UNIVERSIDAD DE VALPARAÍSO

FACULTAD DE CIENCIAS ECONOMICAS Y ADMINISTRATIVAS

ESCUELA DE AUDITORIA

"APLICACIÓN, SEGÚN NORMAS COBIT, DE LA ADMINISTRACIÓN DE RECURSOS HUMANOS, EN COLEGIO DE LA REGIÓN DE VALPARAÍSO"

TESIS PARA OPTAR AL TÍTULO DE CONTADOR PÚBLICO AUDITOR Y AL GRADO DE LICENCIADO EN SISTEMAS DE INFORMACIÓN Y CONTROL DE GESTIÓN

Tesistas: Mariluz Fuentes Saavedra
Jessica Tapia Antimán

Profesor Guía: Ricardo Acevedo.

Valparaíso 2009

Índice

Resumen

En la actualidad los temas relativos a la auditoria informática cobran cada vez más relevancia, debido a que la información se ha convertido en el activo más importante de las empresas. Al representar una ventaja estratégica éstas invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información, con el fin de obtener la mayor productividad y calidad posibles.

Hoy en día, las empresas y organizaciones dependen de las pautas económicas, industriales y sociales en las que se encuentran. Por lo tanto, si las tendencias tecnológicas y los entornos económicos e industriales cambian, deben adaptarse rápidamente a las nuevas circunstancias para sobrevivir.

Este cambio es muy rápido y afecta al mundo entero, y su comprensión es fundamental para las organizaciones de todo tipo, particularmente en el contexto de los sistemas y tecnologías de información. Así, aunque los avances tecnológicos de los últimos veinte años han sido constantes y espectaculares, en los últimos cinco se ha producido una verdadera revolución tecnológica de gran envergadura e impacto para la propia industria informática, así como de consecuencias importantes para el resto de sectores.

Dado que cada vez más empresas y organizaciones consideran que la información y la tecnología asociadas a ellas representan sus activos más importantes, se les exige – al igual que al resto de activos - requerimientos de calidad, controles, seguridad e información. La gerencia, por ende, debe establecer un sistema de control interno adecuado y tal sistema debe soportar debidamente los procesos del negocio.

Haciendo eco de estas tendencias, la Organización ISACA (Information Systems Audit and Control Association), a través de su Fundación, publicó en diciembre de 1995 el COBIT cuya sigla significa objetivos de control para tecnología de información y tecnologías relacionadas, como resultado de cuatro años de intensa investigación y del trabajo de un gran equipo de expertos internacionales, siendo está metodología el marco de una definición de estándares y conducta profesional para la gestión y el control de los Sistemas de Información (en adelante, SI), en todos sus aspectos, unificando diferentes estándares, métodos de evaluación y controles anteriores. Adicionalmente, esta metodología aporta la orientación hacia el negocio y está diseñada no sólo para ser utilizada por usuarios y auditores, sino también como una extensa guía para gestionar los procesos de negocios.

La misión y objetivo principal de COBIT es investigar, desarrollar, publicar y promocionar objetivos de control de Tecnología de Información (en adelante, TI) internacionales, actualizados a la realidad del momento para ser usados por los gerentes de negocios y auditores.

COBIT ha sido desarrollado como estándares generalmente aplicables y aceptados para mejorar las prácticas de control y seguridad de las TI, que provean un marco de referencia para la administración, los usuarios y los auditores de cualquier tipo. Básicamente consta de 4 pasos, los cuales conforman el planeamiento y realización de una auditoria, ellos son:

- Resumen Ejecutivo
- Antecedentes y Marco de Referencia
- Guías de Auditoría
- Herramientas de Implementación

En función de lo anterior, el siguiente trabajo tiene la finalidad de exponer las Normas COBIT de manera simple y comprensible. Para ello, además de realizar un desarrollo teórico de las mismas, se incluye un análisis de la situación

actual del Departamento de Recursos Humanos de la organización COLEGIO PARTICULAR PUMANQUE de San Felipe, explicándose si sus procedimientos respetan o no la norma, y entregándose indicaciones para que aplique y cumpla con un determinado proceso de la norma.

El cuerpo del trabajo está dividido en dos partes principales las cuales reflejan las características y estructura de COBIT, el relevamiento y aplicación de las Normas COBIT en el establecimiento educacional. Además, se incluyen dos Apéndices: el apéndice I indica los componentes de COBIT como Producto y en el apéndice II incorpora la lista completa de dominios, procesos y objetivos de control.

Marco Teórico

1. COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas).

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de TI. Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

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

Misión:

- Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores.

Usuarios:

- La Gerencia, para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
- Los Usuarios Finales, quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

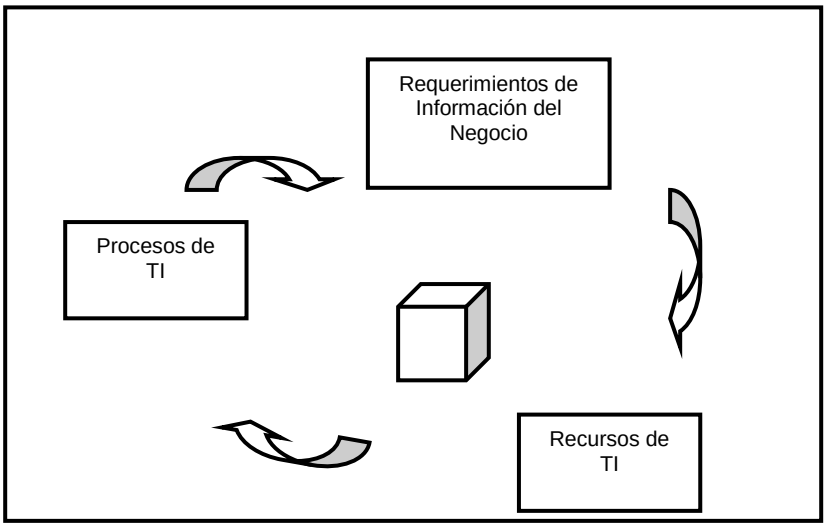
- Los Auditores, para basar sus opiniones en los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.
- Los Responsables de TI, para identificar los controles que requieren en sus áreas.

También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio (siendo el encargado de controlar los aspectos de información del proceso) y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

Características:

- Orientado al negocio.
- Alineado con estándares y regulaciones “de facto”.
- Basado en una revisión crítica y analítica de las tareas y actividades en TI.
- Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA).

Principios:



El enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI.

- Requerimientos de la información del negocio.

  Para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos criterios:

1. Requerimientos de Calidad: Calidad, costo y entrega del servicio.

2. Requerimientos Fiduciarios: Efectividad y eficiencia operacional, confiabilidad de los reportes financieros y cumplimiento de las leyes y regulaciones.

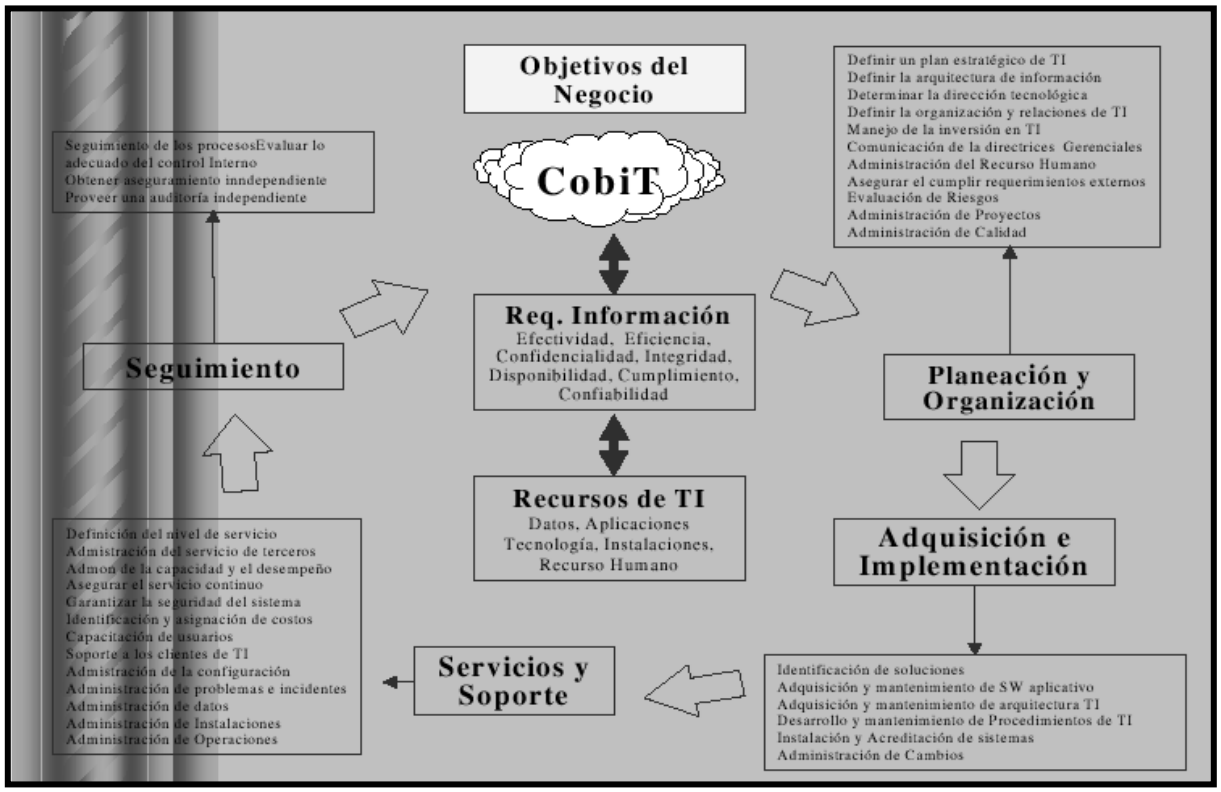
   2.1. *Efectividad*: La información debe ser relevante y pertinente para los procesos del negocio, así como también ser proporcionada en forma oportuna, correcta, consistente y utilizable.
   2.2. *Eficiencia* : Proporcionar información mediante el empleo óptimo de los recursos (la forma más productiva y económica).
   2.3. *Confiabilidad*: Proveer la información apropiada para una buena toma decisiones y cumplir con sus responsabilidades.
   2.4. *Cumplimiento*: De las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.

3. Requerimientos de Seguridad: Confidencialidad, integridad y disponibilidad.

   3.1. *Confidencialidad*: Protección de la información sensible contra la divulgación no autorizada.

3.2. *Integridad*: Refiere a lo exacto y completo de la información, así como, a su validez de acuerdo con las expectativas de la empresa.

3.3. *Disponibilidad*: Accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a la misma.

