UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE CIENCIAS ECONÓMICAS Y FINACIERAS

CARRERA DE CONTADURÍA PÚBLICA

UNIDAD DE POSTGRADO

AUDITORÍA INFORMÁTICA DEL SISTEMA CONTABLE FINANCIERO DE LA EMPRESA M & F Ltda.

(Estudio de Caso)

Materia: Taller de Grado

Docente: Mg. Sc. Ruth Benítez

Maestrante: Olesia Dalenkevitch

Fecha: Agosto 2017

TABLA DE CONTENIDOS

AUDITORÍA INFORMÁTICA DEL SISTEMA CONTABLE FINANCIERO DE LA EMPRESA “M&F Ltda.” (Estudio de caso)

1. MARCO PRÁCTICO

1.1. INTRODUCCIÓN

La Contraloría General del Estado de Bolivia (CGE), (2012) define este proceso de la siguiente manera:

> «**Auditoría de tecnologías de la información y la comunicación**
>
> Es el examen objetivo, crítico, metodológico y selectivo de evidencia relacionada con políticas, prácticas, procesos y procedimientos en materia de tecnologías de la información y la comunicación, para expresar una opinión independiente respecto:
>
> a) A la confidencialidad, integridad, disponibilidad y confiabilidad de la información.
>
> b) Al uso eficaz de los recursos tecnológicos.
>
> c) A la eficacia del control interno asociado a los procesos de las Tecnologías de la Información y la Comunicación.
>
> Los incisos señalados, podrán ser considerados en forma individual o en conjunto. La auditoría de tecnologías de la información y la comunicación está definida principalmente por sus objetivos y puede ser orientada hacia uno o varios de los siguientes enfoques:
>
> a) Enfoque a las seguridades: Consiste en evaluar los controles de seguridad implementados en los sistemas de información con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información.
>
> b) Enfoque a la información: Consiste en evaluar la estructura, integridad y confiabilidad de la información gestionada por el sistema de información.
>
> c) Enfoque a la infraestructura tecnológica: Consiste en evaluar la correspondencia de los recursos tecnológicos en relación a los objetivos previstos.
>
> d) Enfoque al software de aplicación: Consiste en evaluar la eficacia de los procesos y controles inmersos en el software de aplicación, que el diseño conceptual de éste cumpla con el ordenamiento jurídico administrativo vigente.
>
> e) Enfoque a las comunicaciones y redes: Consiste en evaluar la confiabilidad y desempeño del sistema de comunicación para mantener la disponibilidad de la información.

Para una adecuada comprensión de las Normas de Auditoría de Tecnologías de la Información y la Comunicación, se deben considerar las siguientes definiciones:

Datos: Son objetos de información, los cuales pueden ser externos o internos, estructurados y no estructurados del tipo gráfico, sonido, imágenes, números, palabras y de otra índole, etc.

Información: Datos que han sido organizados, sistematizados y presentados de manera que los patrones subyacentes resulten claros.

Tecnología: Es un conjunto ordenado de instrumentos, conocimientos, procedimientos y métodos aplicados a las áreas.

Tecnologías de la Información y la Comunicación (TIC): Comprende al conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión y recepción de información, voz, datos, texto, video e imágenes. Se consideran como sus componentes el hardware, el software y los servicios.

Sistema de Información (SI): Se refiere a un conjunto de procesos y recursos de información organizados con el objetivo de proveer la información necesaria (pasada, presente, futura) en forma precisa y oportuna para apoyar la toma de decisiones en una entidad.

Software de aplicación: Se refiere a un elemento de los Sistemas de Información, es un conjunto de programas de computador diseñados y escritos para realizar tareas específicas del negocio y que permiten la interacción entre el usuario y el computador.

Sistemas de comunicación: Se refiere a la tecnología que se emplea para el intercambio de información.

Confidencialidad de la información: Se refiere a la protección de la información crítica contra su divulgación no autorizada.

Integridad de la información: Se vincula con la exactitud y la totalidad de la información así como también con su validez de acuerdo con los valores y las expectativas de la entidad.

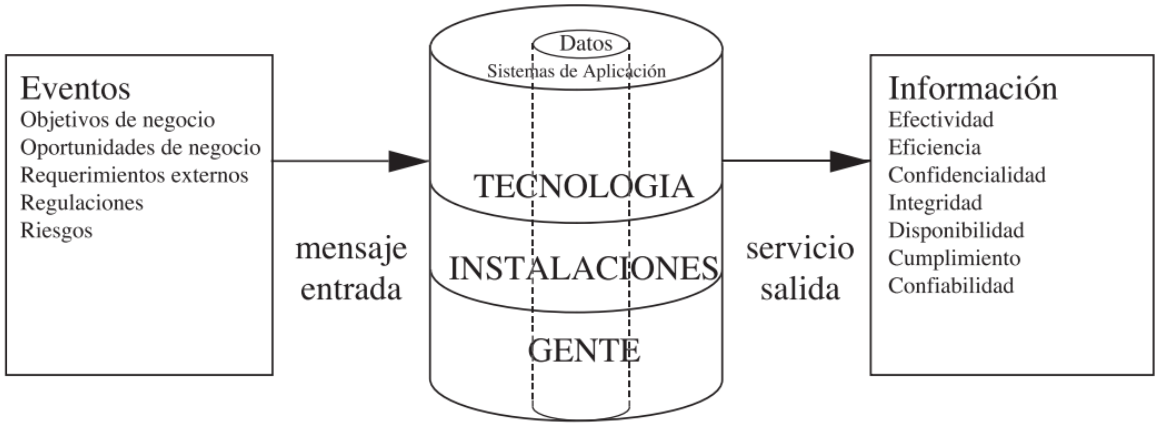
Confiabilidad de la información: Se vincula con la provisión oportuna e íntegra de la información para coadyuvar a la consecución de los objetivos de la entidad. Disponibilidad de la información: Se vincula con el hecho de que la información se encuentre disponible cuando el proceso la requiera. También se asocia con la protección de los recursos necesarios y las capacidades asociadas.

Técnicas de Auditoría Asistidas por Computador (TAAC): Se refiere a las técnicas de auditoría que contemplan herramientas informáticas con el objetivo de realizar más eficazmente, eficientemente y en menor tiempo pruebas de auditoría.»

De acuerdo a las actividades que lleva a cabo la Organización, se procede a realizar la identificación de que parte de sus actividades se pondrá bajo observación para conocer la situación actual y, si es necesario, corregirla.

GRÁFICO N° 1

CICLO DE FUNCIONAMIENTO DE LAS ACTIVIDADES EN LA ORGANIZACIÓN

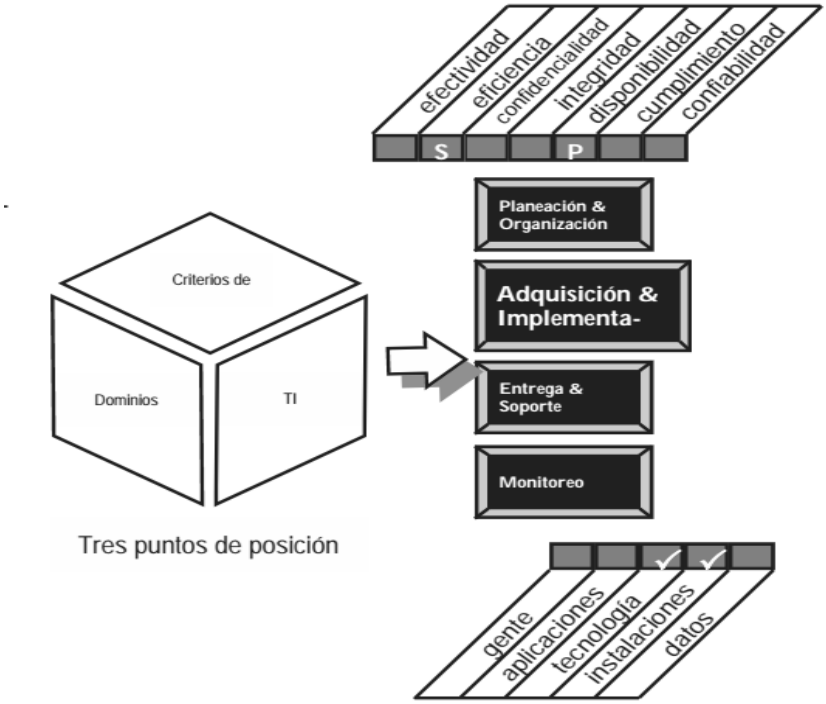


FUENTE: MODELO COBIT (ISACA, 2000)

