UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

AUDITORÍA SARBANES-OXLEY DE LA INDUSTRIA FARMACEÚTICA

INFORME DE ACTIVIDADES PROFESIONALES

Para obtener el título de Ingeniero en Computación

Presenta

Sergio Raymundo González Cruz

Asesor Académico: M.C. María Jaquelina López Barrientos

Asesor Laboral: Ing. Manuel Alejandro Orozco Juárez

MÉXICO, D.F. **2012**

DEDICATORIAS

A mis padres,

Por brindarme día a día su cariño, demostrarme cómo enfrentar los retos y sobre todo su apoyo incondicional para facilitarme el logro de mis metas.

A mis hermanos,

Que con su ejemplo de dedicación y logro de metas sin encontrar límites, me inspiraron para lograr ser un gran profesional en todos los aspectos.

A mi esposa SARAI,

Por todo este tiempo que ha estado a mi lado y que me ha llenado de amor, cariño, apoyo y sobre todo esa comunicación tan estrecha que no me ha permitido caer en ningún momento.

Sergio Raymundo González Cruz

AGRADECIMIENTOS

A la ***Universidad Nacional Autónoma de México*** y en especial a la ***Facultad de Ingeniería*** por la formación de calidad, de principios y de riqueza en conocimientos.

A todos los ***profesores*** que participaron en mí desarrollo profesional durante la carrera, gracias al conocimiento trasferido, consejos otorgados, calidez y esmero en cada clase que me proporcionaron.

A la ***Mtra. Jacqueline López Barrientos*** mí asesora y guía que me ha apoyado con gran entusiasmo, a pesar de mis atrasos en la elaboración de este informe.

A ***Deloitte*** que me ha brindado un lugar de formación profesional y aprendizaje día a día.

G R A C I A S

Sergio Raymundo González Cruz

Contenido

INTRODUCCIÓN

En las dos últimas décadas se han dado grandes desarrollos dentro del ámbito de las tecnologías de la información que han originado la necesidad de examinar y evaluar la veracidad, objetividad y exactitud de la información operacional y administrativa. Es por ello que surge con mayor impacto y necesidad, el concepto de auditoría que tiene como función analizar y apreciar, las acciones correctivas, el control interno que tienen las empresas para contar con la posibilidad de avalar la integridad de sus activos, la autenticidad de la información y la eficacia de los sistemas de gestión.

De hecho a finales del 2001, escándalos contables y financieros ocurrieron especialmente en corporaciones multinacionales con tecnologías de información avanzadas, originando una disminución de la confianza del público inversor en la información financiera de las empresas, así como la necesidad de revisar la legislación al respecto. Es así como el 30 de julio del 2002, el Congreso de los Estados Unidos de América aprobó la Ley Sarbanes-Oxley, teniendo como objetivo principal la fijación de lineamientos a las compañías públicas, es decir, aquellas que están inscritas en la Security Exchange Comission –SEC (Bolsa de Valores de los Estados Unidos de América).

El Comité de Supervisión de Contabilidad para empresas públicas (Public Company Accounting Oversight Board/PCAOB) fue creado para auditar las compañías que se encuentran sujetas a las leyes, con el fin de proteger los intereses de los inversores y dar a conocer al público interesado en la preparación de reportes de auditoría independientes, informativos y correctos. A partir de esa fecha, cualquier empresa que cotice en la Bolsa de Valores de EUA, ha sido obligada a ser certificada por un ente independiente que avale el correcto procesamiento de la información financiera a través de sus sistemas tecnológicos.

Así, el objetivo actual del presente informe de actividades es: Realizar una auditoría bajo la ley Sarbanes-Oxley a una compañía que requiere le sea proporcionada una certificación que avale el íntegro procesamiento de la información financiera.

CAPÍTULO 1

TRAYECTORIA DE QUIÉN PRESENTA EL INFORME DE ACTIVIDADES PROFESIONALES

En el presente capítulo, se menciona el panorama general de mi trayectoria estudiantil hasta llegar al ámbito laboral.

Haciendo énfasis en los conocimientos adquiridos durante la vida en la Facultad de Ingeniería.

1.1 Trayectoria estudiantil

Durante mi infancia siempre disfrute del uso de las computadoras (aquellas con disco duro de 2 GB y aún con la unidad de diskette 3 ½) ya sea por jugar, por escribir algo en el procesador de texto o por realizar operaciones aritméticas en las hojas de cálculo. Además al contar con 3 hermanos profesionistas, siempre tuve la suficiente motivación para poder seleccionar una carrera acorde a mi creatividad y más aún cuando uno de ellos es Ingeniero en Computación egresado de la ENEP Aragón.

Por todo lo anterior y una vez concluidos mis estudios de bachillerato en la Escuela Nacional Preparatoria No. 5 en el año 2000 decidí realizar mi examen de ingreso a Ciudad Universitaria en la Facultad de Ingeniería para estudiar la carrera de Ingeniería en Computación.

Meses después, recibí una carta donde me era informado que el resultado del examen había sido exitoso, por lo cual con mucho agrado y felicidad asistí a mi primer día en la facultad donde además note que entré a un grupo piloto llamado “estudiantes expertos” que contaba con la primicia de tener clases con excelentes profesores así como tener clases adicionales (fuera del horario normal de clases), el plan de estudios fue el 408 y la generación fue 2001-2005.

Ese primer semestre tuve la oportunidad de convivir con excelentes personas, ahora con un puesto laboral importante o estudiando en el extranjero, de las cuales aprendí a trabajar en equipo, ser colaborativo y sobre todo a adoptar una metodología de estudio que me sirvió para mis semestres posteriores. Fue así como cursé 4 semestres del tronco común que aunque no fueron calificaciones del todo satisfactorias, logré obtener conocimientos sólidos que me fortalecieron para desenvolverme de mejor manera en las siguientes asignaturas: Cálculo II, Cálculo III, Ecuaciones Diferenciales y Matemáticas Avanzadas.

Sin embargo, las asignaturas que más disfrute en general fueron: Estructuras de Datos, Ingeniería de Programación, Base de Datos, Memorias y Periféricos y Redes de Computadoras y Seguridad fueron de mi completo agrado al relacionarse totalmente con lo que quería aprender y aplicar en un futuro.

Cada semestre viví un ambiente intenso de mucha presión pero con la filosofía de que estaba estudiando lo que me gustaba, pude superar cualquier adversidad que al día de hoy agradezco ya que me ayudó a crecer y formarme como profesionista. Conté con excelentes maestros que siempre tuvieron la disposición de proporcionarme su conocimiento en cualquier momento.

.

La vida dentro de la UNAM fue fabulosa y de total aprendizaje, no sólo escolar, sino también cultural y de madurez. Estoy agradecido de pertenecer a nuestra máxima casa de estudios.

1.2 Conclusión de créditos

La carrera de Ingeniería en Computación la finalice en el primer semestre de 2006 (2006-1) de manera ordinaria, sin la necesidad de llegar a ningún un examen extraordinario, y sin atraso con respecto a los años de duración de la carrera. Fueron un total de 56 materias aprobadas con el 100% de los créditos cumplidos y promedio final de **8.44.**

1.3 Transición estudiantil a laboral

En Julio de 2005 finalice los créditos requeridos conforme lo indica el plan de estudios de la carrera, para después subir mi curriculum en un sitio de Internet para localización de trabajo.

A finales de Agosto del mismo año recibí la notificación de ir a cuatro entrevistas con Recursos Humanos y Gerentes del área en la que me encuentro actualmente, de la compañía con razón social Galaz, Yamazaqui, Ruiz, Urquiza, S.C. conocida bajo la marca Deloitte.

En las entrevistas realicé exámenes de conocimientos, lógica, psicológicos y de inglés teniendo resultados positivos y agradables para el personal del área solicitante.

