Orbe Zavaleta, Piero Angel
Rodriguez Custodio, Jhonatan

# TALLER DE APLICACIÓN DE LAS PRÁCTICAS DE ASEGURAMIENTO DE LA TI APLICANDO COBIT

## OBJETIVO

Identificar los Prácticas y Actividades de Gobierno/Gestión que debieron aplicarse para prevenir las situaciones o debilidades descritas.

## PROCEDIMIENTO

El evaluador utilizará como marco de referencia el modelo de procesos de TI COBIT, las metas de TI asociadas a cada proceso y las tablas RACI. Se utilizará el siguiente formato como papel de trabajo:

| Dominio | Proceso | Práctica | Actividad | Metas TI relacionadas | Responsables |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## DESCRIPCIÓN DE LAS SITUACIONES O DEBILIDADES ENCONTRADAS

### Situación 1. Administración de Requerimientos al Departamento de Desarrollo de Sistemas.

La atención de requerimientos (mejoras adaptaciones a los sistemas) solicitados por los usuarios al Dpto. de Desarrollo de Sistemas son realizadas a través de un procedimiento manual no aprobado (Hoja de Requerimientos), que en ocasiones no permite realizar el seguimiento oportuno del requerimiento quedando pendientes algunas solicitudes de cambios o mejoras de los sistemas.

| Dominio | Proceso | Práctica | Actividad | Metas TI relacionadas | Responsables |
|---|---|---|---|---|---|
| Construir, Adquirir e Implementar | Gestionar la Definición de Requisitos | Definir y mantener los requerimientos técnicos y funcionales de negocio. | Hacer seguimiento y controlar el alcance, los requerimientos y los cambios a lo largo del ciclo de vida de la solución durante el proyecto según evolucione la comprensión de la solución. | Alineamiento de TI y estrategia de negocio, entrega de servicios de TI de acuerdo a los requisitos del negocio, Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio. | Propietarios de los procesos de negocio, Oficina de Gestion de Proyectos, Jefe de arquitectura del Negocio, Jefe de Desarrollo |

### Situación 2. Carencia de Documentación de las Pruebas de Programas y de Sistemas.

Durante nuestra revisión se apreció la ausencia de procedimientos formales que documenten apropiadamente el plan de pruebas de nuevas funcionalidades; en cuanto a descripción de las mismas, datos a ser usados, metodología para el desarrollo de dichos datos y los resultados esperados.

| Dominio | Proceso | Práctica | Actividad | Metas TI relacionadas | Responsables |
|---|---|---|---|---|---|
| Construir, Adquirir e Implementar | Gestionar la Aceptación del Cambio y la Transición | Planificar pruebas de aceptación. | Desarrollar y documentar el plan de pruebas, de forma que esté alineado con el programa y plan de calidad del proyecto y estándares relevantes de la organización. Comunicar y consultar con los propietarios de procesos de negocio y grupos de interés de TI adecuados. | Uso adecuado de aplicaciones, informacion y soluciones tecnologicas. Capacitacion y soporte de procesos de negocios integrando aplicaciones y tecnologia en procesos de negocio. | Propietarios de los procesos de negocio, Comite estrategico, Jefe de desarrollo, Jefe de operaciones de TI, Gestor de seguridad de la informacion, Gestor de continuidad de negocio. |

## Situación 3. Catalogación de Versiones de Programas Fuentes

En nuestra revisión hemos observado que el Dpto. de Micro computación y Redes tiene el control de los programas fuentes de los aplicativos almacenados en un servidor. Además se apreció la falta de procedimientos para el control de estos programas fuentes. Sin embargo el Dpto. de Desarrollo de Sistemas debería considerar un inventario de los programas fuentes y sus versiones instaladas en los computadores así como también un procedimiento para la actualización de estas versiones.

| Dominio | Proceso | Práctica | Actividad | Metas TI relacionadas | Responsables |
|---|---|---|---|---|---|
| Construir, Adquirir e Implementar | Gestionar la Configuración | Establecer y mantener un modelo de configuración. | Establecer y mantener un modelo lógico para la gestión de la configuración, incluyendo información sobre los tipos de elementos de configuración, atributos de los elementos de configuración, tipos de relaciones, atributos de relación y códigos de estado. | Cumplimiento y soporte de TI al cumplimineto del negocio de las leyes y regulaciones externas. Optimizacion de activos, recursos y capacidades de TI. Disponibilidad de informacion util y relevante para la toma de decisiones. | Jefe de Administracion TI, Gestor de servicio. |

## Situación 4. Carencia de Procedimientos Estándares de desarrollo (Programas, Pantallas y Diseño de Tablas)

Durante nuestra revisión se apreció la ausencia de procedimientos que estandaricen el trabajo de los analistas y programadores de los sistemas en lo referente a las estructuras de elaboración del código de los programas y diseños de las pantallas de ambiente visual.
Se observó que algunos sistemas tienen el manual de diseño lógico y no el de diseño físico. Además, contienen: Nivel Cero, Diccionario de Datos y La relación de tablas (Bosquejo final sin normalizar).

