alienadas al giro del negocio de la empresa.

1.5 Meta y metodología del proceso de la Auditoria

La meta es determinar la situación actual de la Coordinación de TIC'S por medio de la matriz de riesgos y de la auditoria a los seis procesos más relevantes identificados en la matriz, usando el marco de referencia COBIT 4.1 y proponer recomendaciones a la Gerencia General de COCASINCLAIR EP, para mejorarlos.

Se realizará una transferencia de conocimientos básicos sobre el marco de referencia COBIT 4.1 al personal técnico que trabaja en la Coordinación de TIC'S a medida que se realice la auditoria, para que sea una buena práctica la utilización de estos lineamientos para sus procesos.

Se utilizará la metodología de la matriz de riesgos aplicada a los procesos de la Coordinación de TIC'S, lo que permitirá tener una mejor visión de la situación actual de las actividades y el nivel de riesgos de los seis procesos más relevantes sujetos a esta auditoría.

1.6 Herramientas y técnicas para la Auditoría.

Dentro de las principales herramientas para realizar esta Auditoria están:

1. 6.1 Cuestionarios

Este es un conjunto de preguntas a las que el sujeto puede responder oralmente o por escrito, cuyo fin es poner en evidencia determinados

aspectos. La auditoría se materializará recabando información y documentación. El informes final será resultados del análisis de la información recopilada.

1.6.2 Entrevistas

Éstas recogen más información y mejor matizadas que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios. Se sigue cuidadosamente un sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con veracidad a una serie de preguntas variadas, también sencillas.

1.6.3 Check list

Es muy parecido a un cuestionario, este en realidad sirven para el cumplimiento sistemático de los cuestionarios.

1.6.4 Trazas y/o Huellas

Con frecuencia, se debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas y no otras. Se pueden apoyar en productos de software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa. Las trazas se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las trazas no deben modificar en absoluto el Sistema.

CAPÍTULO 2

GOBERNABILIDAD DE LA TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (TIC'S)

2.1 Generalidades y conceptos

La administración o gobernabilidad de las TIC'S puede ser un tema complejo por la gran cantidad de aspectos que involucra las Tecnologías de Información y Comunicación, a esto se le debe sumar el sinnúmero de herramientas de hardware y de software existentes en el mercado que en algún momento deben conjugarse en una empresa.

El activo más importante para una empresa ha llegado a ser sin duda la INFORMACIÓN que esta posee, justamente la administración de las TIC'S busca entre otros criterios, el asegurar este recurso a través de procesos estructurados y políticas para el área de TIC'S que permitan a la Gerencia tomar decisiones oportunas.

Consecuente con lo señalado en el párrafo anterior, a continuación se presentarán algunos conceptos de la información, su tratamiento y lo que busca una auditoría de TIC'S orientados a la aplicación de un estándar o un marco de referencia de buenas prácticas que permitan administrar las TIC'S.

2.1.1 La Información y su importancia

La información ha pasado a convertirse en un activo estratégico y en muchas ocasiones el más valioso de las organizaciones, que permite fundamentalmente tomar decisiones oportunas, esta puede estar almacenada en medios electrónicos o físicos. No importa el tipo o a qué área pertenece la información, la categorización o la importancia lo define cada empresa, pudiendo ser de carácter financiera, legal, administrativa, entre otras.

Por lo señalado anteriormente, este activo es necesario protegerlo, así como los sistemas que lo almacenan o procesan. Toda empresa posee información que necesita protegerla, a manera de ejemplo, la información de movimientos financieros de la empresa, nómina de empleados, análisis de la competencia, ventas, etc.

A continuación, se muestra una categorización de la información:

- **Información de acceso público,** la que no representa algún riesgo para la empresa.

- **Información de acceso autorizado,** requiere controles que garanticen el acceso y al tratamiento posterior, generalmente realizados en un sistema, como ejemplo: lectura, escritura, impresión, modificación y

eliminación. Es importante registrar este tratamiento por medio de bitácoras que permitan identificar la fecha, autor y proceso realizado.

- **Información sensible**, el acceso a este tipo de información requiere un tratamiento especial, que puede ser: encriptar la información, bloqueo de copia a dispositivos extraíbles, bloqueo de envió de archivos por correo electrónico que contenga el logotipo de la empresa, etc.

2.1.2 Seguridad de la Información.

La Seguridad de la Información, se enfoca en garantizar a través del uso de técnicas o estándares la confidencialidad, integridad y disponibilidad de la información almacenada en un sistema informático, además de la implementación de los elementos de control que regulen los aspectos físicos, lógicos y legales del sistema.

Actualmente se encuentra vigente la Norma Internacional ISO 27002, que es un conjunto de buenas prácticas en la Seguridad de la Información orientadas a cualquier empresa, esta Norma contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

2.1.3 ¿Qué es la Auditoria?

En términos generales, una Auditoria es una “Revisión independiente de una actividad determinada”, esta debe ser lo suficientemente objetiva, con la finalidad de evitar cualquier tipo de desconfianza de los resultados obtenidos.

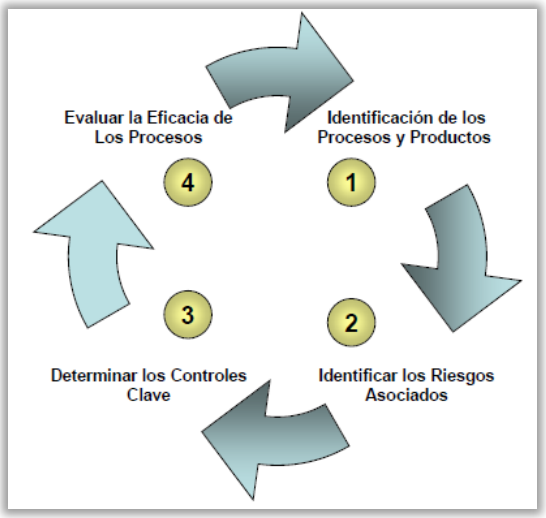


Figura No. 2-1 Metodología general de una auditoria

(Fuente: Administración y Auditoría de TIC’S – Ing. Giovanni Roldán)

La definición de Auditoria más aceptada es la formulada por el Comité de Conceptos de la Auditoria de la Asociación Americana de Contabilidad, que manifiesta lo siguiente:

“Un proceso sistemático para obtener y evaluar evidencia de una manera objetiva respecto de las afirmaciones concernientes a actos económicos y eventos para determinar el grado de correspondencia entre

estas afirmaciones y criterios establecidos y comunicar los resultados a los usuarios interesados" [1]

Los aspectos más importantes de esta definición son: al ser un proceso sistemático tiene una metodología, es decir son actividades estructuradas que siguen una secuencia lógica; al evaluar la evidencia en forma objetiva, los resultados de la auditoria estarán libres de suspicacia; y finalmente, la comunicación de resultados, hace referencia a la preparación de informes documentados y sustentados que son comunicados a la máxima autoridad con los resultados obtenidos en la Auditoria.

2.1.4 Auditoría en Informática

Así como existen muchas definiciones de auditoría, también existe gran variedad de definiciones de auditoría en informática que van de acuerdo al criterio de cada autor.

Solo para citar una de ellas, la Auditoría Informática se refiere a la revisión práctica que se realiza sobre los recursos informáticos con que cuenta una empresa u organización con la finalidad de emitir un informe sobre la situación en que se desarrollan y se utilizan esos recursos (José de Jesús Aguirre Bautista).

[1] Comité de Conceptos de la Auditoria de la Asociación Americana de Contabilidad

Luego de analizar varias fuentes de información, se puede concluir que la auditoría en Informática es la revisión y evaluación de los controles, sistemas y procedimientos de la informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; comparados con criterios establecidos, que dan como resultado un informe que contiene las recomendaciones para mejorar y optimizar sus procesos.

2.1.5 Normas para la práctica profesional de Auditoría

- Independencia
- Posición dentro de la Organización
- Objetividad con el uso de las evidencias
- Conocimientos de los procesos y del negocio
- Supervisión, en todos sus niveles.
- Cumplimiento de normas de conducta.
- Relaciones humanas y comunicaciones.
- Confiabilidad e integridad de la información.
- Cumplimiento de las leyes, políticas, estándares y procedimientos
- Resguardo de activos.
- Uso eficiente y económico de los recursos, a través de los controles.
- Logro de los Objetivos y Metas establecidas para las Operaciones.
- Planificación de la Auditoria.
- Examen y evaluación de la información.
- Comunicación de los resultados.
- Seguimiento de las recomendaciones anteriores.

Los auditores deben conceptualizar cada proceso de negocio luego que se hayan identificado los principales riesgos. Adicionalmente, conocer las partes estratégicas y operativas de la organización, y finalmente evaluar los aspectos de control.

2.1.6 Objetivos de la Auditoria Informática

El objetivo de la auditoria está enmarcado en el alance y en el área que será sujeta de la revisión, particularmente, en una auditoria informática los objetivos podrían ser:

- Analizar la eficiencia de los Sistemas Informáticos.
- Verificar el cumplimiento de la Normativa en este ámbito.
- Revisar la eficaz gestión de los recursos informáticos.
- Cumplir las metas y objetivos alineados al negocio.
- Brindar advertencia temprana de desviaciones o falta de controles, etc.

Para este trabajo de tesis, se tienen identificados el objetivo general y los objetivos específicos detallados en el numeral 1.3 Objetivos contenidos en el Capítulo I. Justamente, se realizará la auditoría utilizando el marco de referencia COBIT 4.1 (**Control Objectives for Information and related Technology**) que será descrito posteriormente en el numeral 2.6.

Es importante señalar que, la implementación de los planes de acción como resultado de las recomendaciones de la auditoría, conllevan a que se

minimicen los riesgos en TI en el corto o largo plazo, esto quiere decir que identificados los riesgos más críticos y luego de que se implementen los controles respectivos para esos riesgos, la administración de TI podrá establecer procesos que le permitan administrar de mejor manera los recursos informáticos, sean estos de hardware, software y servicios que brinda la Coordinación de TIC'S en COCASINCLAIR EP.

2.1.7 Importancia de la Auditoria Informática.

Uno de los activos más importantes para las empresas es la información que ellos disponen, para la empresa COCASINCLAIR EP es un recurso estratégico por el tipo y la complejidad del diseño utilizado para la construcción de la Central Hidroeléctrica. Mucha de esta información se encuentra en los servidores, medios de almacenamiento y equipos de computación de los usuarios finales, que requieren una revisión de cómo ésta está siendo tratada, así como la revisión de los controles en los procesos que se realizan dentro de la Coordinación de TIC'S para salvaguardar este recurso.

Los mecanismos o controles implementados, buscan mejorar la administración de las TIC'S, justamente la importancia de una auditoria de TIC'S es llegar a determinar la situación de la Coordinación utilizando el marco de referencia COBIT 4.1 y posteriormente detallar las recomendaciones en el informe para la Gerencia General. Se debe aclarar

que un plan de acción no está contemplado dentro del alcance de este trabajo de tesis.

De igual manera, las auditorías son importantes realizarlas porque puede existir rotación de personal interno en la Coordinación y es necesario que los procesos estén claramente definidos y conozcan los controles que se deben ejecutar. Adicionalmente, pueden existir cambios en las normativas o procedimientos dentro de COCASINCLAIR EP que requieren una revisión, y finalmente, porque es saludable un informe imparcial que determine la situación de la Coordinación de TIC'S que permita implementar mejoras en sus procesos.

2.1.8 Fases de una Auditoria Informática.

Las fases de una auditoria son:

- Planeación
- Revisión Preliminar
- Revisión Detallada
- Examen y evaluación de la información
- Pruebas de consentimiento
- Pruebas de controles de los usuarios, y
- Pruebas sustantivas.

Para realizar una correcta auditoría, es necesario realizar una efectiva planeación, esta es la primera fase, en la que se contempla las actividades más importantes como ejemplo: personal involucrado, recursos a utilizar, tiempo estimado, claramente debe estar señalado el objetivo y el alcance de la auditoría.

Luego de la planeación, se debe proceder con la revisión preliminar. El objetivo de esta fase es obtener la información necesaria para que el auditor conozca cómo proceder con la auditoría.

La tercera fase de una auditoría, es la revisión detallada. Esta consiste en obtener información para tener un profundo conocimiento de los controles implementados en el área de informática.

Posteriormente, se encuentran las fases de examen y evaluación de la información, seguida de la fase de pruebas de consentimiento, pruebas de controles de los usuarios y finalmente las pruebas sustantivas. En esta última fase se obtiene la evidencia suficiente que le permite al auditor emitir las conclusiones y recomendaciones de la revisión.

De acuerdo a lo señalado en el alcance de este trabajo de tesis, la auditoría se lo realizará evaluando el cumplimiento de los objetivos de control de los procesos relevantes, que son el resultado de aplicar los criterios de seguridad de la información (confidencialidad, integridad y disponibilidad).

2.1.9 Ejemplo de propuesta de servicios de una Auditoría en Informática.

En el Anexo No.1, se muestra a manera de ejemplo, una propuesta utilizando una metodología tradicional de una Auditoría Informática.

2.2 La Auditoria y el Control Interno

El Control Interno, es un proceso integrado a los demás procesos de una organización, diseñado con el objeto de proporcionar una garantía razonable para el logro de objetivos incluidos en las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes, reglamentos y políticas. [2]

Al tratarse el Control Interno como un proceso, se hace referencia a una cadena de acciones extendida a todas las actividades, inherentes a la gestión e integrados a los demás procesos básicos de la empresa: planificación, ejecución y supervisión. Las acciones se hallan incorporadas a la estructura orgánica de COCASINCLAIR EP, para influir en el cumplimiento de los objetivos estratégicos y operativos de las Subgerencias y Coordinaciones.

[2] Tomado del Informe COSO

El Control Interno relaciona a todas las áreas de la empresa que realizan algún tipo de control de acuerdo a sus funciones o su ámbito de acción, estas áreas son las siguientes:

- Directorio
- Gerencia General
- Auditoría Interna
- Toda la Organización o Empresa.

En el caso particular de la empresa COCASINCLAIR EP, el Directorio que está compuesto por el Ministro de Electricidad y Energía Renovable (Presidente), Secretario Nacional de Planificación o su Delegado y un Delgado de la Presidencia de la República, que son quienes determinan la visión global de la supervisión del proyecto hidroeléctrico. A través de reuniones de Directorio, se presenta la información requerida por este cuerpo colegiado por parte de la Gerencia General y se establecen las directrices para el funcionamiento de la Empresa. En muchas ocasiones, la información puede ser requerida por aspectos particulares, en momentos diferentes y no necesariamente para una sesión de Directorio, lo importante es contar con la información oportuna y que a su vez ésta sirva de medio de control para conocer la situación actual de la Empresa.

La otra área importante del Control Interno dentro de la empresa COCASINCLAIR EP es la Gerencia General, quien a más de establecer las directrices también las implementa a través de políticas y procedimientos de control (controles) más específicos por Subgerencias y hasta

Coordinaciones. De acuerdo al control que se quiere implementar o realizar un seguimiento, la Gerencia General delega funciones de control y de seguimiento a la Subgerencia de Gestión y Planificación en temas específicos como son: Gobierno por Resultados, Implementación del Sistema de Gestión Integrado (normas ISO 9000, 14000 y 18000), entre otros.

Figura No. 2-2 Relación de la Auditoría y el Control Interno

(Fuente: Administración y Auditoría de TIC'S – Ing. Giovanni Roldán)

La tercera área que realiza el Control Interno es propiamente la Auditoría Interna de la Empresa, la que entre sus obligaciones está el realizar las revisiones planificadas y periódicas de los controles internos diseñados e implementados. Justamente, la revisión del diseño o las salidas

de los controles permiten al Auditor determinar el grado de cumplimiento del control contrastando con los objetivos que se persiguen.

Finalmente, toda la empresa COCASINCLAIR EP, realiza el Control Interno por medio de la verificación del cumplimiento de los criterios establecidos contra las evidencias encontradas para determinar los hallazgos, los mismos que son comunicados a las Sugerencias para que se tomen las acciones pertinentes. Los hallazgos pueden ser problemas o novedades que necesitan atención por parte de las Subgerencias o la Gerencia General, sean estas detectadas en las oficinas en Quito o en el Campamento de San Rafael.

Como información adicional referente al Control Interno, según la Comisión de Normas de Control Interno de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), el Control Interno puede ser definido como el plan de la organización, y el conjunto de planes, métodos, procedimientos y otras medidas de una institución, tendientes a ofrecer una garantía razonable de que se cumplan los siguientes objetivos principales:

- Promover operaciones metódicas, económicas, eficientes y eficaces, así como productos y servicios de la calidad esperada.

- Preservar al patrimonio de pérdidas por despilfarro, abuso, mala gestión, errores, fraudes o irregularidades.

- Respetar las leyes y reglamentaciones, como también las directivas y estimular al mismo tiempo la adhesión de los integrantes de la organización a las políticas y objetivos de la misma.

- Obtener datos financieros y de gestión completos y confiables y presentados a través de informes oportunos.

2.3 Control Interno Informático

"Es aquel control, que controla diariamente que todas las actividades de los sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la Dirección de la Organización y/o la Dirección de Informática, así como los requerimientos legales" [3].

Para realizar este control se lo puede hacer por medio de un Comité, el que debe encargarse de hacer cumplir los objetivos de control, tales como: las actividades se realicen cumpliendo los procedimientos y normas fijadas, asesoramiento en las normas, apoyar el trabajo de la auditoría informática, entre otros.

[3] Tomado del libro: Auditoría Informática Un enfoque práctico, Mario Piattini y Emilio del Peso

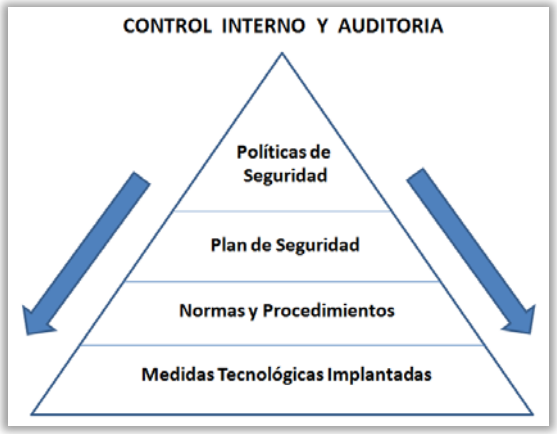


Figura. No. 2-3 Control Interno Informático

Existen varios tipos de control interno, entre los que podemos destacar:

Controles preventivos: para tratar de evitar el hecho, a manera de ejemplo puede ser el software de seguridad que impida el acceso no autorizado al sistema.

Controles detectivos: estos aparecen cuando fallan los controles preventivos, como, el registro de intentos de acceso no autorizado.

Controles correctivos: por medio de ellos, se vuelve a la normalidad cuando se hayan producido incidencias.

2.4 Componentes del Control Interno

C.O.S.O por sus siglas en inglés, The **Committee of Sponsoring Organizations** of the Treadway Commission, es un marco de referencia

(Informe COSO) que define el control interno como un proceso diseñado para proveer un margen razonable de confiabilidad en relación al alcance de los objetivos de control en las siguientes categorías:

- Eficiencia y eficacia de las operaciones,
- Confianza en los sistemas de reportes financieros
- Adherencia con las leyes y regulaciones existentes.

En COSO se menciona 5 componentes relacionados entre sí y su implementación depende del tamaño de la empresa. Estos componentes son:

1) Ambiente de control.

2) Evaluación de riesgos.

3) Actividades de control.

4) Información y comunicación.

5) Supervisión y monitoreo.

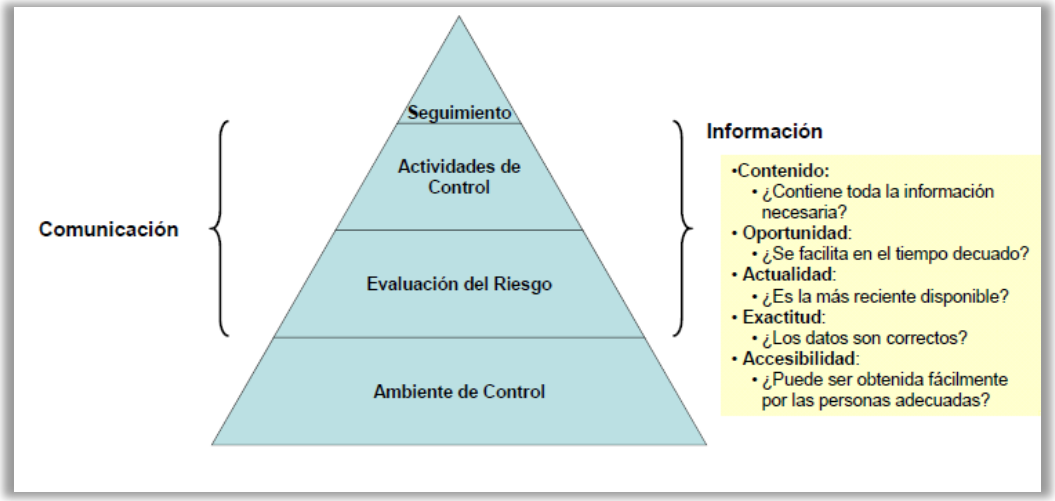


Figura No. 2-4 Pirámide COSO

(Fuente: Administración y Auditoría de TIC'S – Ing. Giovanni Roldán)

2.4.1 Ambiente de control

Define al conjunto de circunstancias que enmarcan el accionar de la organización desde la perspectiva del control interno y que son por lo tanto determinantes del grado en que los principios del control interno dominan sobre las conductas y los procedimientos organizacionales.

Sobre este punto, el ambiente laboral o el clima organizacional, están definidos por la socialización de su Plan Estratégico y Operativo a las Subgerencias y Coordinacións en COCASINCALIR EP, los funcionarios se sienten identificados con la empresa y con las 3C (compromiso, cumplimiento y calidad). En el mes de septiembre de 2012, se aprobó el estatuto por procesos de la Empresa a través de su Directorio.

Se espera que en los meses siguientes, se obtenga la certificación en el Sistema de Gestión Integrado, esto es la certificación en las normas ISO 9000, 14000 y 18000, lo que permitirá realizar un mejor control de la supervisión del proyecto hidroeléctrico por medio de la revisión del cumplimiento de estas normas.

Los principales factores del ambiente de control, en forma general son:

- La filosofía y estilo de la dirección y la gerencia.
- La estructura de la empresa, el plan organizacional, los reglamentos y los manuales de procedimiento.

- La integridad, los valores éticos, la competencia profesional y el compromiso de todos los componentes de la organización, así como su adhesión a las políticas y objetivos establecidos.
- Las formas de asignación de responsabilidades y de administración y desarrollo del personal.
- El grado de documentación de políticas y decisiones, y de formulación de programas que contengan metas, objetivos e indicadores de rendimiento.

2.4.2 Evaluación del riesgo

El Control Interno ha sido pensado esencialmente para controlar o minimizar los riesgos que afectan a las actividades de las organizaciones. A través de la revisión de los procesos más relevantes de la Coordinación de TIC'S y de acuerdo a los resultados obtenidos de los controles implementados, se busca neutralizar esos riesgos y evaluar la vulnerabilidad.

El grado de conocimiento de las áreas de la empresa COCASINCLAIR EP y particularmente de la Coordinación de TIC'S, la estructura orgánica, los procesos internos, las atribuciones y responsabilidades, así como de los productos o servicios de esta Coordinación, permitirán identificar los puntos débiles, enfocados en priorizar los riesgos.

El grado de cumplimiento de los controles en los procesos identificados, serán evaluados utilizando el marco de referencia COBIT 4.1. Los riesgos que se identifiquen en el capítulo III, corresponderán al resultado de la elaboración de una matriz de riesgos, en la que se pueda identificar los procesos relevantes, tomando en cuenta la confidencialidad, integridad y disponibilidad de la información (Seguridad de la Información).

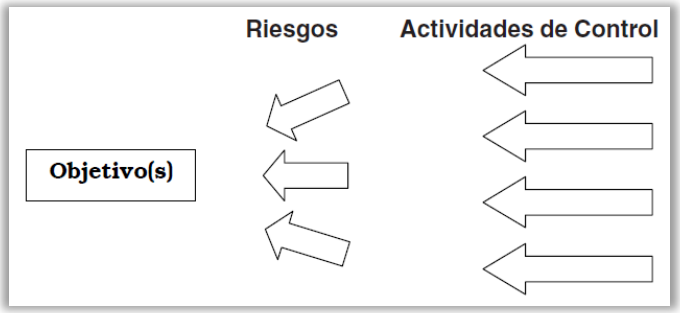


Figura No. 2-5 Evaluación de Riesgos

El escogimiento de los riesgos estará relacionado con el impacto potencial en los cambios en el entorno de la Coordinación de TIC'S, redefiniciones de la política interna, reorganización de la Coordinación, nuevos sistemas informáticos, procedimientos y tecnologías implementadas en la empresa COCASINCLAIR EP.

2.4.3 Actividades de control

Las actividades de control se ejecutan en todos los niveles de la empresa COCASINCLAIR EP y en cada una de las etapas de la gestión (Subgerencias y Coordinaciones) como ya se mencionó anteriormente en la Figura No. 2-2 Relación de la Auditoría y el Control Interno.

Identificados los riesgos, se deben implementar los controles destinados a evitarlos o minimizarlos, los cuales estarán enfocados con la parte operativa de la Coordinación de TIC'S.

2.4.4 Información y comunicación

La comunicación es inherente a los sistemas de información. Dentro de la Coordinación de TIC'S no están detalladas de manera formal las responsabilidades de gestión y control para cada funcionario, se espera determinar la manera como comunicar la información relevante que se genere en Quito y en el Campamento San Rafael a un nivel superior, en este caso la Subgerencia Administrativa, por medio de un canal establecido interno, que puede ser correo electrónico o memorandos.

Se presentará de forma periódica y oportuna la información en la Coordinación de TIC'S con la finalidad que permita orientar sus acciones, hacia el mejor logro de los objetivos.

2.4.5 Supervisión y Monitoreo

El objetivo es asegurar que el control interno funciona adecuadamente, a través de dos modalidades de supervisión: actividades continuas o evaluaciones puntuales.

Por medio del Sistema de Gestión Integrado de la empresa COCASINCLAIR EP, utilizado como una herramienta de gestión, se realizará el monitoreo del cumplimiento de los controles establecidos para el proceso TIC'S detallados en la matriz de caracterización del proceso. Además por los informes de las auditorías internas y de gestión realizadas en la Empresa.

2.5 Continuidad del Negocio

Los riesgos que se presentan en una empresa, están relacionados directamente a una posible afectación de las operaciones del negocio o en no poder seguir prestando el servicio en óptimas condiciones. Por consiguiente es necesario elaborar un plan que garantice la continuidad del negocio, partiendo de realizar acciones para mitigar los riesgos críticos.

Un Plan de Continuidad del Negocio (BCP, por sus siglas en inglés), tiene como objetivo el mantenimiento de los servicios y procesos críticos de una empresa, así como la reducción de impactos ante imprevistos de indisponibilidad o desastres para un plazo y costo razonable, es decir, se debe contar con un plan global que garantice la cobertura técnica y organizativa adecuada de las áreas críticas de negocio para que sigan prestando su servicio cuando se presente una amenaza.

El objetivo de un BCP, es que los servicios o procesos del negocio vuelvan al estado normal de producción que tenían antes de la interrupción. Generalmente, un BCP, es una concepción gerencial que se basa en el

entendimiento de los procesos críticos de la empresa, los elementos que soportan la operación (recursos - infraestructura tecnológica) y el riesgo que representa la paralización total o parcial del mismo en términos de pérdidas financieras u oportunidades de negocio.

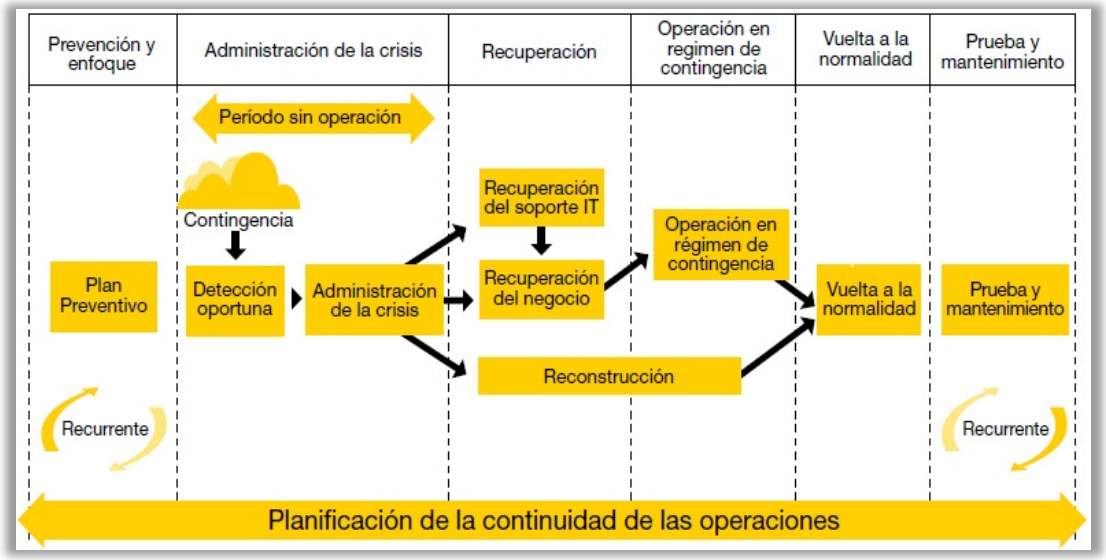


Figura No. 2-6 Enfoque Fast Track para desarrollar un BCP

(Fuente: Desarrollando un Plan de Continuidad del Negocio, PricewaterhouseCoopers)

Es fundamental que para la implementación exitosa de un BCP, contar con la participación y compromiso del personal involucrado (60%) y disponer de la infraestructura requerida (35%) para sustentar las estrategias de recuperación en el Plan (5%).

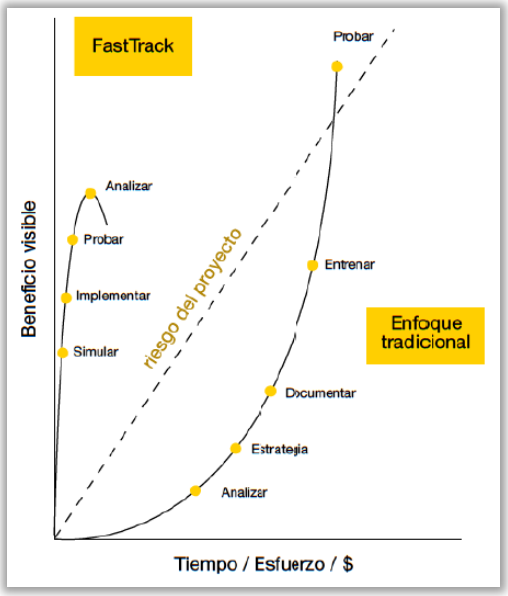


Figura No. 2-7 Enfoque Fast Track para el desarrollo del BCP

(Fuente: Desarrollando un Plan de Continuidad del Negocio, PricewaterhouseCoopers)

El BCP es lo mismo que un Plan de Contingencias, “Es una estrategia planificada construida por: un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio afectados por una paralización total o parcial de la capacidad operativa de la empresa” [4].

El Plan de Continencias, consiste en los pasos que el personal debe realizar para hacer frente a las situaciones inesperadas que pueden afectar a la continuidad de su negocio. Puesto que el tiempo es un factor crucial en las situaciones de emergencia, se hace necesario disponer de planes de

[4] Fuente: Auditoria Informática- Un enfoque práctico, Mario Piattini y Emilio del Peso.

respaldo que permitan una rápida reacción ante cualquier incidencia producida por hackers, virus, desastres naturales, caídas de redes, etc.

No solo comprende los sistemas informáticos, sino también la integración de los mismos con su modelo de negocio y se desarrolla situaciones hipotéticas que pudieran afectar a la continuidad del servicio de los sistemas informáticos.

Las fases de un plan de contingencia son las siguientes:

1. Análisis y diseño (se enfoca en el análisis de riesgos e impactos en el negocio).
2. Desarrollo del plan (desarrollo de la estrategia, implantación de acciones, plan de vuelta a la normalidad)
3. Pruebas y mantenimiento (se definen estrategias y procedimientos)

En la empresa COCASINCLAIR EP, no se dispone de un Plan de Contingencias, se tiene previsto implementar en el presente año.

Una vez realizado el Análisis de Riesgos, es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre, ya sea natural o técnico, considerando todas las áreas críticas de la empresa.

Es importante contar con la documentación completa del plan de contingencias para ser usada en caso de un desastre. En plan de

recuperación de desastres también debe ser documentado, registrado (datos, archivos, papelería) y los recursos necesarios para operar en óptimas condiciones.

Como todo plan, se debe entrar en una fase de prueba de recuperación para asegurase de que el plan funciona en forma eficiente, tanto en forma separada como integral (sistema).

Los planes deben ser periódicamente actualizados o revisados, dependiendo de cuando exista un cambio en los procesos de las áreas críticas identificadas dentro del plan.

2.6 Marco de Referencia Cobit 4.1

2.6.1 Generalidades

La administración o gobernabilidad de las TIC'S involucra muchos aspectos de tecnologías de información, que van acompañados de un sinnúmero de herramientas de hardware y de software existentes en el mercado que en algún momento deben conjugarse. Precisamente, para hacer más fácil la administración de las TIC'S, debe existir un conjunto de políticas y estándares que nacen de las buenas prácticas orientadas a procesos y alineadas con las estrategias de la empresa.

Gestionar las TIC'S, requiere la definición de responsabilidades para los miembros del área, mecanismos para un uso eficiente y eficaz de los recursos, concienciar a la alta gerencia acerca de los costos de TI, brindar soporte técnico a la empresa con parámetros de evaluación del servicio, así como proponer la reducción de costos mediante la estandarización.

La definición de Gobernabilidad de Tecnologías de Información de acuerdo al IT Governance Institute, es "El manejo o administración de las TIC es responsabilidad tanto de la dirección tanto como de la administración ejecutiva. Es parte integral del manejo empresarial y consiste en el liderazgo, las estructuras de la organización y los procesos para asegurar que TI mantenga y amplíe los objetivos y estrategias de la empresa." [5]

"Una estructura de relaciones y procesos para dirigir y controlar la empresa con el fin de alcanzar los objetivos empresariales mediante la adición de valor que balancean el riesgo frente a TI y sus procesos." [6]

2.6.2 Estándares en el mercado para la administración de TIC'S

El objetivo de los estándares es proveer marcos referenciales de tal manera que el Director de Tecnología provea a la Gerencia General capacidades para entender mejor los servicios y procesos de TI.

[5] COBIT 4.1
[6] COBIT 4.1

Las organizaciones podrán considerar y usar una variedad de modelos, estándares y mejores prácticas de TI. Estos deben ser comprendidos para analizar cómo pueden ser utilizados en conjunto.

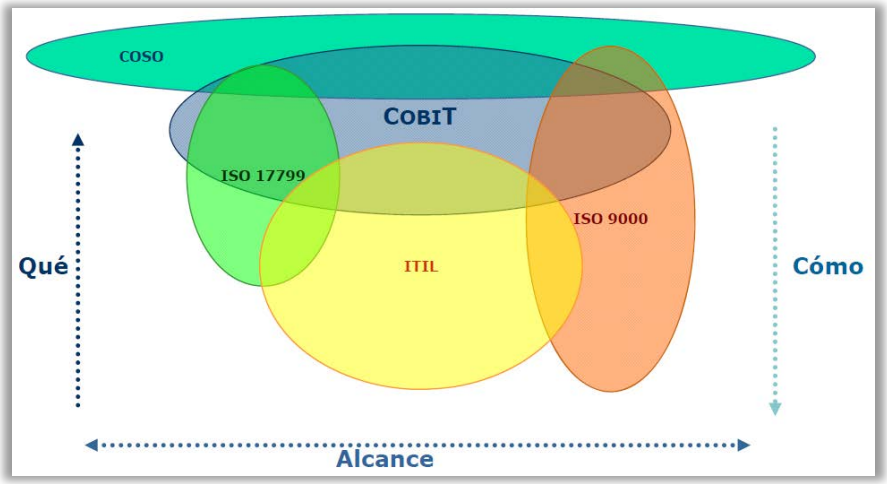


Figura No. 2-8 Estándares y mejores prácticas en el mercado

(Fuente: Administración y Auditoría de TIC'S – Ing. Giovanni Roldán)

- COSO, The **Committee of Sponsoring Organizations** of the Treadway Commission, es un marco de referencia de control ampliamente aceptado para gobierno corporativo y para la administración de riesgos, así como a marcos compatibles similares.

- COBIT, **Control Objectives for Information and related Technology,** es un marco de referencia para la administración de TIC'S que provee herramientas administrativas como métricas y modelos de madurez para complementar el marco de referencia de control, propuesto por el IT Governance Institute.

- ITIL IT Infrastructure Library, es una colección de “best practices” en la administración del servicio de TIC.

- CMMi Capability Maturity Model Integrated, modelo que propone un conjunto de prácticas maduras para mejorar la calidad del proceso de desarrollo del software y de los sistemas.

- ISO/IEC 17799:2000, 27001:2005 Code of Practice for Information Security Management, estándar internacional de seguridad de la información.

- ISO 9001, específica los requisitos para un Sistema de Gestión de la Calidad (SGC) que pueden utilizarse para su aplicación interna por las organizaciones.

COBIT brinda 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.

Como se muestra en la siguiente figura, COBIT fue concebido únicamente como una herramienta de apoyo para la auditoria,

posteriormente se fueron actualizando las versiones hasta llegar a considerarse como un estándar que involucra el gobierno de TI.

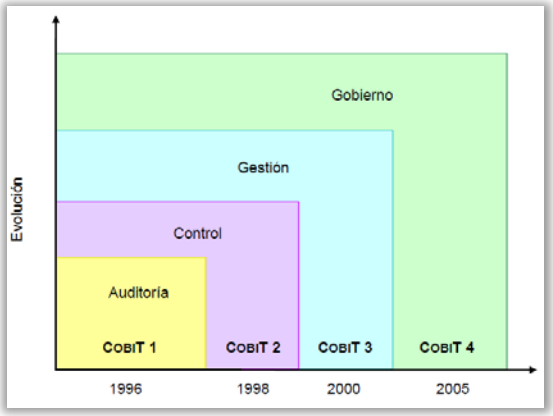


Figura No. 2-9 Actualizaciones de COBIT

(Fuente: Actualizaciones de COBIT, www.isaca.org/cobit)

"La misión de COBIT es 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" [7],es esto es justamente lo plasmado en la versión 4.1.

COBIT es un marco de referencia y no un "recetario" entendido como la panacea de la administración de TI, COBIT está alineado con otros estándares y buenas prácticas y puede ser usado junto con ellos. Las organizaciones deben analizar sus requerimientos de control y adaptar

[7] COBIT 4.1

COBIT con base a sus impulsores de valor, perfil de riesgos o la infraestructura, organización y portafolio de proyectos de TI.