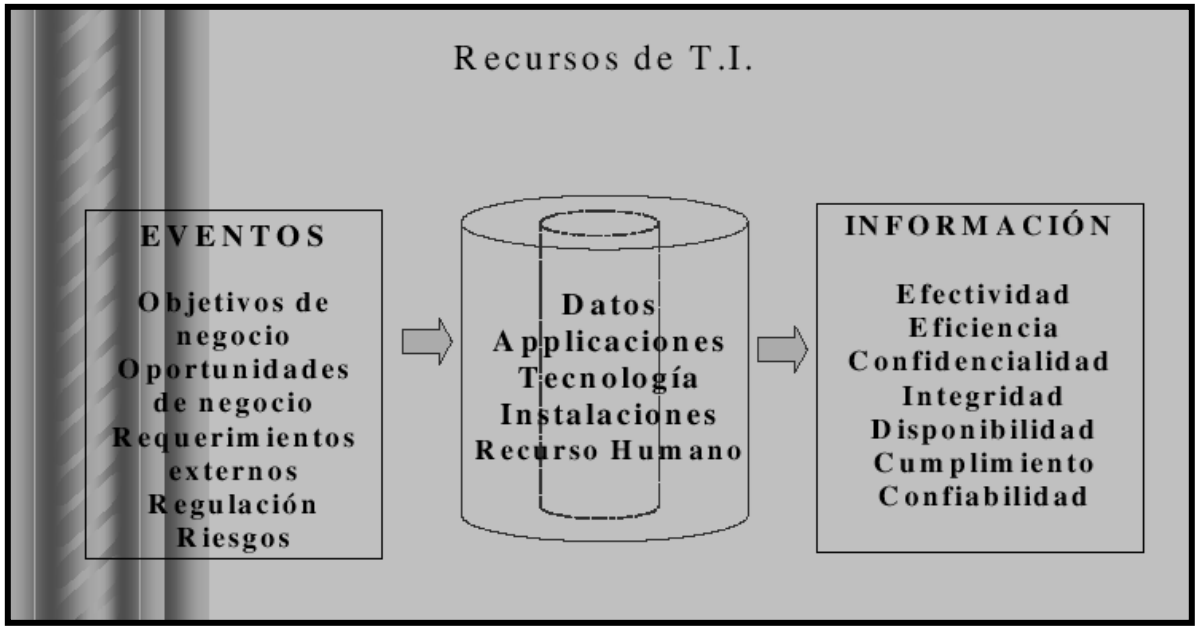


- Recursos de TI

En COBIT se establecen los siguientes recursos en TI necesarios para alcanzar los objetivos de negocio:

1. *Datos*: Considera información interna y externa, estructurada o no, gráficas, sonidos, etc.
2. *Aplicaciones*: Sistemas de información, que integran procedimientos manuales y sistematizados.

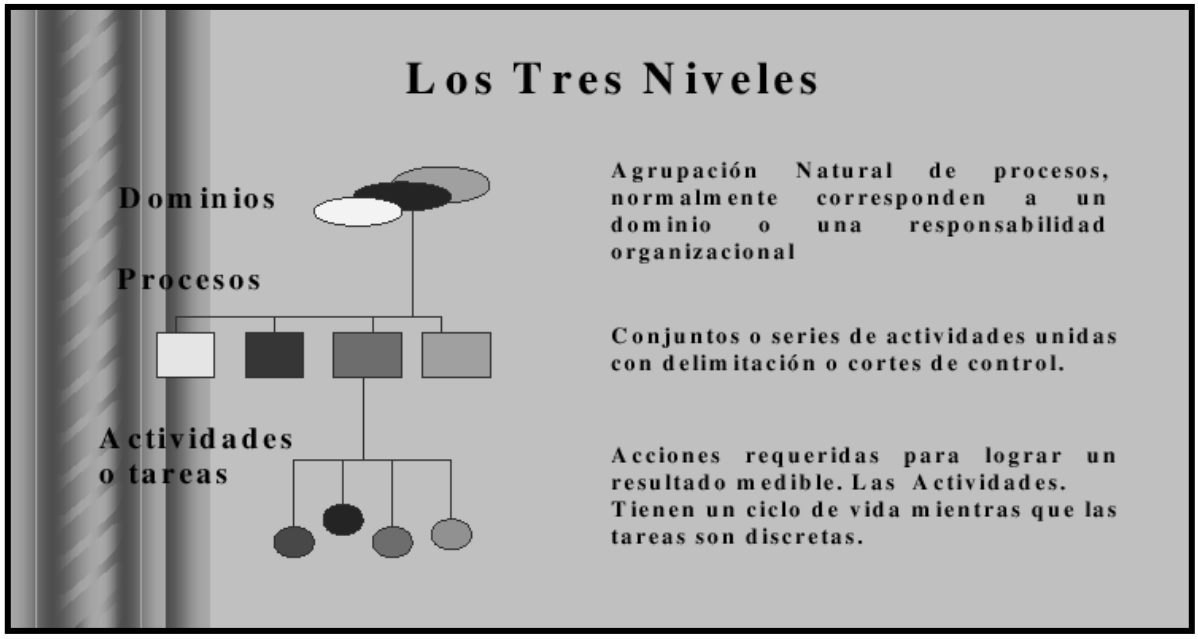
3. *Tecnología*: Se refiere al hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.
4. *Instalaciones*: Corresponde a los recursos necesarios para alojar y dar soporte a los sistemas de información.
5. *Recurso Humano*: Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información.



- Procesos de TI

La estructura de COBIT se define a partir de una premisa simple y pragmática: "Los recursos de las Tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos". COBIT se divide en tres niveles:

- *Dominios*: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
- *Procesos*: Conjuntos o series de actividades unidas con delimitación o cortes de control.
- *Actividades*: Acciones requeridas para lograr un resultado medible.



Se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI. Estos procesos están agrupados en cuatro grandes dominios:

- Planeación y organización (PO)
- Adquisición e implementación (AI)
- Presentación y soporte (DS)
- Monitoreo (M)

A continuación se detallan junto con sus procesos y una descripción general de las actividades de cada uno:

1. Planificación y Organización.

Este dominio se refiere a la identificación de la forma en que la tecnología de información puede contribuir al logro de los objetivos de negocio. La consecución de la visión estratégica necesita, además, ser planeada, comunicada y administrada desde diferentes perspectivas para finalmente establecer una organización y una infraestructura tecnológica apropiadas.

1.1. Procesos:

- PO1 Definición un plan estratégico para TI.

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

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

1. La definición de objetivos de negocio y necesidades de TI: la alta gerencia es responsable de desarrollar e implementar planes a corto y largo plazo que satisfagan las metas generales y la misión de la organización.
2. El inventario de soluciones tecnológicas e infraestructura actual: evalúa los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.

3. Cambios organizacionales: Se asegura que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI.
4. Estudios de factibilidad oportunos: Obtención de resultados efectivos.

❖ PO2 Definición de la arquitectura de información.

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

1. La documentación guarda consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.
2. El diccionario de datos, incorpora las reglas de sintaxis de datos de la organización y se actualiza continuamente.
3. La propiedad de la información y la clasificación de severidad con el que se establece un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información.

❖ PO3 Determinación de la dirección tecnológica.

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

1. La capacidad de adecuación y evolución de la infraestructura actual, concuerda con los planes a corto y largo plazo de tecnología de

información y abarca aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.

2. El monitoreo de desarrollo tecnológico es tomado en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.
3. Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evalúa sistemáticamente el plan de infraestructura tecnológica.
4. Planes de adquisición, los cuales reflejan las necesidades identificadas en el plan de infraestructura tecnológica.

❖ PO4 Definición de la organización y de las relaciones de TI.

Objetivo: Prestación de servicios de TI.

Se realiza por medio de una organización, favorable en número y habilidades, con tareas, responsabilidades definidas y comunicadas, considerando:

1. El comité de dirección, se encarga de vigilar la función de servicios de información y sus actividades.
2. Propiedad y custodia, la Gerencia crea una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades están claramente definidas.
3. Supervisión, asegura que las funciones y responsabilidades sean llevadas a cabo apropiadamente.
4. Segregación de funciones, evita que un individuo resuelva solo un proceso crítico.
5. Los roles y responsabilidades, la gerencia asegura que todo el personal conoce y cuenta con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que les hayan sido asignadas.

6. La descripción de puestos, define las habilidades y la experiencia necesaria para el cargo, así como la autoridad y responsabilidad apropiadas para su utilización en evaluaciones de desempeño.
7. Los niveles de asignación de personal realizan evaluaciones de requerimientos regularmente para asegurar una asignación de personal adecuada en el presente y en el futuro.
8. El personal clave, la gerencia identifica al personal clave de tecnología de información.

❖ PO5 Administración de la inversión en TI.

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

1. Se investiga diferentes alternativas de financiamiento.
2. El control de gasto real, se considera como base el sistema de contabilidad de la organización, en el cual se registra, procesa y reporta rutinariamente los costos asociados con las actividades de la función de servicios de información.
3. La justificación de costos y beneficios, establece un control gerencial que garantiza, que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos. Los beneficios derivados de las actividades de TI serán analizados en forma similar.

❖ PO6 Comunicación de metas y dirección de la gerencia.

Objetivo: Asegura el conocimiento y comprensión de los usuarios sobre las aspiraciones de la Gerencia. Se concreta a través de políticas establecidas y transmitidas a la comunidad de usuarios, requiriéndose para estos estándares, traducir las opciones estratégicas en reglas de usuarios prácticas y utilizables.

Toma en cuenta:

1. Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno es establecido por la Alta Gerencia y promueve a través del ejemplo.
2. Las directrices tecnológicas.
3. La Gerencia debe asegurar y monitorear la implementación y el cumplimiento de sus políticas.
4. El compromiso con la calidad. La Gerencia de la función de servicios de información, define, documenta y mantiene una filosofía de calidad debiendo ser comprendidos, implementados y mantenidos por todos los niveles de la función de servicios de información.
5. Las políticas de seguridad y control interno. La alta gerencia verifica que esta política de seguridad y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento de éstas.

❖ PO7 Administración de recursos humanos.

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

1. El reclutamiento y promoción. Tiene como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.
2. Los requerimientos de calificaciones. El personal debe estar calificado, tomando como base la educación, entrenamiento y/o experiencia apropiados, según se requiera.

3. La capacitación. Los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.
4. Evaluación objetiva del desempeño. Consiste en afirma que las evaluaciones sean llevadas a cabo regularmente según los estándares establecidos y las responsabilidades específicas del cargo. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

❖ PO8 Garantizar el cumplimiento de requisitos externos.

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales.

Para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos.