| Dominio | Proceso | Práctica | Actividad | Metas TI relacionadas | Responsables |
|---|---|---|---|---|---|
| Alinear, Planificar y Organizar | Gestionar la Arquitectura Empresarial | Definir la arquitectura de referencia | Mantener un modelo de arquitectura de procesos como parte de las descripciones de dominio de referencia y objetivo. Estandarizar las descripciones y la documentación de los procesos. Definir las funciones y responsabilidades de los que deciden el proceso, el propietario del proceso, los usuarios del proceso, el equipo del proceso y cualquier otra parte interesada que debieran estar involucrados. | Alineamiento de TI y estrategia del negocio, agilidad de las TI, optimizacion de activos, recursos y capacidades de las TI. | Ejecutivos del negocio, comité ejecutivo estrategico, consejo de arquitectura de la empresa, director de informatica, jefe de arquitectura del negocio. |

## Situación 5. Carencia de Herramientas de Modelamiento de datos

Se ha observado que el Departamento de Desarrollo de Sistemas, no cuenta con herramientas de tecnología de información que permita realizar las actividades de Modelamiento de Datos y Elaboración de Diagramas de Entidad Relación.

| Dominio | Proceso | Práctica | Actividad | Metas TI relacionadas | Responsables |
|---|---|---|---|---|---|
| Construir, Adquirir e Implementar | Gestionar la Aceptación del Cambio y la Transición | Establecer un entorno de pruebas. | 1. Crear una base de datos de pruebas que sea representativa del entorno de producción. Sanear los datos reales usados en el entorno de pruebas de acuerdo a las necesidades de negocio y estándares de la organización (ej. considere si los requisitos de cumplimiento normativo o legal obligan al uso de datos saneados). | Uso adecuado de las aplicaciones, información y soluciones tecnológicas. | Propietarios de los procesos de negocio, comité estrategico, jefe de desarrollo, jefe de TI, gestor de la seguridad de la información, gestor de contunuidad del negocio |

## Situación 6. Existencia de Software Aislado

Durante nuestra revisión evidenciamos la existencia de un software que es utilizado para el “Manejo de las Planillas” administrado por el usuario. Este sistema no esta integrado a los sistemas actualmente existentes y los Departamentos de desarrollo de sistemas y redes de micro computación no brindan el soporte correspondiente a este aplicativo.

## Situación 7. Carencia de Pistas de Auditoría

En el proceso de relevamiento evidenciamos que algunos aplicativos existentes no guardan información acerca de pistas de auditoría originando que no existan mecanismos para realizar las actividades de control de los procesos del negocio.

| Dominio | Proceso | Práctica | Actividad | Metas TI relacionadas | Responsables |
|---|---|---|---|---|---|
| Entrega, Servicio y Soporte | Gestionar Controles de Proceso de Negocio | Asegurar los activos de información. | 4. Identificar e implementar procesos, herramientas y técnicas para verificar razonablemente el cumplimiento. | Riesgo de negocio relacionados con las TI gestionados, entrega de servicios de TI de acuerdo a los requisitos del negocio. | Director General Financiero |

## Situación 8. Bitácoras de Actividad.

Hemos observado que no existe un registro (log de actividades) en donde se aprecie cronológicamente los trabajos, cambios o modificaciones ocurridas durante el tiempo de funcionamiento de los computadores, así como también un registro histórico de las paradas de los sistemas y de los mantenimientos realizados a los servidores.

## Situación 9. Carencia de Procedimientos de Respaldo y Recuperación de programas fuentes

Hemos evidenciado la carencia de procedimientos formales de respaldo y recuperación en tal sentido solo se realizan estas actividades para ciertos servidores como los ubicados en la sede Tomas Valle.

## Situación 10. Plan de Contingencias

Hemos evidenciado que no existe un procedimiento formal por escrito y coordinado que evidencie la preparación de los sectores ante alguna posible contingencias. Solo se ha evidenciado un programa de los mantenimientos efectuados a algunos equipos.

## Situación 11. Inventario de Hardware y Software

Hemos observado que no se encuentra un inventario debidamente actualizado y que contenga además información necesaria para poder realizar actividades de control. En tal sentido solo se encuentran inventarios que no son lo suficientemente fáciles de revisar y actualizar.

**Situación 12. Política Antivirus**

Uno de los principales riesgos en lo que respecta a la Seguridad de la Información es el impacto que tienen los Virus Informáticos sobre la información que maneja la compañía.

En nuestra evaluación hemos evidenciado que la Sub Gerencia de Informática y Racionalización de ABCD cuenta con un antivirus denominado MATABICHO el que no ofrece las características de un antivirus corporativo que debe estar instalado en los Servidores y en los equipos de cómputo de los usuarios.