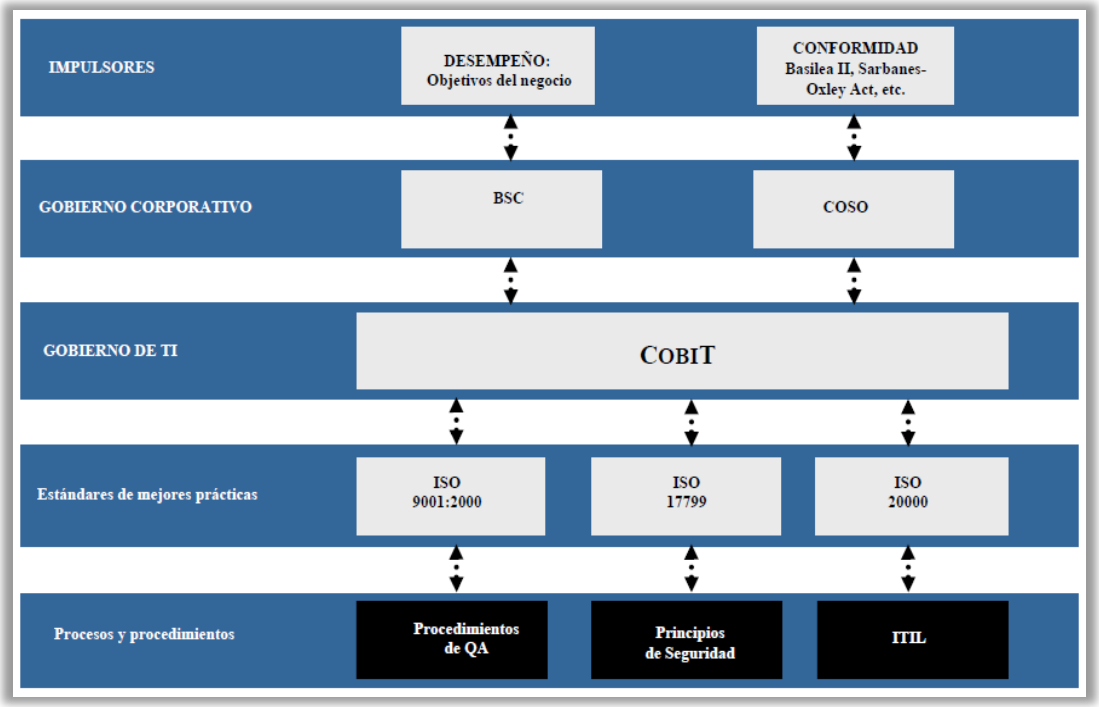


Figura No. 2-10 COBIT dentro de una empresa

(Fuente: Gobernabilidad de la Tecnología – Ing. Giovanni Roldán C.)

El marco de referencia COBIT se basa en la premisa de que TI debe entregar la información que la empresa requiere para alcanzar sus objetivos.

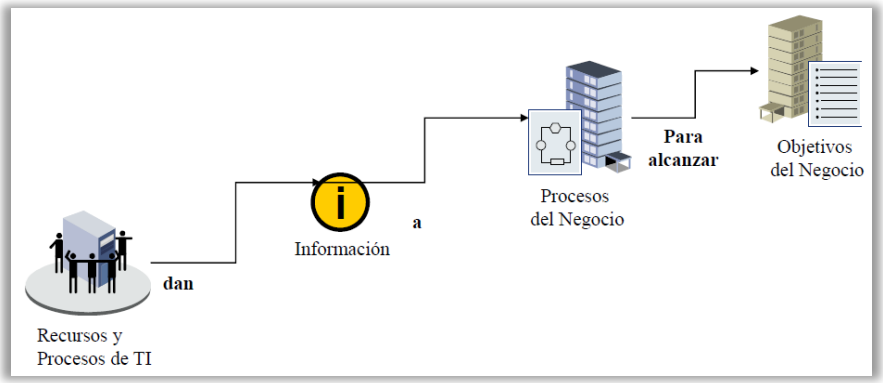


Figura No. 2-11 Premisa de COBIT

(Fuente: Gobernabilidad de la Tecnología – Ing. Giovanni Roldán C.)

2.6.3 Áreas de enfoque del gobierno de TI

COBIT da soporte al gobierno de TI al brindar un marco de trabajo que garantiza que:

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

La medición del desempeño es esencial para el gobierno de TI. COBIT le da soporte e incluye el establecimiento y el monitoreo de objetivos que se puedan medir, referentes a lo que los procesos de TI que requieren generar (resultado del proceso) y cómo lo generan (capacidad y desempeño del proceso).

Figura No. 2-12 Áreas de enfoque del gobierno de TI

(Fuente: COBIT 4.1)

- Alineamiento Estratégico.- Centrado en garantizar el vínculo entre los planes del negocio y los de TI; en definir, mantener y validar las propuestas de valor de TI; y en alinear las operaciones de TI con las de la empresa.

- Entrega de Valor.- Tiene que ver con la ejecución de la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI entregue los beneficios prometidos en la estrategia, concentrándose en la optimización de costos y en brindar el valor intrínseco de TI.

- Gestión de Recursos.- Se refiere a la optimización de las inversiones y la adecuada administración de los recursos críticos de TI: aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización del conocimiento y de la infraestructura.

- Gestión de Riesgos.- Requiere una conciencia de los riesgos en los más altos ejecutivos de la organización, una clara comprensión del apetito al riesgo de la empresa, el entendimiento de los requerimientos de cumplimiento, transparencia acerca del significado de los riesgos, y una clara determinación de las responsabilidades relacionadas con los riesgos en la organización.

- Evaluación de Desempeño.-. Seguimiento y monitoreo de la implementación de la estrategia, la ejecución de los proyectos,

utilización de recursos, desempeño de los procesos y entrega de servicios mediante la utilización, por ejemplo, de BSC que traduzca la estrategia en acción para posibilitar la medición de los objetivos más allá de la contabilidad convencional.

2.6.4 Componentes de COBIT

Como respuesta a las necesidades del gobierno de TI, 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.

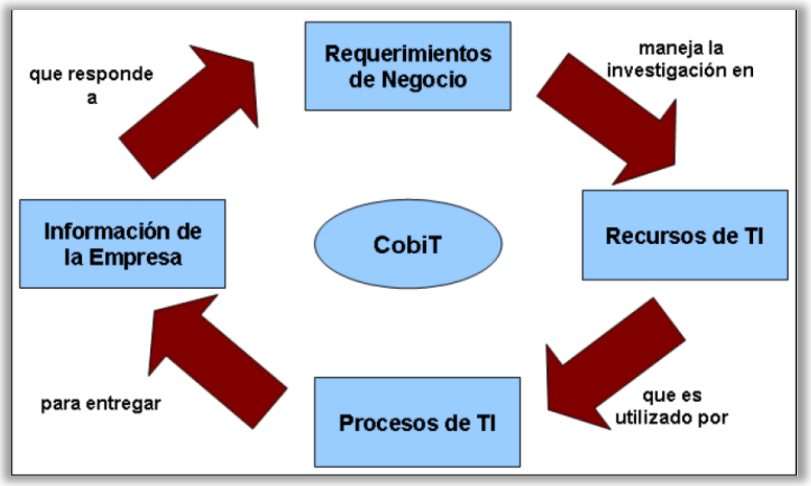


Figura No. 2-13 Principio Básico de COBIT

(Fuente: COBIT 4.1)

2.6.4.1 Criterios o requerimientos de información

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:

- 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.

- Eficiencia, consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.

- Confidencialidad, se refiere a la protección de información sensitiva contra revelación no autorizada.

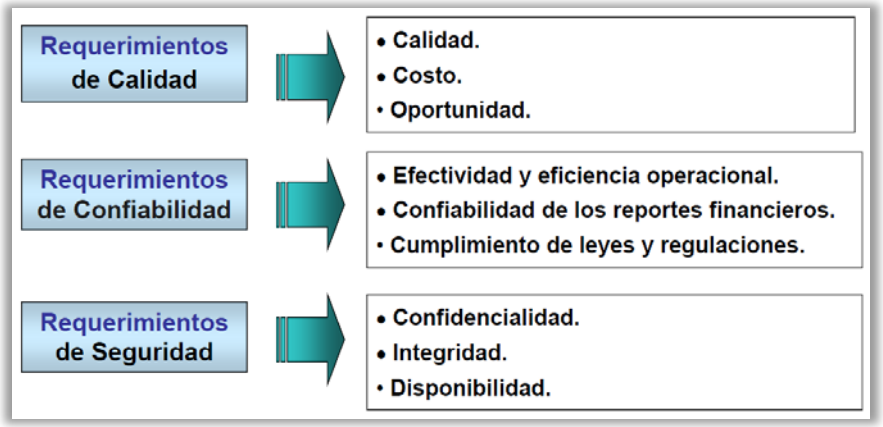


Figura No. 2-14 Criterios o requerimientos de información

- 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.

- 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.

- 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.

- Confiabilidad, se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

2.6.4.2 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.

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

- Aplicaciones, incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

- 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.

- 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.

- 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.

2.6.4.3 Procesos de TI

Los principales procesos de TI que incluye COBIT entre sus componentes son:

- **Arquitectura,** COBIT es un marco de referencia para entender y evaluar las iniciativas de largo y corto plazo de la organización, es un estándar para implementar y soportar las TIC'S alineado a las metas de la empresa.

- **Seguridad de información,** el considerarse la información como un activo, se debe buscar la Confidencialidad, Integridad y Disponibilidad de la misma. Como aspectos relacionados con la seguridad, también están la identificación, autorización, controles de acceso y administración, responsabilidad, detección de incidentes.

La seguridad de la información se aplica a todos las aplicaciones, procesos, productos/servicios y tecnologías.

Figura No. 2-15 Principales procesos de la administración de TI.

(Fuente: Gobernabilidad de Tecnología – Giovanni Roldán C.)

- Manejo del cambio, proceso para planear, calendarizar, aplicar, distribuir y hacer seguimiento de cambios. El objetivo es asegurar la integridad y confiabilidad de los ambientes de todas las TIC´s y otros servicios como energía, aire, incendios, etc., además, aplica a procedimientos referentes a clasificación, riesgo, impacto, análisis y revisión post-implementación.

- Manejo del software, se refiere al control estricto y adecuado de las licencias de uso del software comercial. Evaluar y documentar la decisión de comprar o desarrollar en términos de calidad, costo, funcionalidad y oportunidad. Además, aquí se controla Procedimiento para controlar la copia, distribución y uso del software.

- Contingencia, es una responsabilidad de todas las áreas de la empresa y no de Tecnología. Se debe considerar como una parte integral de la operación del negocio. Debe ser implementado por medio de procesos documentados por áreas con planes formales de prueba, capacitación y entrenamiento.

Como objetivos de la contingencia son:

Prevenir: minimizar la probabilidad de interrumpir las operaciones.

Minimizar: mantener los niveles de servicio disponibles al máximo posible.

Recuperar: restaurar los servicios en el menor tiempo posible y con el menor impacto.

- Manejo de problemas, este proceso trata de asegurar la resolución temprana de problemas y comunicar el impacto. Mejorar la disponibilidad y eficiencia de los servicios minimizando la interrupción por problemas.

- Contrataciones y tercerización, se refiere a evaluar al proveedor de su capacidad para entregar el servicio, experiencia y condición financiera. Se debe tener la capacidad para implementar controles, como si fuera un proceso Interno y debe haber un plan de contingencia del proveedor o servicio.

- Manejo de proyectos, para la implementación exitosa de los proyectos, se requiere que el producto final cumpla con los objetivos de negocio en términos de funcionalidad, tiempo y presupuesto. Como puntos a considerar, los proyectos deben contener: autorización, alcance escrito y acordado con el auspiciante, planeamiento, planificación, recursos, costos, ciclos de vida definidos y entregables, roles y responsabilidades, comunicación, identificación y plan de riesgos, seguimiento y administración, manejo del cambio, revisiones gerenciales y revisiones post-implementación.

- Manejo de recursos, el objetivo es asegurar la integridad, disponibilidad, confiabilidad y eficiencia de los recursos necesarios para soportar el procesamiento de la información. Involucra la administración de niveles de servicio interno y externo, administración de infraestructura y procesos, control y seguimiento del inventario Hardware y Software.

2.6.4.4 Dominios

COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

Para gobernar efectivamente TI, es importante determinar actividades y los riesgos que requieren ser administrados.
Estos dominios son:

- 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.

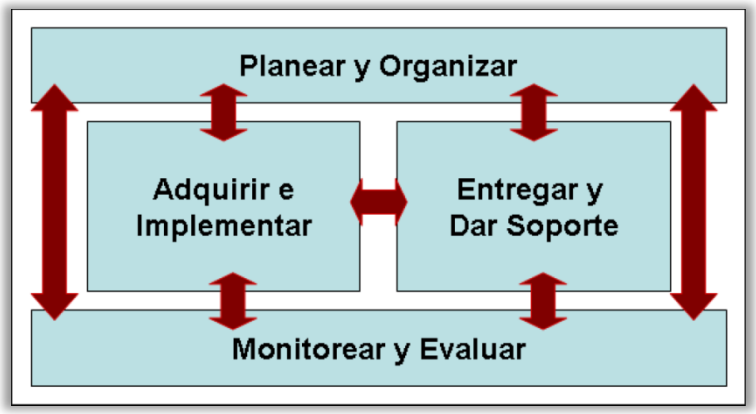


Figura No. 2-16 Los cuatro dominios interrelacionados de COBIT.

2.6.4.4.1 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:

¿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?

2.6.4.4.2 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 sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

Este dominio, por lo general, cubre los siguientes cuestionamientos:

¿Es probable que los nuevos proyectos generen 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?

2.6.4.4.3 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.

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?

2.6.4.4.4 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.

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 4.1 ha identificado 34 procesos de TI que pueden ser utilizados para verificar que se completen las actividades y responsabilidades; sin embargo, no es necesario que se apliquen todas, y, aún más, se pueden combinar como se necesite por cada empresa.

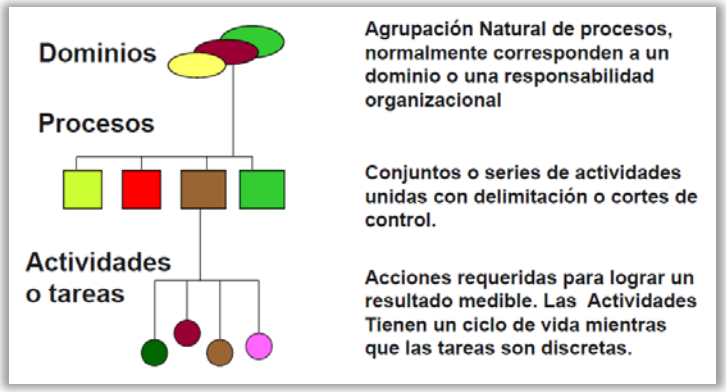


Figura No. 2-17 Niveles de COBIT

(Fuente: Gobernabilidad de las TIC'S, Ing. Giovanni Roldán C.)

Para cada uno de estos 34 procesos, tiene un enlace a las metas de negocio y metas de 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.

2.6.5 Cubo de COBIT

El marco de trabajo COBIT, relaciona los requerimientos de información y de gobierno a los objetivos de la función de servicios de TI. El modelo de procesos COBIT permite que las actividades de TI y los recursos que los soportan sean administrados y controlados basados en los objetivos de control de COBIT, y alineados y monitoreados usando las metas y métricas de COBIT.

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.

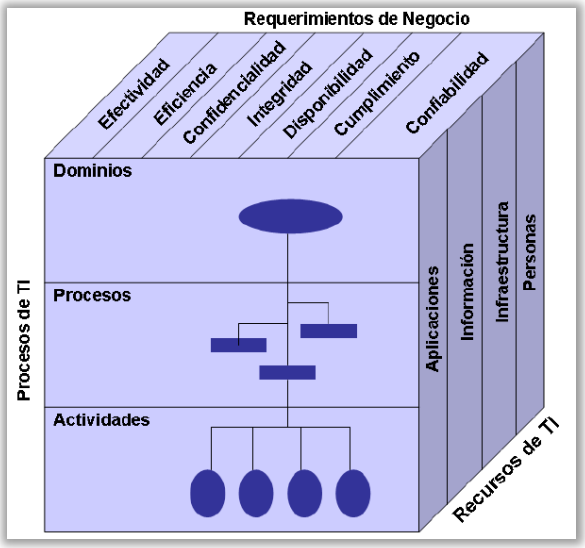


Figura No. 2-18 El Cubo de COBIT

2.6.6 Modelos de madurez

Para conocer que tan bien está administrado TI, se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información, se debe considerar el equilibrio del costo beneficio.

La dirección de TI busca 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 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 (SEI) definió para la madurez de la capacidad del desarrollo de software.

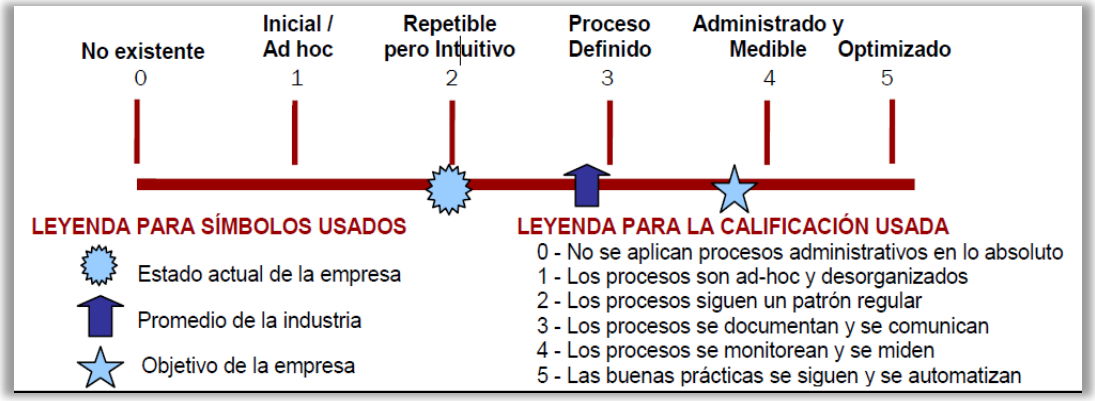


Figura No. 2-19 Representación Gráfica de los Modelos de Madurez

(Fuente: COBIT 4.1)

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.

La ventaja de un modelo de madurez es que es relativamente fácil para la dirección ubicarse a sí misma en la escala y evaluar qué se debe hacer si se requiere desarrollar una mejora. La escala incluye al 0 ya que es muy posible que no existan procesos en lo absoluto. La escala del 0-5 se basa en una escala de madurez simple que muestra como un proceso evoluciona desde una capacidad no existente hasta una capacidad optimizada.

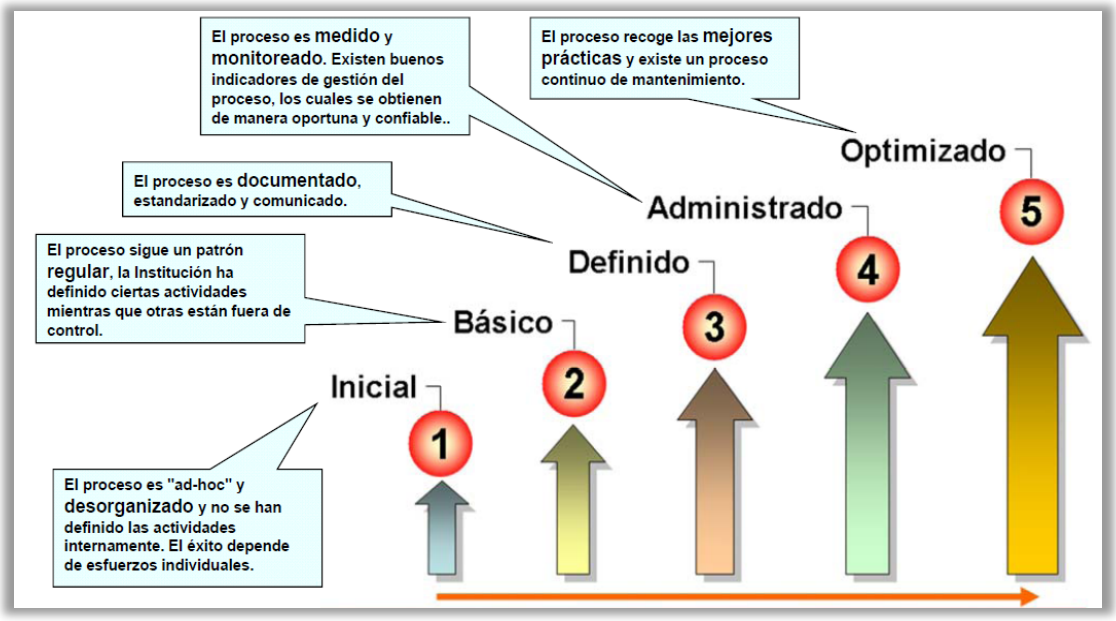


Figura No. 2-20 Niveles de Madurez

(Fuente: La Madurez de los Procesos Empresariales – Ing. Giovanni Roldán)

A continuación se detallan los atributos o factores de evaluación de la Madurez.

Nivel	Conciencia y Comunicación	Políticas, Estándares y Procedimientos	Herramientas y Automatización	Habilidades y Experiencia	Responsabilidad y Rendición de Cuentas	Establecimiento y Medición de Metas
1	Surge el reconocimiento de la necesidad del proceso. Existe comunicación esporádica de los problemas.	Existen enfoques ad hoc hacia los procesos y las prácticas. Los procesos y las prácticas no están definidos	Pueden existir algunas herramientas; el uso se basa en herramienta estándar de escritorio. No existe un enfoque planeado para el uso de herramientas	No están definidas las habilidades requeridas para el proceso. No existe un plan de entrenamiento y no hay entrenamiento formal.	No existe definición de responsabilidades y de rendición de cuentas. Las personas toman la propiedad de los problemas con base en su propia iniciativa de manera reactiva.	Las metas no están claras y no existen las mediciones.
2	Existe conciencia de la necesidad de actuar. La gerencia comunica los problemas generales.	Surgen procesos similares y comunes pero en su mayoría son intuitivos y parten de la experiencia individual. Algunos aspectos de los procesos son	Existen enfoques comunes para el uso de herramientas pero se basan en soluciones desarrolladas por individuos clave. Pueden haberse	Se identifican los requerimientos mínimos de habilidades para áreas críticas. Se da entrenamiento como respuesta a las necesidades, en lugar	Un individuo asume su responsabilidad, y por lo general debe rendir cuentas aún si esto no está acordado de modo formal. Existe confusión acerca de	Existen algunas metas; se establecen algunas mediciones financieras pero solo las conoce la alta dirección. Hay monitoreo inconsistente en áreas

Continua …

Nivel	Conciencia y Comunicación	Políticas, Estándares y Procedimientos	Herramientas y Automatización	Habilidades y Experiencia	Responsabilidad y Rendición de Cuentas	Establecimiento y Medición de Metas
		repetibles debido a la experiencia individual, y puede existir alguna documentación y entendimiento informal de políticas y procedimientos.	adquirido herramientas de proveedores, pero probablemente no se aplican de forma correcta o incluso no usarse.	de hacerlo con base en un plan acordado. Existe entrenamiento informal sobre la marcha.	la responsabilidad cuando ocurren problemas y una cultura de culpas tiende a existir.	aisladas.
3	Existe el entendimiento de la necesidad de actuar. La gerencia es más formal y estructurada en su comunicación.	Surge el uso de buenas prácticas. Los procesos, políticas y procedimientos están definidos y documentados para todas las actividades clave.	Existe un plan para el uso y estandarización de las herramientas para automatizar el proceso. Se usan herramientas por su propósito básico, pero pueden no estar de acuerdo al plan acordado.	Se definen y documentan los requerimientos y habilidades para todas las áreas. Existe un plan de entrenamiento formal pero todavía se basa en iniciativas individuales.	La responsabilidad y la rendición de cuentas sobre los procesos están definidas y se han identificado a los dueños de los procesos de negocio. Es poco probable que el dueño del proceso	Se establecen algunas mediciones y metas de efectividad, pero no se comunican, y existe una relación clara con las metas del negocio. Surgen los procesos de medición pero no se aplican de modo consistente.

Continua …

Nivel	Conciencia y Comunicación	Políticas, Estándares y Procedimientos	Herramientas y Automatización	Habilidades y Experiencia	Responsabilidad y Rendición de Cuentas	Establecimiento y Medición de Metas
					tenga la autoridad plena para modificar el proceso.	
4	Hay entendimiento de los requerimientos completos. Se aplican técnicas maduras de comunicación y se usan herramientas estándar de comunicación.	El proceso es sólido y completo; se aplican las mejores prácticas internas. Todos los aspectos del proceso están documentados y son repetibles. La dirección ha terminado y aprobado las políticas. Se adoptan y siguen estándares para el desarrollo y mantenimiento.	Se implantan las herramientas de acuerdo a un plan estándar y algunas se han integrado con otras herramientas relacionadas. Se usan herramientas en las principales áreas para automatizar la administración del proceso y monitorear las actividades y controles.	Los requerimientos de habilidades se actualizan rutinariamente para todas las áreas, se asegura la capacidad para todas las áreas críticas y se fomenta la certificación. Se aplican técnicas maduras de entrenamiento de acuerdo al plan de entrenamiento y se fomenta la	Las responsabilidades y la rendición de cuentas sobre los procesos están aceptadas y funcionan de modo que se permite al dueño del proceso descargar sus responsabilidades. Existe una cultura de recompensas que activa la acción positiva.	La eficiencia y la efectividad se miden y comunican y están ligadas a las metas del negocio y al plan estratégico de TI. Se implementa el balance score card de TI en algunas áreas, con excepciones conocidas por la gerencia y se está estandarizando el análisis.

Continua …

Nivel	Conciencia y Comunicación	Políticas, Estándares y Procedimientos	Herramientas y Automatización	Habilidades y Experiencia	Responsabilidad y Rendición de Cuentas	Establecimiento y Medición de Metas
				compartición del conocimiento.		
5	Existe un entendimiento avanzado y a futuro de los requerimientos. Existe una comunicación proactiva de los problemas, basada en las tendencias, se aplican técnicas maduras de comunicación y se usan herramientas	Se aplican las mejores prácticas y estándares externos. La documentación de procesos ha evolucionado a flujos de trabajo automatizados. Los procesos, las políticas y los procedimientos están estandarizados e integrados para permitir una administración y mejora extremo a extremo.	Se usan juegos de herramientas estandarizados a lo largo de la empresa. Las herramientas están completamente integradas con otras herramientas relacionadas para permitir un soporte integral de los procesos. Se usan las herramientas para dar soporte a la mejora de los	La organización fomenta de manera formal la mejora continua de las habilidades, con base en metas personales y organizacionales claramente definidas. El entrenamiento y la educación dan soporte a las mejores prácticas externas y al uso de conceptos y técnicas. Compartir el conocimiento es una cultura empresarial, y	Los dueños de procesos tienen la facultad de tomar decisiones y medidas. La aceptación de la responsabilidad ha descendido en cascada a través de la organización de forma consistente.	Existe un sistema de medición de desempeño integrado que liga al desempeño de TI con las metas del negocio por la aplicación global del balance score card de TI. La dirección nota las excepciones de forma global y consistente y el análisis de causas raíz

Continua …

Nivel	Conciencia y Comunicación	Políticas, Estándares y Procedimientos	Herramientas y Automatización	Habilidades y Experiencia	Responsabilidad y Rendición de Cuentas	Establecimiento y Medición de Metas
	integradas de comunicación		procesos y automáticamente detectar excepciones a los controles.	se están desarrollando sistemas basados en el conocimiento. Expertos externos y líderes industriales se emplean como guía.		

Tabla No. 2-1 Atributos o factores de evaluación de la Madurez

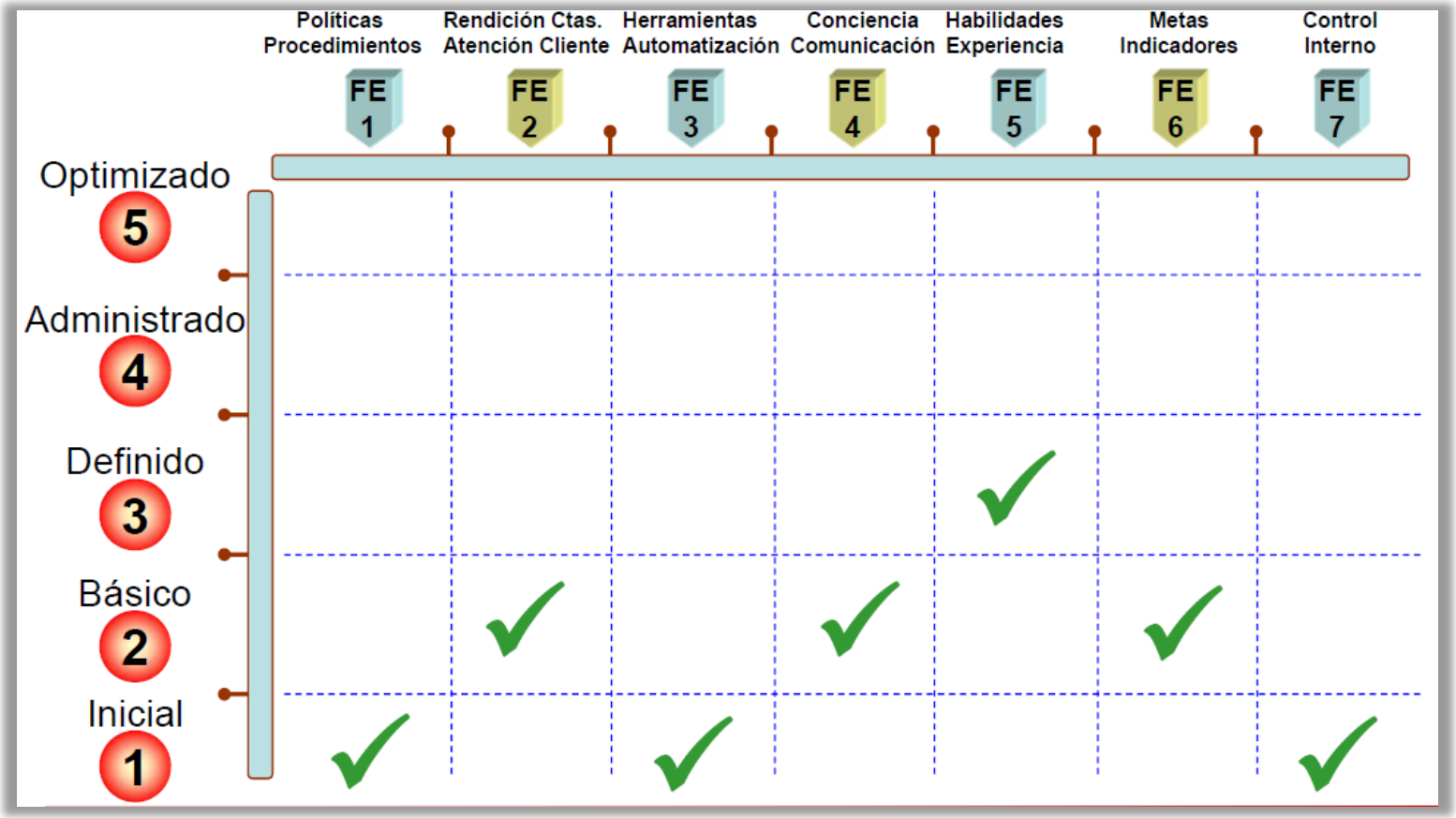


Figura No. 2-21 Matriz de evaluación de acuerdo a los atributos de la Madurez

(Fuente: La Madurez de los Procesos Empresariales – Ing. Giovanni Roldán)

Finalmente, el marco de trabajo general COBIT se muestra gráficamente en la Figura No. 2-21, con el modelo de procesos de COBIT compuesto de cuatro dominios que contienen 34 procesos genéricos, administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno.

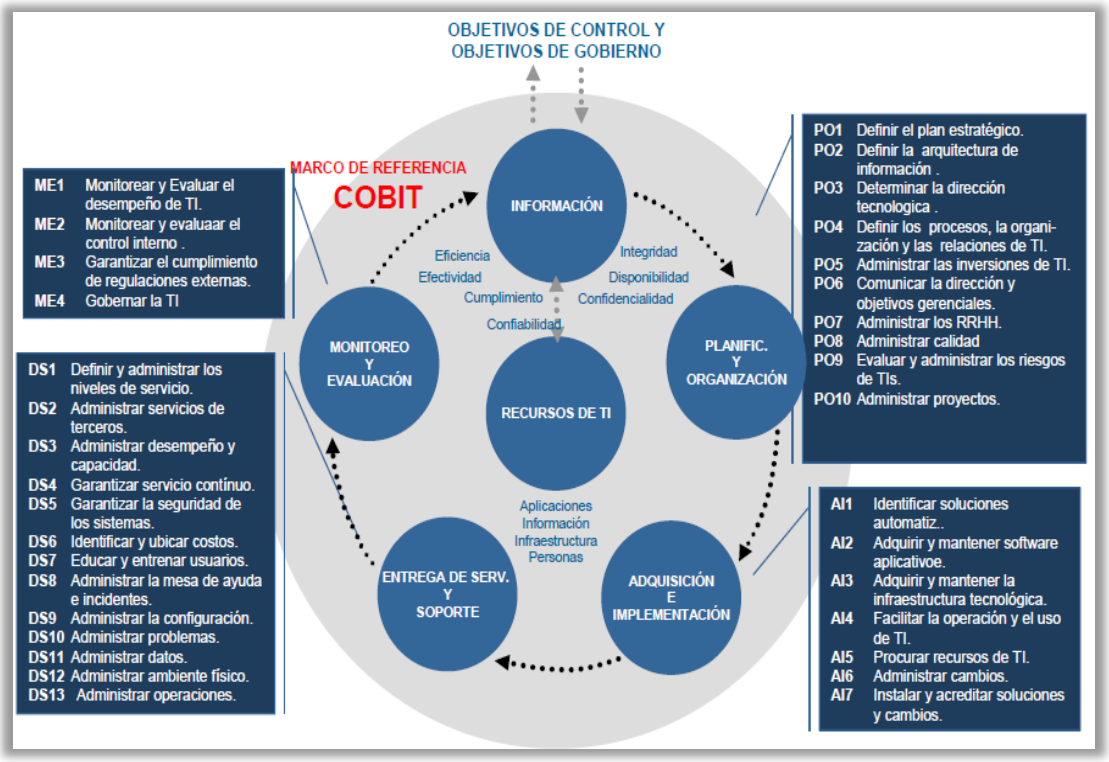


Figura No. 2-22 Marco de trabajo general COBIT

CAPÍTULO 3

RIESGOS DE LAS TECNOLOGÍAS DE INFORMACIÓN

3.1 Generalidades

El riesgo es la probabilidad de que un evento ocurra y éste afecte o tenga consecuencias negativas.

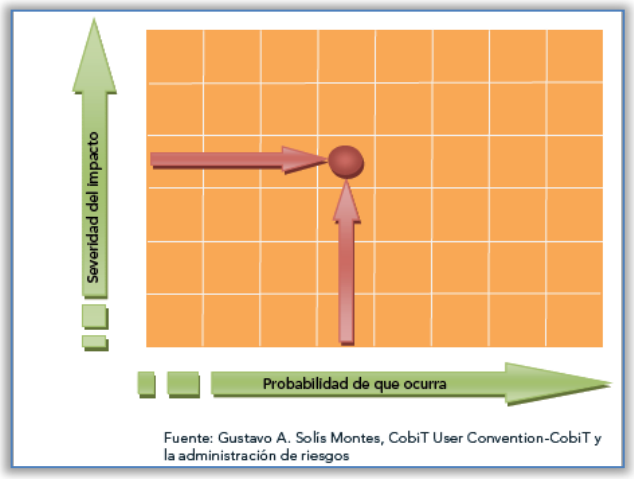


Figura No. 3-1 Niveles de riesgos

Los factores que componen el riesgo son: la amenaza (probabilidad que ocurra) y la vulnerabilidad (severidad del impacto).

La Amenaza es una condición peligrosa que puede ocasionar la pérdida de servicios informáticos. La amenaza se determina en función de la intensidad y la frecuencia.

La Vulnerabilidad son las características y las circunstancias de un sistema que los hacen susceptibles a los efectos dañinos de una amenaza.

RIESGO = Probabilidad que ocurra (AMENAZA) x Severidad del impacto (VULNERABILIDAD)

Sin embargo los riesgos pueden reducirse o manejarse, es decir se puede gestionar el riesgo.

Figura No. 3-2 Gestión del Riesgo

La Gestión de Riesgo es un proceso estructurado para determinar, analizar, valorar y clasificar el riesgo que afectan al logro de los objetivos, para posteriormente implementar mecanismos que permitan controlarlo.

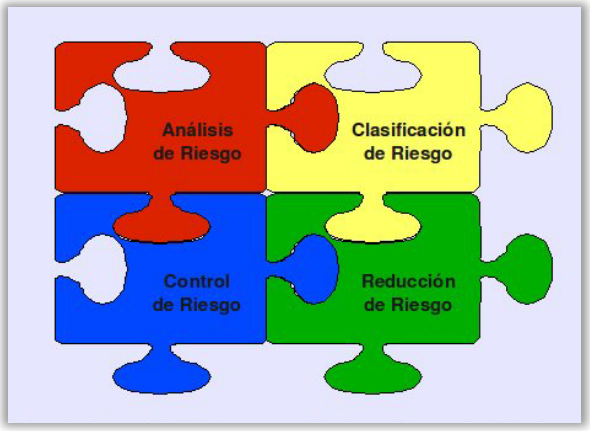


Figura No. 3-3 Gestión del riesgo visto desde la Seguridad Informática

3.1.1 Análisis de riesgos

Tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

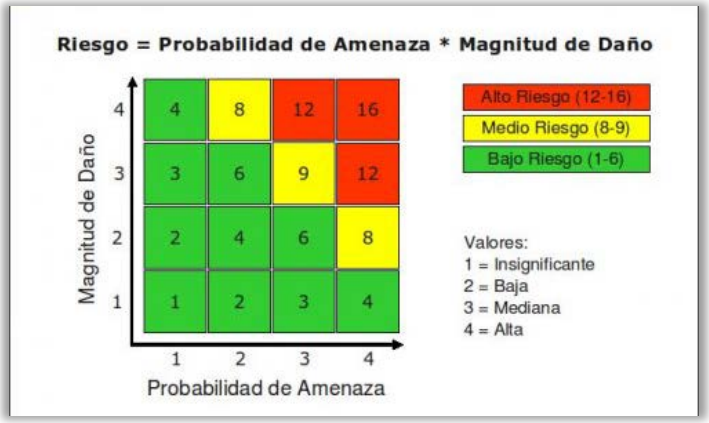


Figura No. 3-4 Análisis del riesgo

(Fuente: Gestión de Riesgo en la Seguridad Informática)

La Probabilidad de Amenaza y Magnitud de Daño (Impacto) pueden tomar condiciones entre Insignificante (1) y Alta (4). El análisis de riesgo permite ubicar el riesgo y conocer los factores que influyen en este.

Entre más alta es la Probabilidad de Amenaza y Magnitud de Daño (Impacto), más grande es el riesgo y el peligro al sistema, lo que quiere decir que es necesario implementar acciones que ayuden a la prevención de que ocurra. La definición de insignificante, baja, media y alta, varía de acuerdo al enfoque o al análisis en particular que se realice, lo importante es señalar que significa cada segmento o que comprende cada uno.

Estimar la Magnitud de Daño generalmente es una tarea muy compleja. La manera más fácil es expresar el daño de manera cuantitativa y cualitativa, lo que significa que aparte del daño económico, también se considera otros valores como daños materiales, imagen, entre otros.

3.1.2 Clasificación de riesgo

El objetivo de la clasificación de riesgo, es determinar hasta qué grado es factible combatir los riesgos encontrados. La factibilidad normalmente depende de la voluntad y posibilidad económica de la Empresa, también del entorno donde nos ubicamos.