Lo anterior es tomando en cuenta que se aplicará para la Auditoría de T.I. el Modelo COBIT, del mismo que se toma su ciclo de funcionamiento de las actividades de la empresa. La identificación del área a observar se determina de a los criterios, basado en COBIT, mostrados a continuación:

GRÁFICO N° 2

DOMINIOS Y CRITERIOS



DE T.I. EN LA ORGANIZACIÓN

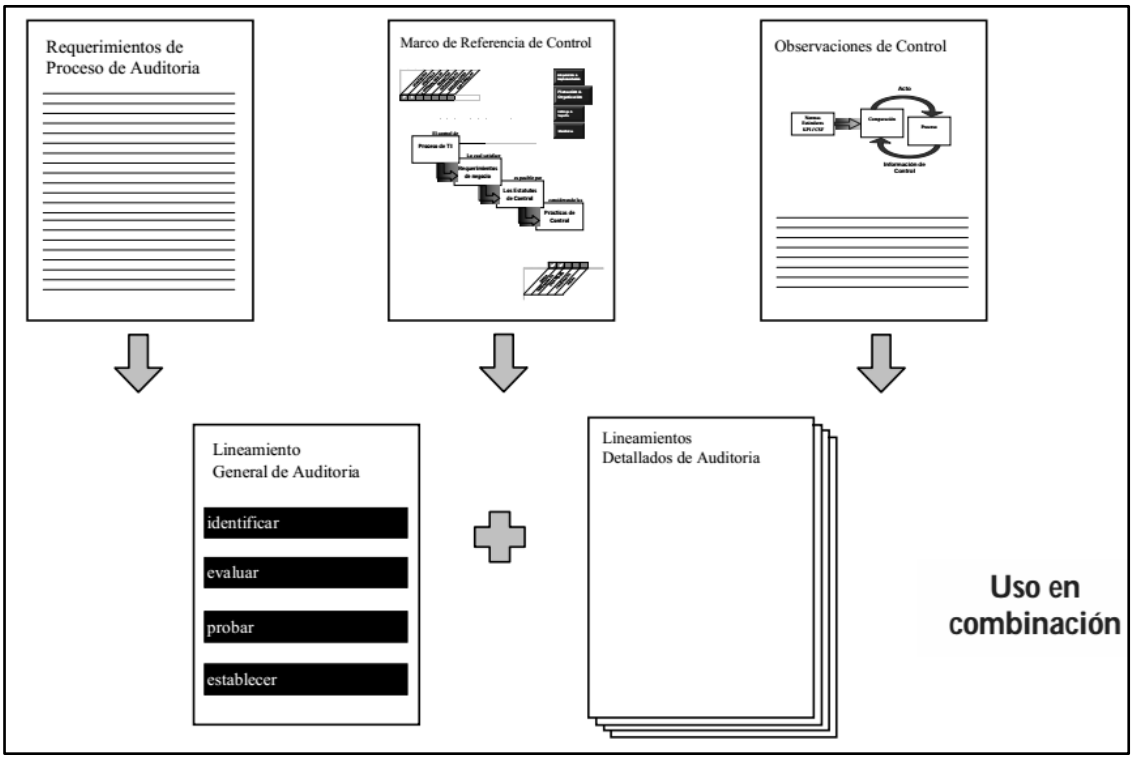
FUENTE: MODELO COBIT (ISACA, 2000)

1.2. DIRECTRIZ GENÉRICA PARA REALIZAR AUDITORÍAS DE T.I.C.s SEGÚN COBIT

Los siguientes criterios son los seguidos por el Modelo COBIT (ISACA, 2000):

DIAGRAMA N°1

ESQUEMA DEL PROCESO DE AUDITORÍA INFORMÁTICA



FUENTE: MODELO COBIT (ISACA, 2000)

PRIMER PASO: OBTENCIÓN DE UNA COMPRENSIÓN

Los pasos de auditoría a realizar para documentar las actividades subyacentes de los objetivos de control, así como también para identificar las medidas de control/procedimientos establecidos existentes.

Entrevistar al personal y directivos para obtener una comprensión de:

- Los requerimientos del negocio y los riesgos asociados
- La estructura organizacional
- Las funciones y responsabilidades
- Las políticas y procedimientos
- Las leyes y regulaciones
- Las medidas de control existentes
- El reporte administrativo (estatus, desempeño, puntos de acción)

Documentar los recursos de los procesos de TI relacionados que están particularmente afectados por los procesos bajo revisión, confirmar el entendimiento del proceso bajo revisión, los Indicadores Clave de Desempeño (KPI) del proceso, las implicaciones del control, por ejemplo mediante una revisión paso a paso del proceso.

SEGUNDO PASO: EVALUACIÓN DE LOS CONTROLES

Los pasos de auditoría a realizar para la evaluación de la eficacia de las medidas de control existentes o el grado en que se logra un objetivo de control. Básicamente, trata de decidir qué, si y cómo probarlo.

Evaluar la suficiencia de las medidas de control para el proceso bajo revisión, por medio de considerar los criterios identificados y las prácticas estándar de la industria, los Factores Críticos de Éxito (CSF) de las medidas de control, y la aplicación del criterio profesional del auditor.

• Existen procesos documentados

• Existen resultados apropiados

• La responsabilidad y el registro son claras y eficaces

• Existen controles compensatorios, donde es necesario

Concluir el grado en el que se cumple el objetivo de control.

TERCER PASO: EVALUACIÓN DEL CUMPLIMIENTO

Los pasos de auditoría a realizar para asegurar que las medidas de control establecidas están funcionando como debiera, de manera consistente y continua, y concluir sobre la suficiencia del ambiente de control.

- Obtener evidencia directa o indirecta para puntos/períodos seleccionados para asegurar que los procedimientos cumplieron en el periodo bajo revisión, utilizando evidencia directa o indirecta.
- Realizar una revisión limitada de la suficiencia de los resultados del proceso.
- Determinar el nivel de pruebas sustantivas y el trabajo adicional necesarios para asegurar que el proceso de TI es adecuado.

CUARTO PASO: JUSTIFICACIÓN / COMPROBACIÓN DEL RIESGO

Los pasos de auditoría a realizar para justificar el riesgo de no cumplir con el objetivo de control mediante el uso de técnicas analíticas y/o consultando a fuentes alternativas. El objetivo es fundamentar la opinión e “impresionar” a la administración para que tome acción. Los auditores deben ser creativos para encontrar y presentar esta información frecuentemente confidencial y sensitiva.

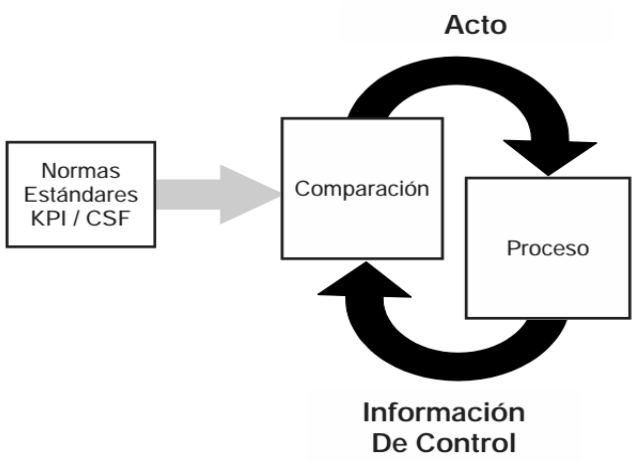
- Documentar las debilidades del control, y las amenazas y vulnerabilidades resultantes.
- Identificar y documentar el impacto real y potencial; por ejemplo, mediante el análisis de causa-raíz.
- Brindar información comparativa; por ejemplo, mediante benchmarks (escalas comparativas).

1.3. PROCESO DE AUDITORÍA

De acuerdo a los preceptos establecidos por el Modelo COBIT (ISACA, 2000), los diagramas de flujo que se muestran a continuación tratan de cada uno de los pasos para la satisfacción de un solo objetivo de control. Define el objetivo del paso y especifica lo que el auditor debe haber alcanzado antes de continuar con el siguiente paso. Finalmente, un diagrama de flujo es la representación gráfica del proceso de recolección de información y toma de decisiones que deben ocurrir en cada uno de los pasos.