A tomar en cuenta:

1. Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continúo de los mismos.
2. Leyes, regulaciones y contratos.
3. Revisiones regulares en cuanto a cambios.
4. Búsqueda de asistencia legal y modificaciones.
5. Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.
6. Privacidad.
7. Propiedad intelectual.
8. Flujo de datos externos y criptografía.

❖ PO9 Evaluación de riesgos.

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

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

1. Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI (por ejemplo: tecnológicos, de seguridad, etc.) de manera que se pueda determinar la forma en que los riesgos deben ser manejados a un nivel aceptable.
2. Definición de alcances, limites de los riesgos y la metodología para las evaluaciones de los riesgos.
3. Actualización de evaluación de riesgos.
4. Metodología de evaluación de riesgos.
5. Medición de riesgos cualitativos y/o cuantitativos.
6. Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continúa.
7. Aceptación de riesgos, dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y que tan económico resulte implementar protecciones y controles.

❖ PO10 Administración de proyectos.

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

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

1. Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada propósito emprendido. La metodología cubre:
   - Asignación de responsabilidades.
   - Determinación de tareas.
   - Realización de presupuestos de tiempo y recursos.
   - Avances.
   - Puntos de revisión.
   - Aprobaciones.
2. El compromiso de los usuarios en el desarrollo, implementación o modificación de los proyectos.
3. Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.
4. Aprobación de las fases del proyecto por parte de los usuarios antes de pasar a la siguiente etapa.
5. Presupuestos de costos y horas hombre.
6. Planes y metodologías de garantía de calidad, los cuales son revisados y acordados por las partes interesadas.
7. Plan de administración de riesgos para minimizar o eliminar los riesgos.
8. Planes de prueba, entrenamiento, revisión post-implementación.

❖ PO11 Administración de calidad.

Objetivo: Satisfacer los requerimientos del cliente.

Consiste en realizar una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización, considerando:

1. Definición y mantenimiento regular del plan de calidad, el cual promueve una filosofía de mejoramiento continuo y contesta a las preguntas básicas qué, quién y cómo.
2. Responsabilidades de asegurar la calidad que determine los tipos de actividades de revisiones, auditorías, inspecciones, entre otros, que deban realizarse para alcanzar los objetivos del plan general de calidad.
3. Metodologías del ciclo de vida de desarrollo de sistemas que rija el proceso de avance, adquisición, implementación y mantenimiento de sistemas de información.
4. Documentación de pruebas de sistemas y programas.
5. Revisiones y reportes para asegura la calidad.

2. Adquisición e Implementación.

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

2.1. **Procesos**:

❖ AI1 Identificación de soluciones automatizadas.

Objetivo: Garantizar un enfoque que cumpla con los requerimientos del usuario.

Se basa en un análisis de las oportunidades alternativas comparadas con los requerimientos de los usuarios. Hay que tener presente:

1. Definición de requerimientos de información para aprobar un proyecto de desarrollo.
2. Estudios de factibilidad con la finalidad de satisfacer los requerimientos del negocio establecidos para el desarrollo de un proyecto.
3. Arquitectura de información considerando el modelo de datos al definir soluciones y analizar la factibilidad de las mismas.
4. Seguridad con relación al costo-beneficio. Controlar que dichos costos no excedan los beneficios.
5. En una auditoría, deben existir mecanismos adecuados. Éstos tienen que proporcionar la capacidad de proteger datos sensitivos, como por ejemplo, la identificación de usuarios contra la divulgación o el mal uso.
6. Contratación de terceros con el objeto de adquirir productos con buena calidad y excelente estado.
7. Aceptación de instalaciones y tecnologías a través de un contrato con el proveedor, donde se acuerda un plan de aceptación para las instalaciones y tecnologías especificas a ser proporcionada.

❖ AI2 Adquisición y mantenimiento del software aplicativo.

Objetivo: Proporciona funciones automatizadas que soporten efectivamente al negocio.

Se fundamenta en la definición de declaraciones específicas sobre requerimientos funcionales, operacionales y una implementación estructurada. Consta de:

1. Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.
2. Requerimientos de archivo, entrada, proceso y salida.
3. Interfase usuario-maquina asegurando que el software sea fácil de utilizar y que sea capaz de auto-documentarse.
4. Personalización de paquetes.

5. Realizar pruebas funcionales (unitarias, de aplicación, de integración, de carga y estrés), de acuerdo con el plan de prueba del proyecto y con los estándares establecidos, antes de ser aprobado por los usuarios.
6. Controles de aplicación y requerimientos funcionales.
7. Documentación (materiales de consulta y soporte para usuarios) con el objeto que los usuarios aprendan a utilizar el sistema y logren aclarar las inquietudes que se puedan presentar.

❖ AI3 Adquisición y mantenimiento de la infraestructura de software.

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

Consta de una evaluación del desempeño del hardware y software; la provisión de mantenimiento preventivo de hardware y la instalación; seguridad y control del software del sistema. Considera:

1. Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general.
2. Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.
3. Seguridad del software de sistema, instalación y mantenimiento para proteger la seguridad de datos y programas, ya almacenados en el mismo.

❖ AI4 Elaboración y mantenimiento de procedimientos.

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

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

1. Manuales de procedimientos de usuarios y controles, actualizados permanentemente para un mejor desempeño y control de los usuarios.
2. Manuales de operaciones y controles, que estén en permanente actualización.
3. Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

❖ AI5 Instalación y acreditación de sistemas.

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

Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas. Considera:

1. Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.
2. Conversión / carga de datos, que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.
3. Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.
4. Acreditar, que la Gerencia de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.
5. Revisiones post-implementación, con el objeto de reportar si el sistema proporciona los beneficios esperados de la manera más económica.

- AI6 Administración de cambios.

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

Se hace posible a través de un sistema de administración que permite el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual. Para esto se considera:

1. Identificación de cambios internos y parte de proveedores.
2. Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.
3. Evaluación del impacto que provocan los cambios.
4. Autorización de cambios.
5. Manejo de liberación de software que se rija por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.
6. Distribución de software, estableciendo medidas de control especificas para asegurar que la distribución de éste sea en el lugar correcto, con integridad y de manera oportuna.

3. Prestación y Soporte.

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, es preciso establecer los procesos de soportes necesarios. Este dominio incluye el procesamiento de datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

3.1. **Procesos**:

❖ Ds1 Definición y administración de niveles de servicio

Objetivo: Establecer una comprensión común del nivel de servicio requerido.

Para ello se establecen convenios de niveles de servicios que formalicen los criterios de desempeño con los cuales se medirá la cantidad y la calidad del servicio. Se basa en:

1. Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.
2. Definición de las responsabilidades de los usuarios y de la función de servicios de información.
3. Procedimientos de desempeños que aseguren que las responsabilidades sobre las relaciones que rigen el desempeño entre las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.
4. Definición de dependencias, asignando un Gerente de nivel de servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.
5. Provisiones para elementos sujetos a cargos en los acuerdos de niveles de servicio para hacer posibles comparaciones y decisiones, contra su costo.
6. Garantías de integridad.

7. Convenios de confidencialidad.
8. Implementación de un programa de mejoramiento del servicio.

❖ Ds2 Administración de servicios de terceros.

Objetivo: Asegurar que las tareas y responsabilidades de terceros estén claramente definidas, logrando satisfacer los requerimientos.

Se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización. Se fundamenta en:

1. Acuerdos de servicios con terceros a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones, según sea apropiado.
2. Acuerdos de confidencialidad. El contrato se define y acuerda para cada relación de servicio con un proveedor.
3. Requerimientos legales regulatorios, que concuerde con los compromisos de seguridad identificados, declarados y acordados.
4. Monitoreo de la entrega de servicio, con el fin de asegurar el cumplimiento de los acuerdos de contrato.

❖ Ds3 Administración de desempeño y capacidad.

Objetivo: Asegurar que la capacidad adecuada esté disponible y que se proceda a efectuar el mejor uso de ella para alcanzar el desempeño deseado.

Se efectúan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos. Consta de:

1. Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información.
2. Monitoreo y reporte de los recursos de tecnología de información.
3. Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.
4. Administración de capacidad, establece un proceso de planeación para la revisión del desempeño y capacidad de hardware con el fin de asegurar que exista una capacidad razonable económica para procesar cargas de trabajo con cantidad y calidad de desempeño.
5. Evitar que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativa de recursos y de prioridad de tareas.

Monitoreo:

- Ds4 Garantizar servicio continuo

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

Para ello se tiene un plan de continuidad, probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con sus requerimientos. Se base en:

1. Planificación de severidad
2. Plan documentado
3. Procedimientos alternativos
4. Respaldo y recuperación
5. Pruebas y entrenamientos sistemáticos y singulares

❖ Ds5 Garantizar seguridad de sistemas

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

Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas esté restringido a usuarios autorizados.

Se debe considerar:

1. Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI. Se debe restringir a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso.
2. Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión y suspensión de cuentas de usuario.
3. Administración de llaves criptográficas implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas.
4. Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos.
5. Prevención y detección de virus, por ejemplo, caballos de troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.
6. Utilización de Firewalls si existe una conexión de internet u otras redes públicas en la organización.

❖ Ds6 Identificación y asignación de costos.

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

Se base en un sistema de contabilidad de costos que asegura que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y toma en consideración:

1. Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios.
2. Procedimientos y políticas de cargo para fomentar el uso apropiado de los recursos de cómputo y asegurar el trato justo de los departamentos de usuarios y sus necesidades.
3. Tarifas definiendo e implementando procedimientos de costeo de prestación de servicios, para ser analizados, monitoreados, evaluados asegurar la economía.

❖ Ds7 Educación y entrenamiento de usuarios.

Objetivo: Asegurar que los usuarios hagan un uso efectivo de la tecnología y sean conscientes de los riesgos y responsabilidades involucrados.

Para ello se realiza un plan completo de entrenamiento y desarrollo. Se tiene en cuenta:

1. Currículo de entrenamiento el cual establece y mantiene procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información.
2. Campañas de concientización, definir los grupos objetivos, asignar entrenadores y organizar oportunamente las sesiones de entrenamiento.

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

❖ Ds8 Ayuda y asesoría a clientes

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

Se efectúa un centro de ayuda que proporcione soporte y asesoría de primera línea. Toma en consideración:

1. Consultas de usuarios y respuesta a problemas estableciendo un soporte de función de buró de ayuda.
2. Monitoreo de consultas y despacho estableciendo procedimientos que aseguren que las preguntas de los clientes puedan ser resueltas, siendo reasignadas al nivel adecuado para atenderlas.
3. Análisis y reporte de tendencias, adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias.

❖ Ds9 Administración de la configuración.