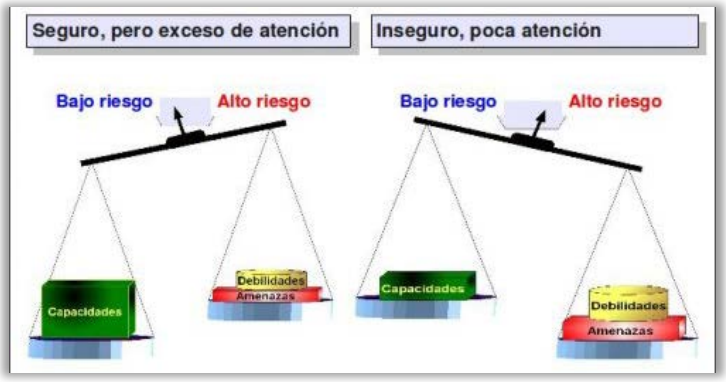


Figura No. 3-5 Clasificación de riesgo

(Fuente: Gestión de Riesgo en la Seguridad Informática)

Implementar acciones para reducir los riesgos significa realizar inversiones, generalmente económicas. El reto es encontrar un buen equilibrio entre cumplir con su objetivo y el esfuerzo económico que tenemos que hacer para su implementación.

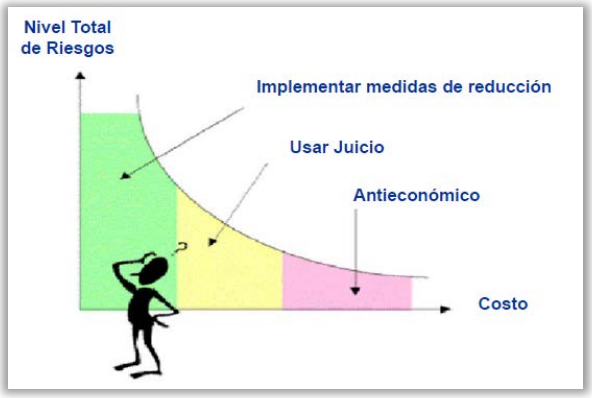


Figura No. 3-6 Riesgos vs Costos de Implementación

(Fuente: Auditoria Informática: Conceptos y Fundamentos Ing. Giovanni Roldán)

El exceso de acciones y procesos de protección, pueden fácilmente paralizar los procesos operativos e impedir el cumplimiento de nuestra

misión, puede ser el caso cuando las inversiones para implementar las acciones superen el valor del recurso que se pretende proteger.

3.1.3 Reducción de riesgo

La reducción de riesgo se logra a través de la implementación de medidas de protección (físicas y técnicas, personales y administrativas), que se manifestaron o fueron resultado del análisis y de la clasificación de riesgo.

Para que las medidas sean exitosas, es esencial que siempre se verifique su factibilidad, es decir que técnicamente funcionan y cumplen su propósito, que están incorporadas en los procesos operativos de la Empresa y que las personas se apropian de estás.

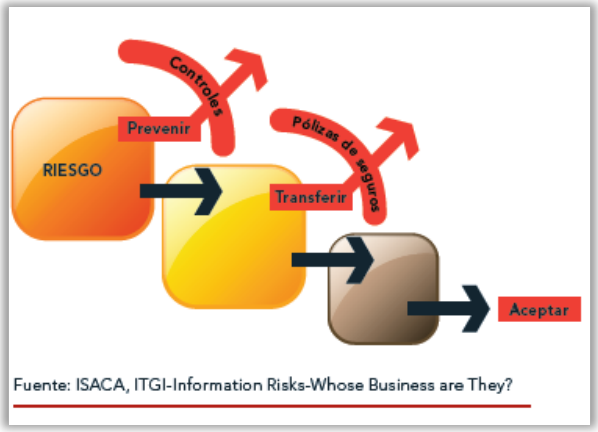


Figura No. 3-7 Tratamiento de riesgos

3.1.4 Control de riesgo

El propósito del control de riesgo es analizar el funcionamiento, la efectividad y el cumplimiento de las medidas de protección, para determinar y ajustar sus deficiencias.

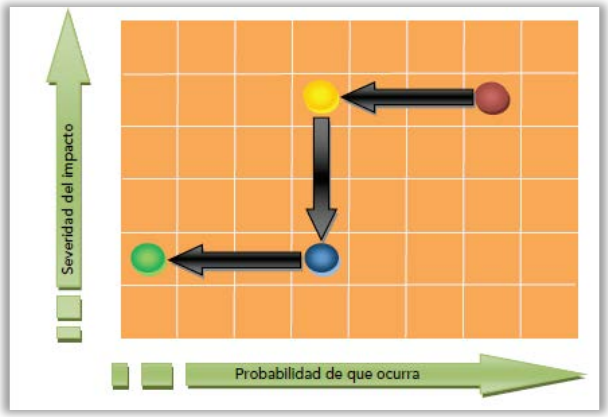


Figura No. 3-8 Efecto esperado de las acciones de control

(Fuente: Gustavo A. Solís Montes, CobiT User Convention-CobiT y la Administración de Riesgos)

Medir el cumplimiento y la efectividad de las medidas de protección requiere un proceso continuo de retroalimentación con documentación de soporte, esto sirve como fuente de información, cuando se realice nuevamente el proceso de análisis de riesgo.

3.1.5 Tipos de riesgo

Los riesgos se pueden encontrar en procesos manuales o automáticos, de acuerdo al avance tecnológico el riesgo se ha ido trasladando y cambiando su complejidad por la gran variedad de

herramientas de software y de hardware que soportan los sistemas computacionales.

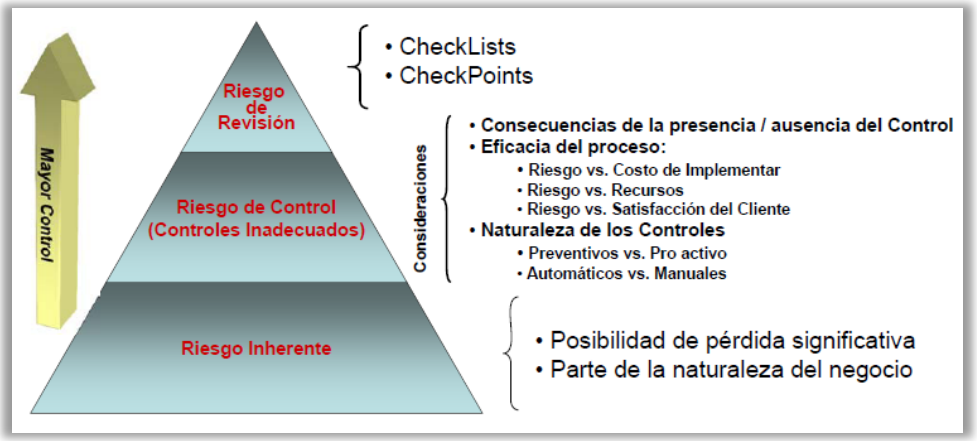


Figura No. 3-9 Tipos de Riesgo

(Fuente: Auditoria Informática: Conceptos y Fundamentos Ing. Giovanni Roldán)

3.1.6 Estructura de Riesgo Integrada para TI

Particularmente, para el área de TIC'S en forma general, se pueden identificar cuáles pueden ser algunos indicadores claves de riesgos:

- Ausencia del software y hardware de seguridad.
- Ausencia de la función de seguridad de activos de información.
- Elevado número de reprocesos.
- Uso significativo de herramientas automatizadas.
- Complejidad tecnológica.
- Falta de formalidad en las políticas y procedimientos.

- Bajo nivel de seguimiento a las violaciones de seguridad y actividades de usuarios en general.

A continuación se muestra la relación de los procesos, aplicaciones y servicios que intervienen en el área de TIC'S y los factores que pueden determinan posibles riesgos asociados a la parte interna y externa de una empresa. No se detallan riesgos físicos (instalaciones) o de personal (capacitación o competencia del personal de TI), la orientación de la figura está encaminada a los procesos, aplicaciones o servicios que provee una área de TI a nivel de infraestructura.

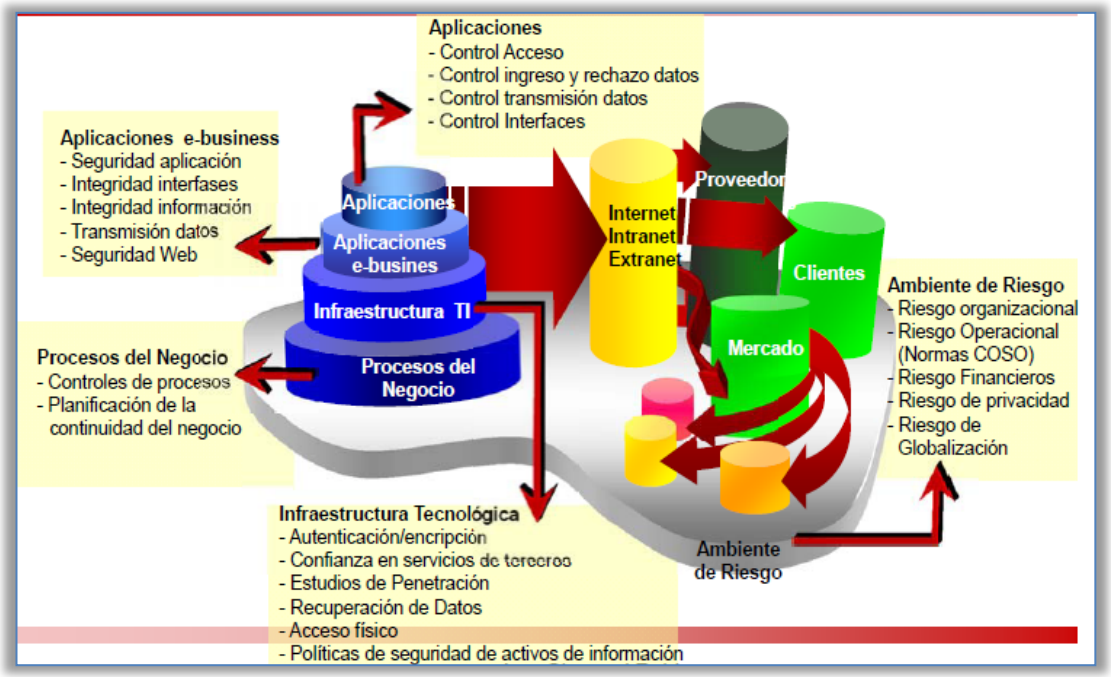


Figura No. 3-10 Estructura de Riesgo Integrada en TI

(Fuente: Auditoria Informática: Conceptos y Fundamentos Ing. Giovanni Roldán)

Para la empresa COCASINCLAIR EP, es importante determinar cuáles podrían ser los riesgos de prioridad alta que se requieren sean gestionados. Posteriormente, a través del análisis de riesgos se identificará los procesos que se requieren realizar la revisión y proponer las medidas de control para gestionarlos.

Como se puede observar en la figura No. 3-10, los riesgos pueden encontrase en toda el área de TI. Los riesgos inherentes son parte del negocio, cada actividad tiene asociada uno o más riesgos. El Control de Acceso, puede tener los siguientes riesgos: pérdida de comunicación con la base de datos, desconfiguración del software de identificación, infección por virus, etc.

Los siguientes riesgos están completamente relacionados con la tecnología y su impacto puede ser directo para el negocio, pues la tecnología es un factor importante para la operación de los negocios hoy en día.

Clasificación del riesgo	Descripción
Seguridad y acceso	El riesgo de que información confidencial o sensitiva quede a disposición de personas que no tienen la autorización apropiada para obtenerla.
Integridad	El riesgo de que la información no sea confiable ya sea porque no está autorizada, está incompleta o es inexacta.
Pertinente	El riesgo asociado a no obtener la información correcta hacia los procesos adecuados en el tiempo preciso para tomar las acciones apropiadas.
Disponibilidad	El riesgo de pérdida de servicio.
Infraestructura	El riesgo de que una organización no cuente con la infraestructura tecnológica que soporte de manera efectiva las necesidades actuales y futuras del negocio.

Fuente: ISACA, ITGI-Information Risks-Whose Business are They?

Tabla No. 3-1 Riesgos tecnológicos que proporciona el ITGI (Information Technology Governance Institute)

A continuación, se muestra una tabla de detección de riesgos relevantes, que se pueden identificar directamente sin tener que realizar un análisis exhaustivo de los eventos.

EVENTO	RIESGOS
Software Pirata	Problemas legales
	Mala imagen ante cliente y proveedores
	Posibilidad de infección de virus.
	Falta de documentación, etc.
Inexistencia de metodologías	Dependencia hacia el personal que maneja proyectos claves.
	Seguimiento nulo a los proyectos de informática
	Trabajo individualistas y no en equipo, etc.
Poca comunicación con la alta gerencia	Desconocimiento de los requerimientos del negocio
	Prioridades mal entendidas
	Proyectos cancelados
	Recursos desperdiciados
	Estrategias y objetivos de negocio no soportados
	Falta de compromiso ejecutivo, etc.

Tabla No. 3-2 Detección de riesgos (ejemplos)

Los riesgos que más frecuentemente se presentan en las empresas en el área de TI y que afectan al negocio, son los siguientes:

ESPACIO EN BLANCO INTENCIONAL

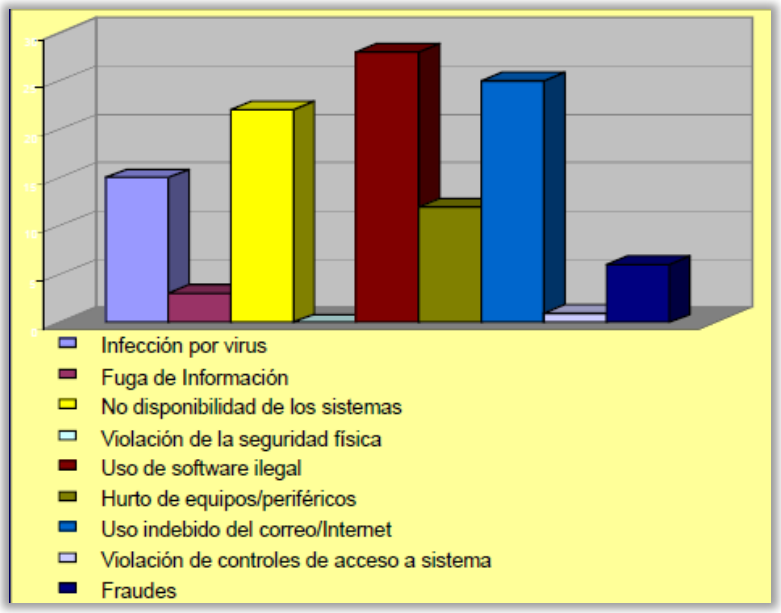


Figura No. 3-11 Riesgos de inseguridad tecnológica (año 2004)

(Fuente: Auditoria Informática: Conceptos y Fundamentos Ing. Giovanni Roldán)

3.1.7 Criterios de control eficaces

Así como existen riesgos, también existen criterios bajo los cuales se deben implementar los controles, es decir se deben tomar en cuenta ciertos parámetros para determinar el tipo de control para gestionar el riesgo. En la Tabla No. 3-3, se muestran estos criterios.

ESPACIO EN BLANCO INTENCIONAL

CRITERIOS	DESCRIPCIÓN
Integridad	¿Qué pasos o procesos aseguran que todas las transacciones y cuentas que deberían incluirse en los estados financieros están efectivamente incluidas? ¿Qué impide que figuren los activos, pasivos o transacciones faltantes?
Existencia	¿Qué pasos o procesos confirman que los activos y pasivos informados realmente existen a la fecha del balance? ¿Qué controles confirman que las transacciones informadas en el estado de resultados efectivamente ocurrieron durante tal período?
Autorización	¿Están definidas y asignadas las tareas de control y procesamiento en la estructura de la organización?
Precisión	¿Qué pasos o procesos deberían seguirse para asegurar que todos los montos financieros están valuados correctamente, son matemáticamente correctos, están asignados al código contable correcto (por partida o descripción) o al período contable adecuado? ¿Qué medidas deberían tomarse para garantizar la integridad y validez de los datos?
Valuación	¿Qué pasos o procesos aseguran que los activos y pasivos están valuados adecuadamente y los ingresos y gastos medidos correctamente?
Propiedad	¿Qué pasos o procesos confirman que la compañía es titular y/o cuenta con un título de propiedad carente de gravámenes sobre los activos y garantías, y que la compañía efectivamente participó en las transacciones informadas?
Presentación	¿Qué pasos o procesos confirman que los activos, pasivos, ingresos y gastos están debidamente descritos y tratados en los estados financieros?

Tabla No. 3-3 Criterios para implementar controles eficaces

(Fuente: Auditoria Informática: Conceptos y Fundamentos Ing. Giovanni Roldán)

3.2 Matriz de Riesgos

Una matriz de riesgo constituye una herramienta de control y de gestión normalmente utilizada para identificar las actividades (procesos y productos) más importantes de una empresa, en el caso de la Coordinación de TIC'S, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos relacionados con estos riesgos (factores de riesgo).

La matriz de riesgo es una guía visual, que facilita determinar prioridades para la atención y toma de decisiones de determinados riesgos identificados. El establecer indicadores dentro de la matriz de riesgos, facilita el análisis y se puede generar planes de acción con responsables, plazos y mecanismos de seguimientos o monitoreo.

Igualmente, una matriz de riesgo permite evaluar la efectividad de una adecuada gestión y administración de los riesgos que pudieran impactar los resultados y por ende al logro de los objetivos de una organización.

Es importante considerar que es clave una adecuada definición de las ponderaciones, por cuanto esto delimita cuales riesgos serían críticos, altos, medios y bajos.

Adicionalmente, la matriz de riesgos debe plasmar la mayoría de riesgos de la Empresa y en este caso particular de la Coordinación de TIC'S. Toda la documentación e información deben presentarse en formatos uniformes para que exista consistencia y mayor objetividad.

3.2.1 Elementos que deben considerarse en el diseño de una matriz de riesgos.

A partir de los objetivos estratégicos y el plan de negocios, la gestión de riesgos debe desarrollar un proceso para la "identificación" de las actividades principales y los riesgos a los cuales estarían expuestas;

entendiéndose como riesgo la eventualidad de que una determinada entidad no pueda cumplir con uno o varios de los objetivos a causa de efectivizarse una amenaza.

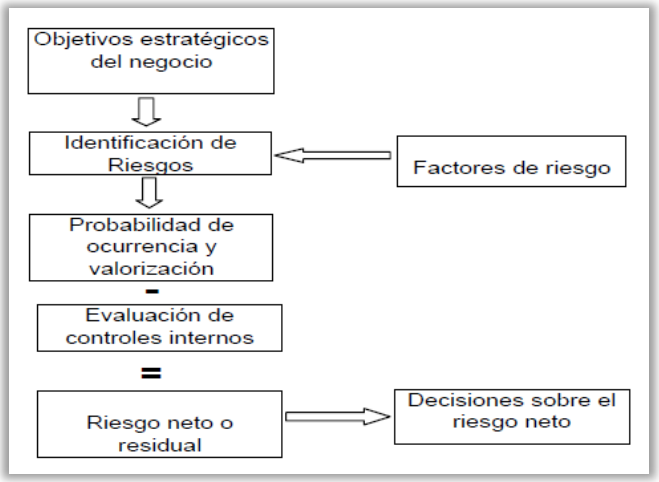


Figura No. 3-12 Fases de elaboración de una matriz de riesgos

(Fuente: http://www.sigweb.cl/biblioteca/MatrizdeRiesgo.pdf)

Una vez establecidas todas las actividades, se deben identificar las fuentes o factores que intervienen en su manifestación y severidad, es decir los llamados “factores de riesgo o riesgos inherentes”. El riesgo inherente es intrínseco a toda actividad.

El siguiente paso consiste en determinar la “probabilidad” de que el riesgo ocurra. La valorización del riesgo implica un análisis conjunto de la probabilidad de ocurrencia y el efecto en los resultados; puede efectuarse en términos cualitativos o cuantitativos, dependiendo de la importancia o disponibilidad de información.

Como ejercicio, la valorización consiste en asignar a los riesgos calificaciones dentro de un rango, que podría ser de 1 a 5 (insignificante (1), baja (2), media (3), moderada (4) o alta (5), dependiendo de la combinación entre impacto y probabilidad.

Luego de que los riesgos han sido valorados, se procede a evaluar la "calidad de la gestión", a fin de determinar, cuáles y cuán eficaces son los controles establecidos por la empresa para mitigar los riesgos identificados.

Actividad I	Nivel de riesgo	Calidad de gestión			Riesgo residual (**)
		Tipo de medidas de control	Efectividad	Promedio (*)	
Riesgo inherente 1	5	Control 1	3	3.6	1.38
		Control 2	4		
		Control 3	4		
Riesgo inherente 2	4	Control 1	5	4.25	0.94
		Control 2	5		
		Control 3	4		
Riesgo inherente 3	4	Control 1	3	3.6	1.11
		Control 2	4		
		Control 3	4		
Riesgo inherente 4	3	Control 1	5	3.5	0.85
		Control 2	2		
Perfil de riesgo (Riesgo residual total) (***)					1.07

(*) Promedio de los datos de efectividad
(**) Resultado de la división entre nivel de riesgo / Promedio de efectividad
(***) Promedio: Se considera un mismo peso de ponderación a los RI.

Tabla No. 3-4 Ejemplo para calcular el riego neto o residual

(Fuente: http://www.sigweb.cl/biblioteca/MatrizdeRiesgo.pdf)

En la medida que los controles sean más eficientes y la gestión de riesgos pro-activa, el indicador de riesgo inherente neto tiende a disminuir.

Finalmente, se calcula el "riesgo neto o residual", que resulta de la relación entre el grado de manifestación de los riesgos inherentes y la gestión de mitigación de riesgos establecida por la administración.

La matriz anteriormente descrita, tiene un enfoque principalmente cualitativo, para lo cual es preciso que quienes la construyan tengan experiencia, conocimiento profundo del negocio y su entorno y un buen juicio de valor.

3.2.2 Ventajas de la matriz de riesgos

- Tiende a buscar objetividad en el análisis y concentrase en los procesos críticos de la empresa, gráficamente se identifican los procesos que requieren una revisión.

- Establece parámetros de comparación, es decir bajo el mismo criterio se evalúa el estado de cada proceso.

- Permite hacer medición de la evolución, esta actividad se lo puede realizar por medio de los indicadores contenidos en la matriz y cada cierto tiempo evaluar el resultado de los controles versus los riesgos identificados.

- Genera participación activa del auditado, por medio de experiencias internas y externas para lograr una matriz más consistente en la conceptualización, formulación y definición.

Products / Functions	Processes	Key Risks	Inherent Risk H/M/L	Key Controls / Control Activity	Quality or Control S/N/U	Residual Risk H/M/L	Test Methodology	Sample Size	Freq.
Internet Management	Granting Access to the Internet	Misuse of Internet access can disrupt productivity and even expose the organization to image and/or legal risks	M	1. Access to internet services must be approved by managers and controlled by IT through filters. 2. Access is granted through the corporate process established for this purpose on a case-by-case basis: Internet Access and Registration. The Manager must review/agree with the reasons why Internet access is being granted to the individual before approving the form. 3. Access is granted by an independent unit that is not involved in Technology Project design, development and implementation.	S	L	1. Verify that accesses to Internet has been approved by direct management and granted TIS (Technology Infrastructure Services) organization. 2. Determine that access to internet services is approved by managers. 3. Determine that access is granted through the corporate process established for this purpose on a case-by-case basis: Internet Access and Registration. Ensure that them manager must review/agrees with the reasons why Internet access is being granted to the individual before approving the form. 4. Verify that access is granted by an independent unit that is not involved in Technology Project design, development and implementation.	Sample 10-20 approvals for user access	A

Tabla No. 3-5 Una matriz de riesgos de TI

(Fuente: Auditoria Informática: Conceptos y Fundamentos Ing. Giovanni Roldán C)

3.2.3 Matriz de riesgos por áreas

Entre los principales servicios de informática que la Coordinación de TIC'S brinda a COCASINCLAIR EP, se pueden señalar los siguientes:

- Administración de la red de área local en Quito, Campamento San Rafael y el enlace entre los dos sitios, por lo que pasa a convertirse en una red de área extensa.
- Planificación informática anual.
- Administración de los Sistemas Informáticos implantados y que están en operación.
- Administración del hardware y software (sistemas y licenciamiento) de propiedad de la Empresa.

- Desarrollo e implementación de nuevos sistemas informáticos (Gestor Documental).
- Soporte técnico a usuarios (capacitación, asesoramientos, etc.)
- Mantenimientos preventivos / correctivos.
- Identificación de nuevas soluciones tecnológicas.
- Administración de la radiocomunicación en el Campamento,
- Otros.

A continuación, se muestra la matriz de riesgos por áreas de tecnología a auditar, relacionando las sub-áreas, componentes y el porcentaje que representa de la auditoría.

Área susceptibles de auditar	**Aspectos o componentes para evaluar el área**	**Registro por componentes**	**Clasificación del riesgo por área (Total)**	**Área para auditar según clasificación**
Administración de Informática	1. Misión y objetivos	%	%	Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado
	2. Organización	%		
	3. Servicios	%		
	4. Parámetros de medición	%		
Dirección y niveles ejecutivos	1. Seguimiento a la función de informática por la dirección	%	%	Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado
	2. Comunicación e integración	%		
	3. Apoyo a toma de decisiones	%		

Continua …

Área susceptibles de auditar	Aspectos o componentes para evaluar el área	Registro por componentes	Clasificación del riesgo por área (Total)	Área para auditar según clasificación
Usuarios de informática	1. Comunicación e integración	%	%	Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado
	2. Proyectos conjuntos	%		
	3. Administración de recursos de informática	%		
	4. Grado de satisfacción	%		
Control Interno	1. Políticas y procedimientos	%	%	Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado
Ciclo de desarrollo e implantación de sistemas de información	1. Metodología	%	%	Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado
	2. Técnicas	%		
	3. Herramientas	%		
	4. Capacitación / Actualización	%		
Sistemas de información	1. Planeación	%	%	Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado
	2. Desarrollo	%		
	3. Operación	%		
	4. Soluciones de mercado	%		

Tabla No. 3-6 Matriz de riesgos por área de revisión

(Fuente: Auditoría en Informática, Enrique Hernández Hernández)

3.3 Matriz de Riesgos de la Coordinación de TIC'S

De acuerdo a los objetivos de esta tesis, se procederá a identificar los riesgos de la Coordinación de TIC'S en la empresa COCASINCLAIR EP orientados a determinar cuáles son críticos, altos, medios o bajos. Siempre interesa enfocarse en los riesgos que pueden tener un impacto alto en el giro del negocio de la Empresa, es decir los riesgos críticos.

3.3.1 Metodología de identificación de Riesgos utilizando COBIT 4.1.

La metodología a utilizar para la identificación de los riesgos de la Coordinación de TIC'S, es la propuesta por Julio R. Jolly Moore & Gerardo Alcarraz, en el documento Auditoría Continua: Mejores Prácticas y Caso Real.

Principalmente, los riesgos de TI se encuentran en no poder satisfacer a la Empresa los requerimientos de información, es decir, la Coordinación de TIC'S debería bridar EFECTIVIDAD, EFICIENCIA, CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD, CUMPLIMIENTO y CONFIABILIDAD de la información que es tratada por las personas, aplicaciones e infraestructura, lo señalado anteriormente, corresponde a los criterios de información y los recursos de TI contenidos en el estándar de la buenas prácticas de COBIT.

La siguiente tabla, muestra los requerimientos de información con un enfoque de riegos.

CRITERIOS	DEFINICIÓN COBIT	DEFINICIÓN RIESGO
EFECTIVIDAD EFICIENCIA	La información sea relevante y pertinente a los procesos del negocio y se brinde de una manera oportuna, correcta, consistente y utilizable, optimizando los recursos.	La Tecnología de Información no cubre las expectativas de negocio en términos de Efectividad y Eficiencia
CONFIDENCIALIDAD	Protección de la información sensitiva contra revelación no autorizada.	La información contenida en los Sistemas puede ser accedida por personas no autorizadas.
INTEGRIDAD	La precisión y completitud de la información, así como con su validez.	La información contenida en los Sistemas puede ser modificada o alterada sin autorización.
DISPONIBILIDAD	La información esté disponible cuando sea requerida por los procesos del negocio.	No se dispone de los Sistemas de información o Infraestructura para operar adecuadamente los procesos del negocio.
CUMPLIMIENTO	Cumplir leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocio.	Incumplimiento de Leyes, Regulaciones y Contratos.
CONFIABILIDAD	Brindar información apropiada para que la Gerencia administre la entidad y ejercite responsabilidades fiduciarias y de gobierno.	La información suministrada no es apropiada y la Gerencia no puede asumir las responsabilidades fiduciarias y de gobierno.

Tabla No. 3-7 Requerimientos de información con un enfoque de riesgos.

Al establecer los requerimientos de información que normalmente solicita la Gerencia General a la Coordinación de TIC'S, y definidos los posibles riesgos de negocio que puedan presentarse, es necesario priorizarlos, para luego asociar los procesos de COBIT 4.1 con los que realizan en el área de TIC'S.

A continuación se muestra la metodología para la elaboración de la matriz de riesgos usando el estándar de las buenas prácticas de COBIT 4.1.

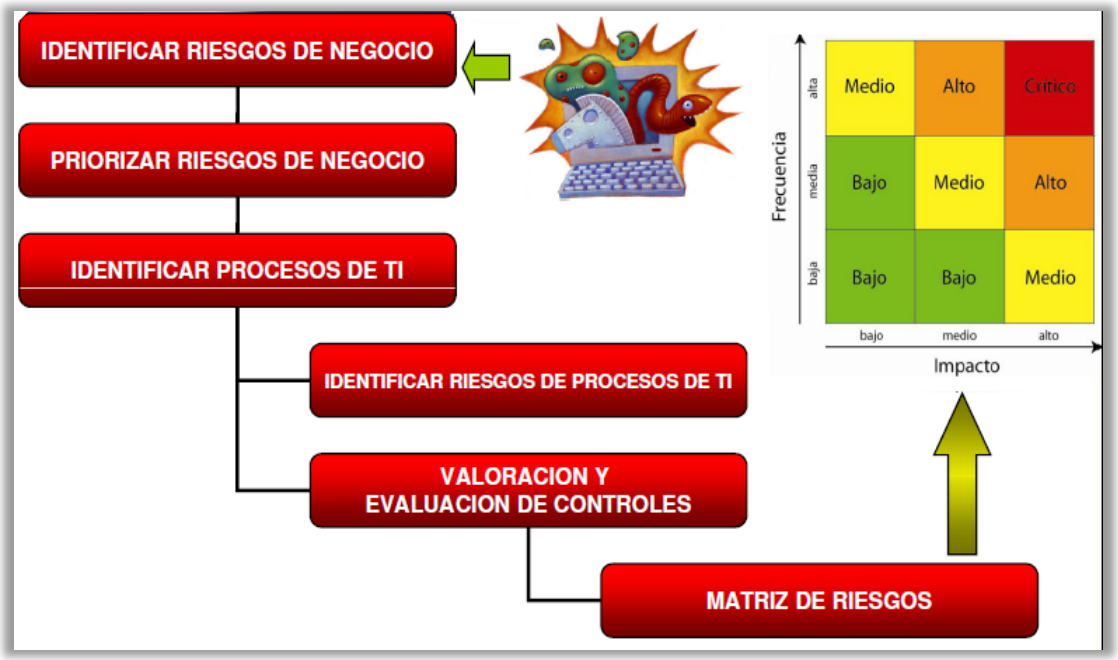


Figura No. 3-13 Metodología de identificación de riesgos usando COBIT.

(Fuente: Auditoría Continua: Mejores Prácticas y Caso Real , Julio R. Jolly Moore & Gerardo Alcarraz)

3.3.2 Aplicación de la metodología para la Coordinación de TIC'S

3.3.2.1 Identificación de riesgos de negocio.

Esta etapa consiste en listar los criterios / requerimientos del estándar de COBIT 4.1 con los riesgos asociados a estos criterios, es decir, el no tener implementados los controles eficiente y eficazmente, puede, ocasionar que las Tecnologías de Información no cubra las expectativas de Negocio.

De igual manera, el riesgo de que la información contenida en los sistemas de información pueda ser accedida por usuarios no autorizados, hace referencia al criterio de Confidencialidad, y así sucesivamente.

En la siguiente figura, se muestra los criterios / requerimientos de información de la Empresa relacionados con sus riesgos.

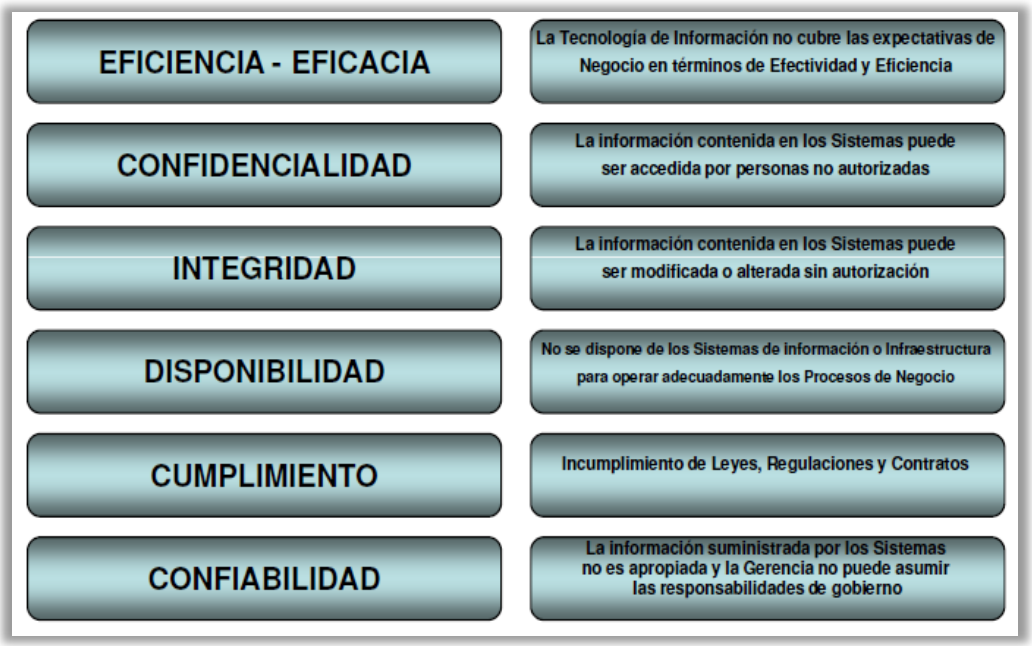


Figura No. 3-14 Criterios / requerimientos de información relacionados con sus riesgos.

3.3.2.2 Priorizar los riesgos de negocio.

Luego de haber identificado los riesgos, se debe proceder a priorizarlos. Con el personal de la Coordinación de TIC'S de la Empresa, se procedió a priorizar los criterios / requerimientos de información de COBIT 4.1. Es decir, se puso un orden de prelación los criterios de acuerdo a su criticidad y enfocados en la seguridad de la información.

Dentro de los productos o servicios que la Coordinación de TIC'S brinda a la Empresa, está el Plan de Gestión de la Seguridad de la Información, señalado en el capítulo I, por tal razón, se determinó que el enfoque para realizar esta auditoría estará enmarcado en revisar los requerimientos de seguridad de la información, cuyos principales componentes son:

- Confidencialidad.
- Integridad, y
- Disponibilidad.

ESPACIO EN BLANCO INTENCIONAL

Por lo tanto se procede a priorizarlos de la siguiente manera:

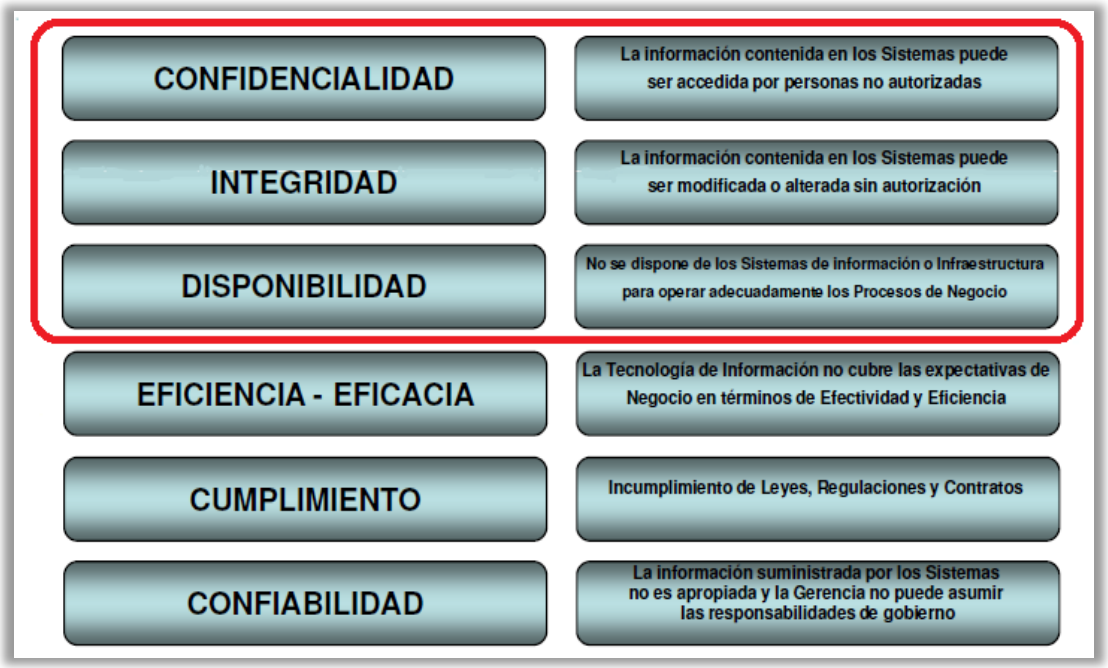
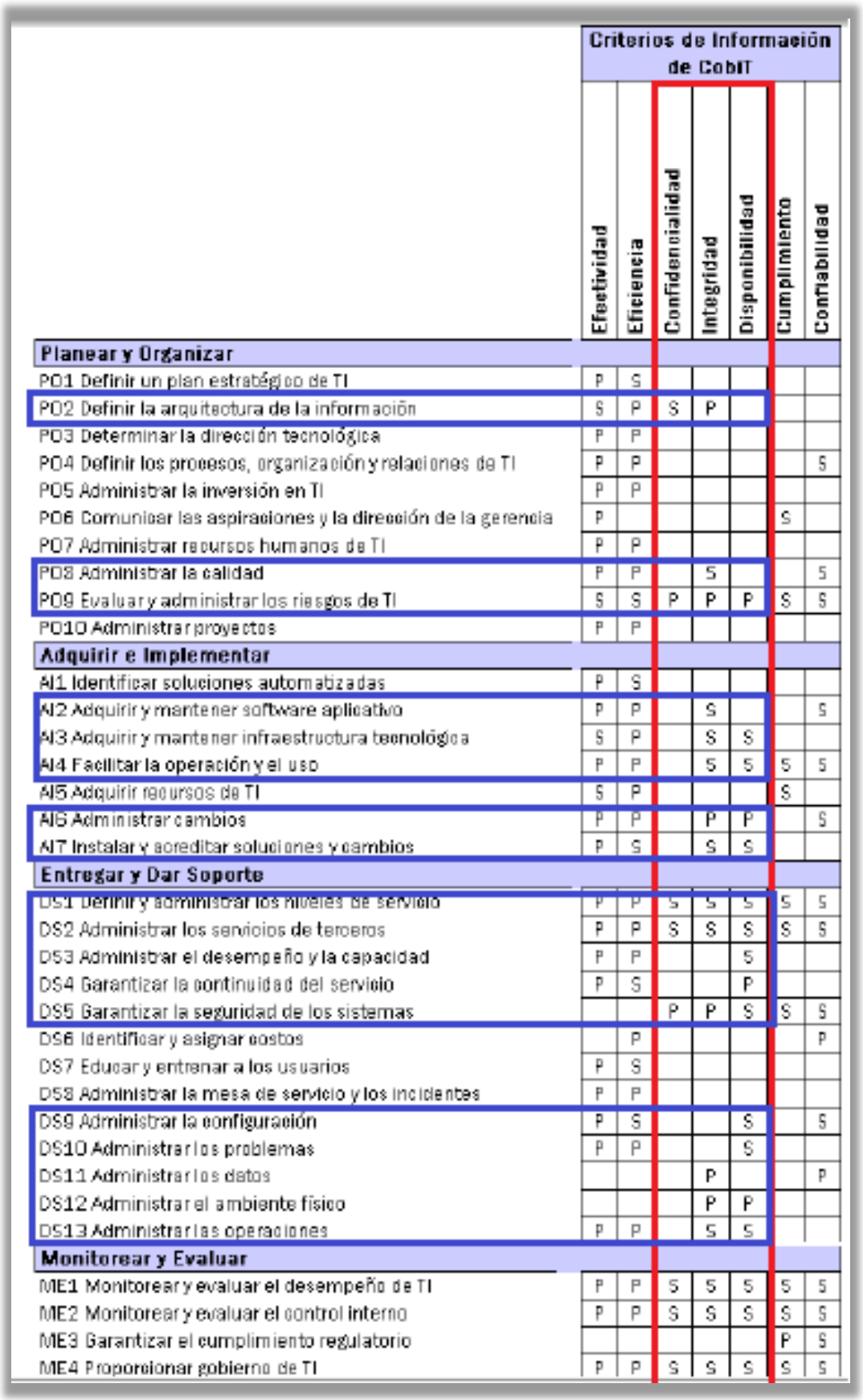


Figura No. 3-15 Priorización de los riesgos de negocio.