Fue hasta el 25 de Octubre del 2005 cuando me fue hecha una propuesta económica e ingresé el 1 de Noviembre del mismo año hasta el día de hoy que continúo desarrollando habilidades y conocimientos.

1.4 Historia Laboral

Diferentes firmas globales se han preocupado por ofrecer los servicios de asistencia en la identificación, evaluación e implantación de metodologías para valorar y mitigar riesgos, así como también, recomendar controles, entre los cuales destacan KPMG, PricewaterhouseCoopers, Ernst & Young y Deloitte, siendo esta última líder en el sector.

Con una red global de firmas miembro en 140 países, **Deloitte** brinda su experiencia y profesionalismo en auditoría, Enterprise Risk Services (ERS), impuestos, consultoría y asesoría financiera a organizaciones públicas y privadas de diversas industrias. En la actualidad, atiende a más del 57 por ciento de las empresas más importantes del país.

Como parte de la línea de servicio de ERS (Enterprise Risk Services), se encuentra el área de Technology Risk (TR) que tiene como objetivo principal ayudar a las organizaciones a diseñar e implementar estrategias que permitan medir y monitorear periódicamente sus procesos para identificar oportunamente los riesgos del negocio y facilitar el mejoramiento continuo.

Los servicios proporcionados, respaldados por las mejores prácticas, permiten integrar la administración de riesgos con la estrategia de la compañía, con el fin de mejorar el desempeño del negocio, generando ventajas competitivas e incrementar el valor del negocio.

Mi ingreso fue al área de ERS y línea de servicio TR como analista del área (primer peldaño de la pirámide). Mis primeras asignaciones laborales en Deloitte se relacionan a auditorías de estados financieros del sector bancario, en la cual tuve una buena experiencia aun cuando no se trata de un sector en el que me interesará desarrollarme.

Fue hasta mi tercera asignación y en la industria energética, donde encontré que esta compañía contaba con el sistema ERP-SAP que llamó poderosamente mi atención por la integración en el flujo de información y su módulo de seguridad que generaba mi curiosidad.

Es ahí donde tomé un rumbo enfocado a este sistema, el cual he estado auditando desde Enero del 2006 hasta la fecha en diferentes industrias (manufactura, farmacéutica, gobierno, medios y de consumo) siendo ahora un experto en la auditoría de procesos o de tecnología donde se encuentre involucrado SAP. Es importante mencionar que desde el 2009, ERS ha estado sufriendo modificaciones reestructúrales y no sólo realizamos auditorías sino que ahora hemos tomado un perfil de consultoría donde apoyamos a las compañías para contar con todo un ambiente de control de acuerdo a las mejores prácticas.

Mi crecimiento dentro de la compañía ha sido constante: Analista (2005-2007), Consultor (2007-2009) y Consultor Snr (2009 a la fecha), en estos momentos me encuentro compitiendo por alcanzar el siguiente nivel que corresponde a Gerente.

La estructura piramidal de la línea de servicio TR con el número de personas en cada puesto se muestra en la Fig. 1.1

Socio (4)
Director (2)
Gerente Snr (5)
Gerente (6)
Consultor Snr (26)
Consultor (14)
Analista (30)

Fig. 1.1 Estructura Piramidal.

1.5 Conocimientos adquiridos durante la etapa escolar para desarrollo laboral

Gracias a la Universidad Autónoma de México a través de su Facultad de Ingeniería y el plan de estudios 408 de la carrera de Ingeniero en Computación adquirí conocimientos que agradeceré todo el tiempo ya que me han permitido desarrollarme en mi vida laboral de manera exitosa. Al día puedo mencionar que la FI me proporcionó las bases para superarme y que ahora aplico día a día en cada uno de los servicios profesionales otorgados a diferentes clientes de distintos sectores.

La auditoría y consultoría dentro de Deloitte exigen conocimiento de arquitectura de computadoras incluyendo historia y desarrollo, así como conocimientos muy específicos sobre seguridad en redes, redes de computadoras, bases de datos, operaciones de centro de cómputo y obviamente metodologías de auditoría en sistemas para cumplir con lo requerido sobre los servicios que ofrece la firma a las distintas industrias.

A continuación se enlistan las asignaturas que me apoyaron a este desarrollo.

1.5.1 Computadoras y Programación

Temas relevantes en mi actividad profesional:

- *Antecedentes históricos de la computación*: Lenguajes, sistemas de numeración, métodos de conteo, calculadoras, entre otras.
- *Era de la información:* 1ª generación (bulbos, perforadora de tarjetas), 2ª generación (transistores, memoria de ferrita, programas almacenados), 3ª. Generación (circuitos integrados), 4ª generación (microprocesadores, sistemas expertos, microcomputadoras) y 5ª generación (inteligencia artificial).
- *Sistemas numéricos*: Decimal, octal, binario y hexadecimal que permiten la transmisión de mensajes.
- *Representación de un algoritmo*: Diagramas de flujo que representan el inicio y el fin de un procedimiento.
- *Lenguajes de programación como C++:* declaraciones de tipo, instrucciones, módulos, estructuras, unidades y apuntadores.

1.5.2 Estadística

Temas relevantes en mi actividad profesional:

- *Conceptos básicos*: estadística, investigación básica, investigación aplicada y etapas de la investigación.
- *Tipos de muestreo*: aleatorio simple, sistemático, estratificado, conglomerado.
- *Tipos de estadística:* paramétrica, no paramétrica, univariable y multivariable.

- Medidas descriptivas: central, dispersión, asimetría y apuntamiento.

1.5.3 Sistemas Operativos

Temas relevantes en mi actividad profesional:

- *Componentes:* Software, Hardware y Firmware.
- *Contexto de un sistema operativo:* software aplicativo, software de base y hardware.
- *Tipos de sistemas operativos:* Monolítico, capas, máquinas virtuales.
- *Modelos:* cliente-servidor y abiertos.
- *Componentes de un sistema operativo actual:* procesador, memoria, drivers, sistemas de archivos, llamadas al sistema, estados de un proceso.
- *Arquitectura de Sistemas Operativos, asignación de memoria y técnicas de planificación.*
- *Topologías de procesadores*

1.5.4 Bases de Datos

Temas relevantes en mi actividad profesional:

- *Conceptos básicos:* definición de una base de datos.
- *Características de una base de datos:* Integridad, Redundancia y Consistencia
- *Sistema Manejador de Bases de Datos:* Arquitectura, seguridad, concurrencia, lenguajes de datos y diccionario de datos.
- *Modelo de datos:* Jerárquico, red, entidad-relación, relacional, orientado a objetos, flujo de datos y consulta de datos.
- *Modelos:* conceptual y relacional
- *Normalización*
- *Organización física de la BD:* indexación, dispersión y autentificación
- *Administración de la base de datos:* respaldo y recuperación.
- *Bases de Datos Distribuidas*
-

1.5.5 Redes de Computadoras

Temas relevantes en mi actividad profesional:

- *Conceptos básicos:* red de computadoras.
- *Topologías de red:* estrella, árbol, anillo, bus, malla e híbridas.
- *Evolución de las redes de datos:* cobertura geográfica, velocidad, control de errores en LAN, MAN, GAN y WAN.
- *Modelo OSI:* Capas física, enlace, red, transporte, sesión, presentación y aplicación.
- *Modelo TCP/IP.*

- *Capa física (*medios de transmisión terrestres: coaxial, par trenzado y fibra óptica; medios de transmisión aéreos: redes inalámbricas, microondas, enlaces satélital, infrarrojo).
- *Cableado estructurado.*
- *Capa enlace:* transmisión de datos y protocolos.
- *Capa red:* protocolo IP, subredes, enrutamiento.
- *Capa transporte:* paquetes, control de flujo y protocolo TCP /UDP.
- *Capa sesión:* puertos y procedimientos remotos.
- *Capa presentación: ASCII y criptografía.*
- *Capa aplicación: Protocolos(HTTP, SMTP, TELNET, FTP).*