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

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

1. Registro de activos estableciendo procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de adquisición.
2. Administración de cambios en la configuración asegurando que los registros de configuración reflejen el estatus real de todos los elementos de la configuración.
3. Chequeo de software no autorizado revisando periódicamente las computadoras personales de la organización.
4. Controles de almacenamiento de software definiendo un área de almacenamiento de archivos para todos los elementos de software válidos en las fases del ciclo de vida del desarrollo del sistemas.

❖ Ds10 Administración de problemas e incidentes.

Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder.

Se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento para resolver de manera eficiente los problemas identificados. Este sistema de administración de problemas realiza un seguimiento de las causas a partir de un incidente dado.

❖ Ds11 Administración de datos

Objetivo: Certificar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento, lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia debe diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.

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

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

- Ds12 Administración de instalaciones

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

- Ds13 Administración de operaciones.

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

Se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia establece y documenta procedimientos para las operaciones de

tecnología de información (incluyendo operaciones de red), los cuales son revisados periódicamente para garantizar su eficiencia y cumplimiento.

4. **Monitoreo**.

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

4.1. **Procesos**:

- M1 Monitorear los procesos

Objetivo: Confirmar el logro de los objetivos establecidos para los procesos de TI. Esto se logra, definiendo por parte de la gerencia, reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte, así como la atención regular a los reportes emitidos.

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

- M2 Evaluar suficiencia de controles internos.

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

La gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias. Evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo revisa la existencia de puntos vulnerables y problemas de seguridad.

- M3 Recabar aseguramiento independiente.

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

La gerencia obtiene una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego la gerencia adopta como trabajo rutinario, hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios y además asegurar el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

- M4 Brincar auditorías independientes

Objetivo: Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes, desarrolladas a intervalos regulares de tiempo. Para ello, la gerencia establece los estatutos para la función de auditoria, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoria. El auditor debe ser independiente del auditado, esto significa que los auditores no tienen que estar relacionados con la sección o departamento que esté siendo auditado y, en lo posible, ser independiente de la propia empresa. Esta auditoría

deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir, que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de auditoría.

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

Para ello, los 34 procesos propuestos se concretan en 32 objetivos de control detallados anteriormente. Para entender este punto, se define por Control a “las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos empresariales se alcancen y que los eventos no deseados se prevean o se detecten, y corrijan”.

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

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

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

5. Aplicación de la norma COBIT.

A continuación, se analiza cómo aplicar las Normas COBIT en una organización, para ello se utiliza una guía de auditoría presentada en la página web www.isaca.org, la misma indica los pasos a seguir para auditar cada uno de los procesos de TI de la norma. Este reporte se confecciona dándole el formato de un informe de auditoría:

- Informe de Auditoría:

  - Entidad Auditada: Colegio Particular Pumanque, San Felipe
  - Alcance de la Auditoría: Esta auditoría comprende el área de Recursos Humanos del Colegio Particular Pumanque, con respecto al cumplimiento del proceso “Administración de Recursos Humanos” de la norma COBIT.
  - Norma Aplicada: COBIT, específicamente el proceso de TI Po7 “Administración de Recursos Humanos”
  - Relevamiento:

- Organización: Colegio Particular Pumanque, brinda un servicio de educación a niños de nivel básico y medio.

- Objetivos de la Organización:

  - Ofrecer el servicio de una excelente educación con orientación bilingüe (Español - Inglés), artístico, deportivo y ecológico en forma personalizada a los niños de nivel básico y medio, y obtener por el servicio un beneficio monetario acorde a las ofertas educativas que brinda la Institución.
  - Incrementar cada año el número de inscritos para obtener mayor rentabilidad y ampliar la comunidad educativa.

- Transmitir a la comunidad en general el perfil institucional y los beneficios que los alumnos obtienen por una educación personalizada.

Departamento de administración de personal: Comprende todo lo relacionado con el desarrollo y administración de políticas y programas que provean una estructura organizativa eficiente, empleados calificados, tratamiento equitativo, oportunidades de progreso, satisfacción en el trabajo y adecuada seguridad de empleo.

Depende de la Gerencia de Administración.

Políticas y Estrategias del Departamento de Administración de Personal

Objetivo: Perfeccionar al personal acorde al perfil Institucional.

- Seleccionar docentes que respondan a los requerimientos del proyecto educativo institucional.

- Realizar durante la selección de personal talleres de capacitación y evaluación de inteligencia emocional y desarrollo de la persona.

- Seleccionar docentes con buenas referencias.

- Los docentes de asignaturas especiales (plástica, música, deportes, etc.) deben tener experiencias mínimas en más de una escuela y estar avalados con referencias por escrito.

- Respetar las decisiones personales de los docentes y no docentes.

- Antes que una persona forme parte de la institución debe conocer y firmar las Normativas Institucionales, donde se especifican todas las medidas, deberes y derechos de todo el personal docente y no docente.

- La dirección general realiza periódicamente evaluaciones del rendimiento de trabajo individual y grupal mediante entrevistas. (Grupales y personales).

Educativas

Objetivo: Lograr una excelencia educativa

- Brindar una educación excelencia y personalizada

- Confeccionar un Proyecto Educativo Institucional (PEI) con los objetivos que cubran las orientaciones bilingüe, deportiva, ecológica y artística.

- Realizar periódicamente talleres de capacitación docente a nivel institucional donde se promueva la inteligencia emocional y el desarrollo personal.

- La Dirección académica debe evaluar constantemente, el trabajo de los docentes y entregar los informes a la dirección general.

Funciones – Subfunciones - Tareas:

1. Realizar el Reclutamiento: lograr que todos los puestos estén cubiertos por personal competente que cubran el perfil institucional por un costo razonable.

   a) Buscar los postulantes (docentes y no docentes)

      - Análisis de las necesidades del cargo.
      - Desarrollo de especificaciones de trabajo.
      - Análisis de las fuentes de empleados potenciales.
      - Atracción de los posibles postulantes.

b) Realizar el proceso de selección: Análisis de la capacidad de los aspirantes para decidir cual tiene mayores posibilidades.

- ❖ Entrevistar a los postulantes.
- ❖ Realizar talleres de Pruebas de inteligencia emocional.
- ❖ Evaluación de los postulantes sobre la base de resultados de los talleres.
- ❖ Confección y entrega de los diferentes tipos de contratos de trabajo (contratos temporales, a plazo fijo, contratos de prueba, pasantías, etc.).

c) Instrucción y entrega de materiales: Entrenamiento, información y entrega de materiales necesarios a los empleados contratados (o nuevos) para que cumplan sus obligaciones eficientemente.

- ❖ Orientación de los nuevos empleados mediante talleres de capacitación y entrega de documentación con las normativas (reglas con las que se rige la institución).
- ❖ Seguimiento de la actuación de los empleados (antiguos y nuevos).
- ❖ Compra de materiales didácticos u otros servicios para entregar a los docentes con el objetivo que puedan dictar sus clases en forma eficiente.

d) Despidos: Terminación legal de las relaciones con los empleados en la forma más beneficiosa para ellos y el colegio.

- ❖ Realización de la entrevista de egreso.
- ❖ Análisis de las bajas.

e) Determinar los servicios sociales para los empleados.

- ❖ Determinación de servicio médicos y otros para los empleados (y alumnos) que cubran la seguridad e integridad física del personal dentro de la organización.
- ❖ Prepara la documentación para la gestión de obras sociales del personal.

2. Administrar sueldos y jornales: lograr que todos los empleados estén remunerados en forma adecuada, equitativa y con horarios justos.

a) Clasificar la posición, responsabilidades y requerimientos de los empleados.

- ❖ Preparación de las normativas institucionales donde están las especificaciones de trabajo.
- ❖ Revisión periódica y corrección de las normativas.
- ❖ Fijar los valores monetarios de los cargos en forma justa y equitativa, respecto a otros cargos en el colegio y a cargos similares en el mercado de trabajo.
- ❖ Efectuar los pagos correspondientes a los sueldos mensuales (el pago y entrega de recibos de sueldo se efectúa en la propia institución).

b) Control de Horarios: Fijación de horas de trabajo y periodos de inasistencia con goce de haberes o sin él, que sean justos tanto para el empleado como para el colegio.

- ❖ Planificación y administración de políticas sobre horarios de trabajos e inasistencias.
- ❖ Planificación y administración de planes de vacaciones.

3. Promocionar las Relaciones institucionales: Asegurar que las relaciones de trabajo entre la dirección general y los empleados, al igual que la satisfacción en el trabajo y oportunidad de progreso del personal, sean desarrollados y mantenidos siguiendo los mejores intereses del colegio y de los empleados. También, su función es la de desarrollar proyectos de Relaciones Institucionales con el medio externo (otras instituciones escolares, clubes, etc.).

a) Realizar negociaciones colectivas: Lograr concordancia con las organizaciones de empleados reconocidas oficialmente y establecidas legalmente, de la manera que mejor contemple los intereses de la escuela y los docentes.

- ❖ Negociación de convenios.
- ❖ Interpretación y administración de estos.

b) Controlar la disciplina del personal.

- ❖ Fijar reglas de conducta y disposiciones mediante las normativas institucionales.
- ❖ Establecer y administrar las medidas disciplinarias con respecto a inasistencias injustificadas.

c) Investigación de Personal.

- ❖ Investigación de referencias de trabajos anteriores.
- ❖ Confirmar las referencias y otras documentaciones a la administración general.
- ❖ Investigar y verificar la documentación presentada por los empleados que luego conformaran el legajo de los mismos (títulos oficiales, registración en la Junta de clasificaciones, etc.).

4. Generar Informes.

Confeccionar todos los informes mensuales, semestrales y anuales con las estadísticas, resúmenes, etc. de las gestiones administrativas del personal.

a) Diagnóstico:

De acuerdo con el Dominio “Planificación y Organización” y el Proceso “Administración de Recursos Humanos”, se desarrolló un análisis en donde se identifican aquellas normas que se están cumpliendo y aquellas que no, definiéndose desde ahí acciones a seguir por la escuela para cumplir con las normas COBIT.

La organización COLEGIO PARTICULAR PUMANQUE, de acuerdo a lo revelado, muestra un adecuado nivel de ajuste a las normas COBIT en cuanto al proceso en cuestión, puesto que la misma cumple con las siguientes actividades o tareas del mismo:

- Reclutamiento y Promoción personal, ya que la Dirección evalúa regularmente los procesos para asegurar que las prácticas de reclutamiento y promoción de personal tengan excelentes resultados, considerando factores como la educación del personal, la experiencia y la responsabilidad.

- Personal Calificado, puesto que verifica que el personal que lleva tareas específicas esté capacitado y, para ello, se realizan talleres docentes.

- Entrenamiento de Personal, dado a que en cuanto ingresa el personal y durante su permanencia en el establecimiento tiene a su disposición toda la información que necesita, así como también

la permanente capacitación. Es importante destacar que no existe un manual de funciones, ni de procedimientos, por lo cual los empleados pueden tener dudas con respecto a ellas.