3.3.2.3 Identificar los procesos de TI

Luego de priorizar los riesgos de negocio, se procede a cruzar con los procesos que se verán afectados y a catalogarlos como primarios (P) o secundarios (S) con respecto a las áreas de enfoque del Gobierno de TI, de acuerdo al estándar de COBIT 4.1.

ESPACIO EN BLANCO INTENCIONAL



	Criterios de Información de CobiT						
	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Planear y Organizar							
PO1 Definir un plan estratégico de TI	P	S					
PO2 Definir la arquitectura de la información	S	P	S	P			
PO3 Determinar la dirección tecnológica	P	P					
PO4 Definir los procesos, organización y relaciones de TI	P	P					S
PO5 Administrar la inversión en TI	P	P					
PO6 Comunicar las aspiraciones y la dirección de la gerencia	P					S	
PO7 Administrar recursos humanos de TI	P	P					
PO8 Administrar la calidad	P	P		S			S
PO9 Evaluar y administrar los riesgos de TI	S	S	P	P	P	S	S
PO10 Administrar proyectos	P	P					
Adquirir e Implementar							
AI1 Identificar soluciones automatizadas	P	S					
AI2 Adquirir y mantener software aplicativo	P	P		S			S
AI3 Adquirir y mantener infraestructura tecnológica	S	P		S	S		
AI4 Facilitar la operación y el uso	P	P		S	S	S	S
AI5 Adquirir recursos de TI	S	P				S	
AI6 Administrar cambios	P	P		P	P		S
AI7 Instalar y acreditar soluciones y cambios	P	S		S	S		
Entregar y Dar Soporte							
DS1 Definir y administrar los niveles de servicio	P	P	S	S	S	S	S
DS2 Administrar los servicios de terceros	P	P	S	S	S	S	S
DS3 Administrar el desempeño y la capacidad	P	P			S		
DS4 Garantizar la continuidad del servicio	P	S			P		
DS5 Garantizar la seguridad de los sistemas			P	P	S	S	S
DS6 Identificar y asignar costos		P					P
DS7 Educar y entrenar a los usuarios	P	S					
DS8 Administrar la mesa de servicio y los incidentes	P	P					
DS9 Administrar la configuración	P	S			S		S
DS10 Administrar los problemas	P	P			S		
DS11 Administrar los datos				P			P
DS12 Administrar el ambiente físico				P	P		
DS13 Administrar las operaciones	P	P		S	S		
Monitorear y Evaluar							
ME1 Monitorear y evaluar el desempeño de TI	P	P	S	S	S	S	S
ME2 Monitorear y evaluar el control interno	P	P	S	S	S	S	S
ME3 Garantizar el cumplimiento regulatorio						P	S
ME4 Proporcionar gobierno de TI	P	P	S	S	S	S	S

Figura No. 3-16 Cruce de los procesos con los criterios de información

Se identificaron 18 procesos, los mismos que se listan a continuación:

PROCESOS DE TI	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
PO2 Definir la arquitectura de información	S	P	
PO8 Asegurar el cumplir requerimientos externos		S	
PO9 Evaluación de Riesgos	P	P	P
AI2 Adquisición y mantenimiento de SW aplicativo		S	
AI3 Adquisición y mantenimiento de arquitectura TI		S	S
AI4 Desarrollo y mantenimiento de Procedimientos de TI		S	S
AI6 Administración de Cambios		P	P
AI7 Instalar y acreditar soluciones y cambios		S	S
DS01 Definición del nivel de servicio	S	S	S
DS02 Administración del servicio de terceros	S	S	S
DS03 Administración de la capacidad y el desempeño			S
DS04 Asegurar el servicio continuo			P
DS05 Garantizar la seguridad del sistema	P	P	S
DS09 Administración de la configuración			S

Continua …

PROCESOS DE TI	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
DS10 Administración de problemas e			S
incidentes			
DS11 Administración de datos		P	
DS12 Administración de Instalaciones		P	P
DS13 Administración de Operaciones		S	S

Tabla No. 3-8 Identificación de procesos COBIT afectados. (P=Primario, S=Secundario)

(Fuente: COBIT 4.1)

Para realizar la valoración de acuerdo a los criterios de información establecidos y la relación entre estos, se procederá de la siguiente manera:

CRITERIOS	RELACIÓN	VALORACIÓN
Confidencialidad	P	6
	S	3
Integridad	P	4
	S	2
Disponibilidad	P	2
	S	1

Tabla No. 3-9 Valoración de criterios

A continuación, se muestran los procesos de TI identificados, con los valores correspondientes de acuerdo a la Tabla No. 3-9.

PROCESOS DE TI	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL CRITERIOS
PO2 Definir la arquitectura de información	3	4		7
PO8 Asegurar el cumplir requerimientos externos		2		2
PO9 Evaluación de Riesgos	6	4	2	12
AI2 Adquisición y mantenimiento de SW aplicativo		2		2
AI3 Adquisición y mantenimiento de arquitectura TI		2	1	3
AI4 Desarrollo y mantenimiento de Procedimientos de TI		2	1	3
AI6 Administración de Cambios		4	2	6
AI7 Instalar y acreditar soluciones y cambios		2	1	3
DS01 Definición del nivel de servicio	3	2	1	6
DS02 Administración del servicio de terceros	3	2	1	6
DS03 Administración de la capacidad y el desempeño			1	1
DS04 Asegurar el servicio			2	2

Continua …

PROCESOS DE TI	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL CRITERIOS
continuo				
DS05 Garantizar la seguridad del sistema	6	4	1	11
DS09 Administración de la configuración			1	1
DS10 Administración de problemas e incidentes			1	1
DS11 Administración de datos		4		4
DS12 Administración de Instalaciones		4	2	6
DS13 Administración de Operaciones		2	1	3

Tabla No. 3-10 Procesos identificados con valoración

Siguiendo con la metodología, se procede a totalizar los criterios y a priorizarlos en orden descendente.

PROCESOS DE TI	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL CRITERIOS
PO9 Evaluación de Riesgos	6	4	2	**12**
DS05 Garantizar la seguridad del sistema	6	4	1	**11**
PO2 Definir la arquitectura de información	3	4		**7**
AI6 Administración de Cambios		4	2	**6**
DS01 Definición del nivel de servicio	3	2	1	**6**

Continua …

PROCESOS DE TI	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL CRITERIOS
DS02 Administración del servicio de terceros	3	2	1	**6**
DS12 Administración de Instalaciones		4	2	**6**
DS11 Administración de datos		4		**4**
AI3 Adquisición y mantenimiento de arquitectura TI		2	1	**3**
AI4 Desarrollo y mantenimiento de Procedimientos de TI		2	1	**3**
AI7 Instalar y acreditar soluciones y cambios		2	1	**3**
DS13 Administración de Operaciones		2	1	**3**
PO8 Asegurar el cumplir requerimientos externos		2		**2**
AI2 Adquisición y mantenimiento de SW aplicativo		2		**2**
DS04 Asegurar el servicio continuo			2	**2**
DS03 Administración de la capacidad y el desempeño			1	**1**
DS09 Administración de la configuración			1	**1**
DS10 Administración de problemas e incidentes			1	**1**

Tabla No. 3-11 Priorización de los procesos identificados

Como se puede observar en la Tabla No. 3-11, los procesos **AI6 Administración de Cambios** y **DS12 Administración de Instalaciones,** tienen el mismo valor; en la empresa COCASINCLAIR EP, los sistemas que están en producción Flexline y el de Control de Asistencias, no se realizan cambios o actualizaciones con parches o modificaciones en sus funcionalidades, el software fue adquirido a terceros con recepción del software tipo “llave en mano”, es decir, posterior a su recepción no han existido requerimientos en sus funcionalidades por parte de COCASINCLAIR EP. En lo que se refiere a los parches o actualizaciones a la infraestructura que soportan estos sistemas, tomando en consideración que la plataforma es Windows, se crean puntos de restauración en el mismo sistema operativo de los servidores y se procede a aplican los parches.

Por lo señalado anteriormente, a pesar de que existen sistemas de información en producción, más importante para esta auditoría y por lo manifestado en la Coordinación de TIC’S, el proceso de Administración de Instalaciones (ambiente físico) es el de mayor relevancia, por cuanto hace unos 9 meses atrás, se realizó la implementación del nuevo Data Center y toda la infraestructura se encuentra en garantía, y como resultado de ésta auditoría se puede determinar posibles fallas en los controles implementados y se estaría a tiempo como para solicitar al proveedor ajustes ya sea en las configuraciones de los equipos o en su instalación.

3.3.2.4 Procesos que serán auditados en la Coordinación de TIC'S.

Como resultado de la priorización, se identificaron los 6 procesos más relevantes de la Coordinación de TIC'S, que serán posteriormente revisados o auditados siguiendo el estándar COBIT 4.1 como se había propuesto en el alcance de este trabajo de tesis.

Consecuentemente, los procesos que serán sujetos de la auditoría son:

PO9: EVALUAR Y ADMINISTRAR RIESGOS DE TI

DS05: GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

PO2: DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN

DS01: DEFINIR Y ADMINISTRAR NIVELES DE SERVICIO

DS02: ADMINISTRAR SERVICIOS DE TERCEROS

DS12: ADMINISTRAR EL AMBIENTE FÍSICO

ESPACIO EN BLANCO INTENCIONAL

3.3.2.5 Identificación de los riesgos relacionados a los procesos de TI.

A continuación, se detallan los riesgos asociados a los procesos anteriormente identificados.

PROCESOS DE TI	DEFINICION DE COBIT	DEFINICION DE RIESGO
PO9 EVALUAR Y ADMINISTRAR RIESGOS	Elaborar un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales.	Los riesgos de TI no son identificados, analizados, tratados y comunicados de manera adecuada.
DS05 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS.	Definir políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.	No se tiene criterios para comparar la gestión de la seguridad de los sistemas (accesos, autorizaciones, modificaciones) antes, durante y después de su uso.
PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN	Establecer un modelo de datos empresarial que incluya un esquema de clasificación de información que garantice la integridad y consistencia de	Datos diversos de varias fuentes, no se mantiene un estándar o formato. Los datos pueden ser modificados y no se puede

Continua …

PROCESOS DE TI	DEFINICION DE COBIT	DEFINICION DE RIESGO
	todos los datos.	determinar la veracidad de los mismos.
DS01 DEFINIR Y ADMINISTRAR NIVELES DE SERVICIO	Identificar los requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.	Incumplir estándares de servicio por falta de control y de seguimiento por servicio. Las especificaciones pueden estar mal detalladas o incompletas.
DS02 ADMINISTRAR SERVICIOS DE TERCEROS	Establecer relaciones y responsabilidades bilaterales con proveedores calificados de servicios cumplidos por terceros, y el monitoreo de la prestación del servicio para verificar y asegurar la adherencia a los convenios.	Desconocimiento de las responsabilidades contractuales de los proveedores por servicio prestado, puede ocasionar incumplimiento de contratos o convenios.
DS12 ADMINISTRAR EL AMBIENTE FÍSICO	Proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo.	Se producen interrupciones en los Servicios de TI debido a problemas físicos de los Equipos y/o Instalaciones.

Tabla No. 3-12 Identificación de los riesgos relacionados a los procesos de TI.

3.3.2.6 Valoración y Evaluación de controles.

De acuerdo al estándar COBIT 4.1, cada uno de los procesos tienen asociados controles, los que posteriormente serán evaluados para determinar su situación y sugerir las recomendaciones respectivas. Se detallan los controles relacionados a los procesos de TI identificados para realizar la auditoría.

PROCESOS DE TI	OBJETIVOS DE CONTROL
PO9 EVALUAR Y ADMINISTRAR RIESGOS	PO9.1 Marco de Trabajo de Administración de Riesgos PO9.2 Establecimiento del Contexto del Riesgo PO9.3 Identificación de Eventos PO9.4 Evaluación de Riesgos de TI PO9.5 Respuesta a los Riesgos PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos
DS05 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	DS5.1 Administración de la Seguridad de TI DS5.2 Plan de Seguridad de TI DS5.3 Administración de Identidad DS5.4 Administración de Cuentas del Usuario DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad DS5.6 Definición de Incidente de Seguridad DS5.7 Protección de la Tecnología de Seguridad DS5.8 Administración de Llaves Criptográficas DS5.9 Prevención, Detección y Corrección de Software Malicioso DS5.10 Seguridad de la Red

Continua …

PROCESOS DE TI	OBJETIVOS DE CONTROL
	DS5.11 Intercambio de Datos Sensitivos
PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN	PO2.1 Modelo de Arquitectura de Información Empresarial PO2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos PO2.3 Esquema de Clasificación de Datos PO2.4 Administración de Integridad
DS01 DEFINIR Y ADMINISTRAR NIVELES DE SERVICIO	DS1.1 Marco de Trabajo de la Administración de los Niveles de Servicio DS1.2 Definición de Servicios DS1.3 Acuerdos de Niveles de Servicio DS1.4 Acuerdos de Niveles de Operación DS1.5 Monitoreo y Reporte del Cumplimento de los Niveles de Servicio DS1.6 Revisión de Acuerdos de Niveles de Servicio y Contratos
DS02 ADMINISTRAR SERVICIOS DE TERCEROS	DS2.1 Identificación de Todas las Relaciones con Proveedores DS2.2 Gestión de Relaciones con Proveedores DS2.3 Administración de Riesgos del Proveedor DS2.4 Monitoreo del Desempeño del Proveedor
DS12 ADMINISTRAR EL AMBIENTE FÍSICO	DS12.1 Selección y Diseño del Centro de Datos DS12.2 Medidas de Seguridad Física DS12.3 Acceso Físico DS12.4 Protección Contra Factores Ambientales DS12.5 Administración de Instalaciones Físicas

Tabla No. 3-13 Detalle de los objetivos de control relacionados a los procesos de TI

3.3.2.7 Matriz de riesgos resultante de la Coordinación de TIC'S

Finalmente, se presenta la matriz de riesgos asociados a los objetivos de control de los procesos identificados anteriormente y que serán sujetos de la revisión.

PROCESO DE TI (No.1)	OBJETIVOS DE CONTROL	RIESGOS
PO9 EVALUAR Y ADMINISTRAR RIESGOS	**PO 9.1 Marco de Trabajo de Administración de Riesgos**	Los riesgos de TI y riesgos de negocio gestionado de forma independiente. El impacto de un riesgo de TI en el negocio sin ser detectado. La falta de control de los costos de gestión de riesgos. Cada riesgo visto como una amenaza individual más que en un contexto global. Apoyo ineficaz para la evaluación del riesgo por la alta dirección.
	PO 9.2 Establecimiento del Contexto del Riesgo	Riesgos irrelevantes considerados importantes Riesgos importantes no se da la debida atención Enfoque inadecuado para la evaluación de riesgos
	PO 9.3 Identificación de Eventos	Los eventos del riesgo irrelevante identificado y enfocado, más adelante puede ser que los eventos más importantes son los que faltan.

	PO 9.4 Evaluación de Riesgos de TI	Riesgos irrelevantes considerados importantes Cada riesgo visto como un único evento en lugar de en un contexto global. La incapacidad para explicar los riesgos significativos para la gestión. Riesgos importantes posiblemente se han perdido Pérdida de los activos de TI. Incumplimiento a la confidencialidad y la integridad de los activos de TI.
	PO 9.5 Respuesta a los Riesgos	Respuestas a los riesgos no efectivas No Identificados los riesgos de negocio residuales El uso ineficiente de los recursos para responder a los riesgos. Exceso de confianza en los pobres controles existentes.
	PO 9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos	Controles de mitigación de riesgos que no funcione como está diseñado. Los controles de compensación que se desvían de los riesgos identificados.

PROCESO DE TI (No.2)	OBJETIVOS DE CONTROL	RIESGOS
DS05 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	**DS 5.1 Administración de la Seguridad de TI**	La falta de seguridad del gobierno de TI Desalineado TI y los objetivos de negocio Datos no protegidos y activos de información
	DS 5.2 Plan de Seguridad de TI	Plan de seguridad de TI no está alineado con los requerimientos del negocio. Plan de seguridad de TI no es rentable. Negocios expuestos a amenazas no contempladas en la estrategia. Diferencias entre planificación y ejecución de medidas de seguridad de TI. Los usuarios no conocen el plan de seguridad de TI. Medidas de seguridad comprometidos por los interesados y usuarios.
	DS 5.3 Administración de Identidad	Los cambios no autorizados en el hardware y el software. La administración de acceso no cumple los requisitos de negocio y ponen en peligro la seguridad de los sistemas críticos de negocio. Sin especificación los requisitos de seguridad para todos los sistemas. Segregación de violaciones de servicio.

		Sistemas de información comprometidos.
	DS 5.4 Administración de Cuentas del Usuario	Brechas de seguridad Usuarios que no cumplan con la política de seguridad Incidentes no resueltos de manera oportuna Incumplimiento de cancelar las cuentas no utilizadas de manera oportuna, puede afectar la seguridad corporativa
	DS 5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad	Mal uso de las cuentas de los usuarios, poniendo en peligro la seguridad organizacional. No se han detectado incumplimientos de seguridad. Registros no confiables de seguridad.
	DS 5.6 Definición de Incidente de Seguridad	No se han detectado incumplimientos de seguridad. Falta de información para realizar reacciones. Falta de clasificación de las infracciones de seguridad.
	DS 5.7 Protección de la Tecnología de Seguridad	Exposición de la información. Abuso de confianza con otras organizaciones Violaciones de los requisitos legales y reglamentarios.
	DS 5.8	Claves mal utilizados por personas no

	Administración de Llaves Criptográficas	autorizadas Registro de usuarios no verificados, lo que compromete la seguridad del sistema. Acceso no autorizado a las claves encriptadas.
	DS 5.9 Prevención, Detección y Corrección de Software Malicioso	Exposición de la información. Violaciones de los requisitos legales y reglamentarios. Sistemas y datos que son propensos a ataques de virus. Medidas ineficaces.
	DS 5.10 Seguridad de la Red	Incumplimiento de las reglas de firewall para reflejar la política de seguridad de la organización No se han detectado modificaciones no autorizadas a las reglas de firewall. Comprometida la arquitectura de seguridad global Las brechas de seguridad no se detectan de manera oportuna.
	DS 5.11 Intercambio de Datos Sensitivos	Información delicada expuesta. Insuficiencia de las medidas de seguridad físicas Conexiones externas no autorizadas a los sitios remotos.

		Divulgación de los activos y la información confidencial accesible para personas no autorizadas.

PROCESO DE TI (No.3)	OBJETIVOS DE CONTROL	RIESGOS
PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN	**PO 2.1 Modelo de Arquitectura de Información Empresarial**	Información insuficiente para funciones del negocio. Inconsistencia entre los requisitos de información y desarrollo de aplicaciones. Incoherencia en los datos entre la organización y los sistemas. Mayor esfuerzo requerido o la imposibilidad de cumplir con las obligaciones mandatorias (por ejemplo, el cumplimiento de informes, la seguridad, la privacidad). Planificación ineficiente de programas de inversión de TI debido a la falta de información. Acumulación de datos que no son relevantes, coherentes o utilizables de una manera económica
	PO 2.2 Diccionario de Datos Empresarial y Reglas de	Información compromete la integridad Datos incompatibles e inconsistentes

	Sintaxis de Datos	Aplicación ineficaz de los Controles
	PO 2.3 Esquema de Clasificación de Datos	Requisitos de seguridad inadecuadas. Inversiones inadecuadas o excesivas en los controles de seguridad. Ocurrencia de la privacidad, la confidencialidad de datos, integridad y disponibilidad de los incidentes Incumplimiento de los requisitos reglamentarios o de terceros. Información inconsistente o ineficaz para la toma de decisiones.
	PO 2.4 Administración de Integridad	Errores de integridad de datos e incidencias. Datos no fiables en los que basan las decisiones de negocios. Incumplimiento de los requisitos reglamentarios o de terceros. Informes externos no creíbles.

PROCESO DE TI (No.4)	**OBJETIVOS DE CONTROL**	**RIESGOS**
DS01 DEFINIR Y ADMINISTRAR NIVELES DE SERVICIO	**DS 1.1 Marco de Trabajo de la Administración de**	Las brechas entre las expectativas y capacidades, dan lugar a controversias. Clientes y proveedores no entienden sus responsabilidades. Prioridad incorrecta para servicios

	los Niveles de Servicio	prestados. Servicio de funcionamiento ineficiente y costoso.
	DS 1.2 Definición de Servicios	Entrega de Servicios inapropiados. Prioridad incorrecta para servicios prestados. Mal entendido el impacto de incidentes, respuesta lenta e un impacto significante en el negocio. Diferentes interpretaciones y malos entendidos de los servicios de TI.
	DS 1.3 Acuerdos de Niveles de Servicio	Incumplimiento de los requisitos de servicio al cliente. Uso ineficiente e ineficaz de los recursos prestados en el servicio. No identificar y responder a los incidentes críticos de servicio.
	DS 1.4 Acuerdos de Niveles de Operación	Incumplimiento de los servicios prestados para cumplir con los requerimientos del negocio. Brechas en la comprensión técnica de los servicios que lleva a incidentes. Uso ineficiente y costoso de los recursos operativos.
	DS 1.5 Monitoreo y Reporte del	Falta de definiciones de medidas importantes para la organización. No Identificados los problemas y las

	Cumplimento de los Niveles de Servicio	cuestiones subyacentes de servicio. Usuarios insatisfechos por la falta de información, independientemente de la calidad del servicio
	DS 1.6 Revisión de los Acuerdos de Niveles de Servicio y de los Contratos	Requisitos comerciales y legales no se cumplen debido a los contratos fuera de fecha. Servicios que no cumplan los requisitos modificados. Pérdidas financieras e incidentes debidos a los servicios desalineados.

PROCESO DE TI (No.5)	**OBJETIVOS DE CONTROL**	**RIESGOS**
DS02 ADMINISTRAR SERVICIOS DE TERCEROS	**DS2.1 Identificación de Todas las Relaciones con Proveedores**	No Identificados los proveedores principales y críticos. Uso ineficiente e ineficaz de los recursos manejados de proveedores. Roles y responsabilidades poco claros que conduce a problemas de comunicación, servicios deficientes e incremento de costos.
	DS 2.2 Gestión de Relaciones con Proveedores	Relación con el proveedor no responde o no está comprometido. Problemas y cuestiones no resueltas. Calidad de los servicios inadecuados.

	DS 2.3 Administración de Riesgos del Proveedor	Incumplimiento de las obligaciones reglamentarias y legales. La seguridad es tratada como otro incidente. Las pérdidas financieras y daños de reputación a causa de la interrupción del servicio.
	DS 2.4 Monitoreo del Desempeño del Proveedor	Degradación del servicio no detectado. Incapacidad para afrontar costos y calidad de servicio. Incapacidad para optimizar la elección de los proveedores.

PROCESO DE TI (No.6)	**OBJETIVOS DE CONTROL**	**RIESGOS**
DS12 ADMINISTRAR EL AMBIENTE FÍSICO	**DS 12.1 Selección y Diseño del Centro de Datos**	Las amenazas a la seguridad física no identificadas. El aumento de la vulnerabilidad a los riesgos de seguridad, como resultado de la ubicación del sitio y / o el diseño.
	DS 12.2 Medidas de Seguridad Física	Amenazas a la seguridad física no identificadas Hardware robado por personas no autorizadas Ataque físico en el sitio de TI. Dispositivos reconfigurados sin

		autorización Información confidencial que se accede por dispositivos configurados para leer la radiación emitida por los equipos inalámbricos.
	DS 12.3 Acceso Físico	Los visitantes tengan acceso no autorizado a los equipos informáticos o información. Entrada no autorizada a las áreas seguras.
	DS12.4 Protección Contra Factores Ambientales	Instalaciones expuestas a los impactos ambientales. Incapacidad de detectar una amenaza ambiental. Medidas inadecuadas para la protección de amenazas del medio ambiente.
	DS 12.5 Administración de Instalaciones Físicas	Incumplimiento de las normas de salud y seguridad. Sistemas de TI fallan debido a la protección inadecuada de los cortes de energía y otros riesgos relacionados con las instalaciones. Accidentes a los miembros del personal

Tabla No. 3-14 Matriz de riesgos relacionados a los procesos de TI.

CAPÍTULO 4

AUDITORÍA A LOS PROCESOS

4.1 Generalidades

Para realizar la auditoria a los procesos de la Coordinación de TIC'S de la empresa COCASINCLAIR EP, se utilizará lo señalado en IT Assurance Guide de COBIT**,** la evaluación a los controles de los procesos se lo efectuará al diseño o a sus salidas (eficacia operacional). Adicionalmente, se determinará las causas y efectos, las recomendaciones de acuerdo a los hallazgos obtenidos y finalmente, se indicará el nivel de madurez de cada proceso.

4.2 IT Assurance Guide

El objetivo de IT Assurance Guide, es proporcionar orientación sobre el uso de COBIT para apoyar la gobernabilidad por medio de procesos de aseguramiento de TI. IT Assurance Guide está diseñada para permitir un desarrollo eficiente y eficaz de las iniciativas de fortalecimiento de TI. También ofrece orientaciones sobre cómo los recursos de COBIT puede utilizarse apoyados por pruebas detalladas basadas en procesos de COBIT y objetivos de control.

4.3 Modelo Genérico de Madurez [8]

A continuación, se detalla la clasificación de un modelo genérico de madurez, como referencia para determinar el nivel de madurez de los procesos que serán auditados.

0 No Existente.- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido que existen problemas a resolver.

1 Inicial.- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad-doc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible.- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

[8] Fuente: COBIT 4.1

3 Definido.- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

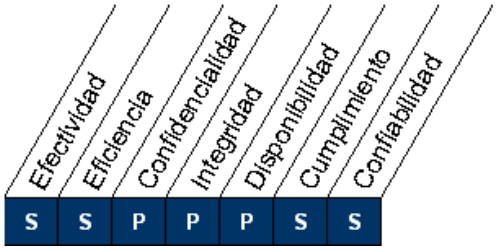
4 Administrado.- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 Optimizado.- Los procesos se han refinado hasta un nivel de mejor práctica, se basa en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y efectividad, haciendo que la empresa se adapte de manera rápida.

4.4 Primer proceso a Auditar: Evaluar y administrar los Riesgos de TI

La metodología para la revisión de este proceso se realizará mediante la evaluación al diseño del control.

DOMINIO	PLANEAR Y ORGANIZAR
NOMBRE DEL PROCESO	PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI
REFERENCIA DE COBIT	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.



Criterios o requerimientos de información

(P=Primario, S=Secundario) [9]

Recursos de TI

Áreas de Gobierno de TI

[9] Las referencias primarias (P) y secundarias (S) de los criterios de información para las 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. Algunos procesos tienen mayor impacto en la meta de TI que otros

4.4.1 Objetivos de Control del proceso

NOMBRE DEL CONTROL	1. MARCO DE TRABAJO DE ADMINISTRACIÓN DE RIESGOS	
REFERENCIA DE COBIT	Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.	
EVALUACIÓN (EVIDENCIAS)		
Revisar si el marco de trabajo de la administración de riesgos de TI se alinea con el marco de trabajo de la administración de riesgos para la organización (empresa) e incluye componentes de negocios impulsados por la estrategia, los programas, proyectos y operaciones. Revisar la clasificación de riesgos de TI para verificar que se basan en un conjunto común de características desde el marco de trabajo de la administración de riesgos de la organización. Revisar si las mediciones de los riesgos de TI están estandarizados, priorizados y si incluyen el impacto, la aceptación del riesgo residual y las probabilidades alineadas con el marco de trabajo de la administración de riesgos de la empresa.	En un documento borrador denominado Política de Servicio, Uso y Seguridad de la Administración de Red (PMC-001), elaborado en julio del 2010, se enuncia que el Departamento de Sistemas identificará los riesgos y amenazas de la Empresa y establecerá planes de mitigación necesarios. Este documento se presentó a la Gerencia General vía correo electrónico el 03 de octubre de 2011, para que se realice observaciones, el mismo que no se ha tenido ninguna respuesta todavía. Como no se tienen identificados los riesgos de TI, no se pueden realizar mediciones o caracterizarlos por prioridad o impacto.	
Verificar si los riesgos son considerados en la elaboración y revisión de los planes estratégicos de TI.	En el plan estratégico de la Empresa, en la **Política No. 8F,** se enuncia estrategias de gestión de riesgos del trabajo y de seguridad integral, más no se hace referencia para el área de TIC'S. Adicionalmente, la Coordinación	

	de TIC'S no ha elaborado su plan estratégico, se indicó que para el próximo año (2013) se elaboraría este documento.
OBSERVACIÓN	
La empresa COCASINCLAIR EP, no cuenta con un marco de trabajo para una administración de riesgos. La Coordinación de TIC'S, tampoco tiene un marco de trabajo para la administración de riesgos. El documento borrador, Política de Servicio, Uso y Seguridad de la Administración de Red (PMC-001), no se le hizo un seguimiento a las políticas enunciadas y tampoco lo revisó la máxima autoridad, consecuentemente no se realizó la identificación de los riesgos y las acciones necesarias que se debían tomar para mitigar los riesgos. La estandarización, priorización, impacto, etc., de los riesgos no se llegó a describir en el documento. La Coordinación de TIC'S, como no ha elaborado su Plan Estratégico, no se puede revisar los riesgos que se pudieran haber considerado para el área, su tratamiento, impacto, recursos, etc., necesarios para gestionarlos.	

NOMBRE DEL CONTROL	**2. ESTABLECIMIENTO DEL CONTEXTO DEL RIESGO**
REFERENCIA DE COBIT	Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.
EVALUACIÓN (EVIDENCIAS)	
Preguntar y confirmar si es que en el contexto apropiado el riesgo ha sido definido de acuerdo con las políticas y principios de la administración de riesgo de la empresa e incluye procesos, tales como sistemas, administración de	Los riesgos no han sido identificados para la Coordinación de TIC'S. No se han definido las políticas y principios de la administración de riesgos de la empresa. Los factores de riesgo internos y

proyectos, ciclos de vida de software aplicativo, administración de operaciones y servicios de TI. Factores de riesgo internos y externos deben ser incluidos.	externos, aunque se han presentado (por ejemplo, robo del cable de fibra óptica del enlace de datos con el Campamento San Rafael), no se les ha gestionado. Se realizan acciones luego de que ocurre un incidente y este se gestiona tratando de restablecer la disponibilidad del servicio. La gestión se realiza al incidente.
Determinar si el contexto de riesgos de TI es comunicado y entendido.	No existe evidencia que demuestre que se han comunicado los riesgos, por el mismo hecho de no haberlos identificado y promovido su gestión.
OBSERVACIÓN	
La falta de identificación de riesgos de la Coordinación de TIC'S, ha ocasionado que no se puedan gestionar adecuadamente. No se ha elaborado un plan de gestión de riesgos por proyectos, sistema o servicios que brinda el área. No se cuenta con políticas y principios de la administración de riesgos de la Empresa.	

NOMBRE DEL CONTROL	**3. IDENTIFICACIÓN DE EVENTOS**
REFERENCIA DE COBIT	Identificar eventos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto y mantener esta información. Registrar y mantener los riesgos relevantes en un registro de riesgos.
EVALUACIÓN (EVIDENCIAS)	
Revisar el proceso utilizado para identificar eventos potenciales y	No se encuentran identificados eventos potenciales. Los incidentes ocurridos

determinar si todos los procesos de TI están incluidos en el análisis. El diseño del proceso debe cubrir eventos internos y externos. La identificación de eventos potenciales pueden incluir los resultados de auditorias anteriores, inspecciones e incidentes identificados, utilizando listas de control, talleres y análisis del flujo de proceso. Delinear los impactos identificados para el riesgo registrado para determinar si el registro está completo, actualizado y alineado con la terminología del marco de trabajo de la administración de riesgos de la empresa.	son registrados en formularios de soporte (servicio de impresoras, por ejemplo) y por tickets de casos (servicios de internet y enlace de datos). No existe evidencia de la identificación de impactos para los riesgos en la Coordinación de TIC'S.
Preguntar si los equipos multi-funcionales son apropiados y están involucrados en las diferentes actividades identificadas de evento e impacto. Revisar una muestra del registro de riesgos por la importancia de las amenazas, vulnerabilidades e impacto y analizar la eficacia del proceso identificado, registrar y juzgar los riesgos.	En la empresa COCASINCALIR EP, se conformaron grupos multifuncionales para elaborar la matriz de riesgos de trabajo, enfocados en cumplir la norma ISO 14001. No se tiene evidencia de la conformación de equipos multifuncionales para la gestión de riesgos de TI (amenazas, vulnerabilidades, impactos) de la Coordinación de TIC'S o de la Empresa.
OBSERVACIÓN	
La informalidad de la administración de riesgos de la Coordinación de TIC'S, no ha permitido identificar los eventos y determinar sus impactos en la Empresa. No se tiene registros de la relevancia de los riesgos y estos son tratados a medida que	

ocurre un incidente. La mayoría de incidentes no se tienen documentados; los servicios de impresión, internet y del enlace de datos si son registrados. No se tiene evidencia que se realice una identificación de eventos. No se han conformado equipos multifuncionales para identificar eventos e impactos en la Empresa COCASINCLAIR EP.

NOMBRE DEL CONTROL	**4. EVALUACIÓN DE RIESGOS DE TI**
REFERENCIA DE COBIT	Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.
EVALUACIÓN (EVIDENCIAS)	
A través del proceso de administración de riesgos determinar si los riesgos inherente y residual están definidos y documentados.	No se presentó documentación que respalde que los riesgos inherentes y residuales están definidos y documentados.
Preguntar y confirmar si es que el proceso de administración de riesgos evalúa los riesgos identificados cualitativamente y / o cuantitativamente.	Como no existe un proceso de administración de riesgos, no se puede evaluar si son tratados cualitativa o cuantitativamente. No hay información al respecto.
Revisar el plan y otra documentación para evaluar la idoneidad de la evaluación de riesgos cualitativa o cuantitativamente.	En la Coordinación de TIC'S, no disponen de la documentación solicitada para revisar este requerimiento.
A través del proceso, determinar si las fuentes de información utilizadas en el análisis son razonables.	Como no se encuentra definido el proceso de administración de riesgos, no se puede identificar las fuentes de información. No se dispone de

	información sobre riesgos inherentes.
Revisar el uso de análisis estadístico y la determinación de probabilidad para medir la probabilidad cualitativa o cuantitativa.	No se dispone de esta información en la Empresa.
Preguntar o revisar si alguna correlación entre los riesgos está identificada. Revisar cualquier correlación para verificar que este está expuesto significativamente a diferentes probabilidades y los resultados de impacto derivados de tales relaciones.	Puede existir correlación entre los riesgos de la misma área. Pero, por la falta de la definición del proceso de administración de riesgos de TI, no se puede revisar la correlación de riesgos. No existen riesgos identificados ni tampoco detallados en la Coordinación de TIC'S.
OBSERVACIÓN	
Por el mismo hecho de no tener definido el proceso de administración de riesgos, no se puede evaluar la probabilidad e impacto con métodos cualitativos o cuantitativos. No se evidencia la identificación de riesgos inherentes y residuales categorizados por servicio, infraestructura, almacenamiento, disponibilidad de los sistemas, etc.,	

NOMBRE DEL CONTROL	**5. RESPUESTA A LOS RIESGOS**
REFERENCIA DE COBIT	Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que controles efectivos en costo mitigan la exposición en forma continua. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.
EVALUACIÓN (EVIDENCIAS)	
Revisar si los resultados de la evaluación de riesgos se asignaron a	No se ha realizado la evaluación de riesgos en la Coordinación de TIC'S.

una respuesta de mitigación para evitar, transferir, reducir, compartir o aceptar cada riesgo y si se alinean con los mecanismos utilizados para la administración de riesgos en la organización.	Como se señaló anteriormente, el proceso de administración de riesgos no se ha efectuado en la Coordinación ni tampoco se han detallado ningún riesgo.
OBSERVACIÓN	
No se evidencia un proceso de administración de riesgos de TI. La falta de una matriz de riesgos, no permite identificar las acciones o estrategias que se deben realizar por cada riesgo identificado. La gestión de riesgos es nula. La Coordinación de TIC'S trata de responder a los incidentes (probabilidad de ocurrencia cumplida), en el menor tiempo. Aun así, no se implementan controles efectivos de bajo costo que mitiguen la ocurrencia repetitiva de incidentes. No se puede realizar ningún tipo de evaluación de riesgos por la falta de identificación de riesgos, no se puede gestionarlos.	

NOMBRE DEL CONTROL	**6. MANTENIMIENTO Y MONITOREO DE UN PLAN DE ACCIÓN DE RIESGOS**
REFERENCIA DE COBIT	Priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Obtener la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas están a cargo del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.
EVALUACIÓN (EVIDENCIAS)	
Preguntar si los riesgos aceptados son formalmente reconocidos y registrados	No están identificados los riesgos, no existe un documento que evidencie el

en un plan de acción de riesgos.	registro de los riesgos.
Evaluar apropiadamente los elementos del plan de administración de riesgos.	No existe un documento que evidencie un plan de administración de riesgos, consecuentemente no se pueden evaluar.
Preguntar o revisar si la ejecución, informe del progreso y las desviaciones son monitoreados.	De la entrevista, se manifiesta que no hay un monitoreo de la evolución de los riesgos, más aún, no están identificados los riesgos de la Coordinación de TIC'S.
Revisar las respuestas al riesgo para las aprobaciones correspondientes.	Las respuestas a los riesgos son de manera reactiva, es decir luego que se presenta el incidente (ocurre el riesgo). Las acciones tomadas no se documentan y el incidente es atendido de inmediato.
Revisar las acciones para verificar si la participación está asignada y documentada.	No se encuentra evidencia sobre este requerimiento.
Revisar si el plan de acción de riesgos se mantiene eficazmente y ajustado.	El plan de acción de riesgos no se ha elaborado.
OBSERVACIÓN	
Falta documentación que refleje el mantenimiento y monitoreo del plan de acción de riesgos. No se tiene identificado los riesgos de la Coordinación de TIC'S. No hay un plan de acción para administrar los riesgos.	