DIAGRAMA N° 2

OBSERVACIONES DE CONTROL



FUENTE: MODELO COBIT (ISACA, 2000)

1.3.1. PASO DE AUDITORÍA DE IDENTIFICACIÓN/DOCUMENTACIÓN

Objetivo del Paso: Familiarizar al auditor con la tarea cubierta por el objetivo de control y la manera en que la administración de SI cree que están siendo controlados.

Esto incluye la identificación de las personas, los procesos y la ubicación donde se realiza esta tarea, y los procedimientos establecidos que los controlan.

Resultados Deseados del Paso: Al finalizar el paso de auditoría de identificación/documentación, el auditor deberá haber identificado, documentado y verificado:

• Quién realiza la tarea cubierta por el objetivo de control

• Dónde se realiza la tarea

• Cuándo se realiza la tarea

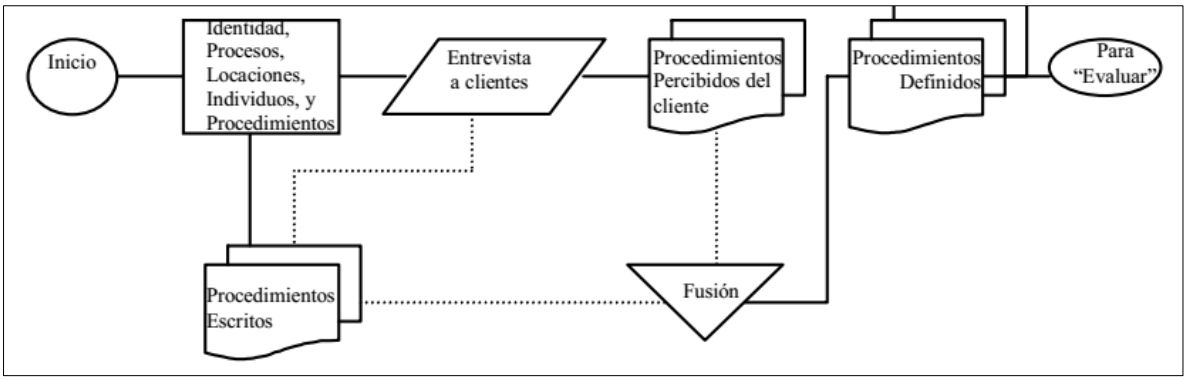
• Sobre qué datos de entrada se realiza la tarea

• Qué datos de salida/resultados se esperan de la tarea, y

• Cuáles son los procedimientos establecidos para realizar la tarea.

FLUJOGRAMA N° 1

IDENTIFICACIÓN / DOCUMENTACIÓN



FUENTE: MODELO COBIT (ISACA, 2000)

1.3.2. PASO DE AUDITORÍA DE EVALUACIÓN

Objetivo del Paso: Evaluar los procedimientos establecidos y determinar si los procedimientos brindan una estructura de control eficaz.

Los procedimientos deben evaluarse contra los criterios identificados, las prácticas estándar de la industria y el criterio del auditor. Una estructura de control eficaz es eficiente en costos y proporciona aseguramiento razonable de que la tarea está siendo realizada y de que se está cumpliendo el objetivo de control.

Resultados Deseados del Paso: Al finalizar el paso de auditoría de evaluación, el auditor debe haber:

• Evaluado las leyes, regulaciones y criterios organizacionales en cuanto a su aplicación sobre los procedimientos

• Evaluado los procedimientos establecidos para determinar si son eficientes en costos y proporcionan aseguramiento razonable de que se está realizando la tarea y de que se está cumpliendo el objetivo de control

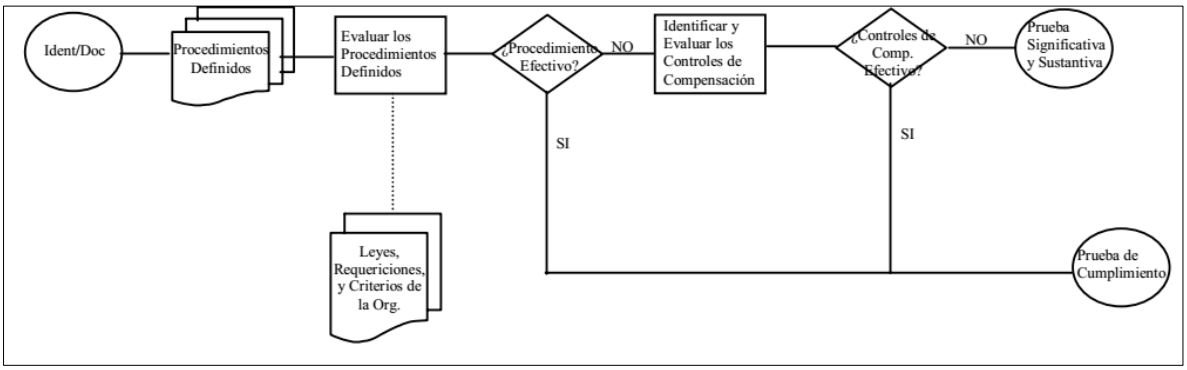
• Evaluado los controles compensatorios utilizados para apoyar procedimientos débiles

• Concluido si los procedimientos establecidos y los controles compensatorios proporcionan conjuntamente una estructura de control eficaz

• Identificado si son apropiadas las pruebas de cumplimiento.

FLUJOGRAMA N° 2

EVALUACIÓN



FUENTE: MODELO COBIT (ISACA, 2000)

1.3.3. PASO DE AUDITORÍA DE PRUEBAS DE CUMPLIMIENTO

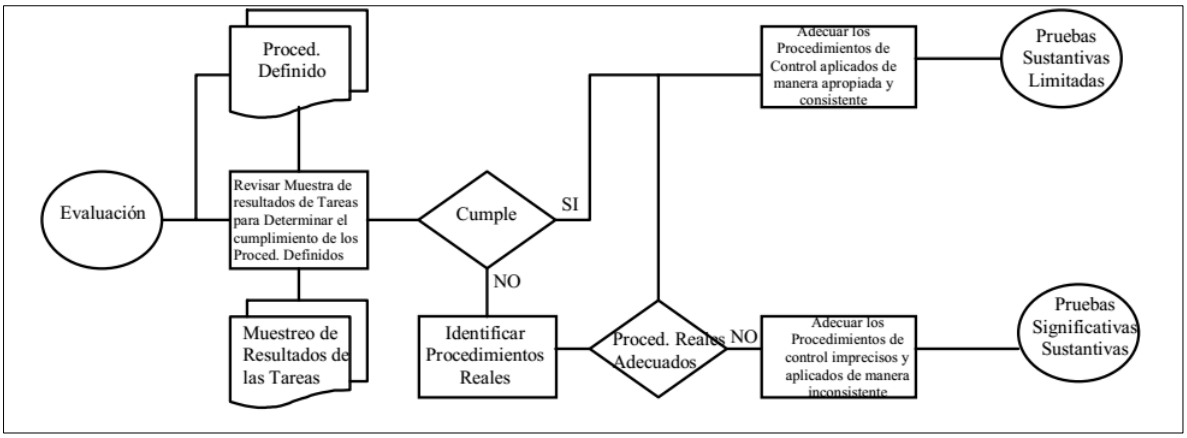
Objetivo del Paso: Analizar la adherencia de una organización a los controles prescritos.

Deberá compararse los procedimientos reales y los controles compensatorios en relación con los procedimientos establecidos, y deberá realizarse entrevistas y revisión de documentos para determinar si los controles están debida y consistentemente aplicados. Las pruebas de cumplimiento solamente se realizan sobre la base de los procedimientos que han sido debida y consistentemente aplicadas.

Resultados Esperados del Paso: Al finalizar el paso de auditoría de pruebas de cumplimiento, el auditor debe haber documentado la adherencia de la organización a los procedimientos identificados anteriormente y debe haber concluido si los procedimientos establecidos y los controles compensatorios están debida y consistentemente aplicados. Basándose en el nivel de cumplimiento, el auditor debe determinar el nivel de pruebas sustantivas necesarias para brindar aseguramiento de que el proceso de control es adecuado.

FLUJOGRAMA N° 3

PRUEBAS DE CUMPLIMIENTO



FUENTE: MODELO COBIT (ISACA, 2000)

1.3.4. PASO DE AUDITORÍA DE PRUEBAS SUSTANTIVAS

Objetivo del Paso: Realizar las pruebas de datos necesarias para brindar aseguramiento o no-aseguramiento total a la administración sobre la consecución de un objetivo de negocios dado.