- Evaluación de Desempeño de los Empleados, debido a que el establecimiento implementa un proceso de evaluación de desempeño de los empleados y asesora a los mismos sobre su rendimiento o conducta de manera apropiada. Aunque las evaluaciones de rendimiento no están definidas formalmente y, por ende, se puede llegar a tener problemas por la subjetividad de la persona que está evaluando el desempeño.

- Cambios de Cargos y Despido, puesto que cuando se toman tales acciones se trata de que sean oportunas y apropiadas, de tal manera que los controles internos y la seguridad no se vean perjudicados por estos eventos.

Es importante destacar que COLEGIO PARTICULAR PUMANQUE tiene dificultades en cuanto a:

- Respaldo de Personal, puesto que no cuenta con suficiente personal de respaldo para solucionar posibles ausencias. Tampoco el personal encargado de cargos delicados como por ejemplo el tesorero cuando toma vacaciones interrumpidas con duración suficiente como para probar la habilidad de la organización para manejar casos de ausencia y detectar actividades fraudulentas.

- Procedimientos de Acreditación de Personal, ya que las investigaciones de seguridad asociada a la contratación no son llevadas a cabo.

b) Conclusiones:

Por lo tanto, podemos especificar que para que el colegio cumpla con las normas COBIT en cuanto al proceso “Administración de Recursos Humanos” debe considerar:

1. Realizar manuales de funciones, de manera que estén definidos todos los cargos y sus correspondientes funciones.
2. Realizar manuales de Procedimientos, de manera que los empleados puedan identificar cuáles son las tareas que deben realizar de acuerdo a su cargo y funciones.
3. Establecer Procedimientos de Acreditación, ya que de lo contrario se pueden tener serios problemas por no haber realizado correctamente las investigaciones de seguridad.
4. Proporcionar un entrenamiento “cruzado” de manera de tener personal de respaldo con la finalidad de solucionar posibles ausencias, debido a que la escuela no puede contar con suficiente personal por su economía actual.
5. Definir y publicar formalmente las evaluaciones de rendimiento, de manera de aplicarlas a la hora de hacer la evaluación de desempeño para evitar problemas con el personal docente y no docente.

Problema

En las organizaciones modernas, tanto públicas como privadas, la misión de las tecnologías de la información es facilitar la consecución de sus objetivos estratégicos. Para ello, se invierte una considerable cantidad de recursos en personal, equipos y tecnología, además de los costos derivados de la posible organización estructural que muchas veces conlleva la introducción de estas tecnologías. Esta importante inversión debe ser constantemente justificada en términos de eficacia y eficiencia. Por tanto, el propósito a alcanzar por una empresa que contrata la auditoria de cualquier parte de sus SI es asegurar que sus objetivos estratégicos son los mismos que los de la propia organización y que los sistemas prestan el apoyo adecuado a la consecución de estos objetivos, tanto en el presente como en su evolución futura.

La presente tesis busca exponer las normas COBIT de manera simple y comprensible, a través de la aplicación de ésta en el Colegio Particular Pumanque de la quinta región durante el segundo semestre del 2008 y parte del primer semestre del 2009.

Objetivos

- Verificar el control de la función informática, asegurando a la alta dirección y al resto de las áreas de la empresa que la información que les llega es la necesaria en el momento oportuno, y es fiable, ya que les sirve de base para tomar decisiones importantes.

- Detectar y prevenir fraudes por manipulación de la información o por accesos de personas no autorizadas a transacciones que exigen traspaso de fondos.

- Ayudar en la creación de manuales necesarios para que las funciones a realizar se encuentren ceñidas bajo las normas COBIT.

Conclusiones

La presente investigación consiste en exponer las normas COBIT de manera simple y comprensible, a través de la aplicación de ésta en el Colegio Particular Pumanque de la quinta región en el área de recursos humanos.

Al respecto, puede decirse que de acuerdo con el Dominio “Planificación y Organización” y el Proceso “Administración de Recursos Humanos”, se desarrolló un análisis en donde se identifican aquellas normas que se están cumpliendo y aquellas que no, definiéndose desde ahí acciones a seguir por la escuela para cumplir con las normas COBIT.

La organización COLEGIO PARTICULAR PUMANQUE, de acuerdo a lo revelado en el informe de auditoría, muestra un adecuado nivel de ajuste a las normas COBIT en cuanto al proceso en cuestión, puesto que la misma cumple con las siguientes actividades o tareas del mismo:

- Reclutamiento y Promoción personal, ya que la Dirección evalúa regularmente los procesos para asegurar que las prácticas de reclutamiento y promoción de personal tengan excelentes resultados, considerando factores como la educación del personal, la experiencia y la responsabilidad.

- Personal Calificado, puesto que verifica que el personal que lleva tareas específicas esté capacitado y, para ello, se realizan talleres docentes.

- Entrenamiento de Personal, dado a que en cuanto ingresa el personal y durante su permanencia en el establecimiento tiene a su disposición toda la información que necesita, así como también la permanente capacitación. Es importante destacar que no existe un manual de funciones, ni de

procedimientos, por lo cual los empleados pueden tener dudas con respecto a ellas.

- Evaluación de Desempeño de los Empleados, debido a que el establecimiento implementa un proceso de evaluación de desempeño de los empleados y asesora a los mismos sobre su rendimiento o conducta de manera apropiada. Aunque las evaluaciones de rendimiento no están definidas formalmente y, por ende, se puede llegar a tener problemas por la subjetividad de la persona que está evaluando el desempeño.

- Cambios de Cargos y Despido, puesto que cuando se toman tales acciones se trata de que sean oportunas y apropiadas, de tal manera que los controles internos y la seguridad no se vean perjudicados por estos eventos.

Es importante destacar que COLEGIO PARTICULAR PUMANQUE tiene dificultades en cuanto a:

- Respaldo de Personal, puesto que no cuenta con suficiente personal de respaldo para solucionar posibles ausencias. Tampoco el personal encargado de puestos delicados como ser el Tesorero toma vacaciones interrumpidas con duración suficiente como para probar la habilidad de la organización para manejar casos de ausencia y detectar actividades fraudulentas.

- Procedimientos de Acreditación de Personal, ya que las investigaciones de seguridad asociada a la contratación no son llevadas a cabo.

Por lo tanto, podemos especificar que, para que el establecimiento educacional cumpla con las normas COBIT en cuanto al proceso “Administración de Recursos Humanos”, debe:

1. Realizar manuales de funciones, de manera que estén definidos todos los cargos de trabajo y sus correspondientes funciones.
2. Realizar manuales de procedimientos, de manera que los empleados puedan identificar cuáles son las tareas que deben realizar de acuerdo a su cargo y funciones.
3. Establecer procedimientos de acreditación, ya que de lo contrario se pueden tener serios problemas por no haber realizado correctamente las investigaciones de seguridad.
4. Proporcionar un entrenamiento “cruzado” de manera de tener personal de respaldo con la finalidad de solucionar posibles ausencias, ya que la escuela no puede contar con suficiente personal por su economía actual.
5. Definir y publicar formalmente las evaluaciones de rendimiento, de manera de aplicarlas a la hora de hacer la evaluación de desempeño para evitar problemas con el personal docente y no docente.

Bibliografía

Libros:

1. Cooper & Librand S.A. (1992), Informe COSO. Instituto de Auditores Internos. España.
2. COBIT, cuerpo metodológico aplicado como apoyo al control de los recursos de Tecnologías de Información en instituciones financieras y gubernamentales. Universidad Católica Cardenal Silva Henríquez. Santiago 2003.
3. Gestión de riesgos corporativos – Marco integrado. Técnicas de aplicación. Septiembre 2004. Committee of Sponsoring Organizations of the Treadway Commission (COSO).
4. Organización Internacional para la Estandarización ISO/IEC 2700.
5. Manual de revisión CISA, ISACA, 2006.
6. Objetivos de control de TI para Sarbanes-Oxley: El rol de la TI en el diseño e implementación de controles internos sobre informes financieros, 2ª edición, instituto de gobierno de gobierno de TI, USA, 2006.
7. Seguridad de Información (ISF). El estándar de buenas prácticas para la seguridad de la información. 2003.

Apuntes:

1. Apuntes tomados en cátedras de la carrera de auditoria en la Universidad Católica Cardenal Raúl Silva Henríquez.

Internet:

1. www.cibertesis.cl
2. www.isaca.org/cobit
3. www.pdffactory.com
4. www.isacachile.cl/cobit.htm
5. www.monografias.com

Mail:

1. pcaneo@ultramar.cl
2. papeshop@hotmail.com

Glosario

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

Calidad: La totalidad de las características de un producto o servicio que le confieren aptitud para satisfacer necesidades establecidas e implícitas.

Capacidad: Contar con los atributos necesarios para realizar o lograr. CEO— Director ejecutivo.

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

COBIT: (Control Objectives for Information Systems and related Technology) Significa Objetivos de Control para Tecnología de Información y Tecnologías relacionadas. Es un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.

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

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

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

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

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

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

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

Diccionario de datos empresarial: El nombre, tipo, rango de valores, fuente, sistema de registro, y autorización de acceso para cada elemento de datos utilizado en la empresa. Indica cuáles programas aplicativos usan esos datos, de tal forma que cuando se contemple una estructura de datos, se pueda generar una lista de los programas afectados. Ver PO2.2.

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

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

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

Eficacia: Logro de los objetivos propuestos. Coherencia entre objetivos y resultados.

Eficiencia: Buen uso y administración de los recursos empleados en un trabajo. Rentabilidad de los recursos utilizados respecto a los resultados obtenidos.

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

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

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

Framework: Es una estructura de soporte definida mediante la cual otro proyecto de software puede ser organizado y desarrollado. Típicamente, puede incluir soporte de programas, bibliotecas y un lenguaje interpretado entre otros software para ayudar a desarrollar y unir los diferentes componentes de un proyecto.

Información: Es un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno.

Information Warfare (Guerra de Información): Consiste en las acciones destinadas a proteger, explotar, corromper, negar, o destruir la información o los recursos de información a fin de lograr una ventaja significativa, objetiva, o la victoria frente a un competidor.

IT Governance (Gobernabilidad TI): Se refiere a la administración y regulación de los sistemas de información que establece una compañía para el logro de sus objetivos.

Madurez: Indica el grado de confiabilidad o dependencia que el negocio puede tener en un proceso, al alcanzar las metas y objetivos deseados.

Marco de control: Una herramienta para los dueños de los procesos de negocio que facilita la descarga de sus responsabilidades a través de la procuración de un modelo de control de soporte.