4.4.2 Resultados de la evaluación del proceso

EVIDENCIAS ENCONTRADAS Y EVALUADAS DEL PROCESO: PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI
Se encontraron como evidencia los siguientes documentos: - Formularios de soporte (servicio de impresoras) y tickets de casos (servicios de internet y enlace de datos) - Política de Servicio, Uso y Seguridad de la Administración de Red (PMC-001) - Plan estratégico de la Empresa 2011-2015.

RESULTADOS DE LA EVALUACIÓN DEL PROCESO: PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI
Como resultado de la evaluación de los objetivos de control del proceso PO9 Evaluar y administrar los Riesgos de TI, se detalla lo siguiente: **Efecto**: El no contar con un proceso claro de administración de riesgos, apegados a un marco de trabajo de la empresa, no permite evaluar los riesgos, mitigar o gestionarlos y comunicar los riesgos residuales. No se pueden identificar los riesgos, consecuentemente no se puede elaborar planes de acción para posteriormente monitorearlos. En la mayoría de los casos, no se documentan cuando ocurren los incidentes, se toman acciones para gestionarlos únicamente. **Causa**: No se le da la importancia necesaria a la administración de riesgos en la Coordinación de TIC'S. Adicionalmente, existe falta de gestión interna para darle continuidad a la Política de Servicio, Uso y Seguridad de la Administración de Red, en este documento ya se enunció que se elaboraría la gestión de riesgos de TI. **Recomendaciones**: Las recomendaciones propuestas para Evaluar y Administrar los Riesgos de TI, son: • Definir una política por parte de la Coordinación de TIC'S, para establecer un marco de trabajo para la administración de riesgos de TI, que permita identificar eventos y evaluar o gestionar los riesgos. • Documentar todos los incidentes de TI y asociar a los riesgos de acuerdo a su nivel o importancia, es decir, riesgos críticos, inherentes o residuales. Esto con la finalidad de generar indicadores de medición y monitoreo del plan de acción

de riesgos.

- Implementar procedimientos para la evaluación de riesgos generales o específicos de TI y documentarlos para que sean presentados a la Subgerencia Administrativa y posteriormente sean aprobados por la Gerencia General de COCASINCLAIR EP. Elaborar planes de acción de riesgos para gestionarlos.

- Reasignar o añadir como un producto o servicio de la Coordinación de TIC'S, la elaboración de la matriz de riesgos de TI y los planes de acción para gestionar los mismos. Comunicar estos riesgos a la Gerencia General y su impacto potencial sobre los procesos y metas de negocio.

4.4.3 Indicadores Clave de Rendimiento (Proceso: PO9 Evaluar y administrar los Riesgos de TI).

	INDICADOR	RESULTADOS
TI	% de objetivos críticos de TI cubiertos por la evaluación de riesgos.	No se dispone de información
	% de evaluaciones de riesgos de TI integrados en el enfoque de evaluación de riesgos de TI.	No se dispone de información
Procesos	% de eventos críticos de TI identificados que han sido evaluados.	No se registran los eventos
	# de riesgos de TI recientemente identificados (comparados con el ejercicio previo)	No se registran los riesgos
	# de incidentes significativos causados por riesgos no identificados por el proceso de evaluación de riesgos.	No se registran los incidentes
	% de riesgos críticos de TI identificados con un plan de acción elaborado.	No se registran los riesgos
Actividades	% del presupuesto de TI gastado en actividades de administración de los riesgos (evaluación y mitigación)	40%
	Frecuencia de la revisión del proceso de administración de riesgos de TI.	Ninguna
	% de evaluaciones de riesgo autorizadas.	No se evalúan los riesgos
	# de reportes de monitoreo de riesgos activados dentro	30 mensual (enlaces)

	de la frecuencia acordada.	3-4 mensual (impresoras)
	% de eventos de TI identificados usados en evaluaciones de riesgo.	No se registran los eventos
	% de planes de acción de administración de riesgos aprobados para su implementación.	No existe un proceso de administración de riesgos

4.4.4 Determinación del Nivel de Madurez (Proceso: PO9 Evaluar y administrar los Riesgos de TI).

NIVEL DE MADUREZ	0 ○ 1 ● **2** ○ 3 ○ 4 ○ 5 ○
REFERENCIA DE COBIT	*La administración del proceso de Evaluar y Administrar los Riesgos de TI que satisfaga el requerimiento de negocio de TI de analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y las metas de negocio es:* **1 Inicial / Ad Hoc:** 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. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.
RAZONES	Por los resultados de la evaluación, la administración de riesgos de TI en la empresa COCASINCLAIR EP, no tienen procesos definidos para identificar, tratar, mitigar y tomar acciones sobre los riesgos.

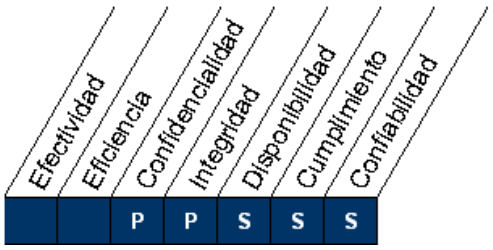
	Los riesgos son asociados a servicios específicos que brinda la Coordinación de TIC'S en los que se respaldan por los formularios de soporte o apertura de casos. Casi no existe documentación referente a los riesgos de soporte. Existe una identificación tácita de los riesgos referente a la disponibilidad de TI, se efectúan acciones de back-up (información) o redundancia (servicios) con la finalidad de minimizar el impacto si se produjera una amenaza que puediera afectar a otras áreas de la Empresa. La informalidad o falta de mecanismos para gestionar los riesgos de TI, queda demostrado en la carencia de documentación que respalde o evidencie los planes de acción y la evaluación de los riesgos.

4.5 Segundo proceso a Auditar: Garantizar la Seguridad de los Sistemas

La metodología para la revisión de este proceso se realizará mediante la evaluación al diseño del control.

DOMINIO	ENTREGAR Y DAR SOPORTE
NOMBRE DEL PROCESO	**DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS**
REFERENCIA DE COBIT	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.



Criterios o requerimientos de información

(P=Primario, S=Secundario) [10]

Áreas de Gobierno de TI

Recursos de TI

4.5.1 Objetivos de Control del proceso

NOMBRE DEL CONTROL	1. ADMINISTRACIÓN DE LA SEGURIDAD DE TI
REFERENCIA DE COBIT	Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.

[10] Las referencias primarias (P) y secundarias (S) de los criterios de información para las 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. Algunos procesos tienen mayor impacto en la meta de TI que otros

EVALUACIÓN (EVIDENCIAS)	
Determinar si existe un comité directivo de seguridad, con representación de las principales áreas funcionales, incluida la auditoría interna, recursos humanos, operaciones, seguridad de TI y legal.	No se ha conformado un comité directivo de seguridad, el área de la auditoría interna empezó a funcionar desde el mes de agosto de 2012. De acuerdo a la estructura orgánica por procesos de la Empresa, es responsabilidad de la Coordinación de TIC'S la seguridad de TI.
Determinar si existe un proceso para priorizar las iniciativas propuestas de seguridad, incluyendo los niveles requeridos de políticas, normas y procedimientos.	Las propuestas de seguridad nacen de la Coordinación de TIC'S, no existe un proceso para priorizar iniciativas de seguridad, tampoco están documentadas las políticas de seguridad.
Preguntar y confirmar si es que existe un documento de seguridad de la información.	No existe un documento de seguridad de la información, en julio del 2010 se elaboró un documento denominado Política de Servicio, Uso y Seguridad de la Administración de Red (PMC-001), sin embargo este se quedó incompleto y solo como borrador.
Revisar y analizar el documento para verificar que se refiere a los riesgos de la organización relativos a la seguridad de la información y que este incluye claramente: - Alcance y objetivos de la función de la gestión de la seguridad. - Las responsabilidades de la función de	Como consecuencia del requerimiento anterior, al no disponer de un documento de Seguridad de la Información, no se puede verificar el alcance, objetivo, responsabilidades de la gestión de la seguridad.

gestión de la seguridad. - Conformidad y riesgo controlado	
Preguntar y confirmar si es que la política de seguridad de la información cubre las responsabilidades del consejo de administración, dirección ejecutiva, gerencias, los miembros del personal de staff y los usuarios de la infraestructura de TI y que se refiere a las normas de seguridad y procedimientos detallados.	La Coordinación de TIC'S, no dispone de un documento de Seguridad de la Información, no se puede verificar si existe una política de seguridad enunciada.
Preguntar y confirmar si es que existe una política de seguridad detallada, las normas y los procedimientos. Ejemplos de políticas, normas y procedimientos incluyen: - Cumplimiento de la Política de Seguridad. - Gestión de la aceptación del riesgo (reconocimiento del incumplimiento de la seguridad). - Política de seguridad de comunicaciones externas. - Política de Firewall. - Políticas de seguridad de E-mail - Un acuerdo para cumplir con las políticas de Seguridad de la Información - Política de seguridad de un computador portátil / escritorio. - Política de uso de Internet	La Coordinación de TIC'S, no cuenta con un documento de Seguridad de la Información, no se puede verificar su política, gestión de riesgos, gestión de comunicaciones. Las políticas de firewall, se encuentran implementadas en el equipo Check Point, no están detalladas en un documento. Las políticas de seguridad de correo, se encuentran implementadas en Exchange Server 2010, no están detalladas en un documento estas políticas. Las políticas de uso del internet, en su mayoría se encuentran implementadas en el firewall, el resto de la política se implementa en la estación de trabajo. Esta política no está detallada en ningún documento. Las políticas de seguridad para estaciones de trabajo se lo hace a través del directorio activo de Windows

	Server 2008 R2, no se documentan estas políticas.
Preguntar y confirmar si que existe una adecuada estructura organizativa y reportes en línea para la seguridad de la información y evaluar si la gestión de la seguridad y las funciones de administración tienen la autoridad suficiente.	No se puede evaluar la gestión de la seguridad de la información, por cuanto no se tiene elaborado el documento de Seguridad de la Información. Los reportes generados por el firewall son requeridos para casos puntuales.
Preguntar y confirmar si es que existe un mecanismo de reportes de gestión de seguridad que informa a la directiva y a la administración de TI de la situación de la seguridad de la información.	No se generan reportes establecidos de seguridad, lo que se ejecutan son reportes en cada herramienta implementada de seguridad, referente a accesos, intentos de violación de políticas, logs de actividades realizadas en los equipos. Estos reportes se generan por demanda de la Subgerencia Administrativa, Gerencia General de la Empresa o por la misma Coordinación de TIC'S.
OBSERVACIÓN	
La empresa COCASINCLAIR EP, no cuenta con un comité directivo de seguridad. Específicamente, un documento de seguridad de la información no tiene la Empresa, consecuentemente no se puede determinar su estructura, contenido, roles, etc. Falta documentar las políticas de seguridad de forma detallada, las políticas se encuentran implementadas en los equipos de seguridad y en las estaciones de trabajo, el control es inconstante. Los reportes son elaborados bajo demanda y no se hace seguimiento a la situación de la seguridad de la información en TI.	

NOMBRE DEL CONTROL	2. PLAN DE SEGURIDAD DE TI
REFERENCIA DE COBIT	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan esta implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.

EVALUACIÓN (EVIDENCIAS)	
Determinar la eficacia de la recolección e integración de los requisitos de seguridad de la información dentro de un plan general de seguridad de TI que responda a las necesidades cambiantes de la organización.	A medida que aparecen nuevas vulnerabilidades en seguridad de la información, la Coordinación de TIC'S realiza ajustes o configuraciones que incrementan la seguridad de los sistemas. No existe un plan general de seguridad de TI.
Verificar que el plan de seguridad de TI considere planes tácticos de TI (PO1), clasificación de datos (PO2), estándares de tecnología (PO3), las políticas de seguridad y control (PO6), administración de riesgo (PO9), y cumplimiento de requerimientos externos (ME3).	La Coordinación de TIC'S no tiene un Plan de Seguridad de TI, no se puede verificar que el mencionado plan considere los procesos referidos en este control.
Determinar si existe un proceso para actualizar periódicamente el plan de seguridad de TI y si el proceso requiere niveles adecuados de revisión por la dirección y la aprobación de los cambios	Por la falta del Plan de Seguridad de TI, no se puede determinar que exista un proceso de actualización, revisión y aprobación de cambios a dicho plan.
Determinar si la línea base de la seguridad de la información de la	La Coordinación de TIC'S, no tiene el documento de Seguridad de la

empresa para todas las plataformas principales son acordes con el plan general de seguridad de TI, si las líneas base se han registrado en la línea base de configuración (DS9) del repositorio central, y si existe un proceso para actualizar periódica de las líneas base basados sobre los cambios en el plan.	Información y tampoco el Plan general de seguridad de TI, no se puede determinar la línea base sobre las plataformas y la existencia de un proceso de actualización de forma periódica.
Determinar si el plan de seguridad de TI incluye lo siguiente: - Un conjunto completo de políticas y estándares de seguridad, de acuerdo con el marco establecido de políticas de seguridad de la información - Los procedimientos para aplicar y hacer cumplir las políticas y normas - Roles y responsabilidades - Necesidades de personal - Conciencia y formación de seguridad - Aplicación de prácticas - Las inversiones en recursos requeridas en seguridad.	La Coordinación de TIC'S no tiene un Plan de Seguridad de TI, consecuentemente no se puede determinar si incluye lo requerido en este ítem dentro del plan.
Determinar si existe un proceso para integrar los requerimientos de seguridad de la información y asesoramiento sobre la ejecución del plan de seguridad de TI en otros procesos, incluyendo el desarrollo de los SLA (Service Level Agreement) y OLAs (Operational Level Agreement) (DS1-DS2), solución de requerimientos automatizados (AI1),	No existe un proceso para integrar los requerimientos de seguridad de la información y asesoramiento sobre le ejecución del plan de seguridad de TI.

software de aplicación (AI2), y componentes de infraestructura de TI (AI3).	
OBSERVACIÓN	
La Empresa no cuenta con un plan general de seguridad de TI, lo que causa que no se pueda contar con el documento de seguridad de la información alineado a las plataformas principales.	

NOMBRE DEL CONTROL	**3. ADMINISTRACIÓN DE IDENTIDAD**
REFERENCIA DE COBIT	Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única. Permitir que el usuario se identifique a través de mecanismos de autenticación. Confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio definidas y documentadas y que los requerimientos de trabajo están adjuntos a las identidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se despliegan técnicas efectivas en coste y procedimientos rentables, y se mantienen actualizados para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.
EVALUACIÓN (EVIDENCIAS)	
Determinar si las prácticas de seguridad requieren que los usuarios y los procesos del sistema sean identificables de manera única y ser configurado en el	Las prácticas de seguridad para los sistemas en la Empresa, es aplicada para que los usuarios sean identificados de manera única. En el

sistema para aplicar la autenticación antes de permitir el acceso.	aplicativo Flexline, correo electrónico y gestor documental, primero se realiza un proceso de autenticación antes de ingresar a los sistemas. No es documentada estas prácticas de seguridad.
Si se predeterminaron y aprobaron roles que son utilizados para permitir el acceso, determinar si los roles claramente delinean responsabilidades basadas sobre privilegios mínimos y garantizar que el establecimiento y la modificación de los roles son aprobados por el dueño de proceso.	Los permisos concedidos a los usuarios para acceder a los sistemas, son especificados por roles que pueden ejecutar en el sistema. En el caso específico del sistema Flexline y el Gestor Documental, explícitamente los permisos son administrados por privilegios. El administrador o el dueño del proceso no tiene documentado cuando es modificado un rol, tampoco cuando un rol es aprobado, esto se lo hizo en la fase de desarrollo para usuarios específicos.
Determinar si el aprovisionamiento de accesos y los mecanismos de control de autenticación se utilizan para controlar el acceso lógico a través de todos los usuarios, procesos del sistema y los recursos de TI, para que los usuarios gestionen de forma local y remota procesos y sistemas.	Se realizaron pruebas de acceso en el Gestor Documental para validar que los usuarios gestionen sus procesos dentro del sistema, se verificó que solo pueden realizar las acciones permitidas en su rol específico. De igual manera se comprobó en el sistema Flexline, los usuarios acceden solo a realizar las funciones específicas del rol asignado.
OBSERVACIÓN	
Los usuarios dentro de los sistemas informáticos implementados en la empresa, son identificados de manera única y primero son autenticados y luego asignado los roles. Las verificaciones se realizaron en el sistema Gestor Documental y Flexline.	

NOMBRE DEL CONTROL	4. ADMINISTRACIÓN DE CUENTAS DEL USUARIO
REFERENCIA DE COBIT	Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados.
EVALUACIÓN (EVIDENCIAS)	
Determinar si existen procedimientos para evaluar periódicamente y certificaciones de acceso al sistema, aplicaciones y autorizaciones.	De las evidencias encontradas, no existen procedimientos que evalúen periódicamente accesos al sistema, lo que existen son registros de acceso a los sistemas, más no su evaluación.
Determinar si existen procedimientos de control de acceso para controlar y gestionar los derechos y privilegios del sistema y aplicaciones de acuerdo con las políticas de seguridad de la organización y el cumplimiento de los requisitos reglamentarios.	Los procedimientos de control de acceso no se encuentran documentados, pero se siguen ciertos pasos para cumplir políticas de acceso y seguridad, principalmente este procedimiento se efectúa cuando se crea un usuario dentro del Directorio Activo y se le asigna permisos para el uso de carpetas compartidas por áreas o de sistemas. No se tiene claro los requisitos reglamentarios cuando se crean usuarios.

Determinar si los sistemas, aplicaciones y datos se han clasificado por niveles de importancia y riesgo, y si los propietarios del proceso se han identificado y asignado.	No se encuentra ninguna clasificación respecto a sistemas, aplicaciones y datos. Los propietarios de los procesos formalmente no han sido asignados, pero saben que son los responsables de su ejecución porque fueron el área requirente para la implementación del sistema o aplicación o fueron administradores de contrato.
Determinar si las políticas de distribución de usuarios, normas y procedimientos se extienden a todos los usuarios y procesos del sistema, incluidos los proveedores de servicios, vendedores y socios de negocios.	Por política interna de la empresa COCASINCLAIR EP, por medio del correo electrónico se hacen conocer las normas y procedimientos al personal. Para el caso particular de usuarios y procesos del sistema, no se pudo comprobar si se incluyen a proveedores de servicios, vendedores y socios de negocios.
OBSERVACIÓN	
Falta documentar los procedimientos referentes al control de acceso a los sistemas, estos no están clasificados por importancia o riesgo. Están implementados algunos controles que son propios de la aplicación.	

NOMBRE DEL CONTROL	**5. PRUEBAS, VIGILANCIA Y MONITOREO DE LA SEGURIDAD**
REFERENCIA DE COBIT	Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.

EVALUACIÓN (EVIDENCIAS)	
Preguntar y confirmar si es que existe un inventario de todos los dispositivos de red, servicios y aplicaciones y que cada componente se le ha asignado una calificación de riesgo de seguridad	Si existe un inventario de todos los dispositivos de red, servicios y aplicaciones, falta por asignar la calificación de riesgo de seguridad. La Coordinación de TIC'S, tiene en archivo digital el diagrama de la red entre Quito y el Campamento San Rafael, se ubican los servidor con sus servicios o sistemas implementados y los equipos de red.
Determinar si existe una línea base de seguridad para todo lo utilizado por TI en la organización.	No se evidenció una línea base se seguridad dentro de la Coordinación de TIC'S, no hay un documento que demuestre este requerimiento.
Determinar si en todas las áreas críticas de la organización, los activos de mayor riesgo de la red están bajo vigilancia constante para eventos de seguridad.	Todos los activos de mayor riesgo de la red están bajo vigilancia dentro del data center con restricciones de acceso por medio de códigos, lector biométrico o por llaves de cerradura. Los equipos de red inalámbricos están sobre el cielo falso en lugares que no es de conocimiento del personal de la Empresa. En el campamento San Rafael, los equipos de red están en el data center, este no cuenta con las seguridades de acceso como el data center de Quito.
Determinar si la función de seguridad de la administración de TI ha sido integrada dentro de las iniciativas de la organización en la gestión de proyectos para asegurar que la seguridad está considerada en los requisitos de	La función de seguridad es considerada dentro del desarrollo y pruebas de los sistemas, no se documenta este requisito, sin embargo, antes de salir a producción se realizan pruebas a los sistemas tanto de

desarrollo, construcción y pruebas, para minimizar el riesgo de los sistemas nuevos o existentes, introduciendo vulnerabilidades de seguridad.	seguridad, funcionalidad y accesibilidad. Este fue el caso particular del Gestor Documental en el que se realizaron pruebas piloto y se solicitan en dos puntos del sistema el ingreso del usuario y la clave.
OBSERVACIÓN	
La Coordinación de TIC'S cuenta una infraestructura de red detallado, con vigilancia constante de los equipos de red y tiene incorporado la función de seguridad en los proyectos nuevos.	

NOMBRE DEL CONTROL	**6. DEFINICIÓN DE INCIDENTE DE SEGURIDAD**
REFERENCIA DE COBIT	Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados propiamente y tratados por el proceso de gestión de incidentes y problemas.
EVALUACIÓN (EVIDENCIAS)	
Determinar si existe un Computer Emergency Response Team (CERT) para reconocer y manejar efectivamente las emergencias de seguridad. Las siguientes áreas deben existir como parte de un proceso eficaz CERT: - *Manejo de incidentes* - Procedimientos generales y específicos, y otros requerimientos para asegurar un manejo eficaz de incidentes y problemas de vulnerabilidad - *Las relaciones con el vendedor* - El rol y responsabilidades del vendedor en la	No existe un CERT (Computer Emergency Response Team) en la empresa COCASINCLAIR EP. Las emergencias de seguridad son tratadas en el momento que se presentan por algún técnico de la Coordinación de TIC'S. Los incidentes de soporte técnico actualmente se están registrando en formatos (FO-ADM-tic-401, FO-ADM-tic-451) tanto para Quito como para el Campamento San Rafael, en este se

prevención de incidentes y de seguimiento, corrección de falla de software, y otras áreas. - *Comunicaciones* – Requerimientos, implementación y operación de emergencia y canales de comunicación habituales entre los miembros clave de la administración. - *Legales y temas de investigación criminal* - Cuestiones controladas por consideraciones legales y los requerimientos o limitaciones resultantes de la participación criminal de organismos de investigación durante un incidente - *Agenda de investigación e interacción* - Identificación de las actividades de investigación y requerimientos existentes y la justificación de la investigación necesaria para responder las actividades - *Modelo de la amenaza* - Desarrollo de un modelo básico que caracteriza a las amenazas y los riesgos potenciales para ayudar a enfocar las actividades que reducirán los riesgos y el progreso en esas actividades. - *Problemas Externos* - Factores que están fuera del control directo de la empresa (por ejemplo, la legislación, las políticas, los requerimientos de procedimiento), pero que podrían afectar al funcionamiento y eficacia de las	detallan los trabajos realizados para cada incidente. Para el caso particular de los incidentes con las impresoras, se registran en hojas de soporte del proveedor referente al servicio realizado, repuestos o insumos y recomendaciones. Referente a la comunicación de emergencias, estos se lo hace por medio de una llamada telefónica generalmente al jefe del área, indicando el incidente. No han existido emergencias de seguridad en la que hayan intervenido o brindado soporte la Subgerencia Jurídica. El resto de requisitos que debería tener el CERT, no existe en la empresa.

actividades de la empresa.	
Determine si el proceso de administración de incidentes de seguridad es adecuada con funciones claves de la organización, incluyendo la mesa de ayuda, los proveedores de servicios externos y la administración de la red.	El proceso de administración de incidentes se encuentra soportado por los formularios que se elaboraron para el cumplimiento de las normas ISO en la Empresa. Dentro de estos formularios, se pueden intercalar al segundo nivel de soporte (proveedores de servicios externos de impresión o de internet o del enlace de datos). Estos formularios no son específicos para incidentes de seguridad.
Evaluar si el proceso de administración de incidentes de seguridad incluye los siguientes elementos clave: - Detección de eventos - Correlación de eventos y evaluación de amenazas / incidentes - Resolución de la amenaza, o la creación o escalamiento de órdenes de trabajo - Criterios para iniciar el proceso de la organización CERT - Verificación y niveles requeridos de documentación de la resolución - Análisis Post-remediación - Cierre órdenes de trabajo/incidente	No se evidencia que el proceso de administración de incidentes contenga lo solicitado en este aspecto, los formularios que se elaboraron fueron en función de las normas ISO, consecuentemente, no se cuenta con estos elementos clave dentro del proceso de administración de incidentes.
OBSERVACIÓN	
No existe un Computer Emergency Response Team (CERT) en la empresa	

COCASINCLAIR EP, varios ítems que incluye el proceso CERT están implementados, la mayoría no lo están.

NOMBRE DEL CONTROL	**7. PROTECCIÓN DE LA TECNOLOGÍA DE SEGURIDAD**
REFERENCIA DE COBIT	Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria.
EVALUACIÓN (EVIDENCIAS)	
Preguntar y confirmar si es que las políticas y los procedimientos se han establecido para hacer frente a las consecuencias de violación de la seguridad (en particular para hacer frente a los controles para la administración de la configuración, acceso a las aplicaciones, los datos de seguridad y los requerimientos de seguridad física).	No se puede determinar si las políticas y los procedimientos se han establecido para hacer frente a las consecuencias de violación de la seguridad, por cuanto no existen políticas y procedimientos para este fin.
Observar los registros de control permitidos y accesos aprobados, registro de intentos fallidos, cierres, el acceso autorizado a los archivos sensibles y/o datos y acceso físico a las instalaciones	Los registros de acceso físico al data center quedan almacenados en el lector biométrico, sean estos permitidos o fallidos. En los logs del servidor del Active Directory, se almacenan los accesos a carpetas compartidas del sistema. Para la aplicación Flexline, también se guarda en los logs del sistema los accesos y los cambios que se han realizado en el aplicativo.
Preguntar y confirmar si es que las características de diseño de seguridad facilitan reglas de contraseña (por ejemplo, la longitud máxima, caracteres,	Las reglas implementadas para autenticarse con el servidor de controlador de dominio, tiene contemplado longitud mínima,

la caducidad, la reutilización).	introducción de caracteres especiales, caducidad de contraseñas y restricción de reutilización de claves.
Preguntar y confirmar si es que el control requiere revisiones anuales de la administración de las características de seguridad de acceso físico y lógico de archivos y datos.	Las revisiones de control se informa que se realizan de forma anual, sin embargo, no se mostró la evidencia de que esto sea así. En el mes de julio se realizó la última actualización de políticas de seguridad en el directorio activo.
Verifique que acceso está autorizado y aprobado adecuadamente	El acceso que se pudo probar es la autenticación al Active Directory con la política de seguridad y aprobada. Se bloquea el usuario luego de 3 intentos fallidos.
Revise los informes de seguridad generados por las herramientas del sistema de red que impiden los ataques de vulnerabilidad o penetración	Se revisó los reportes que genera el SmartViewTracker del equipo Check Point con respecto a ataques de código malicioso, bloqueo de acceso a sitios restringidos, navegación. Adicionalmente, se revisó los logs de los intentos de penetración a la red interna.
OBSERVACIÓN	
Faltan las políticas y procedimientos para hacer frente a las consecuencias de violación de la seguridad. Se lleva un registro de los controles permitidos, accesos fallidos y no autorizados. Para las estaciones de trabajo, están implementadas la seguridad con reglas de contraseña. No está documentada la revisión de los controles de seguridad de acceso físico y lógico a los datos o archivos.	

NOMBRE DEL CONTROL	8. ADMINISTRACIÓN DE LLAVES CRIPTOGRÁFICAS
REFERENCIA DE COBIT	Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.

EVALUACIÓN (EVIDENCIAS)	
Determinar si existe definida una clave del ciclo de vida en el proceso de administración. El proceso debe incluir: - Tamaños mínimos de clave necesaria para la generación de claves fuertes. - Uso requerido de algoritmos de generación de claves. - Identificación de estándares requeridos para la generación de claves. - Propósito para los cuales las claves se deberían utilizar y restringir. - Admitir uso de períodos o ciclos de vida para las claves. - Aceptar métodos de distribución de claves. - Copia de seguridad de la clave, archivo y destrucción.	En la empresa COCASINCLAIR EP, no se utilizan claves criptográficas, no se tiene políticas y procedimientos implementados para la administración del ciclo de vida de claves.
Evaluar si los controles existentes sobre las claves privadas hacen cumplir la confidencialidad e integridad. Se debe considerar lo siguiente: - Almacenamiento de claves de firma privadas en dispositivos criptográficos	No se utilizan claves privadas, por ende no tienen implementados controles referentes a confidencialidad e integridad.

seguros (por ejemplo, FIPS 140-1, ISO 15782-1, ANSI X9.66) - Las claves privadas no son exportadas de un módulo criptográfico seguro - Las copias de las claves privadas, almacenamiento y recuperación sólo puede ser usado por personal autorizado y con control dual en un entorno físicamente seguro	
Preguntar y confirmar si es que la organización ha puesto en marcha la clasificación de la información y los controles de protección asociados a la información que dan cuenta de la necesidades de la organización para compartir o restringir la información y los impactos organizacionales asociados a esas necesidades.	Para el mes de diciembre de 2012, se clasificará la información con la finalidad de restringir su salida por medios electrónicos. La herramienta a utilizar para este fin es el DLP de McAfee (Data Loss Prevention), las licencias de uso ya tienen adquiridas.
Determinar si los procedimientos están definidos para garantizar que el etiquetado de información y la manipulación se realiza de acuerdo con el esquema de clasificación de la información de la organización.	No se puede evidenciar este requisito hasta que se haya implementado la herramienta antes mencionada (DLP).
OBSERVACIÓN	
No se utilizan claves criptográficas en la Empresa, consecuentemente, no se tiene políticas y procedimientos implementados para la administración de claves criptográficas, de igual manera, no se utilizan claves privadas. No tienen procedimientos definidos para garantizar que el etiquetado de información.	

NOMBRE DEL CONTROL	9. PREVENCIÓN, DETECCIÓN Y CORRECCIÓN DE SOFTWARE MALICIOSO
REFERENCIA DE COBIT	Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correo basura)..
EVALUACIÓN (EVIDENCIAS)	
Preguntar y confirmar si es que una política de prevención de software malicioso está establecida, documentada y comunicada a través de la organización.	Se encuentra implementada una solución de prevención de software malicioso en la empresa, sin embargo, no está documentada una política de prevención, tampoco está comunicada a los funcionarios la política.
Asegúrese que los controles automatizados se han implementado para proporcionar protección contra virus o violaciones y son comunicadas apropiadamente.	La misma solución de seguridad de protección contra virus, tiene los controles automatizados de actualización y ejecución en las estaciones de trabajo. No hay evidencia que se hayan comunicado los controles automatizados.
Preguntar al personal clave si son conscientes de la política de prevención software malicioso y su responsabilidad para asegurar el cumplimiento	Por parte del personal clave, asumen que el software implementado va a prevenir el software malicioso en los equipos de la empresa. La política de prevención no está documentada, no se puede asegurar su cumplimiento.
De una muestra de las estaciones de trabajo de usuario, observe si una herramienta de protección antivirus ha sido instalada e incluye los archivos de definición de virus y la última vez que se han actualizado las definiciones.	En todas las estaciones de trabajo están instaladas una herramienta de antivirus con la última actualización y definición de virus.

Preguntar y confirmar si es que el software de protección es centralmente distribuida (a nivel de versión y parches) usando una configuración centralizada y el proceso de administración de cambios	Se encuentra distribuida la actualización del antivirus, la consola de administración está que Quito y un repositorio está en el Campamento, un solo servidor es el que descarga la actualización y definición de virus desde el Internet.
Revisar el proceso de distribución para determinar la efectividad operativa.	Está implementada una política de distribución 3 veces al día en el lapso de 2 a 3 y media de la tarde.
Preguntar y confirmar si es que la información sobre nuevas amenazas potenciales es regularmente revisado y evaluado y de ser necesario, actualizar manualmente los archivos de definición de virus.	Las nuevas amenazas se reciben por correo electrónico, se analizan y si es del caso se actualiza la definición de virus de forma manual o se espera para que automáticamente sea actualizada.
Revisar el proceso de revisión y evaluación para determinar la efectividad operativa	La revisión lo hacen las tres personas de la Coordinación de TIC'S de Quito, si es del caso se actualiza sin seguir un procedimiento de evaluación.
Preguntar y confirmar si es que el correo electrónico entrante se filtra adecuadamente contra la información no solicitada.	Está implementada una herramienta anti spam en el servidor de correo para filtrar correo electrónico entrante no deseado, se realizó una prueba con resultados satisfactorios.
Revisar el proceso de filtrado para determinar la efectividad operativa o revisar el proceso automatizado establecido para efectos de filtrado.	Se revisó el proceso de filtrado y se hicieron pruebas con la creación de nuevas políticas de filtrado para determinar su efectividad, la prueba fue satisfactoria.

OBSERVACIÓN
Falta documentar la política de prevención de software malicioso y comunicar a la Empresa, está implementada una solución de prevención de software malicioso con resultados satisfactorios.

NOMBRE DEL CONTROL	10. SEGURIDAD DE LA RED
REFERENCIA DE COBIT	Uso de técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.
EVALUACIÓN (EVIDENCIAS)	
Preguntar y confirmar si es que la política de seguridad de la red (por ejemplo, los servicios prestados, el tráfico permitido, tipos de conexiones permitidas) se ha establecido y se mantiene.	La política de seguridad de la red no está documentada, sin embargo, en el firewall de la empresa se encuentra implementado los controles para permitir tráfico, sitios para navegación, prevención de intrusos, acceso a puertos, bloqueo o calendarización de aplicaciones, etc.
Preguntar y confirmar si es que los procedimientos y directrices para la administración de todos los componentes de red crítica (por ejemplo, los routers de core, DMZ, switches VPN) son establecidos y actualizados periódicamente por el personal clave de la administración y los cambios para la documentación son realizados siguiendo un historial del documento.	No están documentados los procedimientos para la administración de los componentes de la red. El firmware de estos equipos son actualizados por un proveedor externo cada, la actualización de la configuración de los componentes de la red lo realiza el personal técnico de la Coordinación de TIC'S.

OBSERVACIÓN
No se tiene documentada la política de seguridad de la red, están implementados los controles en los equipos de red (firewall). La administración de los equipos de red lo hace el personal de la Coordinación de TIC'S, la actualización del firmware lo realiza el proveedor.

NOMBRE DEL CONTROL	11. INTERCAMBIO DE DATOS SENSIBLES
REFERENCIA DE COBIT	Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.

EVALUACIÓN (EVIDENCIAS)	
Preguntar y confirmar si es que las transmisiones de datos fuera de la organización requieren formato encriptado antes de la transmisión.	Únicamente, para la comunicación por medio de la VPN con los usuarios que se encuentran en la Fiscalización la información viaja encriptada. Para la comunicación que viaja por el enlace al campamento San Rafael, esta está segura por el enlace dedicado por el proveedor externo que brinda el servicio.
Preguntar y confirmar si es que los datos corporativos están clasificados según el nivel de exposición y el esquema de clasificación (por ejemplo, confidencial, sensible).	No se encuentran clasificados los datos según el nivel de exposición, para el mes de diciembre de 2012, se realizará una revisión de la información que tiene la empresa para prevenir la fuga de información.
Preguntar y confirmar si es que el procesamiento de los datos delicados se controla a través de los controles de la aplicación que validan la transacción	No se tiene implementado este tipo de control, en el software adquirido que se implementará en el mes de diciembre de 2012, se implementarán controles

antes de la transmisión	en las aplicaciones como por ejemplo el correo electrónico, para que primero se verifique el contenido de la información antes de que esta salga de la empresa.
Revisar que los logs de la aplicación o el procesamiento se detiene para las transacciones no válidas o incompletas.	La herramienta que se implementará para prevención de fuga de información, maneja logs de la información enviada, si concuerda el tag de un archivo con la clasificación de la información como sensible, el software bloquea el envío y presenta un mensaje de violación.
OBSERVACIÓN	
No se encuentra clasificada la información para determinar cuál es sensible o confidencial según el nivel de exposición. No se valida si la información que sale de la Empresa es confidencial antes de que ésta sea transmitida.	

4.5.2 Resultados de la evaluación del proceso

EVIDENCIAS ENCONTRADAS Y EVALUADAS DEL PROCESO: DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS
Se encontraron como evidencia los siguientes documentos: - Formatos FO-ADM-tic-401 y FO-ADM-tic-451para registrar los incidentes - Formularios de soporte (servicio de impresoras) y por tickets de casos (servicios de internet y enlace de datos) - Política de Servicio, Uso y Seguridad de la Administración de Red (PMC-001) - Contrato para la provisión de DLP de McAfee (Data Loss Prevention). - Contrato de la solución TPE (Total Prevention Enterprise) de McAfee para seguridad de punto final (incluye prevención de software malicioso y filtrado de información no deseada. - Estructura orgánica por procesos de la Empresa COCASINCLAIR EP. - Diagrama de la red entre Quito y el Campamento San Rafael.

RESULTADOS DE LA EVALUACIÓN DEL PROCESO:
DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

Como resultado de la evaluación de los objetivos de control del proceso: DS5 Garantizar la Seguridad de los Sistemas, se detalla lo siguiente:

Efecto: Ser sujetos de observación por los Entes de control por no contar por lo menos con políticas de seguridad de TI en la Jefatura. Posibilidad de que las herramientas informáticas que se implementen, no tengan un respaldo documentado y aprobado que reflejen las acciones que se toman con la información que es tratada en los sistemas.
Los usuarios de los sistemas, pueden percibir un trato desigual con la información de su área, al verse afectados por las políticas implementadas en los equipos de red por ejemplo o un servidor y que éstas no fueron comunicadas.

Causa: En la Coordinación de TIC'S se prioriza las implementaciones o soluciones a los incidentes que se presentan y queda en segundo plano la elaboración de la documentación de soporte y en muchos casos, la aprobación de los procedimientos o políticas lo realiza la Gerencia General de la Empresa, lo que se vuelve un trámite interno que demora. Adicionalmente, se desconoce internamente en la Coordinación de TIC'S, el contenido que deben tener los documentos faltantes, sean de políticas o procedimientos de seguridad de la información.

Recomendaciones: Las recomendaciones propuestas para Garantizar la Seguridad de los Sistemas, son:

- Elaborar un documento de Seguridad de la Información, en el que contenga la política de Seguridad de la Información de la Empresa, roles y responsabilidades de seguridad, estándares y procedimientos de TI, alcance y objetivos, gestión de la aceptación del riesgo, política de seguridad de comunicaciones externas, política de Firewall, de seguridad de E-mail, política de seguridad de una estación de trabajo, política de uso de Internet, etc.

- Elaborar un plan general de seguridad de TI, que contenga los requerimientos de negocio, riesgos y cumplimiento, teniendo en consideración la infraestructura de TI (software y hardware).

- Detallar el procedimiento referente al control de acceso a los sistemas, estos deben ser clasificados por importancia o riesgo y aplicarse a todos los usuarios, incluyendo a administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia.