Resultados Deseados del Paso: Al finalizar el paso de auditoría de pruebas sustantivas, el auditor deberá haber realizado pruebas suficientes sobre los resultados de la tarea para concluir si se está alcanzando un objetivo de control dado. Deberán realizarse pruebas sustantivas si:

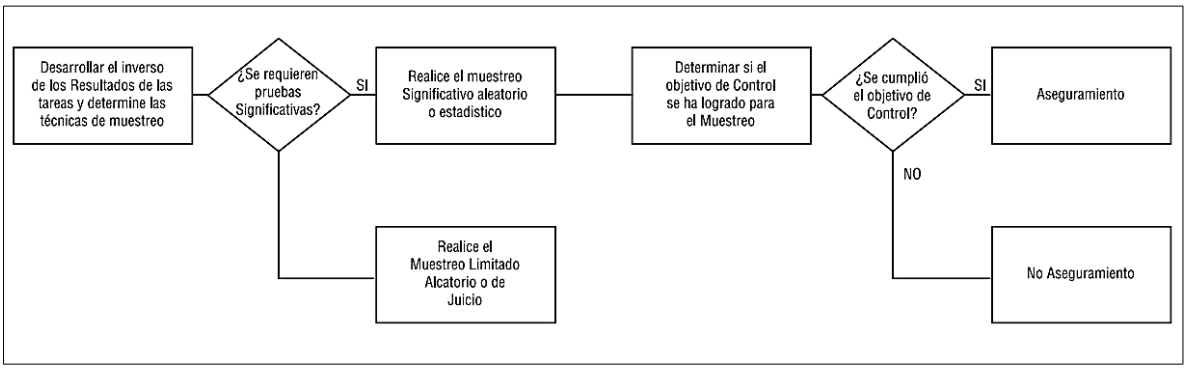
• No existen medidas de control

• Las medidas de control han sido calificadas como no satisfactorias, o

• Las pruebas de cumplimiento indican que las medidas de control no han sido debida y consistentemente aplicadas.

FLUJOGRAMA N° 4

PRUEBAS SUSTANTIVAS



FUENTE: MODELO COBIT (ISACA, 2000)

1.4 ESTUDIO DE CASO

Se efectúa el proceso de Auditoría de T.I. en la Organización M&F Ltda., en el área Financiera, respecto al Sistema de Información Contable y Financiera, enfocado específicamente en **LA INFORMACIÓN**, aplicando el Método COBIT.

Siendo este estudio de caso, como todos los Estudios de Casos, una descripción y análisis detallados de una unidad social única (YIN, 1989) y, considerando el alcance de la presente Auditoría muy amplio respecto a su explicación práctica, se ha determinado tomar como unidades de estudio dentro la organización, dos áreas específicas:

Primer Objetivo: La generación de la información de los procesos, cuyo resultado es el Libro de Ventas IVA

Segundo Objetivo: La generación de la información de los procesos, cuyo resultado es el Registro de los Ingresos por Ventas.

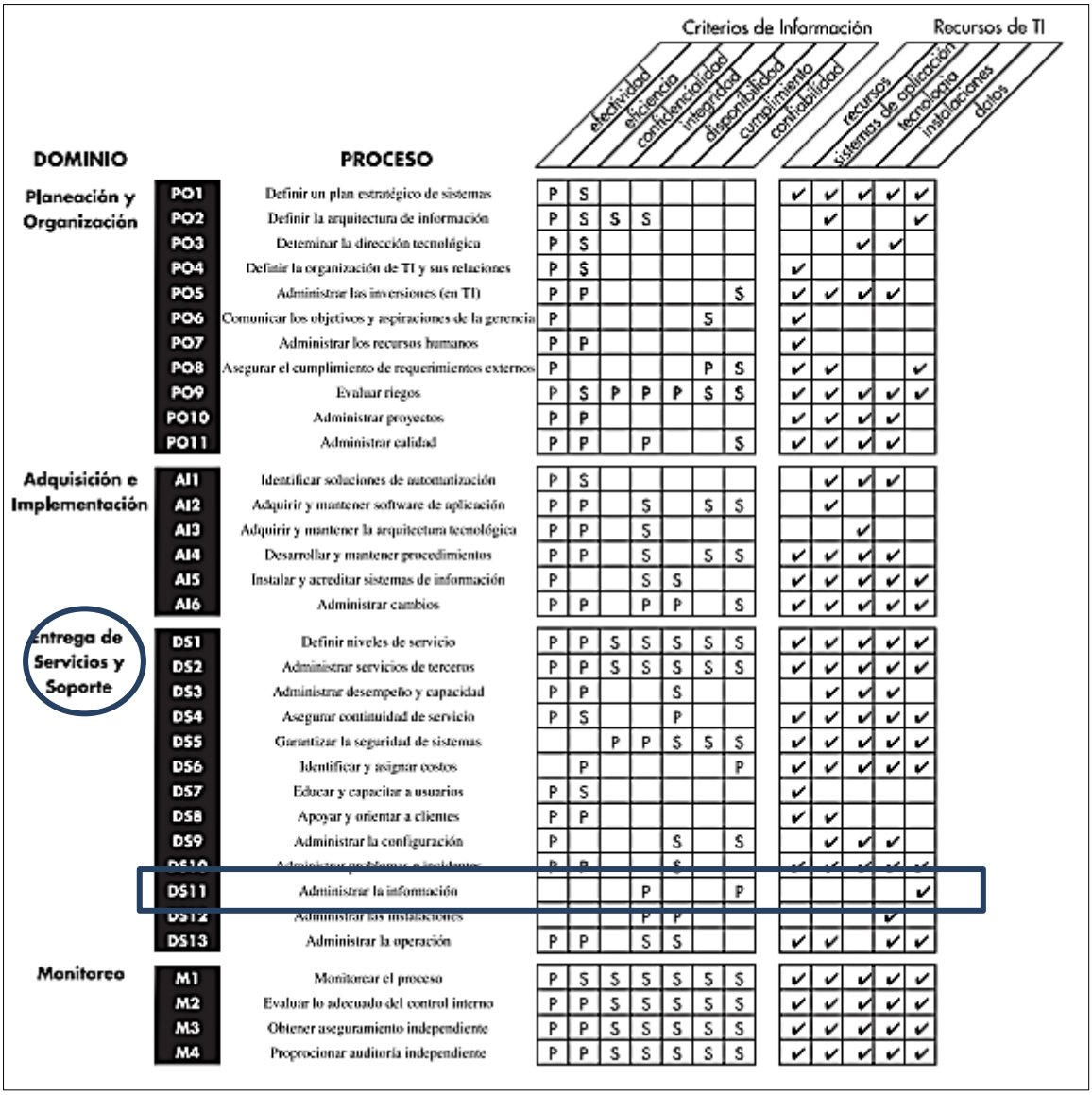
Además la Auditoría está inserta en **una Auditoría enfocada a la información**, consistente en evaluar la estructura, integridad y confiabilidad de la información gestionada por el sistema de información, de acuerdo a la clasificación dada por la Contraloría General del Estado de Bolivia (CGE, 2012).

Ya dentro la nomenclatura de COBIT, el **Dominio** de la presente Auditoría es: **ENTREGA DE SERVICIOS Y SOPORTE**, correspondiente al **Proceso**

DS11: Administrar la Información, cuyos **Criterios de Información** son **asegurar la DISPONIBILIDAD y CONFIABILIDAD de los DATOS procesados por el S.I.**, que resultan ser los **Recursos de T.I.** en las unidades de estudio escogidas:

DIAGRAMA N° 3

TABLA RESUMEN DE OBJETIVOS DE CONTROL



FUENTE: MODELO COBIT (ISACA, 2000) (El resaltado es Elaboración Propia).