1.5.6 Optativa: Temas Especiales de Computación (Seguridad Informática)

Temas relevantes en mi actividad profesional:

- *Conceptos básicos:* contexto de la seguridad y sus relaciones.
- *Esquema de seguridad:* objeto de evaluación, entorno, hipótesis, amenazas, políticas, requerimientos funcionales y garantía.
- *Servicios de seguridad:* Confidencialidad, autenticación, integridad, no repudio, control de acceso y disponibilidad.
- *Amenazas y vulnerabilidades.*
- *Tipos de ataques y técnicas de intrusión:* obtención de información, identificación de vulnerabilidades, instalaciones físicas y explotación de acceso a sistemas y redes.
- *Políticas de Seguridad Informática y planes de contingencia.*
- *Análisis de riesgo en activos, impactos, manejo, controles.*

1.5.7 Optativa: Organización y Administración de Centros de Cómputo

Temas relevantes en mi actividad profesional:

- *Vitalidad de una empresa y liderazgo del dirigente.*
- *Planeación estratégica del área de sistemas.*
- *Organización, dirección y administración.*
- *Organigrama.*
- *Instalaciones del centro de cómputo:* espacio, piso, puertas, equipos de controles ambientales.
- *Selección de hardware y software.*
- *Contratos y arrendamientos.*
- *Políticas, normas y procedimientos para homogeneizar el desarrollo de sistemas de información.*
- *Estrategias de reingeniería de programación:* mantenimiento del software, nuevas tecnologías, reestructuración.
- *Procesamiento centralizado y distribuido.*
- *Arquitectura cliente/servidor:* condiciones, razones, definición, impactos.
- *Administración de redes.*
- *Auditoría Informática:* conceptos y objetivos.

- *Auditoría a equipos, aplicaciones, seguridad, HW y SW.*
- *Outsourcing.*

CAPÍTULO 2

PRINCIPALES PROYECTOS LABORALES

En el presente capítulo, se mencionan los proyectos laborales que han dejado huella en mí vida laboral en experiencia, conocimiento y desarrollo de aptitudes.

Estos proyectos dan la pauta para el desarrollo de este informe de actividades.

2.1 Introducción

La línea de servicio ERS (Enterprise Risk Services) desde el 2005 hasta el 2009 el principal ingreso del área incurría en auditorías financieras, externas e internas y es a partir del 2009, que el área ha entrado en una transición donde se ofrecen servicios de consultoría relacionados a seguridad y controles como lo son:

- Revisión de cumplimiento de seguridad lógica en sistemas
- Evaluación de roles y perfiles
- Análisis de volumetría
- Implementación de herramientas relacionadas con control interno
- Diagnósticos de Segregación de Funciones
- Documentación de Políticas y procedimientos
- Hackeo ético y pruebas de penetración
- Análisis de datos
- Análisis de accesos a sistemas

Debido a esta evolución interna, el personal de área se ha envuelto en un aprendizaje mucho más integrado desarrollando temas técnicos (configuraciones, uso de herramientas, programación) y al mismo tiempo administrativos (manejo de tiempos de entrega estrictos, entregables, eficiencia) que permiten fortalecer al personal y sobre todo al área que se espera cuente con un ingreso mayor al de muchas otras áreas y líneas de servicio de la firma.

2.2 Primer Proyecto Importante

2.2.1 Compañía

Compañía 1

Empresa líder en la industria química y petroquímica latinoamericana. Cuenta con más de 50 años de trayectoria en sus campos de actividad y más de 30 de cotizar en la Bolsa de Valores de México. Esta compañía produce y comercializa una gran variedad de materias primas, derivados industriales y productos terminados, que responden a la demanda de bienes esenciales para la construcción, el suministro y saneamiento de agua, la generación de energía, el transporte, las comunicaciones y el cuidado de la salud, entre muchos otros.

Sus compañías, integradas verticalmente en cadenas productivas del cloro-vinilo, el flúor y los productos transformados, compiten exitosamente en el mercado global, donde la calidad, la eficiencia y la agilidad son factores determinantes.

2.2.2 Objetivo

El objetivo de este proyecto fue realizar en 2 meses la auditoría de soporte a los estados financieros relacionada a los sistemas para esta compañía en constante crecimiento.

2.2.3 Principales logros

Esta compañía es uno de los principales clientes para Deloitte en la parte de auditoría, esto debido a la estructura organizacional e infraestructura tecnológica que comprende subsidiarias de otros países como lo son: Brasil, Argentina, Colombia, Venezuela, Inglaterra, Estados Unidos y la mayor parte de Centroamérica. Los principales logros durante este proyecto fueron:

- Administración conjunta del proyecto con otros países.
- Centralización de información.
- Desarrollo de conocimientos técnicos en equipos de red por infraestructura compleja: VLAN, oficinas remotas y satélites.
- Conocimiento de seguridad en el sistema SAP ERP.
- Extracción de la información financiera para análisis de datos.
- Relaciones laborales exitosas al trabajar con usuarios “difíciles” de tratar.
- Resultados satisfactorios en tiempo y forma en circunstancias de trabajo bajo presión.
- Promoción a **Consultor Snr.**

El logro general y que permitió ser exitoso fue la administración y coordinación correcta del proyecto sobre todo el control y contacto con otros países.

2.3 Segundo Proyecto Importante

2.3.1 Compañía

Compañía 2

Empresa líder en consumo, fundada en 1925, es líder en la elaboración, distribución y venta de cerveza en México**.** Cuenta con una capacidad instalada de 65 millones de hectolitros anuales de cerveza. Actualmente tiene trece marcas, de las cuales exporta seis contando con su presencia en 170 países. Como parte de las ganancias por bebidas también produce y distribuye agua embotellada a lo largo y ancho en el país.

2.3.2 Objetivo

El objetivo de este proyecto fue realizar un análisis de segregación de funciones sobre los roles y perfiles actualmente construidos en la compañía con el fin de contar con roles libres de conflictos.

2.3.3 Principales logros

Derivado de la necesidad de apoyo de consultoría por parte de la compañía para contar con un sistema nuevo que controle toda la administración y operación, Deloitte ha sido una parte importante en el logro de este objetivo al liderar este enfoque nuevo. En este proyecto, mis principales logros fueron:

- Entendimiento de la compañía en un tiempo muy reducido
- Conocimiento de seguridad de roles en SAP
- Desarrollo de herramientas para análisis de SoD (Segregación de Funciones)
- Adaptarse a proyectos nunca antes realizados
- Resultados satisfactorios en tiempo y forma
- Sin necesidad de superiores que monitorearan mi labor.

Este proyecto fue mi consolidación como Consultor Snr que permitió desarrollar habilidades técnicas y administrativas a mayor grado.

2.4 Tercer Proyecto Importante

2.4.1 Compañía

Compañía 3

Sobre una superficie de 26,000 metros cuadrados y más de mil trescientos colaboradores, esta empresa fabrica y comercializa productos farmacéuticos oncológicos, cardiometabólicos, primary care y de alta especialidad (biotecnológicos).

En su división Consumer Health comercializa productos OTC y, en su división Química, una amplia gama de productos químicos (pigmentos, cosméticos, biociencias y alimentos) para diversas industrias.

Colaboradores distribuidos en las áreas de producción, ventas, tecnología, recursos humanos, finanzas, marketing, entre otras, hacen de la organización la filial con mejores resultados en Latinoamérica y que busca ser la empresa modelo Farma y Química de México.

2.4.2 Objetivo

El objetivo de este proyecto fue realizar un análisis de segregación de funciones y diseño de controles mitigantes que permitan mantener controlados los riesgos de accesos posibles en la compañía.

2.4.3 Principales logros

Este cliente no fue un servicio planeado, otra área de la firma solicitó apoyo para facilitar otro punto de vista al cliente, esto por el conocimiento en controles y riesgos, los cuales es el "núcleo" de nuestra área.