- Documentar las políticas y procedimientos para hacer frente a las consecuencias de violación de la seguridad, llevar un registro de los controles permitidos, accesos fallidos y no autorizados, además, documentar la revisión de los controles de seguridad de acceso físico y lógico a los datos o archivos.

- Documentar la política de prevención de software malicioso y comunicar a toda la Empresa, no basta con implementar una herramienta de prevención de software malicioso sino va acompañado de una política que detalle las medidas preventivas, detectivas y correctivas para la prevención de virus, gusanos, spyware o correo basura.

- Elaborar en un documento referente a la política de seguridad de la red, los controles implementados en los equipos de red tendrán mayor importancia cuando estén respaldados por una política.

- Detallar en un documento el procedimiento para clasificar la información de la Empresa, en este se debe determinar cuál es sensible o confidencial según el nivel de exposición e implementar un control que valide si la información que sale de la Empresa es confidencial antes de que ésta sea transmitida.

4.5.3 Indicadores Clave de Rendimiento (Proceso: DS5 Garantizar la Seguridad de los Sistemas).

	INDICADOR	RESULTADOS
TI	# de incidentes con impacto al negocio (en un mes)	2
	# de sistemas que no cumplen con los requerimientos de seguridad.	0
	Tiempo para otorgar, cambiar o eliminar privilegios de acceso	1 hora

Procesos	# y tipo de violaciones de acceso reales y sospechadas.	3 Navegación a sitios restringidos
	# de violaciones en la segregación de funciones	No Determinado (N/D)
	% de usuarios que no cumplen con los estándares de contraseñas.	0 %
	# y tipo de código malicioso prevenido	500 al mes (Spam)
Actividades	Frecuencia y revisión del tipo de eventos de seguridad a ser monitoreados	Diaria Intrusión, Virus, Spyware
	# y tipo de cuentas obsoletas	5 Usuarios de Dominio
	# de direcciones IP no autorizadas, puertos y tipos de tráfico denegados **(*)**	5 direcciones IP, Puerto 21, 4000 – 5000, otros. FTP, video, otro.
	% de llaves criptográficas comprometidas y revocadas	No utilizan llaves criptográficas
	# de derechos de acceso autorizados, revocados, restaurados o cambiados (un mes).	120 accesos autorizados, 5 accesos revocados, 4 accesos cambiados.

(*) El detalle de esta actividad está configurada dentro del firewall, por seguridad, ésta no fue proporcionada.

4.5.4 Determinación del Nivel de Madurez (Proceso: DS5 Garantizar la Seguridad de los Sistemas).

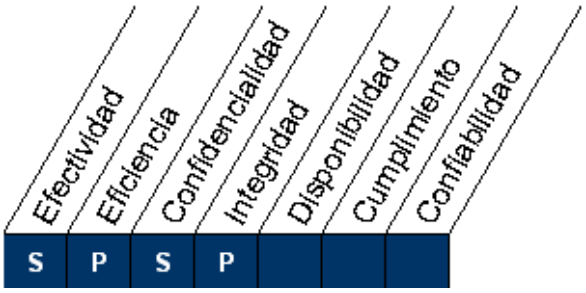
NIVEL DE MADUREZ	0 ○ 1 ○ **2** ● 3 ○ 4 ○ 5 ○
	La administración del proceso de Garantizar la seguridad de los sistemas que satisfaga el requerimiento de negocio de TI de

REFERENCIA DE COBIT	*mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad es:* **2 Repetible pero Intuitivo.-** 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 habilitación sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.
RAZONES	Por los resultados de la evaluación de este proceso, la Coordinación de TIC'S, no tienen ningún tipo de documentación referente a la seguiridad de la infomación ni tampoco un Plan de Seguridad de TI, pero esto no significa que no tenga implentadas políticas de seguridad en los equipos de red, firewall, correo, estaciones de trabajo, servidores, navegación por internet, etc. Los sistemas tienen implementadas las seguridades de acceso, así como la identificación de usuario para acceder al mismo. Incluye software de terceros para brindar seguridad a las estaciones de trabajo. Tiene herramientas de seguridad implantada, sin que se tenga una política de seguridad. Es responsabilidad de la Coordinación de TIC'S brindar la seguridad de la información a la Empresa, la Gerencia General no le ha dado la importancia necesaria a la seguridad de la información.

4.6 Tercer proceso a Auditar: Definir la Arquitectura de la Información

La metodología para la revisión de este proceso se realizará mediante la evaluación al diseño del control.

DOMINIO	PLANEAR Y ORGANIZAR
NOMBRE DEL PROCESO	PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN
REFERENCIA DE COBIT	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.



Criterios o requerimientos de información

(P=Primario, S=Secundario) [11]

Recursos de TI

Áreas de Gobierno de TI

[11] Las referencias primarias (P) y secundarias (S) de los criterios de información para las 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. Algunos procesos tienen mayor impacto en la meta de TI que otros

4.6.1 Objetivos de Control del proceso

<table>
<tr><td>NOMBRE DEL CONTROL</td><td colspan="2">1. MODELO DE ARQUITECTURA DE INFORMACIÓN EMPRESARIAL</td></tr>
<tr><td>REFERENCIA DE COBIT</td><td colspan="2">Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI como se describen en P01. El modelo debe facilitar la creación, uso y el compartir en forma óptima la información por parte del negocio de tal manera que se mantenga su integridad, sea flexible, funcional, rentable, oportuna, segura y tolerante a fallos.</td></tr>
<tr><td colspan="3">EVALUACIÓN (EVIDENCIAS)</td></tr>
<tr><td>Comprobar si existe un modelo de información empresarial, basado en estándares bien aceptados y si conocen adecuadamente los interesados del negocio y los de TI.</td><td colspan="2">De la información recopilada, no se puede comprobar si existe un modelo de información empresarial de COCASINCLAIR EP, la Coordinación de TIC’S no conoce ningún modelo.</td></tr>
<tr><td>Verifique si el modelo es eficazmente usado y se mantienen en paralelo con el proceso que traduce la estrategia de TI en planes tácticos de TI y dentro de los planes tácticos de los proyectos.</td><td colspan="2">La Empresa no cuenta con un modelo de información empresarial, no se puede verificar el requisito del control.</td></tr>
<tr><td>Evaluar si el modelo tiene en cuenta la flexibilidad, funcionalidad, rentabilidad, seguridad, resistencia de falla, cumplimiento, etc.</td><td colspan="2">La Empresa no cuenta con un modelo de información empresarial, no se puede evaluar el modelo.</td></tr>
<tr><td colspan="3">OBSERVACIÓN</td></tr>
<tr><td colspan="3">No existe un modelo de información empresarial de COCASINCLAIR EP, consecuentemente, no se puede comparar con algún modelo similar. La Coordinación de TIC’S no cuenta con un plan estratégico de TI.</td></tr>
</table>

NOMBRE DEL CONTROL	2. DICCIONARIO DE DATOS EMPRESARIAL Y REGLAS DE SINTAXIS DE DATOS	
REFERENCIA DE COBIT	Mantener un diccionario de datos empresarial que incluya las reglas de sintaxis de datos de la organización. El diccionario facilita compartir elementos de datos entre las aplicaciones y los sistemas, fomenta un entendimiento común de datos entre los usuarios de TI y del negocio, y previene la creación de elementos de datos incompatibles.	
EVALUACIÓN (EVIDENCIAS)		
Preguntar y confirmar si es que las directrices de sintaxis de los datos se mantienen.		No se evidencia que exista alguna directriz de sintaxis de los datos. Cada sistema implementado maneja su propio diccionario de datos con estructuras diferentes para cada aplicación y son independientes.
Preguntar y confirmar si es que el diccionario de datos está definido para identificar la redundancia e incompatibilidad de los datos y que el impacto de cualquier modificación o cambio en el diccionario de datos se comunican eficazmente.		La aplicación Flexline, tiene un diccionario de datos que justamente identifica la redundancia e incompatibilidad, este software fue implementado por terceros en la Empresa. No se evidencia si existía un proceso de comunicación cuando había algún cambio en el diccionario.
Revisar varios sistemas y proyectos de desarrollo para verificar que el diccionario de datos se utiliza para definiciones de datos.		El sistema que utiliza un diccionario de datos es Flexline, tanto el Gestor Documental como el sistema de Control de Asistencias no tienen un diccionario de datos.
Preguntar y confirmar si es que los altos directivos están de acuerdo sobre las reglas del proceso de definición de sintaxis de los datos, las reglas de validación de datos y reglas de negocio (por ejemplo, la coherencia, integridad,		El área responsable del tratamiento de la información es la Coordinación de TIC'S. Los altos directivos de acuerdo a la estructura por procesos de la Empresa, no tienen atribuciones para las definiciones de las sintaxis de los

calidad).	datos, sin embargo al ser consultado el Subgerente Administrativo, indicó que están de acuerdo a lo que indique la Coordinación de TIC'S sobre este requisito.
Inspeccionar los planes programados de calidad de datos, políticas y procedimientos y que estén evaluados eficazmente.	La Coordinación de TIC'S no cuenta con planes de calidad de los datos, tampoco con políticas y procedimientos, a medida que se desarrolla un aplicativo se realiza una revisión de la calidad de los datos. No se tiene documentado algún plan de calidad de los datos.
OBSERVACIÓN	
La empresa no cuenta con un diccionario de datos empresarial, es responsabilidad de la Coordinación de TIC'S la definición, sintaxis y reglas de validación de los datos y reglas del negocio. No cuentan con un plan de calidad de datos, políticas y procedimientos.	

NOMBRE DEL CONTROL	**3. ESQUEMA DE CLASIFICACIÓN DE DATOS**
REFERENCIA DE COBIT	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o cifrado.
EVALUACIÓN (EVIDENCIAS)	
Revisar el esquema de clasificación de	La Coordinación de TIC'S no tiene un

datos y verificar que todos los componentes importantes están cubiertos y completos, y que el esquema es razonable en el balance de costo versus riesgo. Esto incluye la propiedad de los datos con los dueños de negocios y la definición de las medidas de seguridad apropiadas relacionadas con los niveles de clasificación.	esquema de clasificación de datos. Para la implementación del DLP (Data Loss Prevention) se indica que se clasificará de acuerdo a los criterios de confidencialidad o pública.
Verificar que las clasificaciones de seguridad han sido discutidas y se confirman con los propietarios del negocio en intervalos regulares.	No se puede verificar este requisito por cuanto no tienen clasificado los datos por el esquema de seguridad.
OBSERVACIÓN	
No se evidencia un esquema de clasificación de datos en la Empresa, no hay un control de la información que sale, podría ser confidencial o no.	

NOMBRE DEL CONTROL	**4. ADMINISTRACIÓN DE INTEGRIDAD**
REFERENCIA DE COBIT	Definir e Implementar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos.
EVALUACIÓN (EVIDENCIAS)	
Preguntar y confirmar si es que los criterios de integridad y consistencia de todos los datos se definen en colaboración con los administradores del negocio.	La integridad de los datos son definen en el momento de la implementación de algún sistema, el administrador de contrato es quien conoce los datos como están almacenados y la integridad en una base de datos viene dada por la misma base de datos.

Preguntar y confirmar si es que los procedimientos están implementados para gestionar y mantener la integridad de los datos y la coherencia en todo el proceso de datos y el ciclo de vida.	No existen procedimientos implementados para mantener y gestionar la integridad de los datos, se asume como una funcionalidad de la base de datos la integridad. En la fase de pruebas de un sistema, se valida la integridad de los datos sin un procedimiento en particular.
Preguntar y confirmar si es que un programa de calidad de datos está implementado para validar y asegurar la integridad de los datos y la coherencia sobre una base regular.	Un programa de calidad de los datos no está implementado en la Empresa. La calidad de los datos se validan cuando se realzan las pruebas en el sistema antes de salir a producción.
OBSERVACIÓN	
La Coordinación de TIC'S, no se tiene implementado un control para asegurar la integridad de los datos. Faltan procedimientos que gestione la integridad de los datos.	

4.6.2 Resultados de la evaluación del proceso

EVIDENCIAS ENCONTRADAS Y EVALUADAS DEL PROCESO: PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN
Se encontraron como evidencia los siguientes documentos: - No se encontró ninguna evidencia documentada.

RESULTADOS DE LA EVALUACIÓN DEL PROCESO:
PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN

Como resultado de la evaluación de los objetivos de control del proceso: PO2 Definir la Arquitectura de la Información, se detalla lo siguiente:

Efecto: No se tiene control de la información que sale de la Empresa por algún medio electrónico sea esta confidencial o no. La integridad de los datos no se validan antes de salir los sistemas a producción, la revisión parcial de la integridad de los datos puede ocasionar desconfianza de los resultados del procesamiento de los sistemas. Ninguna de las aplicaciones se comunican para compartir un solo diccionario de datos.

Causa: Poco conocimiento de la Coordinación de TIC'S de la importancia de tener una arquitectura empresarial de información, clasificación y niveles de seguridad. No se ha reportado formalmente un incidente de fuga de información confidencial o delicada, por lo que no se han tomado acciones y no se han buscado alternativas de protección y estandarización de los datos.

Recomendaciones: Las recomendaciones propuestas para Definir la Arquitectura de la Información, son:

- Promover por parte de la Coordinación de TIC'S, la elaboración de un modelo de información empresarial para la Empresa, partiendo de la planificación estratégica de TI que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones.

- Crear un diccionario de datos empresarial, que permita compartir elementos de datos entre las aplicaciones y los sistemas. Adicionalmente, elaborar un plan o un procedimiento para validar la calidad de los datos antes de salir a producción y que sea de aplicación para todos los sistemas.

- Definir un esquema de clasificación de los datos que permita identificar si es confidencial o pública, crítica o común, de acuerdo a parámetros establecidos conjuntamente por la Gerencia General o los propietarios de esa información.

- Implementar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en las bases de datos y archivos, aprobados por la Subgerencia Administrativa. Las bases de datos pueden ser heterogéneas pero el procedimiento debe ser el mismo.

- Documentar todos los resultados obtenidos cuando se aplique el modelo de información empresarial, esto permitirá poder generar los indicadores necesarios para medir las actividades, procesos y metas de TI.

4.6.3 Indicadores Clave de Rendimiento (Proceso: PO2 Definir la Arquitectura de la Información).

	INDICADOR	RESULTADOS
TI	% de satisfacción de los usuarios respecto al modelo de información (esto es, ¿el modelo de datos es fácil de usar?)	No aplica
	% de elementos de datos redundantes / duplicados	No aplica
Procesos	% de elementos de datos que no son parte del modelo de datos empresarial	No aplica
	% de falta de cumplimiento del esquema de clasificación de datos	No aplica
	% de aplicaciones que no cumplen con la arquitectura de información	No aplica
Actividades	Frecuencia de actualizaciones al modelo empresarial de datos	No aplica
	% de elementos de datos que no tienen Dueño	0 %
	Frecuencia de actividades de validación de datos (durante el desarrollo)	10 %
	Nivel de participación de la comunidad de usuarios	Bajo

No aplica: significa que la Empresa COCASINCLAIR EP, no tiene datos para generar los indicadores de este proceso.

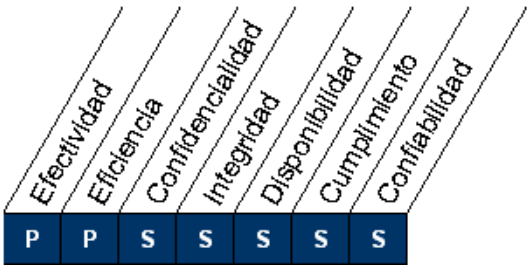
4.6.4 Determinación del Nivel de Madurez (Proceso: PO2 Definir la Arquitectura de la Información).

NIVEL DE MADUREZ	0 ○ 1 ● **2** ○ 3 ○ 4 ○ 5 ○
REFERENCIA DE COBIT	*La administración del proceso de Definir la arquitectura de la información que satisface el requerimiento de negocio de TI de agilizar la respuesta a los requerimientos, para brindar información confiable y consistente y para integrar de forma transparente las aplicaciones hacia los procesos de negocio es:* **1 Inicial / Ad Hoc**.- La gerencia reconoce la necesidad de una arquitectura de información. El desarrollo de algunos componentes de una arquitectura de información ocurre de manera ad hoc. 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.
RAZONES	Por los resultados de la evaluación de este proceso, la Coordinación de TIC'S, no tienen claro un esquema de tratamiento y clasificación de la información, no existe un documento que evidencie alguna clasificación. Solo una aplicación tiene un diccionario de datos. La calidad de los datos es revisada únicamente en la fase de pruebas del el ciclo de vida de una aplicación conjuntamente con el proveedor de la aplicación. Se confía que los datos almacenados en las base de datos son íntegros y consistentes, por el mismo motor de base de datos.

4.7 Cuarto proceso a Auditar: Definir y Administrar los Niveles de Servicio.

La metodología para la revisión de este proceso se realizará mediante la evaluación al diseño del control.

DOMINIO	ENTREGAR Y DAR SOPORTE
NOMBRE DEL PROCESO	DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO.
REFERENCIA DE COBIT	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



Criterios o requerimientos de información

(P=Primario, S=Secundario) [12]

[12] Las referencias primarias (P) y secundarias (S) de los criterios de información para las 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. Algunos procesos tienen mayor impacto en la meta de TI que otros

Recursos de TI

Áreas de Gobierno de TI

4.7.1 Objetivos de Control del proceso

NOMBRE DEL CONTROL	1. MARCO DE TRABAJO DE LA ADMINISTRACIÓN DE LOS NIVELES DE SERVICIO
REFERENCIA DE COBIT	Definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el cliente y el prestador de servicio. El marco de trabajo mantiene una alineación continua con los requerimientos y las prioridades de negocio y facilita el entendimiento común entre el cliente y el(los) prestador(es) de servicio. El marco de trabajo incluye procesos para la creación de requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLAs), acuerdos de niveles de operación (OLAs) y las fuentes de financiamiento. Estos atributos están organizados en un catálogo de servicios. El marco de trabajo define la estructura organizacional para la administración del nivel de servicio, incluyendo los roles, tareas y responsabilidades de los proveedores externos e internos y de los clientes.
EVALUACIÓN (EVIDENCIAS)	
Revisar las políticas y procedimientos del SLA para que se alineen con los	El SLA que se revisó es el firmado con el proveedor para el enlace de datos

objetivos del SLA y las medidas de desempeño con los objetivos de negocio y estrategias de TI.	desde Quito hasta el Campamento San Rafael. El formato del SLA es propuesto por el proveedor, este se enfoca en dar continuidad del servicio entre los dos sitios. La estrategia de TI, *dar comunicación entre los dos sitios*, se cumple por este acuerdo. También disponen de un SLA con el proveedor de Internet.
Preguntar y confirmar si es que existen las políticas para la alineación de los objetivos del SLA y las medidas de desempeño con los objetivos de negocio y las estrategias de TI.	Como políticas para que se alineen con los objetivos del SLA no se tienen enunciadas o documentadas, se trata de cumplir con lo señalado en los SLA's, no se evidencia las medidas de desempeño con los objetivos de negocio.
Revise el catálogo de servicios y verifique que incorpora los requisitos de servicio, definiciones de servicios, SLA's, OLA's y fuentes de financiamiento.	La Coordinación de TIC'S no cuenta con un catálogo de servicios, mediante una consultoría se indica que se levantarían los requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLA's), acuerdos de niveles de operación (OLA's) y las fuentes de financiamiento, tanto entre áreas internas de la Empresa como con proveedores.
Preguntar a los miembros del staff responsables del SLA el avance y resolución para determinar si los procedimientos o métodos establecidos de los niveles de servicios son razonables para responder a los	Como se señaló en el requisito anterior, la Coordinación de TIC'S no cuenta con un catálogo de servicios, no hay miembros del staff que puedan evaluar si los niveles de servicios están bien definidos para responder a los problemas, no existe ninguna

problemas.	designación.
Revisar una muestra de los cambios relevantes y verificar que los cambios fueron aplicados de conformidad con el proceso de gestión del cambio.	No existe un proceso de gestión de cambios definido ni tampoco documentado, cuando se realizan los cambios en un software específico, el mismo proveedor es quien asume que los cambios efectuados no afecten al funcionamiento del software. COCASINCLAIR EP, tiene firmados contratos de soporte técnico con los proveedores.
Revisar el diseño del programa de mejora de los servicios por normas para medir el desempeño.	Como no se tienen definidos el portafolio o catálogo de servicios de la Coordinación de TIC'S, no existe un programa de mejora de estos.
OBSERVACIÓN	
La Coordinación de TIC'S no ha definido el catálogo / portafolio de servicios (requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLA's), acuerdos de niveles de operación (OLA's) y las fuentes de financiamiento) tanto entre áreas internas como con proveedores.	

NOMBRE DEL CONTROL	**2. DEFINICIÓN DE SERVICIOS**
REFERENCIA DE COBIT	Definiciones base de los servicios de TI sobre las características del servicio y los requerimientos de negocio, organizados y almacenados de manera centralizada por medio de la implantación de un enfoque de catálogo/portafolio de servicios.

EVALUACIÓN (EVIDENCIAS)	
Preguntar y confirmar si es que existe un proceso para desarrollo, revisión y ajuste del catálogo o portafolio de servicios.	No existe un proceso para desarrollo, revisión y ajuste de servicios de la Coordinación de TIC'S. No se ha definido el catálogo/portafolio de servicios.
Confirmar la existencia de un proceso de gestión para asegurar que el catálogo o portafolio de servicios está disponible, completo y actualizado.	No se tiene elaborado un proceso de gestión del catálogo de servicios, más aún no se ha definido un catálogo/portafolio de servicios, por lo tanto no se puede verificar que este esté disponible, completo y actualizado.
Revisar el proceso de catálogo o portafolio de servicios para verificar que este está revisado de forma periódica.	El proceso de catálogo o portafolio de servicios no está definido, no se puede verificar si éste se revisa de forma periódica.
OBSERVACIÓN	
No están documentados los servicios que brinda la Coordinación de TIC'S, existe una declaración general de los servicios de esta Coordinación dentro de las Responsabilidades y Atribuciones contenidas en el Estatuto Orgánico Funcional por Procesos de la Empresa. La Coordinación de TIC'S no ha definido el catálogo / portafolio de servicios.	

NOMBRE DEL CONTROL	3. ACUERDOS DE NIVELES DE SERVICIO
REFERENCIA DE COBIT	Definir y acordar convenios de niveles de servicio para todos los procesos críticos de TI con base en los requerimientos del cliente y las capacidades en TI. Esto incluye los compromisos del cliente, los requerimientos de soporte para el servicio, métricas cualitativas y cuantitativas para la medición del servicio firmado por los interesados, en

	caso de aplicar, los arreglos comerciales y de financiamiento, y los roles y responsabilidades, incluyendo la revisión del SLA. Los puntos a considerar son disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, planeación de continuidad, seguridad y restricciones de demanda.
EVALUACIÓN (EVIDENCIAS)	
Preguntar y confirmar si es que las partes interesadas acuerdan, registran y comunican el SLA y que se incluye en el formato y en el contenido del SLA.	Existen dos SLA's firmados con empresas de telecomunicaciones para el enlace dedicado de datos y otro para el internet, cada uno tiene su propio formato y contenido de acuerdo a cada proveedor. Los SLA's tienen formatos diferentes para cada empresa y COCASINCLAIR EP solo puede solicitar se revisen ciertas cláusulas del acuerdo.
Revisar el formato del contenido de los SLA's para verificar que incluya exclusiones, arreglos comerciales y OLA's.	Del SLA revisado, si incluye exclusiones y los arreglos comerciales (por si no se cumple los niveles de servicio). No se detalla los OLA en el SLA revisado.
Revisar el proceso de gestión del SLA para verificar que las medidas de los SLA's (cualitativas y cuantitativas) controlan los objetivos del SLA.	Se efectúo una revisión de la disponibilidad del servicio detallado en el SLA de la empresa que provee el servicio del enlace dedicado de datos y se verificó que era menor a la contratada, razón por lo que se solicitó la respectiva nota de crédito en la factura correspondiente al mes afectado. El proveedor otorgó la nota de crédito.
Revisar los SLA's para su aprobación y	Los SLA's se firman conjuntamente luego de que estos han sido revisados

firmas correspondientes.	por las partes.
Observar y revisar el proceso de revisión del SLA para evaluar si este es adecuado.	La Coordinación de TIC'S, no tiene documentado el proceso de revisión de los SLA's, no se puede determinar si el proceso de revisión es adecuado o no.
Verificar que el proceso para mejoras o ajustes a los SLA's se basa sobre la retroalimentación del desempeño y los cambios en los requerimientos del cliente y del negocio.	No se tiene evidencia que demuestre algún proceso de mejoras o de ajustes a los SLA's. Los SLA's revisados son propuestos por los proveedores y rigen por el tiempo contratado del servicio, no se realizan cambios a los SLA's luego de haberlos firmados. Se firman nuevos SLA's cuando se realizan renovaciones del servicio contratado.
Preguntar a los miembros claves del staff si es que los servicios que están siendo prestados no están documentados en el SLA.	Actualmente, no se tiene ningún SLA elaborado y firmado con las áreas internas de la Empresa, consecuentemente, no se puede verificar si no están documentados los servicios. No hay miembros del staff designados.
OBSERVACIÓN	
La Coordinación de TIC'S tiene firmado dos SLA's con proveedores externos de Empresa, internamente no se ha firmado o acordado ningún SLA referente a los servicios que brinda esta Coordinación con las áreas internas. No están identificados cuáles son los procesos críticos de TI.	

NOMBRE DEL CONTROL	**4. ACUERDOS DE NIVELES DE OPERACIÓN**
REFERENCIA DE COBIT	Asegurar que los acuerdos de niveles de operación expliquen cómo serán entregados técnicamente los servicios para soportar el (los) SLA(s) de manera óptima.

	Los OLAs especifican los procesos técnicos en términos entendibles para el proveedor y pueden soportar diversos SLAs.
EVALUACIÓN (EVIDENCIAS)	
Preguntar y confirmar si es que un proceso se ha definido para desarrollar, administrar, revisar y ajustar los OLA's.	No se tiene un proceso definido para gestionar los OLA's. La Coordinación de TIC'S no tiene definido ningún SLA's interno o externo.
Revisar el SLA(s) y confirmar que el OLA soporta los requerimientos técnicos del respectivo SLA(s).	En el SLA revisado de la empresa de telecomunicaciones que brinda el servicio del internet, no está detallado un OLA, en el SLA se menciona que se va a garantizar el servicio contratado y que el proveedor con su infraestructura instalada proveerá el servicio. De acuerdo al contrato, es responsabilidad del proveedor garantizar el servicio con los requerimientos técnicos solicitados por parte de COCASINCLAIR EP.
Obtener una muestra representativa de OLA's y evaluar si es que los OLA's contienen definiciones operables y óptimas para entrega de servicios.	No se detallan los OLA's en los dos SLA's revisados, COCASINCLAIR EP, espera que se cumpla con lo solicitado al proveedor por medio de un contrato.
OBSERVACIÓN	
Ninguno de los dos SLA's firmados por COCASINCLAIR EP, detalla los OLA's. Se garantiza la disponibilidad del servicio contratado por medio de la infraestructura implementada por el proveedor, no se indica cómo serán entregados técnicamente los servicios para soportar el (los) SLA(s).	

NOMBRE DEL CONTROL	5. MONITOREO Y REPORTE DEL CUMPLIMENTO DE LOS NIVELES DE SERVICIO
REFERENCIA DE COBIT	Monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento de los niveles de servicio deben emitirse en un formato que sea entendible para los interesados. Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas tanto de servicios individuales como de los servicios en conjunto.

EVALUACIÓN (EVIDENCIAS)	
A través de entrevistas con miembros claves del staff, responsables del monitoreo del desempeño del nivel de servicio, determinar los criterios de presentación de informes.	No se puede determinar el cumplimiento de este requisito, no se tienen definidos SLA's internos con otras áreas. No se han designado miembros del staff, responsables de monitoreo de desempeño.
Obtener muestras de reportes de desempeño de los SLA's y verificar la distribución.	Siendo consecuente con lo señalado en el requisito anterior, no se puede revisar los reportes de desempeño de los SLA'S.
Revisar opiniones de pronósticos y tendencias en el desempeño del nivel de servicios.	Este requerimiento es inaplicable, por cuanto no se dispone de servicios documentados.

OBSERVACIÓN
Internamente no se ha firmado o acordado ningún SLA referente a los servicios que brinda la Coordinación de TIC'S. Para los SLA's firmados con proveedores externos, los reportes que se emiten a través del software propio del proveedor, se determinó el incumplimiento de uno de los requerimientos contratados en el SLA. Se solicitó una nota de crédito al proveedor.

NOMBRE DEL CONTROL	6. REVISIÓN DE LOS ACUERDOS DE NIVELES DE SERVICIO Y DE LOS CONTRATOS
REFERENCIA DE COBIT	Revisar regularmente con los proveedores internos y externos los acuerdos de niveles de servicio y los contratos de apoyo, para asegurar que son efectivos, que están actualizados y que se han tomado en cuenta los cambios en requerimientos.
EVALUACIÓN (EVIDENCIAS)	
Revisar los SLA's, comparar el contrato de soporte y determinar la eficacia y vigencia de los cambios.	Los SLA's revisados y que forman parte de los contratos, se mantienen durante el tiempo de vigencia del contrato sin cambios en los niveles de servicio. A medida que son renovados o son contratos nuevos, se pueden modificar los SLA's.
Obtener una vista rápida de los requisitos de documentación del SLA.	Los requisitos de documentación en los SLA's, se refieren a la evidencia en la que muestre los niveles de servicio contratado, no se tiene un formato específico para la documentación pero si los medios (herramientas) para revisar que se cumpla el nivel de servicio.
Revisar los SLA's y los contratos de soporte y confirmar que se alinean con los objetivos de negocio y se evalúa de forma periódica.	De la revisión efectuada, si se alinean los SLA's y los contratos de soporte con los objetivos del negocio. No existe un evaluación formal sobre la alineación, lo que existe es una evaluación mensual de que se cumpla el servicio contrato y con el nivel requerido.

OBSERVACIÓN
No existe un proceso o procedimiento documentado para revisar periódicamente los SLA's firmados, aleatoriamente se revisa el nivel de servicio para verificar si es lo acordado.

4.7.2 Resultados de la evaluación del proceso

EVIDENCIAS ENCONTRADAS Y EVALUADAS DEL PROCESO: DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO
Se encontraron como evidencia los siguientes documentos: - Acuerdos de nivel de servicios SLA de las dos empresas de telecomunicaciones. - Estatuto Orgánico Funcional por Procesos de la Empresa. - Documento en el que se solicita la nota de crédito por incumplimiento del nivel de servicio.

RESULTADOS DE LA EVALUACIÓN DEL PROCESO: DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO
Como resultado de la evaluación de los objetivos de control del proceso DS1 Definir y Administrar los Niveles de Servicio, se detalla lo siguiente: **Efecto**: No poder medir la eficiencia – eficacia de los servicios, contar con incompleto catálogo / portafolio de servicios de la Coordinación y no poder monitorear el cumplimiento de los niveles de servicios. No jerarquizar los servicios críticos y asociarlos a los niveles de servicio que deberían tener para garantizar una continuidad del negocio. **Causa**: Informalidad para documentar y comunicar los servicios que brinda la Coordinación de TIC'S. Se asume que los servicios no se podían medir y se hacía lo necesario con la finalidad de dar el "mejor servicio". **Recomendaciones**: Las recomendaciones propuestas para Definir y Administrar los Niveles de Servicio, son:

- Definir el catálogo / portafolio de servicios (requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLA's), acuerdos de niveles de operación (OLA's) y las fuentes de financiamiento –si es del caso-) tanto entre áreas internas como con proveedores de la Empresa.

- Documentar los servicios que brinda la Coordinación de TIC'S, apegándose a lo señalado en las Responsabilidades y Atribuciones contenidas en el Estatuto Orgánico Funcional por Procesos de la Empresa.

- Definir y acordar convenios de niveles de servicio para todos los procesos críticos de la Coordinación de TIC'S, con base en los requerimientos de los usuarios y las capacidades técnicas en TI, incluyendo los acuerdos de niveles de operación OLA's para soportar el (los) SLA(s) de manera óptima.

- Luego de que se hayan definido los SLA's de la Coordinación de TIC'S, se debería elaborar un procedimiento para realizar un monitoreo (revisión) de los niveles de servicio.

4.7.3 Indicadores Clave de Rendimiento (Proceso: DS1 Definir y Administrar los Niveles de Servicio).

	INDICADOR	RESULTADOS
TI	% de interesados del negocio satisfechos de que los servicios entregados cumplen con los niveles de servicio acordados	98 %
	% de usuarios satisfechos de que los servicios entregados cumplen con los niveles de servicio acordados.	90 %
Procesos	% de servicios entregados que no están en el catálogo.	100 %
	% de servicios que cumplen con los niveles de servicio.	0 %
	% de niveles de servicio que se miden.	100 %

Actividades	Número de reuniones formales de revisión de los SLA's con los responsables de negocio por año.	2
	% de niveles de servicio reportados. (*)	100 %
	% de niveles de servicio reportados de forma automatizada. (*)	100 %
	Número de días de trabajo transcurridos para ajustar un nivel de servicio después del acuerdo con el cliente.	2

(*) Por medio del uso de una herramienta de monitoreo para el enlace de datos y del internet.

4.7.4 Determinación del Nivel de Madurez (Proceso: DS1 Definir y Administrar los Niveles de Servicio).

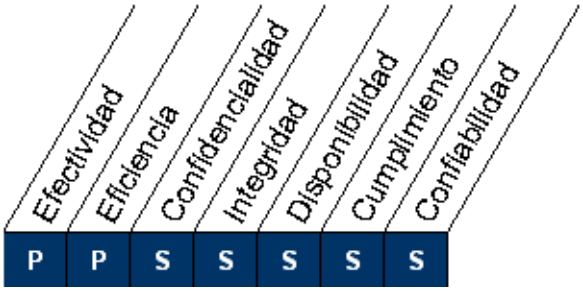
NIVEL DE MADUREZ	0 ○ 1 ○ **2** ● 3 ○ 4 ○ 5 ○
REFERENCIA DE COBIT	*La administración del proceso de Definir y administrar niveles de servicio que satisfacen el requerimiento de negocio para TI de asegurar la alineación de servicios claves de TI con la estrategia de negocio es:* **2. Repetible pero Intuitivo.-** 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. Si existe un proceso para el cumplimiento de los acuerdos de niveles de servicio es voluntario y no está implementado.
RAZONES	Por los resultados de la evaluación de este proceso, la Coordinación de TIC'S, no tienen definido un catálogo / portafolio de servicios. Los SLA's analizados corresponden a proveedores de telecomunicaciones que prestan un servicio a COCASINCLAIR EP. Los reportes del nivel de servicio se

	generan es por medio de un software del proveedor. Internamente, la Coordinación de TIC'S tiene niveles de servicio que están acordados pero son informales entre las áreas. Se trata de cumplir los niveles de servicio por medio de registro de incidentes resueltos del servicio soporte técnico. El resto de servicios de la Coordinación no se han descrito formalmente, pero el administrador de ese servicio sí realiza el monitoreo de la disponibilidad, seguridad y accesos a los servicios. El personal de la Coordinación de TIC'S brinda y trata de cumplir un nivel de servicios aunque éste no esté documentado.

4.8 Quinto proceso a Auditar: Administrar los Servicios de Terceros

La metodología para la revisión de este proceso se realizará mediante la evaluación al diseño del control.

DOMINIO	**ENTREGAR Y DAR SOPORTE**
NOMBRE DEL PROCESO	**DS2 ADMINISTRAR LOS SERVICIOS DE TERCEROS.**
REFERENCIA DE COBIT	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.



Criterios o requerimientos de información

(P=Primario, S=Secundario) [13]

Recursos de TI

Áreas de Gobierno de TI

4.8.1 Objetivos de Control del proceso

NOMBRE DEL CONTROL	1. IDENTIFICACIÓN DE TODAS LAS RELACIONES CON PROVEEDORES
REFERENCIA DE COBIT	Identificar todos los servicios de los proveedores y categorizarlos de acuerdo al tipo de proveedor, significado y criticidad. Mantener documentación formal de relaciones técnicas y organizacionales que cubren los roles y responsabilidades, metas, entregables esperados y credenciales de los representantes de estos proveedores.

[13] Las referencias primarias (P) y secundarias (S) de los criterios de información para las 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. Algunos procesos tienen mayor impacto en la meta de TI que otros.

EVALUACIÓN (EVIDENCIAS)	
Preguntar y confirmar si es que un registro de relaciones con los proveedores se mantiene.	En la Coordinación de TIC'S, se registran los contratos de los proveedores y los servicios que brindan, sin embargo, no se documentan las relaciones con estos, por medio de hojas de soporte se registran las asistencias técnicas.
Obtener y revisar los criterios de relación con proveedores por razonabilidad e integridad categorizados por tipo de proveedor, importancia y criticidad.	No existe una definición de criterios de relación con proveedores. No están categorizados por ningún aspecto.
Determinar si el esquema de categorización del proveedor está suficientemente detallado para clasificar todas las relaciones con los proveedores basadas en la naturaleza de los servicios contratados.	Ningún esquema de categorización existe en la Coordinación de TICS, no se puede determinar el nivel de detalle para clasificar todas las relaciones con los proveedores.
Verificar si las referencias pasadas sobre la selección / rechazo de proveedores se mantienen y se utilizan.	En la Coordinación de Compras Públicas se guarda la documentación de procesos anteriores para una contratación específica de todas las áreas de la Empresa. Adicionalmente, se dispone de los informes anteriores de los administradores de contrato referentes al cumplimiento del proveedor.
Revisar el registro de relaciones con los proveedores para asegurarse de que está actualizado a la fecha, debidamente clasificados y suficientemente detallado para garantizar que proporciona una base para el control de los proveedores	La Coordinación de TIC'S, no dispone de un registro de relaciones con los proveedores, no se puede determinar el detalle que garantice una base para el control de los proveedores

existentes.	existentes.
Revisar una muestra representativa de los contratos con proveedores, SLAs y otra documentación, para asegurarse de que ellos corresponden con el registro del proveedor.	De la muestra seleccionada, todos los proveedores tienen sus datos registrados por el tipo de servicio detallado en el mismo contrato. No se lleva un registro externo por cada proveedor.
OBSERVACIÓN	
No se dispone de un registro de proveedores por categorías de servicio, importancia o criticidad en la Coordinación de TIC'S. No se evalúa el tipo de relación por proveedor, existe una percepción del servicio que no está documentada, pero esta sirve de referencia para futuras contrataciones.	