Resumiendo, la Auditoría de T.I. en las unidades de estudio tienen las siguientes características:

DOMINIO:	Entrega de Servicios y Soporte
PROCESO:	DS11 Administrar la Información
CRITERIOS DE INFORMACIÓN:	Disponibilidad y Confiabilidad
RECURSOS DE T.I.:	Datos

La metodología COBIT (ISACA, 2000) establece que: el control sobre el proceso de TI de **Administración de información** que satisface los requerimientos de negocio de asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento, se hace posible a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de T.I. y toma en consideración:

- Diseño de formatos
- Controles de documentos fuente
- Controles de entrada, procesamiento y salida
- Identificación, movimiento y administración de la librería de medios
- Recuperación y respaldo de datos
- Autenticación e integridad
- Propiedad de datos
- Políticas de administración de datos
- Modelo de datos y estándares de representación de datos
- Integración y consistencia a través de plataformas
- Requerimientos legales y regulatorios

Los Objetivos de control para el proceso DS11, previstos en COBIT (ISACA, 2000) son:

11.0 Administración de Datos

- 11.1 Procedimientos de Preparación de Datos
- 11.2 Procedimientos de Autorización de Documentos Fuente
- 11.3 Recopilación de Datos de Documentos Fuente
- 11.4 Manejo de Errores de Documentos Fuente
- 11.5 Retención de Documentos Fuente
- 11.6 Procedimientos para la Autorización de Entrada de Datos
- 11.7 Chequeos de Exactitud, Suficiencia y Autorización
- 11.8 Manejo de Errores en la Entrada de Datos
- 11.9 Integridad de Procesamiento de Datos
- 11.10 Validación y Edición de Procesamiento de Datos
- 11.11 Manejo de Errores en el Procesamiento de Datos
- 11.12 Manejo y Retención de Datos de Salida
- 11.13 Distribución de Datos de Salida
- 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 Sensitiva durante transmisión y transporte

11.18 Protección de Información Sensitiva a ser Desechada

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

11.23 Respaldo y Restauración

11.24 Funciones de Respaldo

11.25 Almacenamiento de Respaldo

11.26 Archivo

11.27 Protección de Mensajes Sensitivos

11.28 Autenticación e Integridad

11.29 Integridad de Transacciones Electrónicas

11.30 Integridad Continua de Datos Almacenados

Transcribiendo literalmente los criterios a seguir en el Proceso de la Auditoría con COBIT como método (ISACA, 2000), se tiene:

LOS OBJETIVOS DE CONTROL TANTO DETALLADOS COMO DE ALTO NIVEL SON AUDITADOS AL:

Obtener un entendimiento a través de:

► Entrevistas:

Administración de operaciones de TI

Administración de bases de datos de TI

Administración de desarrollo de aplicaciones de TI

Administración de entrenamiento/recursos humanos de TI

Administración de soporte de sistemas de TI

Administración de la seguridad del sitio de respaldo

Administraciones de diferentes usuarios para aplicaciones de misión crítica

► Obteniendo:

Políticas y procedimientos organizacionales relacionados con la naturaleza y administración de datos, incluyendo:

- Flujo de datos dentro de la función de TI y hacia/desde los usuarios de los datos
- Puntos en la organización en los que los datos son originados, concentrados en grupos o tandas (“batched”), editados, capturados, procesados, extraídos, revisados, corregidos y remitidos, y distribuidos a los usuarios
- Proceso de autorización de documentos fuente
- Procesos de recolección, seguimiento y transmisión de datos
- Procedimientos para asegurar la suficiencia, precisión, registro y transmisión de documentos fuente completos para su captura
- Procedimientos utilizados para identificar y corregir errores durante la creación de datos
- Procedimientos para asegurar la integridad, confidencialidad y no rechazo de los mensajes sensitivos transmitidos por Internet o cualquier otra red pública
- Métodos utilizados por la organización para retener documentos fuente (archivo, imágenes, etc.), para definir qué documentos deben ser retenidos, los requerimientos de retención legales y regulatorios, etc.
- Sistemas de interfaz que proporcionen y utilicen datos para las funciones de TI
- Contratos de proveedores para llevar a cabo tareas de administración de datos
- Reportes administrativos utilizados para monitorear actividades e inventarios

Una lista de todas las aplicaciones mayores, así como de la documentación de usuario relacionada con:

- Módulos que lleven a cabo revisiones de precisión, suficiencia y autorización de captura en el ingreso de datos
- Funciones que lleven a cabo entradas de datos para cada aplicación
- Funciones que lleven a cabo rutinas de corrección de errores de entrada de datos
- Métodos utilizados para prevenir (por medios manuales y programados), detectar y corregir errores
- Control de la integridad de los procesos de datos enviados a proceso

- Edición y autenticación de la validación del procesamiento de datos tan cerca del punto de origen como sea posible
- Manejo y retención de salidas creadas por aplicaciones
- Salidas, distribución de salidas y sistemas de interfase que utilizan salidas
- Procedimientos de balanceo de salidas para control de totales y conciliación de variaciones
- Revisión de la precisión de los reportes de salida y de la información
- Seguridad en el procesamiento distribuido de los reportes
- Seguridad de los datos transmitidos y entre aplicaciones
- Disposición de documentación sensible de entrada, proceso y salida
- Procedimientos de control de proveedores como terceras partes con respecto a preparación, entrada, procesamiento y salida

Políticas y procedimientos relacionados con cualquier repositorio central de bases de datos de la organización, incluyendo:

- Organización de la base de datos y diccionario de datos
- Procedimientos de mantenimiento y seguridad de bases de datos
- Determinación y mantenimiento de la propiedad de las bases de datos
- Procedimientos de control de cambios sobre el diseño y contenido de la base de datos
- Reportes administrativos y pistas de auditoría que definen actividades de bases de datos

Políticas y procedimientos relacionados con la librería de medios y con el almacenamiento de datos externo, incluyendo:

- Administración de la librería de medios y del sistema de administración de la librería
- Requerir la identificación externa de todos los medios
- Requerir el inventario actual de todos los contenidos y procesos para actividades de control
- Procesos de administración/depuración para proteger los recursos de datos
- Procedimientos de reconciliación entre registros actuales y registros de datos almacenados
- Reciclaje de datos y rotación de medios de datos
- Inventario de datos de prueba y pruebas de recuperación llevadas a cabo

- Medios y funciones del personal en el sitio alterno en el plan de continuidad

Evaluar los controles:

► Considerando si:

Para la preparación de datos:

- Los procedimientos de preparación de datos aseguran suficiencia, precisión y validez
- Existen procedimientos de autorización para todos los documentos fuente
- Existe una separación de funciones entre el origen, la aprobación y la conversión de documentos fuente a datos
- Los datos autorizados permanecen completos, precisos y válidos a través de la creación de documentos fuente
- Los datos son transmitidos de una manera oportuna
- Se lleva a cabo una revisión periódica de los documentos fuente en cuanto a su suficiencia y aprobaciones apropiadas
- Se lleva a cabo un manejo apropiado de documentos fuente erróneos
- Existe un control adecuado de información sensitiva en documentos fuente para su protección contra eventos que los puedan comprometer
- Los procedimientos aseguran suficiencia y precisión de documentos fuente, registro/contabilización apropiada para documentos fuente y conversión oportuna
- La retención de documentos fuente es lo suficientemente larga para permitir la reconstrucción en caso de pérdida, la disponibilidad para revisiones y auditoría, las consultas legales o requerimientos regulatorios

Para la entrada de datos:

- Los documentos fuente siguen un proceso de aprobación apropiada antes de su captura
- Existe una separación de funciones apropiada entre las actividades de envío, aprobación, autorización y entrada de datos
- Existen códigos únicos de terminal o estación e identificaciones seguras de operadores

- Existen procesos de uso, mantenimiento y control de códigos de estación e IDs de operador
- Existen pistas de auditoría para identificar la fuente de entrada
- Existen rutinas de verificación para la edición de los datos capturados tan cerca del punto de origen como sea posible
- Existen procesos apropiados de manejo de datos de entrada erróneos
- Se asignan claramente las responsabilidades para hacer cumplir una autorización apropiada sobre los datos

Para el procesamiento de datos:

Los programas contienen rutinas de prevención, detección y corrección de errores:

- Los programas deben probar las entradas en cuanto a errores (por ejemplo, validación y edición)
- Los programas deben validar todas las transacciones contra una lista maestra
- Los programas deben rechazar la anulación de condiciones de error

Los procesos de manejo de errores incluyen:

- La corrección de errores y reenvío de la transacción debe ser aprobada
- La definición de responsabilidades individuales para el manejo de archivos en suspenso
- La generación de reportes de errores no resueltos emitidos a partir de los archivos en suspenso
- La disponibilidad del esquema de priorización de archivos suspendidos tomando como base la edad y el tipo

Existen bitácoras de los programas ejecutados y las transacciones procesadas/rechazadas para pistas de auditoría

Existe un grupo de control para monitorear las actividades de entrada e investigar los eventos no-estándar, así como balancear las cuentas de registros y totales de control para todos los datos procesados