El reto fue entender la problemática, determinar los riesgos y explicarlos en un lenguaje claro y comprensible de manera que dichos riesgos quedarán explícitos en términos del lenguaje de la compañía. Los principales logros fueron:

- Reconocimiento de los riesgos en la industria farmacéutica.
- Aporte de mi experiencia para definición de controles mitigantes.
- El cliente ha solicitado que este servicio sea recurrente.

CAPÍTULO 3
CASO DE ESTUDIO

En el presente capítulo, se menciona el caso de estudio que será desarrollado en este informe. Haciendo énfasis en las características y necesidades del cliente.

3.1 Cliente

La compañía internacional “x” está especializada en desarrollar y comercializar productos de prescripción y sin receta farmacéutica que marcan una diferencia significativa en la vida de los pacientes.

Esta compañía “x” se enfoca en las áreas terapéuticas de neurología y dermatología principalmente en Estados Unidos, Canadá, México, Brasil, Europa y Australia, empleando aproximadamente 4,000 empleados en todo el mundo siendo los sitios de manufactura en Canadá, Brasil, Polonia y México.

Hasta Agosto del 2011, la compañía “x” contó con ingresos de $609 millones de dólares anuales que se componen por ventas, alianzas, acuerdos comerciales y otros ingresos.

La compañía “x” emplea a 1300 personas, está conformado por un grupo de compañías, encontrándose la principal en Estados Unidos, quien es primordialmente responsable de la manufacturación y comercialización de productos, principalmente en las áreas de ginecología, dermatología y dolor.

3.2 Antecedentes

“x” es una compañía fundada en 1970 y que ha crecido con el tiempo, esto es, por las inversiones que han realizado últimamente al fusionarse con otras compañías que han permitido incrementar la oferta de productos para la salud y en consecuencia han beneficiado en ganancias a la empresa.

Al estar inscrita en la bolsa de valores de Nueva York, permite que los inversionistas canalicen sus recursos económicos a esta compañía en busca de capital para ambas partes, sin embargo, esas inversiones conllevan a un nivel de confianza entre el inversionista y la compañía. Para el establecimiento de esa confianza es requerida una auditoría.

El concepto de auditoría fue desarrollada en los años 50´s bajo una época de investigación y artículos que sirvieron como base para generar un código de ética, responsabilidades de un auditor, conocimientos generales y creación de certificaciones que avalan como auditor interno, sin embargo, esto no fue suficiente, ya que con la aparición de vulnerabilidades y riesgos (por la misma evolución de los sistemas de información) así como la falta de definición de un ambiente de control permitió al personal realizar fraudes que generaron grandes pérdidas financieras.

Para tratar de disminuir estos fraudes, en el 2002, la **SEC** (Securities and Exchange Commission) – Agencia independiente del gobierno de Estados Unidos que tiene la responsabilidad principal de hacer cumplir las leyes federales de los valores, los mercados financieros de la nación, así como las bolsas de valores, de opciones y valores electrónicos – reformó sus reglas donde mencionan que "*en el informe anual debe incluirse un reporte hecho por la dirección respecto a la efectividad del control interno sobre la información financiera, así como un reporte hecho por los auditores externos*".

Lo anterior es conocido como la ley Sarbanes-Oxley (SOX) de la cual se conocen 11 leyes y 65 secciones (*véase Apéndice A1*), la cual es obligatoria desde el 2004 para todas las compañías que cotizan en la bolsa de valores de Nueva York, lo que implica que anualmente un auditor externo (en este caso Deloitte) debe evaluar la eficacia de los controles en la empresa "x" y efectuar un reporte de hallazgos.

CAPÍTULO 4
OBJETIVOS

En el presente capítulo, se describen los objetivos del proyecto y personales que son los buscados para la ejecución del proyecto.

4.1 Objetivos del Proyecto

- El objetivo principal del proyecto es realizar la auditoría bajo la ley Sarbanes Oxley de la compañía “x”.

- Objetivos adicionales:

  - ✓ Proveer un aseguramiento respecto a los controles internos implementados en los ambientes de procesamiento de la información sobre los que reside la información financiera de la compañía “x”.

  - ✓ Identificar debilidades de control o puntos de mejora en el ambiente de control.

  - ✓ Facultar a Deloitte para expresar una opinión de confianza acerca de la integridad, exactitud y validez de la información financiera generada en los sistemas.

  - ✓ Proporcionar un servicio excelente a la compañía a manera de que Deloitte continúe consolidándose como líder en servicios de auditoría.

4.2 Objetivos Personales

- El objetivo principal personal es aplicar conocimientos adquiridos durante mi trayectoria estudiantil y la experiencia laboral adquirida que permitan fortalecer mis habilidades para la ejecución de una auditoría.

- Objetivos adicionales:

  - ✓ Conocimiento del área de tecnología de la compañía.
  - ✓ Contacto con estándares, metodologías y matrices SOX.
  - ✓ Toma de decisiones y administración del proyecto.
  - ✓ Conocimiento de herramientas propias de la compañía.

CAPÍTULO 5
MARCO TEÓRICO

En el presente capítulo, se mencionan los conceptos básicos, necesarios para el desarrollo de la auditoría, desde la fase de planeación hasta la fase de documentación y reporte a la administración.

5.1 Auditoría

La Auditoría es una función de dirección cuya finalidad es analizar y apreciar, con vistas a las eventuales acciones correctivas, el control interno de las organizaciones para garantizar la integridad de su patrimonio, la veracidad de su información y el mantenimiento de la eficacia de sus sistemas de gestión.

5.1.1. Importancia de una auditoría

Algunas de las razones más importantes para realizar una auditoría pueden ser las siguientes:

a) Cambios en el marco legislativo.
La liberación o la legislación cambian el entorno, convirtiéndolo en menos previsible, ya que se sustituye una situación perfectamente definida por unas leyes reguladoras por otra regida por las fuerzas de la competencia.
La privatización de organizaciones cambia la orientación de las mismas, obligándolas a evolucionar desde un modelo burocrático a un modelo orientado al servicio al cliente y a la eficiencia de las actuaciones.
La supresión de barreras comerciales obliga a la apertura de horizontes hacia unos mercados de competencia internacional en lugar de unos mercados cerrados internos.

b) Fluctuaciones del mercado.
Los ciclos económicos obligan a las organizaciones a adoptar estrategias diferenciadas y, por consiguiente, a cambiar su orientación.
La innovación tecnología puede convertir de forma repentina en obsoletas a empresas y sectores industriales enteros. La empresa debe adaptarse a esos cambios.

Es conveniente realizar una auditoría entre la firma de los acuerdos iniciales y el final de la misma, con la finalidad de valorar la capacidad de gestión del equipo directivo coparticipe y analizar la posición competitiva de la empresa.

(a) La reorganización de la empresa.
Puede venir motivada por diversas causas: debilitamiento en el equipo directivo, un cambio en la propiedad de la empresa, un cambio de estrategia o la creación de un nuevo producto.

(b) La emisión de ofertas públicas en mercados financieros.
El éxito de una oferta pública radica en la capacidad de convicción de la empresa de cara a su mercado de potencial crecimiento. La publicidad de los resultados de la auditoría puede servir para anunciar las ventajas competitivas de la empresa y el talento de sus gestores actuales.

5.2 Auditoría Sarbanes-Oxley (SOX)

La ley SOX contiene 11 leyes y numerosas secciones, regulando diferentes aspectos e involucrando a los ejecutivos de las empresas, directorio, gobiernos corporativos, comités de Auditoría, agentes de valores, corredores de bolsa, clasificadoras de riesgo y firmas auditoras, entre otros.

Se aplica a todas las empresas que están registradas en la New York Stock Exchange (NYSE) y la National Association of Securities Dealers by Automatic Quotation, conocida como NASDAQ, y bajo la supervisión de la Securities and Exchange Commission (SEC).