NOMBRE DEL CONTROL	**2. GESTIÓN DE RELACIONES CON PROVEEDORES**
REFERENCIA DE COBIT	Formalizar el proceso de gestión de relaciones con proveedores para cada proveedor. Los dueños de las relaciones deben enlazar las cuestiones del cliente y proveedor y asegurar la calidad de las relaciones basadas en la confianza y transparencia. (Ej.: a través de SLAs)
EVALUACIÓN (EVIDENCIAS)	
Revisar la documentación del proveedor de servicios para evidenciar la formalización de roles y responsabilidades y determinar si los roles de gestión de los proveedores han sido documentadas y comunicadas dentro de la organización.	Dentro de cada contrato con proveedores, se detallan las responsabilidades / obligaciones con la Empresa. La documentación de la gestión con los proveedores se evidencia por las actas, informes, manuales, etc., que fueron requeridos como entregables para el contrato. No se realiza una comunicación interna en la empresa, por cuanto depende del objeto de cada contrato y las responsabilidades que tiene el

	administrador del contrato.
Determinar si existen políticas para hacer frente a la necesidad de los contratos formales, definición del contenido de los contratos y la asignación propia o relación de responsabilidades manejadas para asegurar que los contratos son creados, mantenidos, monitoreados y renegociados según sea requerido.	El contenido de los contratos, es revisado siempre por algún miembro de la Coordinación de TIC'S, se definen las responsabilidades del proveedor y se realiza un control de la ejecución del contrato por parte del administrador del mismo. Se tiene definido por parte de la Subgerencia Jurídica el contenido y la forma de los contratos por su tipo u objeto de contratación, la política depende de esta Subgerencia. De acuerdo a la normativa vigente que se aplica a la Empresa, no existe la posibilidad de una renegociación de los términos o condiciones, todo debe estar definido en los documentos precontractuales.
Evaluar si la asignación de los roles para la gestión de proveedores es razonable y basado sobre el nivel y las habilidades técnicas requeridas para gestionar eficazmente la relación.	La definición de roles para el proveedor se realiza en el fase precontractual de cada proceso, en los términos de referencia o servicios que se espera que cumpla el proveedor. La relación se basa en cumplimiento de todo lo solicitado en la fase precontractual y detallado en el contrato.
OBSERVACIÓN	
Las relaciones que se mantienen con los proveedores se detallan en el contrato en la cláusula de responsabilidades y obligaciones de LA CONTRATISTA. Las políticas referentes al contenido y relación con los proveedores son definidas por la Subgerencia Jurídica dentro del contrato.	

NOMBRE DEL CONTROL	3. ADMINISTRACIÓN DE RIESGOS DEL PROVEEDOR
REFERENCIA DE COBIT	Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de entrega de forma segura y eficiente sobre una base de continuidad. Asegurar que los contratos están de acuerdo con los requerimientos legales y regulatorios de los estándares universales del negocio. La administración del riesgo debe considerar además acuerdos de confidencialidad (NDAs), contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos, etc.
EVALUACIÓN (EVIDENCIAS)	
Preguntar si los riesgos asociados con la incapacidad de cumplir con los contratos con los proveedores están definidos.	Para mitigar los riesgos de incumplimiento en los contratos, se le solicita al proveedor garantías financieras (buen uso de anticipo, fiel cumplimiento de contrato) y técnicas, según sea del caso. Se prevé una holgura en el plazo para la ejecución del contrato para evitar ampliaciones de plazo.
Preguntar si los recursos fueron considerados cuando se definió el contrato con el proveedor.	Dependiendo del tipo de contratación, en los Pliegos del proceso, se detallan los requerimientos y los recursos con los que contará el proveedor adjudicado para cumplir con el objeto de contratación.
Examinar la documentación del contrato como evidencia de la revisión.	Toda la documentación de la fase precontractual, forma parte de los contratos, por ejemplo: Pliegos, Ofertas, Actas, etc. Estos documentos

	son revisados por una Comisión Técnica antes de la elaboración del contrato.
Preguntar a los miembros clave del staff si existe un proceso de gestión del riesgo para identificar y monitorear los riesgos con proveedores.	No se tiene definido o documentado un proceso de gestión de riesgo para identificar y monitorear riesgos de proveedores. Mediante la aplicación de la normativa y las responsabilidades detalladas en los contratos, se mitigan los riesgos con los proveedores.
Determinar si existen políticas que requieren independencia dentro del proceso de selección y contratación de proveedores y entre la administración del personal dentro de la organización.	Los distintos procesos de contratación, se realizan de acuerdo a la Ley del Sistema Nacional de Contratación Pública, su Reglamento, Resoluciones del Instituto Nacional de Contratación Pública, Código de Trabajo, Ley Orgánica del Servicio Público, éstas norman los procedimientos de contratación, sean para la parte administrativa de personal o para proveedores, cada una en su ámbito de aplicación.
OBSERVACIÓN	
Dependiendo del tipo de contrato, la Subgerencia Jurídica añade las cláusulas legales y de regulación para que tengan validez el contrato para su ejecución así como el detalle de las garantías (financieras o técnicas, acuerdo de confidencialidad) que debe contener el contrato. La mitigación del riesgo se logra detallando claramente las responsabilidades y obligaciones del proveedor en el contrato, acuerdos y garantías.	

NOMBRE DEL CONTROL	4. MONITOREO DEL DESEMPEÑO DEL PROVEEDOR
REFERENCIA DE COBIT	Establecer un proceso para monitorear la prestación del servicio para asegurar que el proveedor está cumpliendo con los requerimientos del negocio actuales y que se adhiere continuamente a los acuerdos del contrato y a SLAs, y que el desempeño es competitivo con proveedores alternativos y las condiciones del mercado.
EVALUACIÓN (EVIDENCIAS)	
Seleccionar una muestra de facturas de proveedores, determinar si se identifican las tarifas por los servicios contratados, como se especifican dentro del contrato de servicios y evaluar la razonabilidad de las tarifas en comparación con el desempeño interno, externo y de la industria.	En la fase precontractual de cada proceso, se detallan los requerimientos y se especifican dependiendo del caso los valores o presupuestos referenciales para el contrato. Es responsabilidad del Administrador de contrato que se cumplan con las características técnicas solicitadas y con las tarifas establecidas. Existe un análisis previo al proceso de contratación, para determinar los valores referenciales a través de cotizaciones de dos o tres proveedores.
Revisar una muestra de reportes de los servicios de proveedores para determinar si el proveedor informa periódicamente sobre los criterios de desempeño acordados y si los reportes de desempeño son objetivos, medibles y se alinean con SLA definido y el contrato del proveedor.	Los reportes que emite el software para el caso específico del enlace dedicado de datos entre las oficinas de Quito y el Campamento San Rafael, son revisados periódicamente por parte del Administrador de contrato. En estos reportes se verifican que cumplan con lo establecido en los requerimientos del contrato y en el SLA. Para el contrato de soporte técnico para impresoras, por ejemplo, se lleva un control del tiempo de respuesta para atender el servicio por medio de formularios de soporte.

OBSERVACIÓN
No se tiene definido un proceso de monitoreo de cumplimiento de la prestación del servicio por parte del proveedor, el control lo realiza el administrador del contrato de acuerdo lo estipulado en el mismo, tanto para los requerimientos técnicos como en las tarifas de los servicios o bienes.

4.8.2 Resultados de la evaluación del proceso

EVIDENCIAS ENCONTRADAS Y EVALUADAS DEL PROCESO: DS2 ADMINISTRAR LOS SERVICIOS DE TERCEROS
Se encontraron como evidencia los siguientes documentos: - Contratos firmados en al año 2012 de la Coordinación de TIC'S - SLA's acordados con las dos empresas de Telecomunicaciones. - Reportes emitidos por el software de monitoreo del enlace de datos y de internet.

RESULTADOS DE LA EVALUACIÓN DEL PROCESO: DS2 ADMINISTRAR LOS SERVICIOS DE TERCEROS
Como resultado de la evaluación de los objetivos de control del proceso DS2 Administrar los Servicios de Terceros, se detalla lo siguiente: **Efecto**: No se conoce claramente cómo queda la relación entre la Empresa y el proveedor luego que finaliza el contrato, no contribuye a una mejor objetividad al momento de seleccionar al proveedor. Se puede contratar nuevamente con un proveedor cuya relación con la Empresa fue deficiente. **Causa**: No se ha identificado la necesidad de contar con un registro de evaluaciones a los proveedores. Se hace cumplir lo señalado en el contrato por parte del Administrador en lo referente al objeto de contratación, obligaciones y responsabilidades del proveedor.

Recomendaciones: Las recomendaciones propuestas para Administrar los Servicios de Terceros, son:

- Llevar un registro de proveedores por categorías de servicio, importancia o criticidad en la Coordinación de TIC'S, que permita evaluar la relación con el proveedor y documentarla para una posterior selección / rechazo.

- Definir un proceso de monitoreo sobre el cumplimiento de la prestación del servicio por parte del proveedor, que apoye a las funciones que realiza el administrador del contrato.

4.8.3 Indicadores Clave de Rendimiento (Proceso: DS2 Administrar los Servicios de Terceros).

	INDICADOR	RESULTADOS
TI	# de quejas de los usuarios debidas a los servicios contratados.	45
	% del gasto dedicado a aprovisionamiento competitivo	15 %
Procesos	% de los principales proveedores que cumplen claramente los requerimientos definidos y los niveles de servicio	95 %
	# de controversias formales con el proveedor	0
	% de facturas del proveedor en controversia	0
Actividades	% de los principales proveedores sujetos a una clara definición de requerimientos y niveles de servicio.	0 %
	% de los principales proveedores sujetos a monitoreo	100 %
	Nivel de satisfacción del negocio con comunicación efectiva por parte del proveedor.	Alto
	Nivel de satisfacción del proveedor con comunicación efectiva por parte del negocio	No se tiene el dato
	# de incidentes significativos por incumplimiento del proveedor en un periodo de tiempo	0

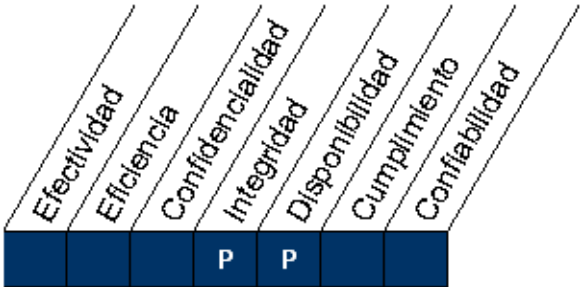
4.8.4 Determinación del Nivel de Madurez (Proceso: DS2 Administrar los Servicios de Terceros).

NIVEL DE MADUREZ	0 ○ 1 ○ **2** ○ 3 ● 4 ○ 5 ○
REFERENCIA DE COBIT	*La administración del proceso de Administrar los servicios de terceros que satisfagan los requerimientos de TI del negocio de brindar servicios de terceros satisfactorios siendo transparentes respecto a los beneficios, costos y riesgos es:* **3. Definido**.- 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. Los términos contractuales se basan en formatos estandarizados. El riesgo del negocio asociado con los servicios del tercero está valorado y reportado.
RAZONES	Por los resultados de la evaluación de este proceso, la Coordinación de TIC'S, dispone de contratos que se detallan las obligaciones y responsabilidades de los proveedores. Existen dos contratos que se anexan SLA's que apoyan al cumplimiento del objeto de contratación. Todos los acuerdos con proveedores se realiza por medio de un documento, sea este un contrato o una orden de servicio, debidamente firmada por las partes. Para el caso de un contrato, este incluye las cláusulas legales, regulatorias, administrativas y de garantías (financieras o técnicas) que minimizan el riesgo de incumplimiento del objeto de contratación por parte del proveedor, adicionalmente, la responsabilidad de la ejecución del contrato es por parte del Administrador, quien es designado por la Gerencia General de COCASINCLAIR EP.

4.9 Sexto proceso a Auditar: Administración del Ambiente Físico

La metodología para la revisión de este proceso, se realizará mediante la evaluación a las salidas del control.

DOMINIO	ENTREGAR Y DAR SOPORTE
NOMBRE DEL PROCESO	DS12 ADMINISTRACIÓN DEL AMBIENTE FÍSICO.
REFERENCIA DE COBIT	La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.



Criterios o requerimientos de información

(P=Primario, S=Secundario) [14]

[14] Las referencias primarias (P) y secundarias (S) de los criterios de información para las 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. Algunos procesos tienen mayor impacto en la meta de TI que otros.

Recursos de TI

Áreas de Gobierno de TI

4.9.1 Objetivos de Control del proceso

NOMBRE DEL CONTROL	**1. SELECCIÓN Y DISEÑO DEL CENTRO DE DATOS**
REFERENCIA DE COBIT	Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.
NOMBRE DEL CONTROL	**2. MEDIDAS DE SEGURIDAD FÍSICA**
REFERENCIA DE COBIT	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las

	responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física
NOMBRE DEL CONTROL	**3. ACCESO FÍSICO**
REFERENCIA DE COBIT	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.
NOMBRE DEL CONTROL	**4. PROTECCIÓN CONTRA FACTORES AMBIENTALES**
REFERENCIA DE COBIT	Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente
NOMBRE DEL CONTROL	**5. ADMINISTRACIÓN DE INSTALACIONES FÍSICAS**
REFERENCIA DE COBIT	Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud
EVALUACIÓN (EVIDENCIAS)	
Revisar el informe de análisis de riesgos para verificar que el informe ha sido actualizado durante el último año.	Como se señaló en la revisión del proceso *PO09 Evaluar y Administrar los Riesgos de TI*, la Coordinación de TIC'S no ha realizado un análisis de riesgos y no tiene definido y documentado los procedimientos para la evaluación de riesgos generales o específicos de TI. No se puede revisar

	el informe de análisis de riesgos.
Revisar las políticas para verificar que las regulaciones nuevas / actualizadas y leyes están reflejadas en las políticas.	En la Coordinación de TIC'S no se ha documentado ninguna política, las políticas de seguridad implementadas en los equipos, tratan de no violar los derechos de los usuarios, como por ejemplo: el acceso a internet, intercambio de información segura, acceso a la información que sea pública, entre otras.
Caminar a través de las áreas para asegurarse de que son seguras de acuerdo con los procedimientos.	Las puertas para el acceso a las áreas en el día permanecen abiertas, en la noche están con llave. Las oficinas se encuentran ubicadas en los pisos 11 y 12 con un guardia de piso. Para el ingreso al Data Center se controla por medio de una llave y lector biométrico. No existe un procedimiento documentado a lo anteriormente señalado.
Revise los registros de seguridad para confirmar los controles de seguridad mínimos.	En el lector biométrico para el acceso al Data Center, se registran los ingresos exitosos así como los intentos fallidos, el usuario, fecha y hora. En la Empresa, no se tienen otros controles de seguridad física a las instalaciones.
Revisar los registros para verificar que se incluye, como mínimo, el nombre del visitante, la empresa, el propósito, el nombre del miembro del grupo de operaciones de TI que autoriza la visita, la fecha y las horas de entrada y la	Este requerimiento, es registrado en el libro de vistas por el personal de la empresa de seguridad, todos los campos son llenados y se lleva un control diario.

salida.	
Seleccionar una muestra de personal con credenciales (tarjetas) y verificar su autorización.	Todos los miembros de la empresa tienen su credencial que le identifica como tal. En el Campamento San Rafael, los funcionarios utilizan diariamente el uniforme con el nombre visible de la Empresa.
Verificar si los gabinetes de cableado están cerradas y tienen acceso restringido	Todos los gabinetes de cableado se encuentran dentro del Data Center. El acceso a esta área es restringida y solo puede ingresar el personal de TIC'S.
Verificar que la documentación para el cableado y los conductos está disponible para referencia.	Toda la documentación del cableado está en la Coordinación de TIC'S, se dispone de diagramas de los puntos de datos, voz y eléctricos de las oficinas en Quito. Por alguna eventualidad de mal funcionamiento de los puntos, se realiza en seguimiento por medio de la documentación del cableado.
Caminar a través de las instalaciones y comparar los resultados con las normas de salud y seguridad.	La empresa COCASINCLAIR EP, como se encuentra en proceso de certificación en las normas ISO 9000, ISO 14000 e ISO 18000, tiene implementados normas de seguridad y salud, principalmente en el Campamento San Rafael.
Entrevistar al personal para evaluar su conocimiento de las directrices.	No todo el personal conoce las reglas o directrices de seguridad, se ha impartido a al personal el Reglamento Interno de Seguridad y Salud en el Trabajo 2012, sin embargo, no ha sido evaluado en el personal de la Empresa su conocimiento.

Pasos para documentar el impacto de las debilidades del control:	
Verifique que las consideraciones especiales están tomadas en cuenta (por ejemplo, la posición geográfica, vecinos, infraestructura). Otros riesgos que hay que considerar son el robo, la temperatura, el fuego, el humo, el agua, la vibración, el terrorismo, el vandalismo, los productos químicos y explosivos.	Para el caso específico del Data Center, se tiene implementado controles de seguridad para temperatura y fuego. Para minimizar los riesgos por robo, todos los equipos informáticos de la Empresa se encuentran asegurados. El acceso a las oficinas, es controlado por medio de la verificación de que si se encuentra la persona a la que van a visitar para permitirle subir al piso 11 al visitante. No se puede verificar si existen controles para minimizar riesgos por terrorismo, vandalismo, productos químicos y explosivos.
Preguntar y confirmar si es que existe un proceso que examina las instalaciones necesarias de TI, para la protección contra las condiciones ambientales y las fluctuaciones de energía y cortes, en conjunción con otros procedimientos de planes de continuidad del negocio.	Como las oficinas de la Empresa son nuevas, el Data Center fue implementado siguiendo estándares internacionales actuales tanto para el cableado como para los equipos de control de acceso, detectores de humo, temperatura, señalética de evacuación, unidades de respaldo de energía para toda la oficina, entre otras. La empresa COCASINCLAIR EP, no dispone de un Plan de Continuidad de Negocio definido y documentado.
OBSERVACIÓN	
No se ha realizado un análisis de riesgos de la infraestructura, incendios, accesos al Data Center, temperatura, entre otros. Los controles implementados para minimizar los impactos en el ambiente físico, se han realizado como una política de buenas prácticas y no por un análisis de vulnerabilidades o requerimientos. No existe documentación donde se enuncien las políticas.	

No se ha elaborado un Plan de Continuidad del Negocio que involucre el aspecto del ambiente físico de la Empresa.

4.9.2 Resultados de la evaluación del proceso

EVIDENCIAS ENCONTRADAS Y EVALUADAS DEL PROCESO: DS12 ADMINISTRACIÓN DEL AMBIENTE FÍSICO
Se encontraron como evidencia los siguientes documentos: - Reglamento Interno de Seguridad y Salud en el Trabajo 2012 - Diagramas de los puntos de datos, voz y eléctricos - Reportes de registros de acceso al Data Center - Documento ejecutivo del contenido de las normas ISO 9000, ISO 14000 e ISO 18000 - Libro diario del control de visitas a la Empresa. - Manuales técnicos del aire acondicionado, extintor de incendios, alarmas, panel de control del fuego, entre otros.

RESULTADOS DE LA EVALUACIÓN DEL PROCESO: DS12 ADMINISTRACIÓN DEL AMBIENTE FÍSICO
Como resultado de la evaluación de los objetivos de control del proceso DS12 Administración del Ambiente Físico, se detalla lo siguiente: **Efecto**: Los controles implementados a través de equipos (sensores) al ambiente físico del Data Center, pueden no ser tan eficaces al el momento que ocurra un incidente, no se evidencia que se haya realizado una prueba de eficacia. **Causa**: El diseño e implementación de los controles del ambiente físico en el Data Center específicamente, se lo realizó por medio de las mejores prácticas y estándares de cableado. Se siguió lo recomendado por el proveedor, se asume que lo sugerido por el proveedor es suficiente. **Recomendaciones**: Las recomendaciones propuestas para la Administración del Ambiente Físico, son: • Elaborar un análisis de riesgos de la infraestructura de TI, incendios, accesos,

temperatura, entre otros, que permita dimensionar la eficacia de los controles implementados en el Data Center.

4.9.3 Indicadores Clave de Rendimiento (Proceso: DS12 Administración del Ambiente Físico).

	INDICADOR	RESULTADOS
TI	Tiempo sin servicio ocasionado por incidentes del ambiente físico	2 horas
	# de lesiones causadas por el ambiente físico.	0
	Riesgos de seguridad causados por incidentes de seguridad física	Acceso a servidores, equipos de comunicación, cableado de red
Procesos	# de incidentes causados por fallas o violaciones a la seguridad física	0
	# de incidentes causados por acceso no autorizado a las instalaciones de cómputo	0
Actividades	Frecuencia de habilitación del personal respecto a medidas de protección, de seguridad y de instalaciones	1 vez al año
	% de personal habilitado en medidas de protección, seguridad y de instalaciones	70 %
	# de pruebas de mitigación de riesgos realizadas en el último año	0
	Frecuencia de las revisiones y evaluaciones de riesgo físico	0

4.9.4 Determinación del Nivel de Madurez (Proceso: DS12 Administración del Ambiente Físico).

NIVEL DE MADUREZ	0 ○ 1 ○ **2** ● 3 ○ 4 ○ 5 ○
REFERENCIA DE COBIT	*La administración del proceso de Administrar el ambiente físico que satisface el requerimiento del negocio de TI de proteger los activos de TI y la información del negocio y minimizar el riesgo de interrupciones en el negocio es:* **2. Repetible pero Intuitivo.-** Los controles ambientales se implementan y monitorean por parte del personal de operaciones. 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
RAZONES	Por los resultados de la evaluación de este proceso, la Coordinación de TIC'S, tiene implementados controles del ambiente físico en el Data Center, tales como: temperatura, acceso, incendios. Estos controles fueron implementados siguiendo las mejores prácticas y estándares de cableado y de seguridad para Centros de Cómputo. Los sensores de los equipos se encuentran conectados en red a una consola de administración centralizada que es administrada por el personal de TIC'S. El mantenimiento que se realiza al aire a condicionado es registrado como soporte técnico, no se sigue un procedimiento para realizar mantenimientos a las instalaciones. No es responsabilidad de la Gerencia General de la Empresa que se cumplan los objetivos de seguridad de tecnología, la Coordinación de TIC'S tiene esa misión.

CAPITULO 5

PRESENTACION DE RESULTADOS

5.1 Informe detallado de la Auditoria

5.1.1 Resultados del proceso: PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI

DOMINIO	PLANEAR Y ORGANIZAR
NOMBRE DEL PROCESO	PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI
REFERENCIA DE COBIT	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.

5.1.1.1 Observaciones del proceso

a. La empresa COCASINCLAIR EP y la Coordinación de TIC'S, no cuenta con un marco de trabajo para una administración de riesgos.

b. No se hizo un seguimiento a las políticas enunciadas en el documento borrador, Política de Servicio, Uso y Seguridad de la Administración de Red (PMC-001). No se realizó la identificación de los riesgos y de las acciones necesarias (tratamiento, impacto, recursos, etc.) que se deberían realizar para mitigar los riesgos.

c. No se ha elaborado un plan de gestión de riesgos por proyectos, sistema o servicios que brinda la Coordinación de TIC'S. No se tiene registros de la relevancia de los riesgos, estos son tratados a medida que ocurren como un incidente y no se documentan.

d. No se han conformado equipos multifuncionales para identificar eventos e impactos en la Empresa COCASINCLAIR EP, lo que genera que no se puede evaluar la probabilidad e impacto con métodos cualitativos o cuantitativos.

e. No se evidencia la identificación de riesgos inherentes y residuales categorizados por servicio, infraestructura, almacenamiento, disponibilidad de los sistemas, etc.,

f. La falta de un proceso de administración de riesgos de TI (matriz de riesgos), no permite identificar las acciones o estrategias que se deben realizar por cada riesgo identificado.

5.1.1.2 Resultados del proceso

PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI

Como resultado de la evaluación de los objetivos de control del proceso PO9 Evaluar y administrar los Riesgos de TI, se detalla lo siguiente:

Efecto: El no contar con un proceso claro de administración de riesgos, apegados a un marco de trabajo de la empresa, no permite evaluar los riesgos, mitigar o gestionarlos y comunicar los riesgos residuales. No se pueden identificar los riesgos, consecuentemente, no se puede elaborar planes de acción para posteriormente monitorearlos. En la mayoría de los casos, no se documenta cuando ocurren los incidentes, se toman acciones puntuales para gestionarlos.

Causa: Existe falta de gestión interna para darle continuidad a la Política de Servicio, Uso y Seguridad de la Administración de Red, en este documento ya se enunció que se elaboraría la gestión de riesgos de TI. No se le da la importancia necesaria a la administración de riesgos en la Coordinación de TIC'S.

Recomendaciones: Las recomendaciones propuestas para Evaluar y Administrar los Riesgos de TI, son:

- Definir una política por parte de la Coordinación de TIC'S, para establecer un marco de trabajo para la administración de riesgos de TI, que permita identificar eventos y gestionar los riesgos.
- Documentar todos los incidentes de TI y asociar a los riesgos de acuerdo a su nivel o importancia, es decir, riesgos críticos, inherentes o residuales; esto con la finalidad de generar indicadores de medición y monitoreo del plan de acción de riesgos.
- Implementar procedimientos para la evaluación de riesgos generales o específicos de TI y documentarlos para que sean presentados a la Subgerencia Administrativa y posteriormente sean aprobados por la Gerencia General de COCASINCLAIR EP. Elaborar planes de acción de riesgos para gestionarlos.

- Reasignar o añadir como un producto o servicio de la Coordinación de TIC'S, la elaboración de la matriz de riesgos de TI y los planes de acción para gestionar los mismos. Comunicar estos riesgos a la Gerencia General y su impacto potencial sobre los procesos y metas de negocio.

5.1.1.3 Determinación del nivel de madurez

NIVEL DE MADUREZ	0 ○ 1 ● **2** ○ 3 ○ 4 ○ 5 ○
REFERENCIA DE COBIT	*La administración del proceso de Evaluar y Administrar los Riesgos de TI que satisfaga el requerimiento de negocio de TI de analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y las metas de negocio es:* **1 Inicial / Ad Hoc:** 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. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.

5.1.2 Resultados del proceso: DS05 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

DOMINIO	ENTREGAR Y DAR SOPORTE
NOMBRE DEL PROCESO	DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS
REFERENCIA DE COBIT	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.

5.1.2.1 Observaciones del proceso

a) La empresa COCASINCLAIR EP, no cuenta con un comité directivo de seguridad. Igualmente no dispone de un documento de seguridad de la información, consecuentemente no se puede determinar su estructura, contenido, roles, etc.

b) Falta documentar las políticas de seguridad en forma detallada, las políticas se encuentran implementadas en los equipos de seguridad y en las estaciones de trabajo, el control es inconstante. Los reportes de seguridad son elaborados bajo demanda y no se hace seguimiento a la situación de la seguridad de la información de TI.

c) COCASINCLAIR EP, no cuenta con un plan general de seguridad de TI, lo que causa que no se pueda contar con el documento de seguridad de la información alineado a las plataformas principales.

d) Falta documentar los procedimientos referentes al control de acceso a los sistemas, estos no están clasificados por importancia o riesgo. Están implementados algunos controles que son propios de la aplicación.

e) Faltan las políticas y procedimientos para hacer frente a las consecuencias de violación a la seguridad de los sistemas. Se lleva un registro de los controles permitidos, accesos fallidos y no autorizados. Para las estaciones de trabajo, están implementadas la seguridad con reglas de contraseña. No está documentada la revisión de los controles de seguridad de acceso físico y lógico a los datos o archivos.

f) No está documentada y comunicada la política de prevención de software malicioso. Está implementada una solución de prevención de software malicioso con resultados satisfactorios.

g) No se tiene documentada la política de seguridad de la red, están implementados los controles en los equipos de red (firewall). La administración de los equipos de red lo hace el personal de la Coordinación de TIC'S, la actualización del firmware de los equipos lo realiza el proveedor.

h) No se encuentra clasificada la información para determinar cuál es sensible o confidencial según el nivel de exposición. No se valida si la información que sale de la Empresa es confidencial antes de que ésta sea transmitida.

5.1.2.2 Resultados del proceso

DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS
Como resultado de la evaluación de los objetivos de control del proceso DS5 Garantizar la Seguridad de los Sistemas, se detalla lo siguiente: **Efecto**: Ser sujetos de observación por los Entes de control por no contar por lo menos con las políticas de seguridad de TI en la Coordinación. Además la posibilidad de que las herramientas informáticas que se implementen, no tengan un respaldo documentado y aprobado que reflejen las acciones que se toman con la información que es tratada en los sistemas. Los usuarios de los sistemas, pueden percibir un trato desigual con la información de su área, al verse afectados por las políticas implementadas en los equipos de red o un servidor y que éstas no fueron comunicadas. **Causa**: En la Coordinación de TIC'S se prioriza las implementaciones o soluciones a los incidentes que se presentan y queda en segundo plano la elaboración de la documentación de soporte y en muchos casos, la aprobación de los procedimientos o políticas lo realiza la Gerencia General de la Empresa, lo que se vuelve un trámite interno que demora. Adicionalmente, se desconoce internamente en la Coordinación de TIC'S, el contenido que deben tener los documentos faltantes, sean de políticas o procedimientos de seguridad de la información. **Recomendaciones**: Las recomendaciones propuestas para Garantizar la Seguridad de los Sistemas, son:

- Elaborar un documento de Seguridad de la Información, en el que contenga la política de Seguridad de la Información de la Empresa, roles y responsabilidades de seguridad, estándares y procedimientos de TI, alcance y objetivos, gestión de la aceptación del riesgo, política de seguridad de comunicaciones externas, política de Firewall, de seguridad de E-mail, política de seguridad de una estación de trabajo, política de uso de Internet, etc.

- Elaborar un plan general de seguridad de TI, que contenga los requerimientos de negocio, riesgos y cumplimiento, teniendo en consideración la infraestructura de TI (software y hardware).

- Detallar el procedimiento referente al control de acceso a los sistemas, estos deben ser clasificados por importancia o riesgo y aplicarse a todos los usuarios, incluyendo a administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia.

- Documentar las políticas y procedimientos para hacer frente a las consecuencias de violación de la seguridad, llevar un registro de los controles permitidos, accesos fallidos y no autorizados, además, documentar la revisión de los controles de seguridad de acceso físico y lógico a los datos o archivos.

- Documentar la política de prevención de software malicioso y comunicar a toda la Empresa, no basta con implementar una herramienta de prevención de software malicioso sino va acompañado de una política que detalle las medidas preventivas y correctivas para la prevención de virus, gusanos, spyware o correo basura.

- Elaborar en un documento referente a la política de seguridad de la red; los controles implementados en los equipos de red tendrán mayor importancia cuando estén respaldados por una política.

- Detallar en un documento el procedimiento para clasificar la información de la Empresa, en este se debe determinar cuál es sensible o confidencial según el nivel de exposición e implementar un control que valide si la información que sale de la Empresa es confidencial antes de que ésta sea transmitida.

5.1.2.3 Determinación del nivel de madurez

NIVEL DE MADUREZ	0 ○ 1 ○ **2** ● 3 ○ 4 ○ 5 ○
REFERENCIA DE COBIT	*La administración del proceso de Garantizar la seguridad de los sistemas que satisfaga el requerimiento de negocio de TI de mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad es:* **2 Repetible pero Intuitivo.-** 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 habilitación sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.

5.1.3 Resultados del proceso: PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN

DOMINIO	PLANEAR Y ORGANIZAR
NOMBRE DEL PROCESO	PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN
REFERENCIA DE COBIT	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.

5.1.3.1 Observaciones del proceso

a) No existe un modelo de información empresarial en COCASINCLAIR EP, consecuentemente, no se puede comparar con algún modelo similar. La Coordinación de TIC'S no cuenta con un plan estratégico de TI.

b) La empresa no cuenta con un diccionario de datos empresarial, es responsabilidad de la Coordinación de TIC'S la definición, sintaxis y

reglas de validación de los datos y reglas del negocio. No cuentan con un plan de calidad de datos, políticas y procedimientos.

c) No se evidencia un esquema de clasificación de datos en la Empresa, no hay un control de la información que sale, podría ser confidencial o no.

d) La Coordinación de TIC'S, no se tiene implementado un control para asegurar la integridad de los datos. Faltan procedimientos que gestione la integridad de los datos.

5.1.3.2 Resultados del proceso

PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN
Como resultado de la evaluación de los objetivos de control del proceso PO2 Definir la Arquitectura de la Información, se detalla lo siguiente: **Efecto**: No se tiene control de la información que sale de la Empresa por algún medio electrónico sea esta confidencial o no. La integridad de los datos no se validan antes de salir los sistemas a producción, la revisión parcial de la integridad de los datos puede ocasionar desconfianza de los resultados del procesamiento de los sistemas. Ninguna de las aplicaciones se comunican para compartir un solo diccionario de datos. **Causa**: Poco conocimiento de la Coordinación de TIC'S de la importancia de tener una arquitectura empresarial de información, clasificación y niveles de seguridad. No se ha reportado formalmente un incidente de fuga de información confidencial o delicada, por lo que no se han tomado acciones y no se han buscado alternativas de protección y estandarización de los datos. **Recomendaciones**: Las recomendaciones propuestas para Definir la Arquitectura

de la Información, son:

- Promover por parte de la Coordinación de TIC'S, la elaboración de un modelo de información empresarial para la Empresa, partiendo de la planificación estratégica de TI que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones.

- Crear un diccionario de datos empresarial, que permita compartir elementos de datos entre las aplicaciones y los sistemas. Adicionalmente, elaborar un plan o un procedimiento para validar la calidad de los datos antes de salir a producción y que sea de aplicación para todos los sistemas.

- Definir un esquema de clasificación de los datos que permita identificar si es confidencial o pública, crítica o común, de acuerdo a parámetros establecidos conjuntamente con la Gerencia General o los propietarios de esa información.

- Implementar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en las bases de datos y archivos, aprobados por la Subgerencia Administrativa. Las bases de datos pueden ser heterogéneas pero el procedimiento deberá ser el mismo.

- Documentar todos los resultados obtenidos cuando se aplique el modelo de información empresarial, esto permitirá poder generar los indicadores necesarios para medir las actividades, procesos y metas de TI.

5.1.3.3 Determinación del nivel de madurez

NIVEL DE MADUREZ	0 ○ 1 ● **2** ○ 3 ○ 4 ○ 5 ○
REFERENCIA DE COBIT	*La administración del proceso de Definir la arquitectura de la información que satisface el requerimiento de negocio de TI de agilizar la respuesta a los requerimientos, para brindar información confiable y consistente y para integrar de forma transparente las aplicaciones hacia los procesos de negocio es:*

	1 Inicial / Ad Hoc.- La gerencia reconoce la necesidad de una arquitectura de información. El desarrollo de algunos componentes de una arquitectura de información ocurre de manera ad hoc. 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.

5.1.4 Resultados del proceso: DS01 DEFINIR Y ADMINISTRAR NIVELES DE SERVICIO

DOMINIO	ENTREGAR Y DAR SOPORTE
NOMBRE DEL PROCESO	**DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO.**
REFERENCIA DE COBIT	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

5.1.4.1 Observaciones del proceso

a) La Coordinación de TIC'S no ha definido el catálogo / portafolio de servicios (requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLA's), acuerdos de niveles de operación (OLA's) y las fuentes de financiamiento) tanto entre áreas internas como con proveedores.

b) No están documentados los servicios que brinda la Coordinación de TIC'S, existe una declaración general de los servicios de esta Coordinación dentro de las Responsabilidades y Atribuciones contenidas en el Estatuto Orgánico Funcional por Procesos de la Empresa.

c) Ninguno de los dos SLA's (Acuerdos de Nivel de Servicio) firmados por COCASINCLAIR EP, detalla los OLA's (Acuerdos de Nivel Operacional). Se garantiza la disponibilidad del servicio contratado por medio de la infraestructura implementada por el proveedor, no se indica cómo serán entregados técnicamente los servicios para soportar el (los) SLA(s).

d) Internamente no se ha firmado o acordado ningún SLA referente a los servicios que brinda la Coordinación de TIC'S y no se han identificados cuáles son los procesos críticos de TI.

e) No existe un proceso o procedimiento documentado para revisar periódicamente los SLA's firmados, aleatoriamente se revisa el nivel de servicio para verificar si se cumple lo acordado.

5.1.4.2 Resultados del proceso

DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO
Como resultado de la evaluación de los objetivos de control del proceso DS1 Definir y Administrar los Niveles de Servicio, se detalla lo siguiente: **Efecto**: No poder medir la eficiencia – eficacia de los servicios, disponer de un incompleto catálogo / portafolio de servicios de la Coordinación y no poder monitorear el cumplimiento de los niveles de servicios. No jerarquizar los servicios críticos y asociarlos a los niveles de servicio que deberían tener para garantizar una continuidad del negocio. **Causa**: Informalidad para documentar y comunicar los servicios que brinda la Coordinación de TIC'S. Se asume que los servicios no se podían medir y se hacía lo necesario con la finalidad de dar el "mejor servicio". **Recomendaciones**: Las recomendaciones propuestas para Definir y Administrar los Niveles de Servicio, son: • Definir el catálogo / portafolio de servicios (requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLA's), acuerdos de niveles de operación (OLA's) y las fuentes de financiamiento –si es del caso-) tanto entre áreas internas como con proveedores de la Empresa. • Documentar los servicios que brinda la Coordinación de TIC'S, apegándose a lo señalado en las Responsabilidades y Atribuciones contenidas en el Estatuto Orgánico Funcional por Procesos de la Empresa. • Definir y acordar convenios de niveles de servicio para todos los procesos críticos de la Coordinación de TIC'S, con base en los requerimientos de los usuarios y las capacidades técnicas en TI, incluyendo los acuerdos de niveles de operación OLA's para soportar el (los) SLA(s) de manera óptima. • Luego de que se hayan definido los SLA's de la Coordinación de TIC'S, se

debería elaborar un procedimiento para realizar un monitoreo (revisión) de los niveles de servicio.

5.1.4.3 Determinación del nivel de madurez

NIVEL DE MADUREZ	0 ○ 1 ○ **2** ● 3 ○ 4 ○ 5 ○
REFERENCIA DE COBIT	*La administración del proceso de Definir y administrar niveles de servicio que satisfacen el requerimiento de negocio para TI de asegurar la alineación de servicios claves de TI con la estrategia de negocio es:* **2. Repetible pero Intuitivo.-** 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. Si existe un proceso para el cumplimiento de los acuerdos de niveles de servicio es voluntario y no está implementado.

5.1.5 Resultados del proceso: DS02 ADMINISTRAR SERVICIOS DE TERCEROS

DOMINIO	**ENTREGAR Y DAR SOPORTE**
NOMBRE DEL PROCESO	**DS2 ADMINISTRAR LOS SERVICIOS DE TERCEROS.**
REFERENCIA DE COBIT	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.

5.1.5.1 Observaciones del proceso

a) No se dispone de un registro de proveedores por categorías de servicio, importancia o criticidad en la Coordinación de TIC'S. No se evalúa el tipo de relación por proveedor, existe una percepción del servicio que no está documentada, pero esta sirve de referencia para futuras contrataciones.
b) No se tiene definido un proceso de monitoreo de cumplimiento de la prestación del servicio del proveedor, el control lo realiza el administrador del contrato de acuerdo lo estipulado en el mismo, tanto para los requerimientos técnicos como en las tarifas de los servicios o bienes.

5.1.5.2 Resultados del proceso

DS2 ADMINISTRAR LOS SERVICIOS DE TERCEROS
Como resultado de la evaluación de los objetivos de control del proceso DS2 Administrar los Servicios de Terceros, se detalla lo siguiente: **Efecto**: No se conoce claramente cómo queda la relación entre la Empresa y el proveedor luego que finaliza el contrato, esto no contribuye a una mejor objetividad

al momento de seleccionar un proveedor. Se podría contratar nuevamente con un proveedor cuya relación con la Empresa no fue buena.

Causa: No se ha identificado la necesidad de contar con un registro de evaluaciones a los proveedores. Se hace cumplir lo señalado en el contrato por parte del Administrador en lo referente al objeto de contratación, obligaciones y responsabilidades del proveedor.

Recomendaciones: Las recomendaciones propuestas para Administrar los Servicios de Terceros, son:

- Llevar un registro de proveedores por categorías de servicio, importancia o criticidad en la Coordinación de TIC'S, que permita evaluar la relación con el proveedor y documentarla para una posterior selección / rechazo.

- Definir un proceso de monitoreo sobre el cumplimiento de la prestación del servicio por parte del proveedor, que apoye a las funciones que realiza el administrador del contrato.