Todos los campos son editados apropiadamente, aún si uno de los campos contiene algún error

Las tablas utilizadas en la validación son revisadas frecuentemente

Existen procedimientos por escrito para la corrección y reenvío de datos con errores incluyendo una solución que no afecte su reprocesamiento

Las transacciones reenviadas son procesadas exactamente como fueron procesadas originalmente

La responsabilidad de la corrección de errores reside dentro de la función de envío original

Los sistemas de Inteligencia Artificial están colocados en un marco referencial de control interactivo con operadores humanos para aseguran que las decisiones importantes se aprueben

Para las salidas, interfaces y distribución:

El acceso a las salidas está restringido física y lógicamente a personal autorizado

Se lleva a cabo una revisión continua de necesidades de salidas

Las salidas son balanceadas rutinariamente con respecto a totales de control

Existen pistas de auditoría para facilitar el seguimiento del procesamiento de transacciones y la reconciliación de datos alterados

La precisión de los reportes de salidas es revisada y los errores contenidos en las salidas son controlados por personal capacitado

Existe una definición clara sobre aspectos de seguridad durante las salidas, interfaces y distribución

Las fallas en seguridad durante cualquier fase son comunicadas a la administración, se llevan a cabo acciones correctivas sobre ellas y son reflejadas apropiadamente en nuevos procedimientos

El proceso y la responsabilidad de desechar/reciclar las salidas está claramente definida

La destrucción de materiales utilizados pero no requeridos después de procesados es presenciada por testigos

Todos los medios de entrada y salida son almacenados en un sitio de almacenamiento alterno en caso de requerirse en un futuro

La información marcada como eliminada cambia de tal forma que no se pueda recuperar

Para la librería de medios:

El contenido de la librería de medios es inventariado sistemáticamente

Las discrepancias descubiertas por el inventario son solucionadas oportunamente

Se toman medidas para mantener la integridad de los medios magnéticos almacenados en la librería

Existen procesos de mantenimiento y limpieza para proteger el contenido de la librería de medios

Las responsabilidades de la administración de la librería de medios han sido asignadas a miembros específicos del personal de TI

Existen estrategias de respaldo y restauración de medios:

Los respaldos de medios se llevan a cabo de acuerdo con la estrategia de respaldos y si la utilidad de los respaldos es verificada regularmente

Los respaldos de medios son almacenados con seguridad y si las localidades de almacenamiento son revisadas periódicamente en cuanto a la seguridad de su acceso físico y a la seguridad de los archivos de datos y otros elementos

Los periodos de retención y almacenamiento están definidos por documentos, datos, programas, reportes y mensajes (entrantes y salientes) así como los datos (llaves, certificados) utilizados para su encriptación y autentificación

Adicional al almacenamiento de documentos fuentes en papel, las conversaciones telefónicas son registradas y almacenadas—si no entra en conflicto con las leyes locales de privacidad—para transacciones y otras actividades que son parte de las actividades tradicionales del negocio que se llevan a cabo mediante el uso del teléfono

Los procedimientos adecuados están activos en relación al archivo de información (datos y programas) en línea con los requerimientos legales y del negocio y reforzando la capacidad de respuesta y reproducción

Para la autenticación e integridad de información:

La integridad de los archivos de datos se verifica periódicamente

Las solicitudes externas a la organización recibidas por vía telefónica o correo de voz se verifican confirmando por teléfono o algún otro medio de autenticación

Un método preestablecido se utiliza independiente a la verificación de la autentificación de la fuente y el contenido de las solicitudes de transacción recibida vía fax o sistemas de imágenes

La firma electrónica o la certificación se utilizan para verificar la integridad y autenticidad de los documentos electrónicos entrantes

Evaluar la suficiencia:

► Probando que:

La preparación de datos:

Para una muestra seleccionada de documentos fuente, existe consistencia evidente con respecto a los procedimientos establecidos relacionados con la autorización, aprobación, precisión, suficiencia y recepción de entrada de datos y si la entrada de datos es oportuna

El personal responsable de la información fuente, de su ingreso y conversión tiene conciencia y comprende los requerimientos de control en la preparación de datos

La entrada de datos:

El envío a proceso de datos de prueba (tanto transacciones correctas como erróneas) para asegurar que se llevan a cabo revisiones de precisión, suficiencia y autorización

Para transacciones seleccionadas se comparan los archivos maestros antes y después de la captura

Existe una apropiada revisión de retención, solución y de la integridad en el manejo de errores

Los procedimientos y acciones de manejo de errores cumplen con las políticas y controles establecidos

El procesamiento de datos:

Se utilizan efectivamente los totales de control corrida-a-corrida y los controles de actualización de archivos maestros

Se envían datos de prueba (tanto transacciones correctas como erróneas) para asegurar que se llevan a cabo la validación, autenticación y edición de procesamiento de datos tan cerca del punto de origen como sea posible

El proceso de manejo de errores es llevado a cabo de acuerdo con los procedimientos y controles establecidos

Se llevan a cabo la retención, solución y revisión apropiada de la integridad en el manejo de errores y que éstas funcionan adecuadamente

Los procedimientos y acciones del manejo de errores cumplen con los procedimientos y controles establecidos

La Salida, Interfaz y Distribución de Datos:

La salida es balanceada rutinariamente contra totales de control relevantes

Las pistas de auditoría son proporcionadas para facilitar el seguimiento del procesamiento de transacciones en la reconciliación de datos confusos o erróneos

Los reportes de salida son revisados en cuanto a su precisión por parte del proveedor y los usuarios relevantes

Existen la retención, solución y revisión apropiada de la integridad en el manejo de errores y que éstas funcionan adecuadamente

Los procedimientos y acciones de manejo de errores cumplen con las políticas y controles establecidos

Los reportes de salidas son asegurados al esperar ser distribuidos, así como aquéllos ya distribuidos a los usuarios de acuerdo con los procedimientos y controles establecidos

Existe la protección adecuada para la información sensible durante la transmisión y transporte contra los accesos no autorizados y las modificaciones

Existe una protección adecuada de información sensitiva durante la transmisión y transporte en cuanto a accesos y modificaciones no autorizadas

Los procedimientos y acciones para el desecho/reciclaje de información sensitiva cumplen con los procedimientos y controles establecidos

La Librería de Medios:

El contenido de la librería de medios es inventariado sistemáticamente, que todas las discrepancias encontradas son solucionadas oportunamente y se toman medidas para mantener la integridad de los medios almacenados en la librería

Los procedimientos de mantenimiento/limpieza diseñados para proteger el contenido de la librería de medios existen y funcionan adecuadamente

Las responsabilidades de la administración de la librería de medios son asignadas apropiadamente

La librería de medios es independiente de las funciones de preparación, entrada, procesamiento y salida

La estrategia de respaldos y restauración de medios es apropiada

Los respaldos de medios se llevan a cabo apropiadamente de acuerdo con la estrategia de respaldo definida

Los sitios de almacenamiento de medios son seguros físicamente y que su inventario está actualizado

El almacenamiento de datos considera los requerimientos de recuperación y la economía o efectividad de costos

Los períodos de retención y los términos de almacenamiento son apropiados para documentos, datos, programas y reportes

► Llevando a cabo:

Mediciones (“Benchmarking”) de la administración de datos contra organizaciones similares o estándares internacionales apropiados reconocidos como mejores prácticas de la industria

Para una selección de transacciones, confirmar lo apropiado del procesamiento durante:

- La preparación de datos
- El procesamiento de entradas
- El procesamiento de datos
- La salida, distribución o integración
- El manejo de errores en todas las fases del procesamiento
- La integridad de los datos a través del manejo de errores en todas las fases del procesamiento
- Retención y destrucción

Pruebas específicas para lo siguiente:

- Suficiencia, precisión y validez durante cada fase del procesamiento
- Aprobaciones y autorizaciones adecuadas
- Existencia de controles preventivos, detectivos y correctivos—dentro del procesamiento o a través del control de funciones manuales de grupo/procedimentales
- Retención de documentos fuente para la revisión posterior de la consistencia con respecto a los requerimientos de retención
- Recuperación de una selección de documentos fuente y transacciones para confirmar la existencia y la precisión
- Análisis de la disponibilidad de pistas de auditoría: existencia, identificación de fuente/operador y asegurar que cualquier

sistema de interfaz cuenta con niveles iguales de control sobre las transacciones