La sección 404 es la aplicable a la evaluación de controles que describe:

a) La responsabilidad de la administración para establecer y mantener una estructura adecuada de control interno y procedimientos para el reporte financiero.
b) Contar con una evaluación, al final del año fiscal, de la efectividad de la estructura del control interno y los procedimientos.

5.3 Marcos de Referencia

La aplicación de una auditoría SOX ha generado una cantidad importante de opiniones y consejos en cuanto a la forma de realizar la auditoría. Las organizaciones consideran que si el sistema de TI es integral, o es una parte significativa de las operaciones auditadas, la auditoría debe incluir el sistema con el fin de proporcionar una seguridad razonable de que la información es producida por el sistema de manera precisa, confiable y completa.

Las organizaciones son: AICPA (American Institute of Certified Public Accountants), IIA (Institute of Internal Auditors Association), ISACA (Information Systems Audit and Control Association) entre otras; esas organizaciones han realizado diversas publicaciones respecto a la forma de ejecutar una auditoría SOX.

Sin embargo, dos marcos de referencia han emergido como una parte importante de la auditoría TI. Esos marcos son con conocidos como COSO y COBIT.

5.3.1 COSO (Committee of Sponsoring Organizations)

En general, el marco de referencia COSO (Committee of Sponsoring Organizations) ha sido aceptado como un estándar de control interno para implementar y evaluar controles acorde con SOX y el estándar PCAOB. COSO aborda como los riesgos deben ser identificados en los procesos y los métodos para mitigar esos riesgos. Este análisis incluye los controles manuales y automatizados y cómo deben ser soportados por controles generales del computador apropiados.

El marco también estipula los objetivos, requerimientos y la necesidad de que los empleados se encuentren sensibilizados y entrenados para un control adecuado dentro de la compañía.

Sin importar el tamaño de las compañías, los datos se transfieren entre múltiples grupos del negocio y de sistemas informáticos desde su inicio transaccional hasta convertirse en un reporte que un CEO o un CFO debe revisar. Esos datos deben ser confiables en todo su recorrido.

COSO permitirá el logro de objetivos de la compañía, estableciendo cuatro categorías:

- **Estratégica:** Metas a alto nivel, alineadas y soportadas con la misión.
- **Operaciones:** Uso efectivo y eficiente de los recursos.
- **Reporteo:** Confiabilidad de la información
- **Cumplimiento:** Cumplimiento con leyes y regulaciones.

Esas categorías distintas pero superpuestas- un objetivo particular puede caer en más de una categoría- manejan las diferentes necesidades de la entidad y pueden ser responsabilidad directa de los ejecutivos. Esta división también permite distinguir entre lo que se puede esperar de cada categoría.

COSO consiste de ocho componentes interrelacionados que se muestran la Fig. 5.1

Fig. 5.1. Cubo COSO.

a) **Internal Environment**: El ambiente interno abarca el tono de una organización y establece las bases de como el riesgo es visto y tratado por una entidad, incluyendo una filosofía de administración de riesgos y apetito por el riesgo, integridad, ética de valores y el ambiente donde operan.

b) **Objective Setting:** Los objetivos deben existir antes de la administración para poder identificar eventos que puedan afectar su logro. Los objetivos deben estar soportados y alineados con la misión de la entidad y consistentes con su apetito del riesgo.

c) Event Identification: Eventos internos o externos que puedan afectar el logro de los objetivos de la entidad deben estar identificados, distinguidos entre riesgos y oportunidades. Las oportunidades son canalizadas de vuelta a la estrategia de la administración o el establecimiento de objetivos.

d) Risk Assessment: Los riesgos son analizados, teniendo en cuenta la probabilidad y el impacto, como base para determinar cómo deben ser gestionados. Se evalúan de manera inherente o residual.

e) **Risk Response:** La administración selecciona las respuestas al riesgo –evitar, aceptar, reducir o compartir riesgos- desarrollando un conjunto de acciones para alinear riesgos con las tolerancias de riesgo y el apetito de riesgo.

f) **Control Activities:** Las políticas y procedimientos establecidos e implementados para asegurar que las respuestas al riesgo son ejecutados en tiempo y forma.

g) **Information and Communication**: Proceso que asegura que la información relevante es identificada, capturada y comunicada en tiempo. La comunicación efectiva se produce en un sentido amplio, fluyendo de un lado a otro por toda la entidad.

h) **Monitoring**: Proceso que determina si el control interno diseñado y ejecutado, es efectivo y adaptable de acuerdo a las necesidades del negocio.

COSO no es estrictamente un proceso serial, donde un componente afecta únicamente al siguiente. Es un proceso multidireccional e iterativo en donde prácticamente cada componente puede influir en otro.

5.3.2. COBIT (Control Objectives for Information Technology)

Numerosos analistas han apuntado que COSO no ayuda lo suficiente a identificar, documentar y evaluar los controles de TI necesarios para cumplir con los requerimientos legales de SOX. El “Control Objectives for Information and Related Technology” o marco de referencia COBIT fue diseñado para cubrir las necesidades de TI que no cubría COSO.

COBIT es una interpretación de COSO desde el punto de vista tecnológico, fue establecido por ITGI (IT Governance Institute) en un reporte llamado “IT Control Objectives for Sarbanes-Oxley”, este reporte describe que la primer prioridad para la compañía debe ser el demostrar que tan fortalecidos se encuentran los controles sobre la información financiera.

Para que TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:
• Estableciendo un vínculo con los requerimientos del negocio
• Organizando las actividades de TI en un modelo de procesos generalmente aceptado
• Identificando los principales recursos de TI a ser utilizados
• Definiendo los objetivos de control gerenciales a ser considerados

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

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

• **Planear y Organizar (PO)** – Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).

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

La última versión COBIT 4.1 comprende de 4 dominios, 34 procesos de IT y 318 objetivos de control relacionados a IT. COBIT está siendo adoptado por muchas corporaciones como guía para sus esfuerzos de cumplimiento con la ley Sarbanes-Oxley.

El esquema COBIT se muestra en la Fig. 5.2.