Modelo de madurez de la capacidad (CMM): El modelo de madurez de la capacidad para software (CMM), del Instituto de Ingeniería de Software (SEI), es un modelo utilizado por muchas organizaciones para identificar las mejores prácticas, las cuales son convenientes para ayudarles a evaluar y mejorarla madurez de su proceso de desarrollo de software.

Objetivo de control: Una declaración del resultado o propósito que se desea alcanzar al Implementar procedimientos de control en un proceso en particular.

Organización: La manera en que una empresa está estructurada.

Plan estratégico de TI: Un plan a largo plazo, en el cual la gerencia del negocio y de TI describen de forma cooperativa cómo los recursos de TI contribuirán a los objetivos estratégicos empresariales (metas).

Plan táctico de TI: Un plan a mediano plazo, Ej., con un horizonte de seis a dieciocho meses, que traduzca la dirección del plan estratégico de TI en las iniciativas requeridas, requisitos de recursos y formas en las que los recursos y los beneficios serán supervisados y administrados.

Política: Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por los equipos gerenciales de la empresa. Además del contenido de la política, esta debe describir las consecuencias de la falta de cumplimiento de la misma, el mecanismo para manejo de excepciones y la manera en que se verificará y medirá el cumplimiento de la política.

Portafolio: Una agrupación de programas, proyectos, servicios o activos seleccionados, administrados y vigilados para optimizar el retorno sobre la inversión.

Práctica de control: Mecanismo clave de control que apoya el logro de los objetivos de control por medio del uso responsable de recursos, la administración apropiada de los riesgos y la alineación de TI con el negocio.

Problema: Causa subyacente desconocida de uno o más incidentes.

Procedimiento: Una descripción de una manera particular de lograr algo; una forma establecida de hacer las cosas; una serie de pasos que se siguen en un orden regular definido, garantizando un enfoque consistente y repetitivo hacia las actividades.

Proceso: Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toma las entradas provenientes de un número de fuentes, incluyendo otros procesos, manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, dueños responsables, roles claros y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño.
Programa: Una agrupación estructurada de proyectos independientes que incluye el alcance completo del negocio, del proceso, de las personas, de la tecnología y las actividades organizacionales que se requieren (tanto necesarias como suficientes) para lograr un resultado de negocios claramente especificado.

Propietario de datos: Individuo por lo general gerentes o directores, que tienen la responsabilidad de la integridad, el uso y el reporte preciso de los datos computarizados.

Proveedor de servicios: Organización externa que presta servicios a la organización.

Proyecto: Un conjunto estructurado de actividades relacionadas con la entrega de una capacidad definida a la organización (la cual es necesaria, aunque no

suficiente para lograr un resultado de negocios requerido) con base en un cronograma y presupuesto acordado.

Riesgo: El potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia.

Segregación/separación de tareas: Un control interno básico que previene y

Tecnología: Rama del conocimiento que comprende la concepción y la utilización de las técnicas. La transferencia de tecnología corresponde a la circulación del saber y de la información.

TIC (Tecnologías de la Información y la Comunicación): Son un conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario.

TCO: Costo total de la propiedad. En TI incluye:

- Costo original del ordenador y del software.
- Actualizaciones de hardware y software.
- Mantenimiento.
- Soporte técnico.
- Entrenamiento.
- Ciertas actividades desarrolladas por los usuarios.

TI: Tecnología de información. Es el estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras. Se ocupa del uso de las computadoras y su software para convertir, almacenar, proteger, procesar, transmitir y recuperar la información.

Usuario: Una persona que utiliza los sistemas empresariales.

Apéndice I

Dominios, procesos y objetivos de control.

PLANEACIÓN Y ORGANIZACIÓN	PLANEACIÓN Y ORGANIZACIÓN
PO1.Definición de un Plan Estratégico de Tecnología de Información.	**P03.Determinación de la dirección tecnológica.**
1.1.Tecnología de Información como parte del Plan de la Organización a corto y largo plazo. 1.2.Plan a largo plazo de Tecnología de Información. 1.3.Plan a largo plazo de Tecnología de Información - Enfoque y Estructura 1.4.Cambios al Plan a largo plazo de Tecnología de Información. 1.5.Planeación a corto plazo para la	3.1.Planeación de la Infraestructura Tecnológica. 3.2.Monitoreo de Tendencias y Regulaciones Futuras. 3.3.Contingencias en la Infraestructura Tecnológica. 3.4.Planes de Adquisición de Hardware y Software. 3.5.Estándares de Tecnología.

función de Servicios de Información. 1.6.Evaluación de sistemas existentes. **P02.Definición de la Arquitectura de Información** 2.1.Modelo de la Arquitectura de Información. 2.2.Diccionario de Datos y Reglas de cinta de datos de la corporación. 2.3.Esquema de Clasificación de Datos 2.4.Niveles de Seguridad **PLANEACIÓN Y ORGANIZACIÓN** **P04.Definición de la Organización y de las Relaciones de TI** 4.7. Propiedad y Custodia. 4.8. Propiedad de Datos y Sistemas. 4.9. Supervisión. 4.10. Segregación de Funciones. 4.11. Asignación de Personal para Tecnología de Información. 4.12. Descripción de Puestos para el Personal de la Función de TI. 4.13. Personal clave de TI. 4.14. Procedimientos para personal por contrato Administración de Proyectos. 4.15. Relaciones. **P05.Manejo de la Inversión en Tecnología de Información**	**P04.Definición de la Organización y de las Relaciones de TI** 4.1.Comité de planeación o dirección de la función de servicios de información 4.2.Ubicación de los servicios de información en la organización 4.3.Revisión de Logros Organizacionales 4.4.Funciones y Responsabilidades 4.5.Responsabilidad del aseguramiento de calidad 4.6.Responsabilidad de la seguridad lógica y física. **PLANEACIÓN Y ORGANIZACIÓN** **P06.Comunicación de la dirección y aspiraciones de la gerencia.** 6.3. Comunicación de las Políticas de la Organización. 6.4.Recursos para la implementación de Políticas 6.5.Mantenimiento de Políticas 6.6.Cumplimiento de Políticas, Procedimientos y Estándares 6.7.Compromiso con la Calidad 6.8.Política sobre el Marco de Referencia para la Seguridad y el Control Interno 6.9.Derechos de propiedad intelectual 6.10.Políticas Específicas 6.11.Comunicación de Conciencia de Seguridad en TI **P07.Administración de Recursos Humanos**

5.1. Presupuesto Operativo Anual para la Función de Servicio de información. 5.2. Monitoreo de Costo – Beneficio. 5.3. Justificación de Costo – Beneficio. **P06.Comunicación de la dirección y aspiraciones de la gerencia** 6.1. Ambiente positivo de control de la información. 6.2. Responsabilidad de la Gerencia en cuanto a Políticas. **PLANEACIÓN Y ORGANIZACIÓN** **P07.Administración de Recursos Humanos** 7.7.Cambios de Puesto y Despidos. **P08.Aseguramiento del Cumplimiento de Requerimientos Externos** 8.1. Revisión de Requerimientos Externos. 8.2.Prácticas y Procedimientos para el Cumplimiento de Requerimientos Externos 8.3. Cumplimiento de los Estándares de Seguridad y Ergonomía. 8.4. Privacidad, Propiedad Intelectual y Flujo de Datos. 8.5. Comercio Electrónico. 8.6. Cumplimiento con Contratos de Seguros.	7.1. Reclutamiento y Promoción de Personal. 7.2. Personal Calificado. 7.3. Entrenamiento de Personal. 7.4. Entrenamiento Cruzado o Respaldo de Personal. 7.5. Procedimientos de Acreditación de Personal. 7.6. Evaluación de Desempeño de los Empleados. **PLANEACIÓN Y ORGANIZACIÓN** **P010.Administración de proyectos.** 10.1. Marco de Referencia para la Administración de Proyectos. 10.2. Participación del Departamento Usuario en la Iniciación de Proyectos. 10.3. Miembros y Responsabilidades del Equipo del Proyecto. 10.4. Definición del Proyecto. 10.5. Aprobación del Proyecto. 10.6. Aprobación de las Fases del Proyecto. 10.7. Plan Maestro del Proyecto. 10.8. Plan de Aseguramiento de la Calidad de Sistemas. 10.9. Planeación de Métodos de Aseguramiento. 10.10. Administración Formal de Riesgos de Proyectos. 10.11. Plan de Prueba. 10.12. Plan de Entrenamiento. 10.13. Plan de Revisión Post

P09.Evaluación de Riesgos 9.1. Evaluación de Riesgos del Negocio. 9.2. Enfoque de Evaluación de Riesgos. 9.3. Identificación de Riesgos. 9.4. Medición de Riesgos. 9.5. Plan de Acción contra Riesgos. 9.6. Aceptación de Riesgos. **PLANEACIÓN Y ORGANIZACIÓN** **PO11.Administración de Calidad** 11.04. Revisión de Aseguramiento de Calidad sobre el Cumplimiento de Estándares y Procedimientos de la Función de Servicios de Información. 11.05. Metodología del Ciclo de Vida de Desarrollo de Sistemas. 11.06. Metodología del Ciclo de Vida de Desarrollo de Sistemas para Cambios Mayores a la Tecnología Actual. 11.07. Actualización de la Metodología del Ciclo de Vida de Desarrollo de Sistemas. 11.08. Coordinación y Comunicación. 11.09. Marco de Referencia de Adquisición y Mantenimiento para la Infraestructura de Tecnología. 11.10. Relaciones con Terceras Partes como Implementadores. 11.11. Estándares para la Documentación de Programas. 11.12.Estándares para Pruebas de	Implementación. **PO11.Administración de Calidad** 11.1. Plan General de Calidad. 11.2. Enfoque de Aseguramiento de Calidad. 11.3. Planeación del Aseguramiento de Calidad. **PLANEACIÓN Y ORGANIZACIÓN** **PO11.Administración de Calidad** 11.17. Revisión del Aseguramiento de Calidad sobre el Logro de los Objetivos de la Función de Servicios de Información. 11.18. Métricas de Calidad. 11.19. Reportes de Revisiones de Aseguramiento de la Calidad.