- Edición de las facilidades de programas de entrada y procesamiento, incluyendo, pero sin limitarse a:
    - Blancos en campos requeridos
    - Validación de códigos de transacciones
    - Montos negativos
    - Cualquier otra condición apropiada
    - Suficiencia de las pruebas de validación internas al procesamiento
    - Archivos suspensos con transacciones defectuosas, incluyendo los siguientes controles:
    - Identificación inmediata del operador que comete el error y aviso del error
    - Todas las transacciones de error son transferidas a estos archivos suspenso
    - El registro es mantenido hasta que la transacción es resuelta y eliminada
    - Las transacciones muestran código de error, fecha y hora de captura, operador y máquina

Comprobar el riesgo de los objetivos de control no alcanzados:

Para la integridad y autenticación de la información

El riesgo de direccionar mensajes (por carta, fax o e-mail) equivocadamente se reduce con los procedimientos adecuados

Existen protecciones adecuadas para asegurar la integridad, confidencialidad y no rechazo de los mensajes sensitivos transmitidos sobre internet o cualquier otra red pública

Los controles normalmente se aplican a un proceso de transacción específico, como faxes o contestadores telefónicos automáticos, también aplica a sistemas computacionales que soportan la transacción o proceso (Ej., software de fax en las computadoras personales)

- Los archivos de suspenso crean reportes de seguimiento para la revisión administrativa, el análisis de tendencias y entrenamiento correctivo
- Separación de las funciones de origen, entrada, procesamiento, verificación y distribución

Para una selección de transacciones de salida:

- Revisar una muestra de listas de transacciones procesadas en cuanto a su suficiencia y precisión
- Revisar una muestra de reportes de salida en cuanto a precisión y suficiencia
- Revisar los calendarios de retención de salidas en cuanto a su adecuación y cumplimiento de los procedimientos
- Confirmar que la distribución real de una muestra de salidas fue llevada a cabo con precisión
- Confirmar el procesamiento integrado confirmando la salida de una bitácora de procesamiento de transacciones de un sistema con la entrada de la bitácora de otro sistema
- Revisar los procedimientos de balanceo para todas las entradas, salidas de procesamiento y otras transacciones usadas por el sistema
- Confirmar que únicamente personal autorizado tiene acceso a reportes sensitivas
- Confirmar la destrucción o reubicación de almacenamientos en sitios externos para todos los medios de datos por políticas y procedimientos de retención
- Confirmar los períodos reales de retención contra los procedimientos de retención
- Atestiguar la entrega o transmisión real de salidas sensitivas y el cumplimiento con los procedimientos de procesamiento, distribución y seguridad
- Confirmar la creación e integridad de los respaldos en asociación con el procesamiento normal, así como para los requerimientos del plan de continuidad

Para la librería de medios:

- Revisar el acceso de los usuarios a los servicios/utilidades/utilitarios sensitivos; determinar que el acceso es apropiado
- Seleccionar una muestra de medios a ser destruida y observar el proceso completo; verificar el cumplimiento de los procedimientos aprobados
- Determinar lo adecuado de los controles para los datos en almacenamientos en el sitio externo y mientras los datos están en tránsito
- Obtener resultados del inventario de la librería de medios más reciente; confirmar su precisión
- Confirmar que los procesadores que mantienen los registros son suficientes para accesar los medios necesarios
- Revisar los controles para restringir el intento de saltar (bypass) las reglas de etiquetado internas y externas

- Probar el cumplimiento de los controles internos y externos vía revisión de medios seleccionados
- Revisar los procedimientos de creación de respaldos para asegurar la existencia de datos suficientes en caso de desastre
- Confirmar las inspecciones de la librería de medios por requerimientos programados de actividades

► Identificando:

- Si cuando los archivos de producción son accesados directamente por los operadores se crean y mantienen imágenes de los archivos “antes” y “después” del acceso
- Formas de entrada y salida sensitivas (por ejemplo, inventario/stock de cheques, certificados de reservas) no protegidas
- Bitácoras no llevadas y mantenidas para totales batch y de control para todas las fases del procesamiento
- Reportes de salidas no útiles a los usuarios: datos no relevantes y útiles, reportes no necesarios, distribución no apropiada, formato y frecuencia no adecuados, acceso en línea no controlado a los reportes

- Datos transmitidos sin controles adicionales, incluyendo:

    - Accesos de envío/recepción de transmisiones limitados
    - Autorización e identificación apropiadas del emisor y del receptor
    - Medios seguros de transmisión
    - Encriptación de datos transmitidos y algoritmos de decodificación apropiados
    - Pruebas de integridad de la transmisión en cuanto a su suficiencia
    - Procedimientos de retransmisión
    - Contratos de proveedores con controles faltantes como servicios de destrucción
    - Deficiencias en el sitio externo con respecto a amenazas ambientales tales como fuego, agua, fallas eléctricas y accesos no autorizados.

Si bien se enumeran todos los criterios establecidos por las Directrices de Auditoría COBIT, no es obligatorio utilizarlos todos, sino solamente los que se

aplican al caso particular, porque su inclusión es adecuar estos criterios de acuerdo a la necesidad práctica de las unidades en estudio u observación, dándole mayor o menor detalle.

1.3.5. ESTUDIO INSTRUMENTAL DEL CASO

Considerando en el presente estudio, el método de estudio instrumental de caso, cuyo propósito, como señala STAKE (1998), es obtener, mediante el análisis, una mayor claridad sobre las unidades en estudio. El caso es el instrumento para conseguir otros fines indagatorios, instrumentos que permiten conocer la situación actual de la empresa e indagar para lograr corregir o mejorar esta situación.

1.3.6. INFORME PRELIMINAR PROCESO INFORMACIÓN LIBRO DE VENTAS IVA

A. ENTIDAD AUDITADA: Empresa M & F Ltda.
B. ALCANCE DE LA AUDITORÍA: El Sistema de Información Contable Financiera, particularmente en los módulos de Generación del Libro de Ventas IVA, respecto al cumplimiento del proceso “Administración de la Información” de la norma COBIT.
C. NORMA APLICADA: COBIT, específicamente el proceso DS11 “Administración de la Información”.
D. RELEVAMIENTO:
    a. Organización: Empresa M & F Ltda., entidad privada con Matrícula de Comercio de FUNDEMPRESA No. 0001057-A, y NIT 4849501019 dedicada a actividades de Comercio en General y Servicios Generales.
    b. Objetivos de la Organización:
        - CREAR, DISEÑAR, COMECIALIZAR, OTORGAR, PROVEER E IMPLANTAR SERVICIOS DE CONSULTORIA EN GENERAL RESPECTO DE ACTIVIDADES INHERENTES AL COMERCIO;
        - COMERCIALIZAR Y PROVEER PRODUCTOS Y SERVICIOS DE FERRETERÍA Y DERIVADOS POR MAYOR Y MENOR, A NIVEL DOMÉSTICO DEL HOGAR Y CORPORATIVO DE ENTIDADES PÚBLICAS Y PRIVADAS.
    c. Unidad de Estudio: Departamento Financiero Contable, respecto al Sistema de Información Contable, en el módulo de Generación de la información para el Libro Mensual de Ventas

I.V.A., que se debe presentar al Servicio Nacional de Impuestos (S.I.N.), el cual debe reflejar fielmente el movimiento mensual de ventas que realizó la entidad, con objetividad y adecuado a la realidad, para dar cumplimiento estricto a la normativa tributaria vigente, que permita realizar declaraciones impositivas oportunas en los plazos establecidos en la norma.

Su dependencia administrativa es Gerencia General y, su dependencia en el Sistema de Información es la Unidad de Sistemas.

d. Políticas y Estrategias del Departamento:

Políticas y estrategias del Sistema de Información:

i) Optimización de las tareas y funciones del personal operativo. ii) Automatización del manejo de la información. iii) Control y seguimiento permanente de las ventas. iv) Registro automático de los libros contables. v) Generación oportuna, verídica y en tiempo real de los Estados Financieros.

Políticas y estrategias de Manejo de la Información:

i) Acceso con niveles de seguridad y perfiles de usuario al Sistema. ii) Validación del registro de la información en el sistema. iii) Generación de Reportes oportuna que reflejan la información en la instancia requerida o solicitada. iv) Respaldo de la información periódica. v) Acceso restringido a las Bases de Datos almacenadas. vi) Acceso restringido y con niveles de seguridad a los equipos que almacenan las bases de datos y a los que ejecutan las aplicaciones informáticas del Sistema de Información.

e. Funciones, Subfunciones y Tareas:

1. Mostrar la información de las Ventas en el periodo actual o seleccionado: Despliegue de la información necesaria de las ventas realizadas, de acuerdo a formato establecido por la norma tributaria.