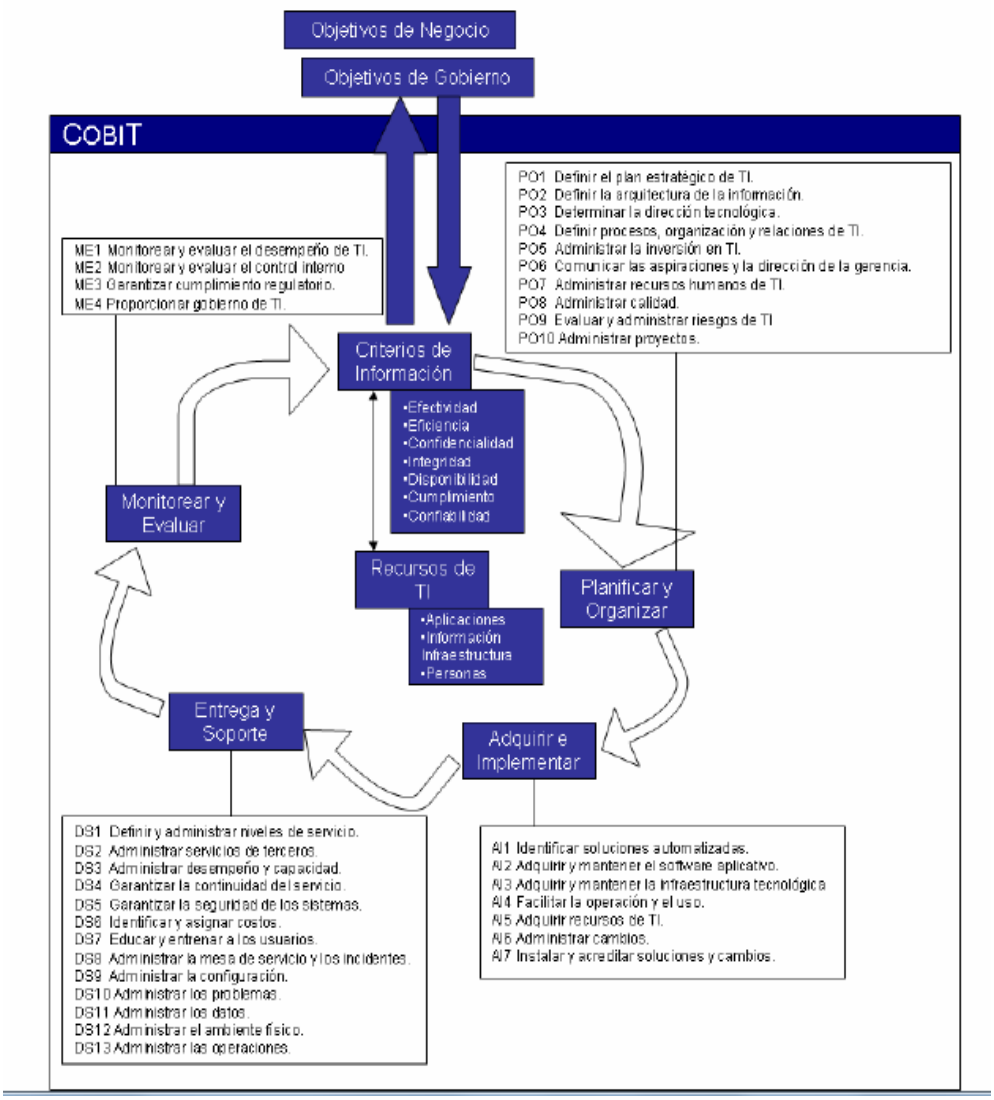

Fig. 5.2 Estándar COBIT

5.3.3 Relación marcos de referencia y estándares

COSO puede ser el marco de referencia utilizado, pero su estatus no oficial permite que otros marcos y/o estándares puedan ser adoptados para SOX-404.

Como se mencionó la falta de detalle sobre ambiente TI de COSO, no permite describir del todo los controles relevantes para la auditoría y la manera de cómo deben ser probados.

Procedimientos en donde los controles de TI deben ser incluidos en la auditoría son diferentes acorde al tipo de compañía auditada. Las pruebas para una compañía en donde su labor es totalmente de sistemas (hosting de aplicaciones) serán diferentes para aquella compañía en donde los sistemas de TI solo hacen tareas de back office.

El enfoque generalmente aceptado es utilizar, cuando aplica, una combinación de COSO y COBIT para crear un marco global que comprenda la evaluación de riesgos y seguridad para los sistemas de TI.

Con base en lo expuesto, se considera conveniente analizar la siguiente aseveración de SOX que ayuda a comprender la necesidad de probar controles en TI:

Los estándares de PCAOB incluyen requerimientos específicos para los auditores a entender el flujo de transacciones, incluyendo como inician, se autorizan, se registran, se procesan y se reportan. Ese flujo normalmente incluye el uso de aplicaciones sistemáticas para los procesos automáticos y además soportar transacciones de un volumen y complejidad importante. La confiabilidad de esas aplicaciones depende de la infraestructura que incluye: bases de datos, redes, sistemas operativos y más. Aquellos sistemas que apoyen en el registro de la información financiera, debería ser considerado en el diseño y evaluación del control interno.

5.4 Enfoque de Solución

Como bien se ha mencionado la fusión de COSO y COBIT es una de las metodologías utilizadas por diferentes firmas (incluyendo Deloitte) que proveen servicios de auditoría SOX, auditoría externa o auditoria TI. La implementación de esta metodología plantea el utilizar un enfoque multidisciplinario que considere los distintos elementos a desarrollar de una manera equilibrada: gente, procesos, tecnología y gestión de proyecto. El enfoque se muestra en la Fig. 5.3.

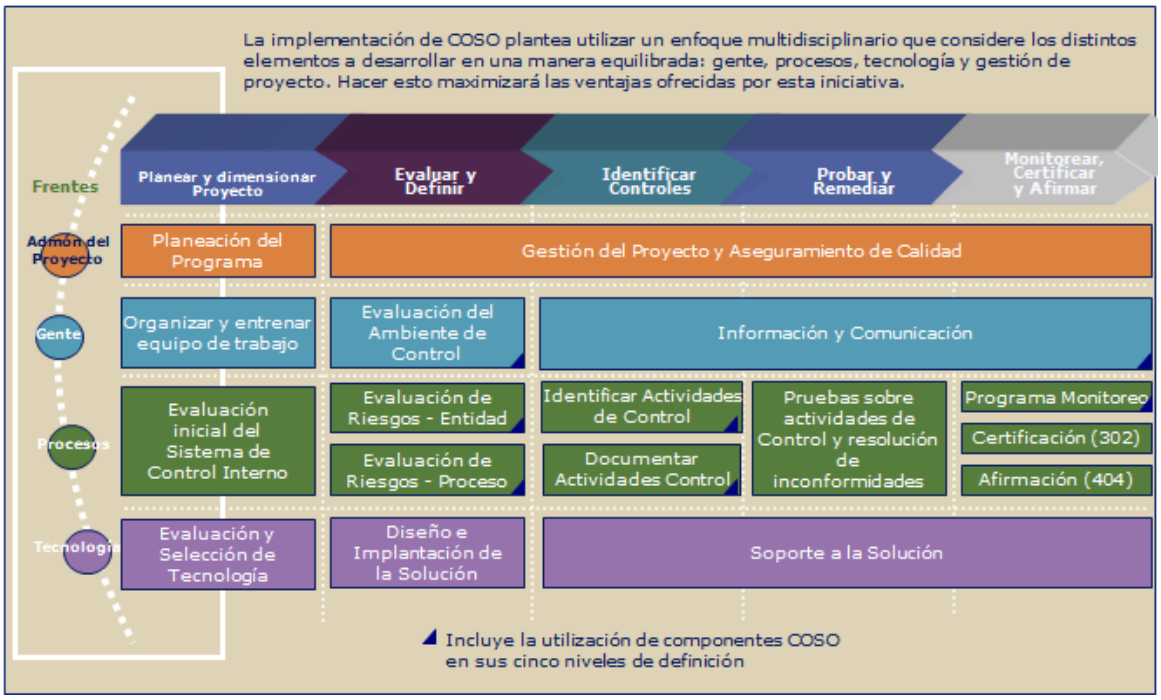

Fig. 5.3. Enfoque de Solución.

Alcance (Planear y dimensionar proyecto)
Determinación de las principales cuentas contables, locaciones geográficas y procesos a evaluar.

Evaluar y Definir
Determinación de riesgos y controles claves en cada proceso asociados a los principales cuentas contables, instrumentos y documentación según PCAOB.

Identificar Controles
Verificar si los controles están adecuadamente documentados y si la forma en cómo fueron diseñados permite mitigar los riesgos clave sobre los reportes financieros.

Probar y Remediar
Verificar la operatividad de los controles clave sobre los estados financieros mediante el examen de muestras (efectividad operativa) de documentación de cada control, incluyendo controles automáticos, controles de nivel de entidad y los controles generales del computador.

Se deberá determinar el nivel de impacto de las deficiencias detectadas conforme a lo establecido por la PCAOB.

Para la parte de remediación, se deberá establecer un plan de acción de la gerencia para minimizar o eliminar el impacto de las deficiencias detectadas.

Monitorear, Certificar y Afirmar

El plan de acción establecido para la remediación de las deficiencias detectadas requiere de una nueva evaluación como parte del proceso de mejoramiento continuo.

Es necesaria la preparación de reportes trimestrales y el reporte anual con la opinión sobre la eficiencia y efectividad del diseño y eficacia operativa de los controles sobre los reportes financieros solo para la sección 404.