Programas 11.13.Estándares para Pruebas de Sistemas 11.14.Pruebas Piloto/En Paralelo 11.15.Documentación de las Pruebas del Sistema 11.16. Evaluación del Aseguramiento de la Calidad sobre el Cumplimiento de Estándar de Desarrollo.	
ADQUISICIÓN E IMPLEMENTACIÓN **AI1.Identificación de Soluciones**	**ADQUISICIÓN E IMPLEMENTACIÓN** **AI2.Adquisición y Mantenimiento de Software de Aplicación.**
1.01. Definición de Requerimientos de Información. 1.02. Formulación de Acciones Alternativas. 1.03. Formulación de Estrategias de Adquisición. 1.04.Requerimientos de Servicios de Terceros 1.05.Estudio de Factibilidad Tecnológica 1.06.Estudio de Factibilidad Económica 1.07.Arquitectura de Información 1.08.Reporte de Análisis de Riesgos 1.09.Controles de Seguridad Económicos 1.10.Diseño de Pistas de Auditoría 1.11.Ergonomía 1.12.Selección de Software de Sistema 1.13.Control de Abastecimiento 1.14.Adquisición de Productos de Software 1.15.Mantenimiento de Software de Terceras Partes 1.16.Contratos de Programación de	2.01. Métodos de Diseño. 2.02. Cambios Significativos a Sistemas Actuales. 2.03. Aprobación del Diseño. 2.04. Definición y Documentación de Requerimientos de Archivos. 2.05. Especificaciones de Programas. 2.06. Diseño para la Recopilación de Datos Fuente. 2.07.Definición y Documentación de Requerimientos de Entrada de Datos 2.08.Definición de Interfases 2.09.Interfases Usuario-Máquina 2.10.Definición y Documentación de Requerimientos de Procesamiento 2.11.Definición y Documentación de Requerimientos de Salida de Datos 2.12.Controlabilidad 2.13.Disponibilidad como Factor Clave de Diseño

Aplicaciones 1.17.Aceptación de Instalaciones 1.18.Aceptación de Tecnología	2.14.Estipulación de Integridad de TI en programas de software de aplicaciones 2.15.Pruebas de Software de Aplicación 2.16.Materiales de Consulta y Soporte para Usuario 2.17.Reevaluación del Diseño del Sistema
ADQUISICIÓN E IMPLEMENTACIÓN **AI3.Adquisición y Mantenimiento de Arquitectura de Tecnología.** 3.01. Evaluación de Nuevo Hardware y Software. 3.02. Mantenimiento Preventivo para Hardware. 3.03. Seguridad del Software del Sistema. 3.04. Instalación del Software del Sistema. 3.05.Mantenimiento del Software del Sistema. 3.06.Controles para Cambios del Software del Sistema. **AI4.Desarrollo y Mantenimiento de Procedimientos relacionados con Tecnología de Información** 4.01.Futuros Requerimientos y Niveles de Servicios Operacionales 4.02.Manual de Procedimientos para Usuario 4.03.Manual de Operación 4.04.Material de Entrenamiento	**ADQUISICIÓN E IMPLEMENTACIÓN** **AI5.Instalación y Acreditación de Sistemas** 5.03. Conversión. 5.04. Pruebas de Cambios. 5.05. Criterios y Desempeño de Pruebas en Paralelo/Piloto. 5.06. Prueba de Aceptación Final. 5.07.Pruebas y Acreditación de Seguridad 5.08. Prueba Operacional. 5.09. Promoción a Producción. 5.10. Evaluación de la Satisfacción de los Requerimientos del Usuario. 5.11. Revisión Gerencial Post – Implementación. **AI6.Administración de Cambios** 6.01. Inicio y Control de Requisiciones de Cambio. 6.02. Evaluación del Impacto. 6.03. Control de Cambios. 6.04. Documentación y Procedimientos. 6.05. Mantenimiento Autorizado. 6.06. Política de Liberación de Software.

AI5.Instalación y Acreditación de Sistemas 5.01. Entrenamiento. 5.02. Adecuación del Desempeño del Software de Aplicación.	6.07. Distribución de Software.
ENTREGA DE SERVICIOS Y SOPORTE	**ENTREGA DE SERVICIOS Y SOPORTE**
DS1.Definición de Niveles de Servicio 1.01. Marco de Referencia para el Convenio de Nivel de Servicio. 1.02. Aspectos sobre los Acuerdos de Nivel de Servicio. 1.03. Procedimientos de Ejecución. 1.04. Monitoreo y Reporte. 1.05. Revisión de Convenios y Contratos de Nivel de Servicio. 1.06. Elementos sujetos a Cargo. 1.07. Programa de Mejoramiento del Servicio.	**DS3.Administración de Desempeño y Capacidad** 3.01. Requerimientos de Disponibilidad y Desempeño. 3.02. Plan de Disponibilidad. 3.03. Monitoreo y Reporte. 3.04. Herramientas de Modelado. 3.05. Manejo de Desempeño Proactivo. 3.06. Pronóstico de Carga de Trabajo. 3.07. Administración de Capacidad de Recursos. 3.08. Disponibilidad de Recursos. 3.09. Calendarización de recursos.
DS2.Administración de Servicios prestados por Terceros. 2.01. Interfases con Proveedores. 2.02. Relaciones de Dueños. 2.03. Contratos con Terceros. 2.04. Calificaciones de terceros. 2.05. Contratos con Outsourcing. 2.06. Continuidad de Servicios. 2.07. Relaciones de Seguridad. 2.08. Monitoreo.	**DS4.Aseguramiento de Servicio Continuo.** 4.01. Marco de Referencia de Continuidad de Tecnología de Información. 4.02. Estrategia y Filosofía de Continuidad de Tecnología de Información. 4.03. Contenido del Plan de Continuidad de Tecnología de Información. 4.04.Minimización de requerimientos de Continuidad de Tecnología de Información

	4.05.Mantenimiento del Plan de Continuidad de Tecnología de Información 4.06. Pruebas del Plan de Continuidad de Tecnología de Información.
ENTREGA DE SERVICIOS Y SOPORTE	**ENTREGA DE SERVICIOS Y SOPORTE**
DS4.Aseguramiento de Servicio Continuo. 4.07.Capacitación sobre el Plan de Continuidad de Tecnología de Información 4.08.Distribución del Plan de Continuidad de Tecnología de Información. 4.09.Procedimientos de Respaldo de Procesamiento para Departamentos Usuarios. 4.10.Recursos críticos de Tecnología de Información. 4.11.Centro de Cómputo y Hardware de respaldo. 4.12 Procedimientos de Refinamiento del Plan de Continuidad de TI.	**DS5.Garantizar la Seguridad de Sistemas.** 5.07.Vigilancia de Seguridad. 5.08.Clasificación de Datos. 5.09.Administración Centralizada de Identificación y Derechos de Acceso. 5.10.Reportes de Violación y de Actividades de Seguridad. 5.11.Manejo de Incidentes. 5.12.Re-acreditación 5.13.Confianza en Contrapartes 5.14.Autorización de Transacciones 5.15.No Rechazo 5.16.Sendero Seguro 5.17.Protección de funciones de seguridad 5.18.Administración de Llave Criptográfica 5.19. Prevención, Detección y Corrección de Software “Malicioso”. 5.20. Arquitecturas de Firewalls y conexión a redes públicas. 5.21. Protección de Valores Electrónicos.
DS5.Garantizar la Seguridad de Sistemas. 5.01. Administrar Medidas de Seguridad. 5.02.Identificación, Autenticación y Acceso 5.03. Seguridad de Acceso a Datos en Línea. 5.04. Administración de Cuentas de Usuario. 5.05.Revisión Gerencial de Cuentas de	**DS6.Identificación y Asignación de Costos.** 6.01.Elementos Sujetos a Cargo 6.02.Procedimientos de Costeo

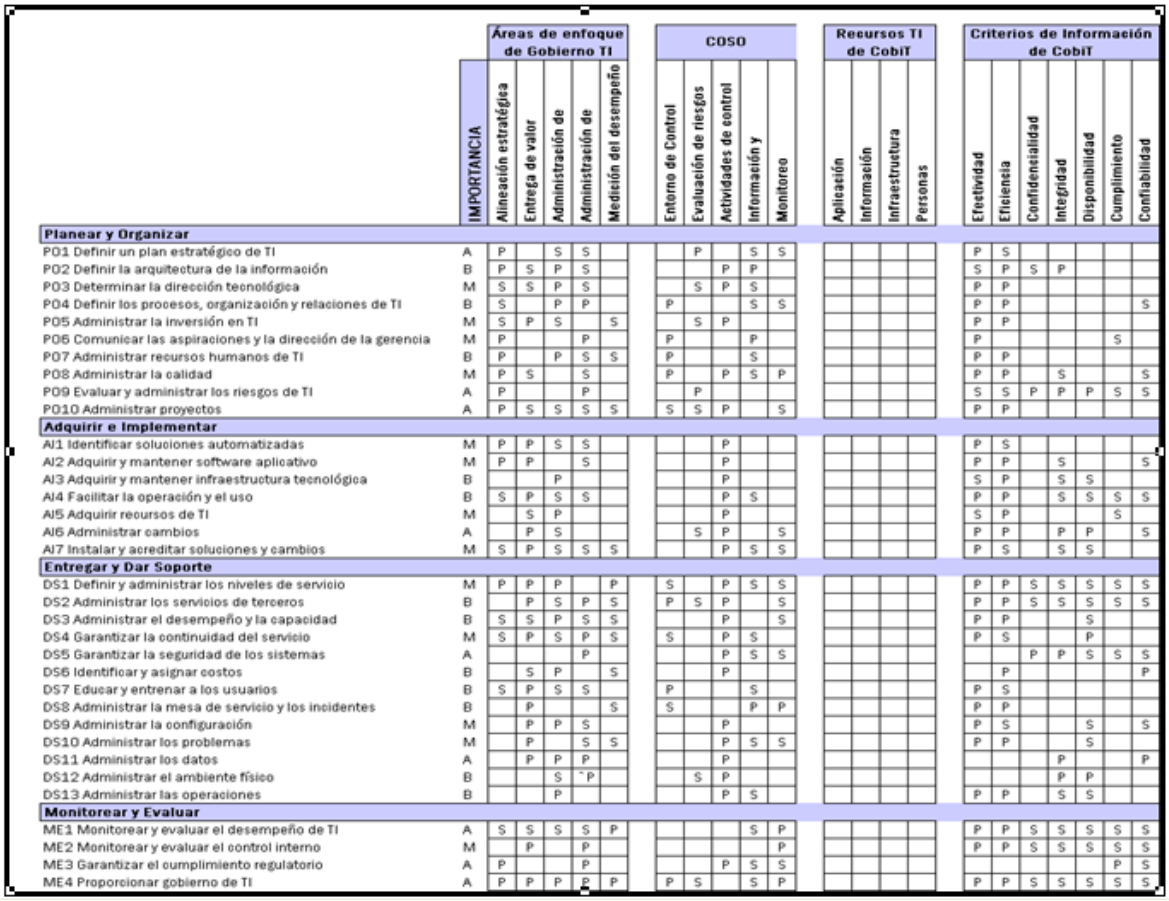
Usuario. 5.06.Control de Usuarios sobre Cuentas de Usuario. **ENTREGA DE SERVICIOS Y SOPORTE** **DS7.Educación y Entrenamiento de Usuarios** 7.01. Identificación de Necesidades de Entrenamiento. 7.02. Organización de Entrenamiento 7.03. Entrenamiento sobre Principios y Conciencia de Seguridad. **DS8.Apoyo y Asistencia a los Clientes de Tecnología de Información.** 8.01.Buró de Ayuda 8.02.Registro de Preguntas del Usuario 8.03.Escalamiento de Preguntas del Cliente 8.04.Monitoreo de Atención a Clientes 8.05.Análisis y Reporte de Tendencias **DS9.Administración de la Configuración** 9.01. Registro de la Configuración. 9.02. Base de la Configuración. 9.03. Registro de Estatus. 9.04. Control de la Configuración.	6.03.Procedimientos de Cargo y Facturación a Usuarios **ENTREGA DE SERVICIOS Y SOPORTE** **DS10.Administración de Problemas e Incidentes** 10.01. Sistema de Administración de Problemas. 10.02. Escalamiento de Problemas. 10.03. Seguimiento de Problemas y Pistas de Auditoría. **DS11.Administración de Datos.** 11.01. Procedimientos de Preparación de Datos. 11.02. Procedimientos de Autorización de Documentos Fuente. 11.03. Recopilación de Datos de Documentos Fuente. 11.04. Manejo de Errores de Documentos Fuente. 11.05. Retención de Documentos Fuente. 11.06. Procedimientos de Autorización de Entrada de Datos. 11.07. Chequeos de Exactitud, Suficiencia y Autorización. 11.08. Manejo de Errores en la Entrada de Datos. 11.09. Integridad de Procesamiento de Datos. 11.10. Validación y Edición de Procesamiento de Datos.