   Tareas que se pueden realizar: Filtros y ordenamiento de la información, por fechas, por números, por clientes, etc.

2. Anulación de facturas:

   Despliegue de detalles de factura por número, etc. para permitir su anulación por sistema.

3. Generación del Libro de Ventas I.V.A.:

   Generar Libro de Ventas del periodo actual a tributar, en el formato que solicita la norma, para su envío posterior a la plataforma virtual del S.I.N.

4. Envío del Libro de Ventas I.V.A. al S.I.N.:

   Escoger y enviar el archivo en el formato establecido por la norma tributaria a la plataforma virtual del S.I.N.

f. Diagnóstico:

De acuerdo con el Dominio “Entrega de Servicios y Soporte” y el Proceso “Administración de la Información”, se ha desarrollado un análisis, donde se identifica con que normas está cumpliendo la organización y con cuáles no.
A partir de este punto se definirá que es lo que la organización debería hacer para cumplir con las normas COBIT, para permitir mejorar o corregir la situación actual.

1.3.7. INFORME PRELIMINAR PROCESO INFORMACIÓN REGISTRO DE INGRESOS POR VENTAS

E. ENTIDAD AUDITADA: Empresa M & F Ltda.
F. ALCANCE DE LA AUDITORÍA: El Sistema de Información Contable Financiera, particularmente en los módulos de Registro de las transacciones de Ingresos por Ventas, respecto al cumplimiento del proceso “Administración de la Información” de la norma COBIT.
G. NORMA APLICADA: COBIT, específicamente el proceso DS11 “Administración de la Información”.
H. RELEVAMIENTO:
   a. Organización: Empresa M & F Ltda., entidad privada con Matrícula de Comercio de FUNDEMPRESA No. 0001057-A, y NIT 4849501019 dedicada a actividades de Comercio en General y Servicios Generales.
   b. Objetivos de la Organización:
      - CREAR, DISEÑAR, COMECIALIZAR, OTORGAR, PROVEER E IMPLANTAR SERVICIOS DE CONSULTORIA EN GENERAL RESPECTO DE ACTIVIDADES INHERENTES AL COMERCIO;
      - COMERCIALIZAR Y PROVEER PRODUCTOS Y SERVICIOS DE FERRETERÍA Y DERIVADOS POR MAYOR Y MENOR, A NIVEL DOMÉSTICO DEL HOGAR Y CORPORATIVO DE ENTIDADES PÚBLICAS Y PRIVADAS.
   c. Unidad de Estudio: Departamento Financiero Contable, respecto al Sistema de Información Contable, en el módulo de Registro de la información de las transacciones de Ingresos por Ventas, que deben reflejar fielmente el movimiento diario de ingresos por ventas que realiza la entidad, con objetividad y adecuado a la realidad, para dar cumplimiento estricto a las políticas establecidas por la administración, que permitan registrar la información de los ingresos por ventas como reflejo digital del movimiento de ventas.

      Su dependencia administrativa es Gerencia General y, su dependencia en el Sistema de Información es la Unidad de Sistemas.
   d. Políticas y Estrategias del Departamento:

      Políticas y estrategias del Sistema de Información:

i) Optimización de las tareas y funciones del personal operativo. ii) Automatización del manejo de la información. iii) Control y seguimiento permanente de las ventas. iv) Registro automático de los libros contables. v) Generación oportuna, verídica y en tiempo real de los Estados Financieros.

Políticas y estrategias de Manejo de la Información:

i) Acceso con niveles de seguridad y perfiles de usuario al Sistema. ii) Validación del registro de la información en el sistema. iii) Generación de Reportes oportuna que reflejan la información en la instancia requerida o solicitada. iv) Respaldo de la información periódica. v) Acceso restringido a las Bases de Datos almacenadas. vi) Acceso restringido y con niveles de seguridad a los equipos que almacenan las bases de datos y a los que ejecutan las aplicaciones informáticas del Sistema de Información.

e. Funciones, Subfunciones y Tareas:

1. Al momento de realizar una venta, registrar la misma en el sistema como registro nuevo, ingresando los datos de la cantidad vendida, los descuentos aplicados, el tipo de pago, los datos del o de los clientes, etc.
2. Si existen algunos cambios, se puede Actualizar la información correspondiente en el sistema.
3. Registrar el pago en el módulo de caja, para guardar el tipo de pago efectuado y generar la factura asociada correspondiente, que refleje la venta oportunamente.
4. Generar la transacción contable correspondiente en el sistema, registrando la información de la venta en el Libro Diario, de acuerdo a las cuentas contables utilizadas, las mismas que se registran automáticamente.
5. Generar el Comprobante de Ingreso correspondiente, asociado a la venta.
6. Generar la Factura de Venta, con los datos proporcionados por el cliente, para la entrega posterior de la factura impresa.
7. Generar el Comprobante de Asiento de Diario para su almacenamiento en la parte contable en formato impreso.

f. Diagnóstico:

De acuerdo con el Dominio “Entrega de Servicios y Soporte” y el Proceso “Administración de la Información”, se ha desarrollado un análisis, donde se identifica con que normas está cumpliendo la organización y con cuáles no.

A partir de este punto se definirá que es lo que la organización debería hacer para cumplir con las normas COBIT, para permitir mejorar o corregir la situación actual.

2. BIBLIOGRAFÍA

AMADO SUÁREZ, A. (2008). *Auditoría de Comunicación.* La Crujía.

COHEN, L., & MANION, L. (1990). *Métodos de Investigación Educativa.* Madrid: La Muralla.

CONTRALORÍA GENERAL DEL ESTADO DE BOLIVIA. (2012). *Normas de Auditoría de Tecnologías de Información y Comunicación NE/CE-017 .* La Paz - Bolivia: CGE.

ELIZONDO LÓPEZ, A. (2004). *Proceso Contable 3.* México D.F.: International Thomson Editores.

ENCICLOPEDIA DE DEFINICIONES (DEFINICION DE:). (2008-2016). *definicion.de*. Recuperado el 25 de 04 de 2016, de http://definicion.de/informatica/

FLICK, U. (2007). *Introducción a la investigación cualitativa.* Madrid - España: Ediciones Morata S.L.

GÓMEZ RAMÍREZ, V. (2014). *Evaluación de la seguridad de la información con la metodología Octave.* Medellín: Institución Universitaria Pascual Bravo.

INFORMATION SYSTEMS AUDIT AND CONTROL, Asociation; IT GOBERNANCE, Institute;. (2000). *COBIT Objetivos de Control.* Illinois, U.S.A.: ISACA / ITGI.

ISACA. (2012). *Metodología COBIT.* U.S.A.: ISACA. Recuperado el 27 de 09 de 2016, de http://www.isaca.org/cobit

LATTUCA, A., MORA, C., & Et Al. (1991). *Manual de Auditoría.* Buenos Aires: Federación Argentina de Consejos Profesionales de Ciencias Económicas.

LAUDON, K. C., & LAUDON, J. P. (2012). *Sistemas de Información Gerencial.* México D.F.: Pearson.

LUCERO GÓMEZ, A. (2012). *Análisis y Gestión de Riesgos utilizando la metodología Magerit.* Cuenca, Ecuador: Universidad de Cuenca.

MARTÍNEZ BONAFÉ, J. (1988). El estudio de casos en la investigación educativa. *Revista Investigación en la Escuela*(6).

PÉREZ SERRANO, G. (1998). *Investigación Cualitativa: Retos e Interrogantes. I. Métodos.* Madrid: La Muralla.

PIATTINI, M., DEL PESO, E., & Et Al. (2001). *Auditoría Informática, un enfoque práctico.* México D.F.: AlfaOmega Grupo Editor.

SOLARTE SOLARTE, F. N. (2014). *Riesgos y Control Informático.* San Juán del Pasto, Nariño, Colombia: Universidad Nacional Abierta y a Distancia UNAD.

STAKE, R. (1998). *Investigación con Estudio de Casos.* México D.F.: Morata.

TAYLOR, S., & BOGDAN, R. (1986). *Introducción a los métodos cualitativos de investigación.* Buenos Aires: PAIDOS.

YIN, R. (1989). *INVESTIGACIÓN SOBRE ESTUDIO DE CASOS Diseño y Métodos.* Londres: SAGE Publications.