5.5 Proceso de una auditoría SOX

Esta sección provee un modelo generalizado de la auditoría SOX. El modelo está diseñado para arreglar problemas específicos donde el costo y tiempo son constantes importantes. Esto significa que la administración debe verificar que los procesos y controles se encuentran debidamente documentados antes de la revisión de los auditores.

Un área de TI proactiva enfocada a la sección 404 debe buscar las deficiencias y trabajar activamente en la remediación antes del arribo de los auditores e idealmente contar con todas esas deficiencias resueltas o por lo menos en el camino de ser resueltas para reducir el reporte del auditor externo a deficiencias significativas u operativas y no “materiales”.

La Fig. 5.4 muestra la ejecución desde la fase de planeación hasta la fase de reporte a la administración.

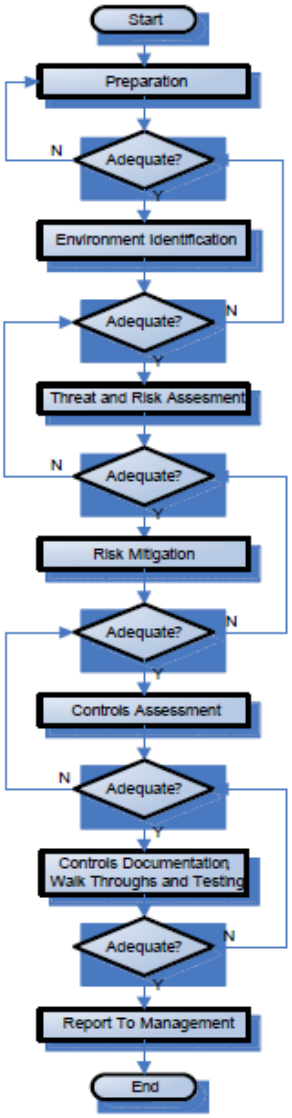

Fig. 5.4. Implementación de una auditoría

A continuación se da el detalle que se realiza en cada fase:

5.5.1 Preparación

La preparación de la auditoría resuelve las deficiencias macro que el auditor puede encontrar durante el transcurso de auditoría. Las pruebas importantes en esta fase son:

- Alcance de la auditoría.
- Factores reguladores a los cuales debe cumplir la auditoría.
- Definición de los factores del negocio.
- Administración de las actividades del proyecto e implementar la auditoría.

5.5.1.1 Alcance de la Auditoría

La definición del alcance es una constante recurrente en todas las auditorías TI, incluyendo SOX 404. Las razones más importantes incluyen el costo del control y la responsabilidad de las deficiencias en la compañía. Las auditorias SOX son muy costosas.

El auditor puede encontrar necesario el añadir un análisis costo-beneficio y un ROI con el fin de obtener apoyo de la administración. Así mismo el auditor puede participar activamente en las tareas de interpretar los requerimientos SOX y decidir que sistemas TI se encuentran en el alcance de la auditoría.

El alcance debe estar documentado y claramente comunicado a todos los involucrados en el proyecto.

5.5.1.2 Regulaciones a la Medida

Sarbanes-Oxley cuenta con cumplimientos legales y de seguridad específicos. Un plan de cumplimiento SOX debería realizarse previo al inicio de la auditoría y debe darse mantenimiento por los participantes clave.

El CFO debe documentar riesgos que enfrenta el negocio, por lo cual el CFO debe estar involucrado en todo el proceso de auditoría SOX 404, particularmente desde que un porcentaje significativo de los riesgos en las compañías corresponden a riesgos en los sistemas de TI. El auditor de TI debe estar preparado para aconsejar y quizá orientar a los ejecutivos de la compañía cuales aspectos de COBIT y COSO son los que mejor le acomodan.

5.5.1.3 Organización del Proyecto

Todas las compañías públicas (incluso las pequeñas) requieren de una auditoría SOX, por lo cual deben contar con los servicios de una administración de proyectos por lo menos. Esto ha sido mencionado como recordatorio al auditor de TI porque la sección 404 es una parte del total de secciones de Sarbanes. (*Véase Apéndice A1*)

5.5.2 Identificación

Identificar el ambiente auditable es una parte crítica del proceso general de auditoría porque a través de una línea puede distinguirse que será lo indispensable dentro del ambiente y lo que no es significativo para auditar.

Para un auditor TI, la identificación del sistema para una auditoría SOX tiene diferencias importantes con la auditoría tradicional de TI. Las diferencias son:

- Punto de vista del sistema del auditor (vs. Cualquier otro componente)
- Enfoque en controles
- Auditoría relacionada a marcos de referencia
- Provisiones de terceros, y
- Exclusión de los auditores externos del proceso SOX.

5.5.2.1 Estructura Organizacional

El organigrama de los participantes es desarrollado con el detalle suficiente para definir los roles y responsabilidades para así ubicar al responsable de las posibles deficiencias encontradas. Ver Fig. 5.5.

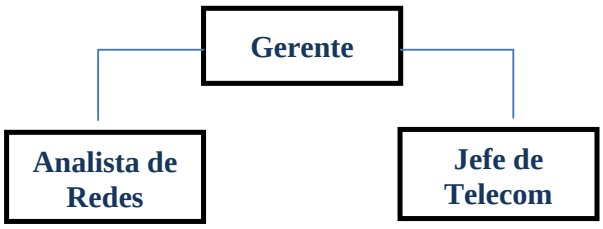

Fig. 5.5. Estructura Organizacional común en un área de TI.

Un control clave documentado y auditado en esta fase es el proceso de ***Segregación de Funciones (SoD)***. Una matriz para cada función (e.g. HR, Ventas) de la organización es desarrollada para documentar la separación de responsabilidades (ver tabla). El organigrama y la matriz de SoD normalmente son incluidos en los papeles de trabajo de la auditoría SOX.
La siguiente es una tabla que ilustra una matriz de Segregación de Funciones únicamente para aquellas compañías que cuentan con el sistema SAP.

Tabla 5.1. Ejemplo de Matriz de Segregación de Funciones

Proceso	Sub-Proceso	Transacción SAP	Roles

5.5.2.2 Ambiente de Procesamiento

El auditor TI define los ambientes de procesamiento en suficiente detalle para identificar las deficiencias de control que pueden ser relevantes en el proceso de una auditoría SOX como lo son las áreas de TI claves: Operaciones, Seguridad física y lógica, Control de Cambios, Respaldos y Recuperación. Estos procesos son normalmente encontrados en los papeles de trabajo de una auditoría SOX.

5.5.3 Evaluación

Una amenaza es definida como una expresión para perjudicar o dañar. El riesgo es la posibilidad de pérdida. Las amenazas causan riesgos y explotan vulnerabilidades, que son definidas como la entrada de ataque. La respuesta de una compañía de la suma de las amenazas, riesgos y vulnerabilidades (Riesgo total), el riesgo tolerable (apetito del riesgo) y que nivel de respuesta es razonable dependiendo de la situación específica. El conjunto de todo lo anterior es llamado “Evaluación de Riesgo” y más reciente, “Administración del riesgo”. Para clarificar el concepto es conveniente considerar el siguiente ejemplo:

- Un granjero mantiene una granja prestigiosa en Kansas. Siendo esta la ubicación, cualquier tornado puede ser una amenaza y puede ser destruida o dañada (impacto) por una tormenta (vulnerabilidad). El granjero sabe que la probabilidad de un tornado es alta (probabilidad de ocurrencia). Él también sabe que no puede hacer nada contra un tornado (Apetito del riesgo/Tolerancia del riesgo).

- El granjero responde a su amenaza construyendo un sótano, con el fin de que él y su familia cuenten con un refugio si el tornado se acerca (Mitigación del Riesgo). Él también reconoce que toda o cierta parte de su granja pude sufrir daño, pero el todavía piensa que puede continuar con su granja en esa ubicación ya que no existe algún otra amenaza (Riesgo Total)

Tal como el granjero, el Auditor TI debe estar alerta de las amenazas y vulnerabilidades de la compañía y consecuentemente los riesgos.