5.1.5.3 Determinación del nivel de madurez

NIVEL DE MADUREZ	0 ○ 1 ○ **2** ○ 3 ● 4 ○ 5 ○
REFERENCIA DE COBIT	*La administración del proceso de Administrar los servicios de terceros que satisfagan los requerimientos de TI del negocio de brindar servicios de terceros satisfactorios siendo transparentes respecto a los beneficios, costos y riesgos es:* **3. Definido**.- 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. Los términos contractuales se basan en formatos estandarizados. El riesgo del negocio asociado con los servicios del tercero está valorado y reportado.

5.1.6 Resultados del proceso: DS12 ADMINISTRAR EL AMBIENTE FÍSICO

DOMINIO	ENTREGAR Y DAR SOPORTE
NOMBRE DEL PROCESO	**DS12 ADMINISTRACIÓN DEL AMBIENTE FÍSICO.**
REFERENCIA DE COBIT	La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.

5.1.6.1 Observaciones del proceso

a) No se ha realizado un análisis de riesgos de la infraestructura, incendios, acceso al Data Center, temperatura, entre otros. Los controles implementados para minimizar los impactos en el ambiente físico, se han realizado como una política de buenas prácticas y no por un análisis de vulnerabilidades o requerimientos. No existe documentación donde se enuncien las políticas.

b) No se ha elaborado un Plan de Continuidad del Negocio que involucre el aspecto del ambiente físico de la Empresa.

5.1.6.2 Resultados del proceso

DS12 ADMINISTRACIÓN DEL AMBIENTE FÍSICO
Como resultado de la evaluación de los objetivos de control del proceso DS12 Administración del Ambiente Físico, se detalla lo siguiente: **Efecto**: Los controles implementados a través de equipos (sensores) al ambiente físico del Data Center, pueden no ser tan eficaces al el momento que ocurra un incidente, no se evidencia que se haya realizado una prueba de eficacia. **Causa**: El diseño e implementación de los controles del ambiente físico en el Data Center específicamente, se lo realizó por medio de las mejores prácticas y estándares de cableado. Se siguió lo recomendado por el proveedor, se asume que lo sugerido por el proveedor es suficiente. **Recomendaciones**: Las recomendaciones propuestas para la Administración del Ambiente Físico, son: • Elaborar un análisis de riesgos de la infraestructura de TI, incendios, accesos, temperatura, entre otros, que permita dimensionar la eficacia de los controles implementados.

5.1.6.3 Determinación del nivel de madurez

NIVEL DE MADUREZ	0 ○ 1 ○ **2** ● 3 ○ 4 ○ 5 ○
REFERENCIA DE COBIT	*La administración del proceso de Administrar el ambiente físico que satisface el requerimiento del negocio de TI de proteger los activos de TI y la información del negocio y minimizar el riesgo de interrupciones en el negocio es:* **2. Repetible pero Intuitivo.-** Los controles ambientales se implementan y monitorean por parte del personal de operaciones. 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

5.1.7 Modelo Genérico de Madurez

A continuación, se detalla la clasificación de un modelo genérico de madurez, como referencia para determinar del nivel de madurez de los procesos que serán auditados.

0 No Existente.- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido que existen problemas a resolver.

1 Inicial.- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad-doc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible.- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 Definido.- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

4 Administrado.- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 Optimizado.- Los procesos se han refinado hasta un nivel de mejor práctica, se basa en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y efectividad, haciendo que la empresa se adapte de manera rápida.

5.1.8 Cuadro resumen del Nivel de Madurez de los procesos auditados en la empresa COCASINCLAIR EP.

No.	DOMINIO	NOMBRE DEL PROCESO	NIVEL DE MADUREZ
1	PLANEAR Y ORGANIZAR	PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI	1
2	ENTREGAR Y DAR SOPORTE	DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	2
3	PLANEAR Y ORGANIZAR	PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN	1
4	ENTREGAR Y DAR SOPORTE	DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO.	2
5	ENTREGAR Y DAR SOPORTE	DS2 ADMINISTRAR LOS SERVICIOS DE TERCEROS	3
6	ENTREGAR Y DAR SOPORTE	DS12 ADMINISTRACIÓN DEL AMBIENTE FÍSICO	2

Esto demuestra en general que los procesos auditados, se encuentran en un nivel básico o repetible, que siguen un patrón regular. La empresa ha definido ciertas actividades o controles para el tratamiento de la información y que se encuentran plasmadas en la infraestructura de TI.

5.2 Informe Ejecutivo

5.2.1 Antecedentes

La Coordinación de TIC'S no ha establecido procedimientos para la entrega de sus productos o servicios, la documentación que respalda su gestión es incompleta. Dentro del Plan Estratégico de la Empresa, se señalan las atribuciones y responsabilidades de la Coordinación de TIC'S, sin embargo no se especifica cómo apoya esta área a las políticas de la Empresa, cómo están sus procesos internos, el nivel de servicios referente al soporte técnico, la seguridad de la plataforma informática implementada y la seguridad de la información que es tratada internamente, entre otros aspectos.

Hechos que han impedido llevar un adecuado control y posterior evaluación de los productos o servicios que brinda esta Coordinación.

Actualmente, la información es un activo estratégico y el más valioso de las organizaciones, que permite fundamentalmente tomar decisiones oportunas. En este contexto, la Seguridad de la Información toma mayor importancia por cuanto se enfoca en garantizar a través del uso de técnicas o estándares la confidencialidad, integridad y disponibilidad de la información almacenada en un sistema informático, además de la implementación de los elementos de control que regulen los aspectos físicos, lógicos y legales del sistema.

Se pueden optimizar los recursos a través del uso de un estándar o mejores prácticas existentes en el mercado, que permitan alinear los objetivos de la Coordinación de TIC'S a los objetivos del negocio desde la planificación, operación, control y finalmente al seguimiento de sus procesos.

5.2.1.1 Objetivo de la Auditoria

5.2.1.1.1 General

Analizar, evaluar y documentar los seis procesos más relevantes, así como los controles implementados de estos procesos en la Coordinación de TIC'S de la empresa COCASINCLAIR EP, utilizando el marco de referencia COBIT 4.1 (Objetivos de Control de Tecnologías de Información) y proponer a la Gerencia General las recomendaciones para mejorarlos.

5.2.1.1.2 Específicos

- Elaborar una matriz de riesgos de la Coordinación de TIC'S, que muestre los seis procesos más relevantes del área, priorizándolos con los criterios de Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad)
- Auditar cada proceso identificado, usando el marco de referencia COBIT 4.1
- Determinar el nivel de madurez de cada proceso analizado.

- Presentar un informe ejecutivo a la Gerencia General de la empresa COCASINCLAIR EP, con las recomendaciones aplicables resultantes de la auditoría realizada.

5.2.1.2 Alcance de la Auditoría

Realizar una auditoría a los seis procesos más relevantes en la Coordinación de TIC'S de la empresa COCASINCLAIR EP, utilizando el marco de referencia COBIT 4.1, partiendo de la matriz de riesgos. Adicionalmente, se cumplirá con los objetivos específicos detallados en el numeral anterior..

5.2.1.3 Meta y metodología de la Auditoria

La meta es la revisión de los seis procesos más relevantes identificados en la matriz de riegos, lo que ayudará a tener una mejor visión de la situación actual de la Coordinación de TIC'S.

Se utilizará la metodología de la matriz de riesgos y el marco de referencia COBIT 4.1, este último permite gobernar o administrar las Tecnologías de Información, a través de un conjunto de herramientas administrativas y modelos de madurez para complementar el marco de referencia de control que permita a la Gerencia General cerrar la brecha entre los requerimientos de control, aspectos técnicos y riesgos de negocios.

Para conocer como está administrado TI, se evalúan los procesos y se determina su nivel de madurez, el mismo que puede ir desde 0 hasta 5. Un nivel recomendado sería 3, considerando que se mantenga un equilibrio del costo - beneficio.

5.2.2 Resultados de los procesos evaluados

5.2.2.1 Proceso: PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI.

DOMINIO	PLANEAR Y ORGANIZAR
NOMBRE DEL PROCESO	PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI
REFERENCIA DE COBIT	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.

5.2.2.1.1 Observaciones del proceso

a) La Coordinación de TIC'S, no cuentan con un marco de trabajo para una administración de riesgos, es así que, no se realizó la

identificación de los riesgos y de las acciones necesarias (tratamiento, análisis de impacto, recursos, etc.) para mitigar los riesgos.

b) No se ha elaborado un plan de gestión de riesgos por proyectos, sistema o servicios que brinda la Coordinación de TIC'S. Los riesgos son tratados a medida que ocurren y no se documentan las acciones realizadas.

c) No se han conformado equipos multifuncionales en la Empresa para identificar eventos e impactos, no se puede evaluar la probabilidad e impacto con métodos cualitativos o cuantitativos.

d) No se evidencia la identificación de riesgos inherentes y residuales categorizados por servicio, infraestructura, almacenamiento, disponibilidad de los sistemas, etc.,

e) No se ha elaborado ni documentado el proceso de administración de riesgos de TI (matriz de riesgos), ni se han identificado las acciones o estrategias que se deben realizar por cada riesgo identificado.

5.2.2.1.2 Efecto del resultado

Las observaciones comentadas no permiten: identificar, evaluar, mitigar o gestionar los riesgos y comunicar los riesgos residuales; consecuentemente, elaborar planes de acción para posteriormente monitorearlos.

5.2.2.1.3 Recomendaciones

- Definir una política por parte de la Coordinación de TIC'S, para establecer un marco de trabajo para la administración de riesgos de TI, que permita identificar eventos y gestionar los riesgos.

- Documentar todos los incidentes de TI y asociar a los riesgos de acuerdo a su nivel o importancia, es decir, riesgos críticos, inherentes o residuales; esto con la finalidad de generar indicadores de medición y monitoreo del plan de acción de riesgos.

- Elaborar procedimientos para la evaluación de riesgos generales o específicos de TI y documentarlos para que sean presentados a la Subgerencia Administrativa y posteriormente sean aprobados por la Gerencia General de COCASINCLAIR EP, para su socialización.

5.2.2.1.4 Nivel de madurez

Luego de la revisión del proceso Evaluar y Administrar los Riesgos de TI, este se encuentra en nivel 1 (Inicial / Ad-hoc), por cuanto no tienen procesos definidos para identificar, tratar, mitigar y tomar acciones sobre los riesgos.

Existe una identificación tácita de los riesgos referente a la disponibilidad de TI, se efectúan acciones de back-up (información) o redundancia (servicios) con la finalidad de minimizar el impacto si se produjera una amenaza que puediera afectar a otras áreas de la Empresa.

La informalidad o falta de mecanismos para gestionar los riesgos de TI, queda demostrado en la carencia de documentación que respalde o evidencie los planes de acción y la evaluación de los riesgos.

5.2.2.2 Proceso: DS05 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

DOMINIO	ENTREGAR Y DAR SOPORTE
NOMBRE DEL PROCESO	DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS
REFERENCIA DE COBIT	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.

5.2.2.2.1 Observaciones del proceso

a) La Coordinación de TIC’s no dispone de un documento de seguridad de la información, que detalle su estructura, contenido, roles, etc, ni con un plan general de seguridad de TI. Además, la empresa COCASINCLAIR EP, no ha conformado un comité directivo de seguridad.

b) A pesar de no estar documentadas las políticas de seguridad, estas se encuentran implementadas en los equipos de seguridad y en las estaciones de trabajo. Los reportes de seguridad son elaborados bajo demanda y no se hace seguimiento a la situación de la seguridad de la información de TI.

c) No se encuentran documentados ni se aplican procedimientos de control de acceso a los sistemas, clasificados por importancia o riesgo, solo se limitan a controles que son propios de la aplicación.

d) No está documentada la revisión de los controles de seguridad de acceso físico y lógico a los datos o archivos. Faltan las políticas y procedimientos frente a las consecuencias de violación a la seguridad de los sistemas.

e) No está documentada y comunicada la política de prevención de software malicioso.

f) La política de seguridad de la red, no está documentada.

g) No se encuentra clasificada la información para determinar cuál es sensible o confidencial según el nivel de exposición. No se valida si la información que genera la Empresa es confidencial antes de que ésta sea transmitida.

5.2.2.2.2 Efecto del resultado

Posibilidad de que las herramientas informáticas que se implementen, no tengan un respaldo documentado y aprobado que reflejen las acciones a tomar con la información que es tratada en los sistemas.

Los usuarios de los sistemas, pueden verse afectados por las políticas implementadas en los equipos de red o un servidor y que éstas no fueron comunicadas.

5.2.2.2.3 Recomendaciones

- Elaborar un documento de Seguridad de la Información, en el que contenga la política de Seguridad de la Información de la Empresa, alcance y objetivos, roles y responsabilidades de seguridad, estándares y procedimientos de TI, gestión de la aceptación del riesgo, política de seguridad de comunicaciones externas, política de Firewall, de seguridad

de E-mail, política de seguridad de una estación de trabajo, política de uso de Internet, etc.

- Elaborar un plan general de seguridad de TI, que contenga los requerimientos de negocio, riesgos y cumplimiento, teniendo en consideración la infraestructura de TI (software y hardware).

- Realizar el procedimiento referente al control de acceso a los sistemas, estos deben ser clasificados por importancia o riesgo y aplicarse a todos los usuarios, incluyendo a administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia.

- Elaborar las políticas y procedimientos frente a las consecuencias de violación de la seguridad; llevar un registro de los controles permitidos, accesos fallidos y no autorizados; y, documentar la revisión de los controles de seguridad de acceso físico y lógico a los datos o archivos.

- Documentar y comunicar a toda la Empresa la política de prevención de software malicioso, detallando las medidas preventivas y correctivas para la detección de virus, gusanos, spyware o correo basura.

- Elaborar la política de seguridad de la red; que contenga los controles a implementarse en los equipos de la red perimetral.

- Documentar el procedimiento para clasificar la información de la Empresa, que detalle los criterios para determinar cuál es sensible o confidencial según el nivel de exposición e implementar un control que valide si la información que se genera en la Empresa es confidencial antes de que ésta sea transmitida.

5.2.2.2.4 Nivel de madurez

El proceso Garantizar la Seguridad de los Sistemas, se encuentra en nivel 2 (Repetible), por cuanto la Coordinación de TIC'S no tiene la documentación referente a la Seguiridad de la Infomación ni un Plan de Seguridad de TI aprobado, sin embargo, tiene implentadas políticas de seguridad en los equipos de red, firewall, correo, estaciones de trabajo, servidores, navegación por internet, etc.

Los sistemas informáticos tienen implementadas las seguridades de acceso, así como la identificación de usuario para acceder al mismo. Incluye software de terceros para brindar seguridad a las estaciones de trabajo. Existen herramientas de seguridad implantadas, sin tener una política de seguridad. Es responsabilidad de la Coordinación de TIC'S brindar la seguridad de la información a la Empresa.

5.2.2.3 Resultados del proceso: PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN

DOMINIO	PLANEAR Y ORGANIZAR
NOMBRE DEL PROCESO	PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN
REFERENCIA DE COBIT	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.

5.2.2.3.1 Observaciones del proceso

a) No existe un plan estratégico de la Coordinación de TIC'S que incluya un modelo de información empresarial de COCASINCLAIR EP.

b) La empresa no cuenta con un diccionario de datos empresarial, ni un plan de calidad de datos, políticas y procedimientos.

c) No se evidencia un esquema de clasificación de datos en la Empresa, que controle la información que se genera por cualquier medio, sea esta confidencial o no.

d) La Coordinación de TIC'S, no tiene implementados procedimientos y controles para asegurar la integridad de los datos y estos no se validan antes de salir los sistemas a la fase de producción.

5.2.2.3.2 Efecto del resultado

No se controla la información que se genera en la Empresa por algún medio electrónico y que podría ser confidencial o no. Ninguna de las aplicaciones se comunican para compartir un solo diccionario de datos.

5.2.2.3.3 Recomendaciones

- Elaborar un modelo de información empresarial para la Empresa, partiendo de la planificación estratégica de TI que facilite el desarrollo de aplicaciones y las actividades de soporte para la toma de decisiones.

- Crear un diccionario de datos empresarial, que permita compartir tipos de datos entre las aplicaciones y los sistemas. Adicionalmente, elaborar un plan o un procedimiento para validar la calidad de los datos antes de salir a la fase de producción en un sistema y que sea de aplicación obligatoria para todos los sistemas.

- Definir un esquema de clasificación de los datos que permita identificar si es confidencial o público, crítico o común, de acuerdo a parámetros establecidos conjuntamente con la Gerencia General o con los propietarios de esa información.

- Implementar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en las bases de datos y archivos, aprobados por la autoridad competente.

- Documentar los resultados obtenidos cuando se aplique el modelo de información empresarial, con la finalidad de generar los indicadores necesarios para medir las actividades, procesos y metas de TI.

5.2.2.3.4 Nivel de madurez

Concluida la revisión del proceso Definir la Arquitectura de la Información, este se encuentra en nivel 1 (Inicial / Ad-hoc), por cuanto la Coordinación de TIC'S, no documenta y aplica un esquema de tratamiento y clasificación de la información. Solo una aplicación tiene un diccionario de datos.

La calidad de los datos es revisada únicamente en la fase de pruebas del ciclo de vida de una aplicación conjuntamente con el proveedor del software. Se confía que los datos almacenados en las base de datos son

íntegros y consistentes por la característica misma del motor de base de datos.

5.2.2.4 Resultados del proceso: DS01 DEFINIR Y ADMINISTRAR NIVELES DE SERVICIO

DOMINIO	ENTREGAR Y DAR SOPORTE
NOMBRE DEL PROCESO	DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO.
REFERENCIA DE COBIT	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

5.2.2.4.1 Observaciones del proceso

a) La Coordinación de TIC'S no ha definido el catálogo / portafolio de servicios (requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio, acuerdos de niveles de operación y las fuentes de financiamiento) tanto entre áreas internas como con proveedores. Dentro de las Responsabilidades y Atribuciones contenidas en el Estatuto Orgánico Funcional por Procesos de la Empresa, se enumeran en forma general los productos y servicios que brinda esta Coordinación.

b) En ninguno de los dos SLA’s (Acuerdos de Nivel de Servicio) firmados con las empresas de telecomunicaciones, se detalla los OLA’s (Acuerdos de Nivel Operacional). Se garantiza la disponibilidad del servicio contratado, por medio de la infraestructura implementada por el proveedor, no se indica cómo serán entregados técnicamente los servicios para soportar el (los) SLA(s).

c) No existe un proceso o procedimiento documentado para revisar periódicamente los SLA’s firmados con los proveedores, aleatoriamente se revisa el nivel de servicio para verificar si se cumple lo acordado.

5.2.2.4.2 Efecto del resultado

No poder monitorear el cumplimiento de los niveles de servicios y garantizar la eficiencia – eficacia de los servicios contratados.

5.2.2.4.3 Recomendaciones

- Definir el catálogo / portafolio de servicios que contenga los requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio, acuerdos de niveles de operación y las fuentes de financiamiento –si es del caso-, tanto entre áreas internas como con proveedores de la Empresa.

- Definir y acordar convenios de niveles de servicio para todos los procesos críticos de la Coordinación de TIC'S, con base en los requerimientos de los usuarios y las capacidades técnicas en TI, incluyendo los acuerdos de niveles de operación para soportar el (los) acuerdos de nivel de servicio de manera óptima.

- Luego de que se hayan definido los SLA's de la Coordinación de TIC'S, se debería elaborar un procedimiento para realizar un monitoreo de los niveles de servicio.

5.2.2.4.4 Nivel de madurez

De la auditoria al proceso Definir y Administrar los Niveles de Servicio, este se determina que está en nivel 2 (Repetible). La Coordinación de TIC'S, no tienen definido un catálogo / portafolio de servicios. Los SLA's analizados corresponden a proveedores de telecomunicaciones que prestan un servicio a COCASINCLAIR EP. Los reportes del nivel de servicio que se generan son por medio de un software del mismo proveedor.

La Coordinación de TIC'S tiene niveles de servicio informales entre las áreas, trata de cumplir los niveles de servicio por medio de un seguimiento a los registro de incidentes de soporte técnico. Varios servicios de la Coordinación no se han descrito formalmente, el técnico responsable

de esos servicios, realiza el monitoreo de la disponibilidad, seguridad y accesos a los mismos.

5.2.2.5 Resultados del proceso: DS02 ADMINISTRAR SERVICIOS DE TERCEROS

DOMINIO	ENTREGAR Y DAR SOPORTE
NOMBRE DEL PROCESO	DS2 ADMINISTRAR LOS SERVICIOS DE TERCEROS.
REFERENCIA DE COBIT	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.

5.2.2.5.1 Observaciones del proceso

a) La Coordinación de TIC'S, no se dispone de un registro de proveedores por categorías de servicio, importancia o criticidad. Tampoco se evalúa el tipo de relación por proveedor, existe una percepción del servicio que no está documentada.

b) No se tiene definido un proceso de monitoreo de cumplimiento de la prestación del servicio del proveedor, el control lo realiza el

administrador del contrato de acuerdo lo estipulado en el mismo, tanto para los requerimientos técnicos como en las tarifas de los servicios o bienes.

5.2.2.5.2 Efecto del resultado

No se conoce claramente la relación entre la Empresa y el proveedor luego que finaliza un contrato, impidiendo tener objetividad al momento de seleccionar un proveedor.

5.2.2.5.3 Recomendaciones

- Llevar un registro de proveedores por categorías de servicio, importancia o criticidad en la Coordinación de TIC'S, que permita evaluar la relación con el proveedor y documentarla para una posterior selección / rechazo.

- Definir un proceso de monitoreo sobre el cumplimiento de la prestación del servicio por parte del proveedor, en los requerimientos técnicos y en las tarifas de los servicios o bienes contratados, actividades que deben estar coordinadas con el administrador del contrato.

5.2.2.5.4 Nivel de madurez

Como resultado de la revisión al proceso Administrar los Servicios de Terceros, este se encuentra en nivel 3 (Definido). La Coordinación de TIC'S, administra contratos en los que se detallan las obligaciones y responsabilidades de los proveedores. Existen dos contratos que anexan SLA's, estos apoyan para al cumplimiento del objeto de contratación.

Los acuerdos con proveedores se realizan por medio de un contrato o una orden de servicio, debidamente firmada por las partes. Para el caso de un contrato, este incluye cláusulas legales, regulatorias, administrativas y de garantías (financieras o técnicas) que minimizan el riesgo de incumplimiento del objeto de contratación por parte del proveedor, adicionalmente, la responsabilidad de la ejecución del contrato es del Administrador, quien es designado por la Gerencia General.

5.2.2.6 Resultados del proceso: DS12 ADMINISTRAR EL AMBIENTE FÍSICO

DOMINIO	ENTREGAR Y DAR SOPORTE
NOMBRE DEL PROCESO	DS12 ADMINISTRACIÓN DEL AMBIENTE FÍSICO.
REFERENCIA DE COBIT	La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores

	ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.

5.2.2.6.1 Observaciones del proceso

a) No se ha elaborado un análisis de riesgos de la infraestructura de TI, incendios, acceso al Data Center, temperatura, entre otros. Los controles implementados para minimizar los impactos en el ambiente físico, se han realizado como una política de buenas prácticas y no como resultado de un análisis de vulnerabilidades o requerimientos.

b) No se ha elaborado un Plan de Continuidad del Negocio que involucre el aspecto del ambiente físico de la Empresa.

5.2.2.6.2 Efecto del resultado

En el caso de presentarse daños a los equipo de cómputo o al personal, existe el riesgo de interrumpir las actividades diarias del negocio.

5.2.2.6.3 Recomendaciones

- Elaborar un análisis de riesgos de la infraestructura de TI, incendios, accesos, temperatura, entre otros, que permita dimensionar la eficacia de los controles implementados.

- Elaborar un Plan de Continuidad del Negocio que involucre el aspecto del ambiente físico de la Empresa y del Data Cener.

5.2.2.6.4 Nivel de madurez

El proceso Administrar el Ambiente Físico, está ubicado en nivel de madurez 2 (Repetible). La Coordinación de TIC'S, tiene implementados controles para el ambiente físico en el Data Center, tales como: temperatura, acceso, incendios. Estos controles fueron implementados siguiendo las mejores prácticas y estándares de cableado y de seguridad para Centros de Cómputo.

Los equipos que tienen implementado los controles, se encuentran conectados en red a una consola de administración centralizada que es administrada por el personal de TIC'S.

El mantenimiento que se realiza al aire a condicionado es registrado como soporte técnico, no se sigue un procedimiento para realizar

mantenimientos a las instalaciones. Es responsabilidad de la Coordinación de TIC'S, que se cumplan los objetivos de seguridad de tecnología.

5.2.2.7 Cuadro resumen del Nivel de Madurez de los procesos auditados en la empresa COCASINCLIAR EP.

No.	DOMINIO	NOMBRE DEL PROCESO	NIVEL DE MADUREZ
1	PLANEAR Y ORGANIZAR	PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI	1
2	ENTREGAR Y DAR SOPORTE	DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	2
3	PLANEAR Y ORGANIZAR	PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN	1
4	ENTREGAR Y DAR SOPORTE	DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO.	2
5	ENTREGAR Y DAR SOPORTE	DS2 ADMINISTRAR LOS SERVICIOS DE TERCEROS	3
6	ENTREGAR Y DAR SOPORTE	DS12 ADMINISTRACIÓN DEL AMBIENTE FÍSICO	2

Esto demuestra en general que los procesos auditados, se encuentran en un nivel básico o repetible, que siguen un patrón regular. . La empresa ha definido ciertas actividades o controles para el tratamiento de la información y que se encuentran plasmadas en la infraestructura de TI.

CAPITULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

A través del uso de un estándar, una metodología o una combinación entre estas, se puede optimizar los recursos tecnológicos y alinear los objetivos de la Coordinación de TIC'S a los objetivos del negocio desde la fases de la planificación, operación, control y finalmente al seguimiento de sus procesos.

Los estándares o marcos de referencia para la administración de las Tecnologías de Información, se han ido desarrollando y mejorando con el pasar de los años y son utilizados por grandes empresas a nivel mundial, lo que ha permitido sustentar los resultados obtenidos de la revisión de los procesos en la Coordinación de TIC'S de la empresa COCASINCLAIR EP.

Las normas o aspectos que se deben considerar para realizar cualquier tipo de auditoría, son muy similares, estas son la independencia, objetividad, relaciones humanas, confiabilidad e integridad de la información, uso eficiente y económico de los recursos, entre otras; el conocimiento de los procesos y el giro del negocio, permiten identificar los principales riesgos y ayudan a determinar el alcance de una auditoria.

Los riesgos que se presentan en una empresa, están relacionados directamente a una posible afectación de las operaciones del negocio o el no poder seguir prestando el servicio en óptimas condiciones. Por consiguiente es necesario elaborar un plan que garantice la continuidad del negocio, partiendo de realizar acciones para mitigar los riesgos críticos. Estos se identificaron en la matriz de riesgos de la Coordinación de TIC'S.

Gestionar o administrar las TIC'S, requiere la definición de responsabilidades para los miembros del área, mecanismos para un uso eficiente y eficaz de los recursos, concienciar a la alta gerencia acerca de los costos de TI, brindar soporte técnico a la empresa con parámetros de evaluación del servicio, así como proponer la reducción de costos mediante la estandarización.

COBIT es un marco de referencia y no un "recetario" entendido como la panacea de la administración de TI, COBIT está alineado con otros estándares y buenas prácticas y puede ser usado junto con ellos. Las organizaciones deben analizar sus requerimientos de control y adaptar COBIT con base a sus impulsores de valor, perfil de riesgos o la infraestructura, organización y portafolio de proyectos de TI.

Los riesgos pueden encontrase en toda la Coordinación de TI, en sus procesos, aplicaciones y servicios que brinda la Coordinación y los factores que pueden determinar posibles riesgos asociados a la parte interna y

externa (proveedores, clientes). Los riesgos inherentes son parte del negocio, cada actividad tiene asociada uno o más riesgos.

Hoy en día es muy importante la administración de los riesgos asociados a la tecnología, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI. La información contenida en el hardware y manipulada a través de un software, es el activo más importante en la empresa COCASINCLAIR EP.

En general, como resultado de los procesos auditados, estos se encuentran en un nivel básico o repetible, que siguen un patrón regular. La empresa COCASINCLAIR EP ha definido ciertas actividades o controles para el tratamiento de la información y que se encuentran plasmadas en la infraestructura de TI.

6.2 Recomendaciones

Realizar un levantamiento de procesos para las diferentes actividades que se realizan en la Coordinación de TIC'S, que permita llevar un mejor control de la infraestructura tecnológica y evaluar los productos o servicios que brinda esta Coordinación.

Se debería realizar la auditoria a los 13 procesos de la Coordinación de TIC'S que fueron identificados en la matriz de riesgos aplicando la

metodología utilizada en este trabajo de tesis, esto ayudaría a determinar de mejor manera su situación actual y poder plantear las recomendaciones para mejorar los procesos y alcanzar el siguiente nivel de madurez.

El control interno debería ser una actividad o una función implícita en todos los puestos de trabajo en la empresa COCASINCLAIR EP, esta sería como una buena práctica de control orientada a minimizar los riesgos y garantizando el uso los recursos financieros o bienes cumpliendo las leyes, reglamentos y políticas internas o externas.

Capacitar al personal de la Coordinación de TIC'S en el marco de referencia COBIT 4.1, que les permita conocer e implementar los controles de mejor manera en la infraestructura tecnológica en base a políticas y procedimientos documentados y aprobados por la Gerencia General.

De acuerdo al cuadro resumen del Nivel de Madurez de los procesos auditados contenidos en el Informe Ejecutivo, los procesos PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI y PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN que tienen un nivel de madurez 1, son los que la Coordinación de TIC'S debería enfocarse en implementar mejores controles, partiendo de un plan de acción o acciones para realizar una correcta gestión de riesgos de TI y que sea parte de un Plan de Continuidad del Negocio, además de la elaboración de un modelo de información empresarial para COCASINCLAIR EP, partiendo de la

planificación estratégica de TI que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones.

Finalmente, se debería analizar y aplicar las recomendaciones sugeridas en el Informe Ejecutivo de este trabajo de tesis, en base a una priorización y disponibilidad de recursos de COCASINCLAIR EP, con la finalidad de incrementar y optimizar los controles ya existentes de los procesos auditados.

ACRÓNIMOS

BCP Plan de Continuidad de Negocio.

COBIT Objetivos de Control de las Tecnologías de Información

ITGI Instituto de Gobernabilidad de las Tecnologías de Información.

ITIL Biblioteca de la Infraestructura de las Tecnologías de Información.

KPI Indicadores Claves de Rendimiento.

OLA Acuerdos de Nivel Operacional.

SLA Acuerdos de Nivel de Servicios.

TIC Tecnologías de Información y Comunicación.

BIBLIOGRAFÍA

Academia de Administración y Sociales. (12 de 2011). *Universidad Autónoma del Estado de Hidalgo.* Obtenido de Auditoria Informática: http://www.uaeh.edu.mx/docencia/P_Presentaciones/tlahuelilpan/sistemas/auditoria_informatica/auditoria_informatica.pdf

Cocasinclair, E. (2011-2015). *Plan Estratégico Institucional.* Quito, Ecuador: Coordinación de Comunicación.

Cocasinclair, E. (2012). *Estructura Orgánica por Procesos.* Quito, Ecudor: Coordinación de Talento Humano.

Cocasinclair, E. (2012). *Plan Anual de Compras (PAC).* Quito, Ecuador: Coordinación de Compras Públicas.

Echenique, J. (2001). *Auditoría en Informática* (2da ed.). México: Mc Graw Hill.

Editorial Sigweb. (05 de 03 de 2012). *Sistemas Integrados de Gestión.* Obtenido de Matriz de Riesgo, Evaluación y Gestión de Riesgos: http://www.sigweb.cl/biblioteca/MatrizdeRiesgo.pdf

Escuela de Ingenieria Civil Informática. (2009). Obtenido de Herramientas y Técnicas de una Auditoria Informática: http://www.google.com.ec/url?sa=t&rct=j&q=herramientas%20de%20auditoria%20informatica&source=web&cd=1&cad=rja&sqi=2&ved=0CCsQFjAA&url=http%3A%2F%2Fwww.eici.ucm.cl%2FAcademicos%2Fygomez%2Fdescargas%2FAud_Seg_Sist%2FHerramientas-Tecnicas-Auditoria-Informati

Espejo, O., & Torres, C. (2006). *Administración de Tecnologías de la Información.* México.

Espejo, O., & Torres, C. (27 de 10 de 2009). *Slideshare.* Obtenido de Administración de Tecnologías de Información: www.slideshare.net/guestfa372b/coso-2361475

Funezalida, R., & Ambrosio, E. (17 de 08 de 2011). *Red de Conocimientos en Auditoria y Control Interno.* Obtenido de Riesgo tecnológico. Su medición como prioridad para el aseguramiento del negocio: http://www.auditool.org/index.php?option=com_content&view=article&id=827:riesgo-tecnologico-su-medicion-como-prioridad-para-el-aseguramiento-del-negocio-&catid=57:auditoria-de-ti&Itemid=112

Hernández, E. (2000). *Auditoría en Informática* (2da ed.). México: CECSA.

Innovation Group. (10 de 2011). *Auditoria de Sistemas.* Obtenido de http://auditoriasistemas.com/plan-de-continuidad-de-negocio/

IT Governance Institute . (2007). *Cobit* (4.1 ed.). Estados Unidos.

IT Governance Institute. (2007). *IT Assurance Guide Using Cobit.* Estados Unidos.

Jolly Moore, J., & Alcarraz, G. (2010). *Auditoría Continua: Mejores Prácticas y Caso Real. Congreso Latinoamericano de Auditoría Interna y Evaluación de Riesgos.* Montevideo, Uruguay.

Piattini, M., & Del Peso, E. (2001). *Auditoría Informática un Enfoque Práctico* (2da ed.). México: Alfaomega.

PriceWaterHouseCoopers. (09 de 2009). *www.pwc.com.* Obtenido de Desarrollo de un Plan de Continuidad de Negocio: Aplicando un enfoque económico, rápido y efectivo: www.pwc.com/ve/es/asesoria-gerencial/boletin/assets/boletin-advisory-edicion-09-2008.pdf

Roldán, G. (2011). *Administración y Auditoria de las TIC'S.* Quito, Ecuador.

ANEXO No. 1

Metodología tradicional de Auditoría Informática.

(Fuente, Auditoría en Informática de José Antonio Echenique García).

(Anotar los antecedentes específicos del proyecto de auditoría.)

II. OBJETIVOS DE LA AUDITORÍA EN INFORMÁTICA

(Anotar el objetivo específico de la auditoría.)

III. ALCANCES DEL PROYECTO

El alcance del proyecto comprende:

1. Evaluación de la dirección de informática en lo que corresponde a:
   - Su organización.
   - Funciones.
   - Objetivos.
   - Estructura.
   - Recursos humanos.
   - Normas y políticas.
   - Capacitación.
   - Planes de trabajo.
   - Controles.
   - Estándares.
   - Condiciones de trabajo.
   - Situación presupuestal y financiera.
2. Evaluación de los sistemas:
   - Evaluación de los diferentes sistemas en operación (flujo, procedimientos, documentación, organización de archivos, estándares de programación, controles, utilización de los sistemas, opiniones de los usuarios).
   - Evaluación de avances de los sistemas en desarrollo y congruencia con el diseño general, control de proyectos, modularidad de los sistemas.
   - Seguridad lógica de los sistemas, confidencialidad y respaldos.
   - Derechos de autor y secretos industriales, de los sistemas propios y los utilizados por la organización.
   - Evaluación de las bases de datos.
3. Evaluación de los equipos:
   - Adquisición.
   - Estandarización.
   - Controles.
   - Nuevos proyectos de adquisición.
   - Almacenamiento.
   - Comunicación.

- Redes.
- Equipos adicionales.

4. Evaluación de la seguridad:

   - Seguridad lógica y confidencialidad.
   - Seguridad en el personal.
   - Seguridad física.
   - Seguridad contra virus.
   - Seguros.
   - Seguridad en la utilización de los equipos.
   - Seguridad en la restauración de los equipos y de los sistemas.
   - Plan de contingencia y procedimientos en caso de desastre.

IV. METODOLOGÍA

La metodología de investigación a utilizar en el proyecto se presenta a continuación:

1. Para la evaluación de la dirección de informática se llevarán a cabo las siguientes actividades:

   - Solicitud de los manuales administrativos, organización, funciones, planes, políticas, estándares utilizados y programas de trabajo.
   - Solicitud de costos y presupuestos de informática.
   - Elaboración de un cuestionario para la evaluación de la dirección.
   - Aplicación del cuestionario al personal, y realización de entrevistas.
   - Entrevistas a líderes de proyectos y a usuarios más relevantes de la dirección de informática.
   - Análisis y evaluación de la información.
   - Elaboración del informe.

2. Para la evaluación de los sistemas tanto en operación como en desarrollo se llevarán a cabo las siguientes actividades:

   - Estudios de viabilidad y costo/beneficio.
   - Solicitud del análisis y diseño de los sistemas en operación y en desarrollo.
   - Solicitud de documentación de los sistemas en operación (manuales técnicos, de operación, de usuario, diseños).
   - Solicitud del plan de trabajo.
   - Solicitud de contratos de compra o renta de software.
   - Solicitud de licencias y derechos de autor.
   - Plan de contingencia y recuperación en casos de desastre.
   - Recopilación y análisis de los procedimientos administrativos de cada sistema.
   - Análisis de bases de datos.

- Análisis de la seguridad lógica y confidencialidad.
- Evaluación de los proyectos en desarrollo, prioridades y personal asignado.
- Evaluación de la participación de auditoría interna.
- Evaluación de controles.
- Evaluación de las licencias, la obtención de derechos de autor y de la confidencialidad de la información.
- Entrevistas con usuarios de los sistemas.
- Evaluación directa de la información obtenida contra las necesidades y requerimientos de los usuarios.
- Análisis objetivo de la estructuración y flujo de los programas.
- Análisis y evaluación de la información compilada.
- Elaboración de informe.

3. Para la evaluación de los equipos se llevarán a cabo las siguientes actividades:

   - Solicitud de los estudios de viabilidad, costo/beneficio y características de los equipos actuales, proyectos sobre adquisición o ampliación de equipo y su actualización.
   - Solicitud de contratos de compra o renta de los equipos.
   - Solicitud de contratos de mantenimiento de los equipos.
   - Solicitud de contratos y convenios de respaldo.
   - Solicitud de contratos de seguros.
   - Bitácoras de los equipos.
   - Elaboración de un cuestionario sobre la utilización de equipos, archivos, unidades de entrada/salida, equipos periféricos, y su seguridad.
   - Visita a las instalaciones y a los lugares de almacenamiento de archivos magnéticos.
   - Visita técnica de comprobación de seguridad física y lógica de las instalaciones.
   - Evaluación técnica del sistema eléctrico y ambiental de los equipos, del local utilizado y en general de las instalaciones.
   - Evaluación de los sistemas de seguridad de acceso.
   - Evaluación de la información recopilada, obtención de gráficas, porcentajes de utilización de los equipos y su justificación.
   - Elaboración de informe.

4. Elaboración del informe final, presentación y discusión del mismo, y presentación de conclusiones y recomendaciones.

V. TIEMPO Y COSTO

(Poner el tiempo en que se realizará el proyecto, de preferencia indicando el tiempo de cada una de las etapas; el costo del mismo, que incluya el personal participante en la auditoría y sus características, y la forma de pago.)