9.05. Software no Autorizado. 9.06. Almacenamiento de Software. **ENTREGA DE SERVICIOS Y SOPORTE** **DS11.Administración de Datos.** 11.11. Manejo de Error en el Procesamiento de Datos. 11.12. Manejo y Retención de Salida de Datos. 11.13. Distribución de Salida de Datos. 11.14. Balanceo y Conciliación de Datos de Salida. 11.15. Revisión de Salida de Datos y Manejo de Errores. 11.16. Provisiones de Seguridad para Reportes de Salida. 11.17. Protección de Información Sensible durante transmisión y transporte. 11.18.Protección de Información Crítica a de los Servicios de TI. 11.19. Administración de Almacenamiento. 11.20. Períodos de Retención y Términos de Almacenamiento. 11.21. Sistema de Administración de la Librería de Medios. 11.22. Responsabilidades de la Administración de la Librería de Medios de proveedores externos de servicios. 11.23. Respaldo y Restauración. 11.24. Funciones de Respaldo. 11.25. Almacenamiento de Respaldo. 11.26. Archivo. 11.27. Protección de Mensajes Sensitivos.	**ENTREGA DE SERVICIOS Y SOPORTE** **DS11.Administración de Datos.** 11.29. Integridad de Transacciones Electrónicas. 11.30.Integridad Continua de Datos Almacenados. **DS12.Administración de Instalaciones** 12.01. Seguridad Física. 12.02. Discreción de las Instalaciones de Tecnología de Información. 12.03. Escolta de Visitantes. 12.04. Salud y Seguridad del Personal. 12.05. Protección contra Factores Ambientales. 12.06. Suministro Ininterrumpido de Energía. **DS13.Administración de Operaciones.** 13.01. Manual de procedimientos de Operación e Instrucciones. 13.02. Documentación del Proceso de Inicio y de Otras Operaciones. 13.03. Calendarización de Trabajos. 13.04. Salidas de la Calendarización de Trabajos Estándar. 13.05. Continuidad de Procesamiento. 13.06. Bitácoras de Operación. 13.07. Operaciones Remotas.

11.28. Autenticación e Integridad. **MONITOREO** **M1.Monitoreo del Proceso.** 1.01. Recolección de Datos de Monitoreo. 1.02. Evaluación de Desempeño. 1.03. Evaluación de la Satisfacción de Clientes. 1.04. Reportes Gerenciales. **M2.Evaluar lo adecuado del Control Interno** 2.01. Monitoreo de Control Interno. 2.02. Operación oportuna del Control Interno. 2.03. Reporte sobre el Nivel de Control Interno. 2.04. Seguridad de operación y aseguramiento de Control Interno.	**MONITOREO** **M3.Obtención de Aseguramiento Independiente.** 3.01. Certificación / Acreditación Independiente de Control y Seguridad de los servicios de TI. 3.02. Certificación / Acreditación Independiente de Control y Seguridad de proveedores externos de servicios. 3.03. Evaluación Independiente de la Efectividad.

Apéndice II

Mapeo de Procesos de TI a las Áreas Focales de Gobierno TI, COSO, Recursos de TI de Cobit y Criterios de Información Cobit.



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

(P=Primario, S=Secundario).

Nota: El mapeo COSO está basado sobre el marco original COSO. El mapeo también aplica sobre el último COSO

Administración de Riesgos Empresarial - Marco Integrado, que expande sobre los controles internos proporcionando un enfoque más robusto y extensivo sobre el sujeto de la gestión de riesgos de la empresa. Mientras ni intenta ni reemplaza el marco de control interno COSO, sino mas bien incorpora el marco de control interno dentro, los usuarios de CobiT pueden elegir referir a ambos marcos de gestión de riesgos de la empresa para satisfacer sus necesidades de

control interno y moverse a través de un proceso de gestión de riesgos más completo.

REFERENCIAS CRUZADAS ENTRE LA 3ª EDICIÓN DE COBIT Y COBIT 4.1

CAMBIOS A NIVEL DE MARCO DE TRABAJO

Los cambios principales al marco de trabajo de COBIT como resultado de la actualización a COBIT 4.1 son los siguientes:

- El dominio M se ha convertido ahora a ME, y significa Monitorear y Evaluar.

- M3 y M4 eran procesos de auditoría y no procesos de TI. Fueron eliminados debido a que están cubiertos de forma adecuada por un número de estándares de auditoría de TI, aunque se han proporcionado referencias dentro del marco de trabajo actualizado para enfatizar la necesidad que tiene la gerencia de usar funciones de aseguramiento.

- ME3 es el proceso relacionado con la supervisión regulatoria, el cual estaba cubierto en PO8 previamente.

- ME4 cubre el proceso de supervisión del gobierno sobre TI, conservando el propósito de COBIT de fungir como un marco de trabajo de gobierno de TI. Al posicionar ese proceso al final de la cadena, se subraya el apoyo que cada proceso previo brinda a la última meta de implementar un gobierno efectivo de TI en la empresa.

- Con la eliminación de PO8 y la necesidad de mantener la numeración para PO9 Evaluar riesgos y PO10 Administrar proyectos de modo consistente con la 3ª edición de COBIT, PO8 ahora se convierte en

Administrar la calidad, que anteriormente era el proceso PO11. El dominio PO ahora tiene 10 procesos en lugar de 11.

- El dominio AI requirió dos cambios: la adición de un proceso de procuración y la necesidad de incluir en AI5 los aspectos de administración de versiones. El último cambio sugirió que este debería ser el último proceso en el dominio AI y por lo tanto se convirtió en AI7. El hueco que se creó en AI5 se usó para añadir el nuevo proceso de procuración. El dominio AI ahora tiene siete procesos en lugar de seis.

COBIT una actualización incremental a COBIT 4.1, incluye:

- Visión general ejecutiva mejorada.

- Explicación de metas y métricas en la sección del marco de trabajo

- Mejores definiciones de los conceptos del núcleo. Es importante mencionar que la definición de objetivo de control se ha cambiado, desplazándose mas hacia una declaración de prácticas de gestión

- Se han mejorado los objetivos de control resultado de unas prácticas de control actualizadas y la actividad de desarrollo de Val TI. Algunos objetivos de control se agruparon y / o reformularon pare evitar superposiciones y hacer la lista de objetivos de control dentro de un proceso más consistente. Estos cambios resultan en la renumeración de los objetivos de control restantes. Algunos de los otros objetivos de control fueron reordenados para hacerlos mas orientados a la acción y consistentes en la redacción. Las revisiones específicas incluyen:

  - AI5.5 y AI5.6 que fueron combinadas en AI5.4
  - AI7.9, AI7.10 y AI7.11 que fueron combinadas en AI7.8
  - ME3 fue revisada para incluir cumplimiento con los requerimientos contractuales además de requerimientos legales y regulatorios.

- Los controles de aplicación han sido revisados para ser más efectivos, basados en el trabajo para soportar la evaluación e informe de la eficacia de los controles. Resultando en una lista de seis controles de aplicación que sustituyen a los 18 controles de aplicación de COBIT 4.1, proporcionado con mayor detalle en Practicas de Control de COBIT, 2ª Edición.

- Se ha mejorado la lista de metas de negocio y de metas de TI en el Apéndice I, basado en nuevas visiones obtenidas durante la investigación de validación realizada por la Universidad de Antwerp Management School (Bélgica).

- La extracción se ha expandido a proporcionar una lista de referencias rápidas de los procesos de COBIT, y el diagrama de visión general que representa los dominios revisados para incluir la referencia para el proceso y elementos de control de aplicación del marco de trabajo de COBIT.

- Las mejoras identificadas por los usuarios de COBIT (COBIT 4.0 y COBIT Online) se han revisado e incorporado de forma apropiada.

OBJETIVOS DE CONTROL DETALLADOS

Como se puede observar en la descripción anterior a nivel del marco de trabajo y en el trabajo para aclarar y enfocar el contenido de los objetivos de control, la actualización del marco de trabajo COBIT ha cambiado significativamente los objetivos de control dentro de éste. Estos componentes se han reducido de 215 a 210, porque todos los materiales genéricos ahora sólo se conservan al nivel de marco de trabajo y no se repiten en cada proceso. Así mismo, todas las referencias a controles aplicativos se movieron al marco de trabajo y los objetivos específicos de control se agregaron en nuevas declaraciones. Para apoyar la actividad de transición en relación con los objetivos de control, los siguientes dos juegos de tablas muestran las referencias cruzadas entre los nuevos y viejos objetivos de control.

DIRECTRICES GERENCIALES

Las entradas y salidas se han añadido para ilustrar lo que los procesos necesitan de otros y lo que típicamente generan. También se proporcionan actividades y responsabilidades asociadas. Las entradas y las metas de las actividades reemplazan a los factores críticos de éxito de COBIT 3ª Edición. Las métricas ahora se basan en una cascada consistente de metas de negocio, de TI, de proceso y de actividades. El juego de métricas de COBIT 3ª Edición también se reviso y mejoró para hacerlo más representativo y medible.