Un riesgo para TI es la medida de peligro que puede ser el resultado de una amenaza y eso, de cierta manera, causar daño en la utilidad operacional o en la misma información. También un riesgo es la medida de probabilidad de que un evento pueda ocurrir.

Las amenazas, vulnerabilidades y riesgos fueron los elementos que promovieron la creación de los controles SOX 404, que permitirán medir la confiabilidad de los sistemas de información. En resumen, debe identificar esos elementos para encontrar una mitigación al riesgo, que el auditor puede encontrar contestando las siguientes preguntas:

Amenazas: ¿Que puede dañar al sistema IT, ambiente de procesamiento o información?
Vulnerabilidades: ¿Cuáles son los huecos entre los procesos/estándares/ especificaciones con los lineamientos de seguridad, técnicos y administrativos?
Impacto o daño: ¿Cuál es el impacto o daño de los activos de una organización o la habilidad de operar si la amenaza detona la vulnerabilidad?
Probabilidad de ocurrencia: ¿Cuál es la probabilidad de que una amenaza explote una brecha?
Apetito del riesgo/tolerancia: ¿Qué cantidad de riesgo es aceptable para la organización?
Riesgo Residual: ¿Qué cantidad de riesgo no puede ser eliminada completamente?
Riesgo total: ¿Cuál es la suma de todas las posibles exposiciones al riesgo?

5.5.3.1 Amenazas

Las amenazas en el sistema de información pueden ocurrir en el sistema o pueden ser ajenas a él. Mientras existe un listado de posibles amenazas, la mayoría de las corporaciones son susceptibles a un limitado y bien entendido set de amenazas. Ver la tabla 5.2

Tabla 5.2. Amenazas comunes en cualquier empresa

Amenaza	Descripción
Abuso de privilegios de acceso por usuarios autorizados	Un usuario autorizado – empleado, becario, externo, puede realizar operaciones que no son autorizados o permitidas para esa persona.
Abuso de privilegios de acceso por empleados	Usuario autorizado según la política de seguridad que realiza ciertas funciones en el sistema pero después atenta para realizar operaciones no autorizadas para él.
Errores Accidentales	Inapropiado uso de la información por falta de capacitación en lugar de una mala intención.
Intentos de acceso no autorizados por un externo	Personas ajenas a la compañía que no están contratadas, intentan obtener acceso al sistema
Pérdida en la comunicación	La inhabilidad de transferir información entre la organización.

Virus	Programa que esparce por si solo códigos o programas "saludables". Después de una infección, el programa puede realizar una variedad de funciones no deseables.
Pérdida de la integridad de la información	Alteración de los datos y/o información.
Ataques deliberados	Esto incluiría Hackers, crackers, espías industriales o corporativos, crimen organizado y terroristas.
Destrucción de los datos	El daño a la información sostenida por la organización que incluye datos de empleados o información personal.
Incendio	Incendios que pueden destruir los recursos
Desastres naturales	Eventos que pueden degradar ciertos aspectos del sistema que no son provocados por el hombre. Ej. Inundaciones, tornados y terremotos.
Continuidad	Cuando el sistema no está disponible para su uso no causado por un desastre; esto incluye mantenimiento, fallas de componentes y choques lógicos.
Pérdida de energía	La pérdida de energía eléctrica provista a los sistemas.
Robos o destrucción de los recursos	El uso no autorizado o daño a la capacidad computacional por cualquiera a través de medios físicos.

5.5.3.2 Vulnerabilidades

Las vulnerabilidades comúnmente se refieren a la debilidad o exposición de la cual una amenaza puede tomar ventaja para explotarla.

Esta debilidad o ausencia de controles de seguridad pueden ser el resultado de deficiencias de procedimientos, de programación, lógicas o físicas.

Las vulnerabilidades incrementan el riesgo porque proveen el camino para que la amenaza dañe al sistema.

El auditor de TI debe estar preparado para examinar las vulnerabilidades del sistema en términos de posibles ataques deliberados (hacker) o una oportunidad de ataque (Ej. empleado que puede ser tentado cuando ve escrito una contraseña en un post-it en el monitor).

5.5.3.3 Impacto

El impacto o daño puede ser derivado identificando el valor del activo que está sujeto a destrucción o daño. Los activos pueden ser tangibles, los cuales incluyen hardware, software y otros elementos como el edificio donde se encuentra el centro de datos. También se incluyen los activos intangibles como la información, datos y la propiedad intelectual. Un análisis simplificado sería:

[Impacto] = [Probabilidad de ocurrencia (w)] * [Costo del daño]

El impacto también se refiere al daño que ocurre a corto, mediano o largo plazo. Estos incluyen la divulgación, modificación, destrucción de la información, pérdida del negocio, denegación de servicio, falla en la en el cumplimiento de la misión de la compañía, pérdida de reputación, violación o privacidad e incluso pérdida de la vida.

5.5.3.4 Probabilidad de Ocurrencia

La teoría de probabilidad describe dos condiciones bajo las cuales se toman las decisiones basadas en la integridad de la información. Esas son: *Decisiones bajo riesgo* y *decisiones bajo incertidumbre*. Una decisión bajo riesgo es cuando todos los posibles resultados son conocidos y la probabilidad de que cualquier resultado pueda ser afirmado. La única pregunta es ¿qué resultado se producirá del riesgo? Un lanzamiento de moneda es un ejemplo clásico de toma de decisiones bajo riesgo.

Una decisión bajo incertidumbre ocurre cuando todos los posibles resultados pueden o no pueden ser conocidos y la probabilidad de que cualquier resultado no puede ser especificado. Como resultado, se utiliza como: “decisiones bajo certeza supuesta”.

Una manifestación común es el atribuir un número pequeño de posibles resultados (ej. Alto-Medio-Bajo) como probabilidad de ocurrencia a un evento.

5.5.3.5 Apetito del Riesgo

Apetito del riesgo es la cantidad de riesgo que una organización está dispuesto a aceptar. La medida del apetito del riesgo puede ser medido en términos cualitativos o cuantitativos. El auditor TI debe estar alerta del apetito del riesgo de la organización. El auditor debería incorporar sus hallazgos en sus papeles de trabajo para que esas conclusiones puedan ser documentadas y revisadas por la administración.

5.5.3.6 Riesgo Residual

Las buenas prácticas de TI reconocen que siempre existirá el riesgo y nunca puede ser completamente eliminado. Este “residuo” es conocido como *riesgo residual.* Las mejores prácticas de seguridad indican que la implementación de los controles apropiados y razonables para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información puede mitigar el riesgo total del sistema.

En otras palabras, el riesgo residual es igual al total de riesgo menos el riesgo que puede ser mitigado por la efectividad de los controles implementados.

[Riesgo Residual] = [Riesgo total] – f (Controles efectivos)

El riesgo residual puede ser utilizado como una prueba de validación del apetito del riesgo.

5.5.3.7 Riesgo Total

El riesgo total de una organización puede ser visto como la suma de todos los posibles eventos, medidos por la probabilidad de ocurrencia (w) de cada evento (E) y para cierto número de eventos ($_n$) y multiplicados por su impacto (medido por el costo u oportunidad del costo).

$$\left(\text{Riesgo Total}\right) = \sum_{n=1} \left(\omega\ \text{E}\right)_n \left(\text{Impacto}\right)_n$$

5.5.3.8 Síntesis del Riesgo

La síntesis del riesgo se refiere a la lista de riesgos para los cuales pueden implementarse controles mitigantes. El auditor TI debiera revisar el proceso para posteriormente establecer un criterio de consistencia y precisión. Consistencia, en este caso, significa que todas las áreas usan las mismas mediciones y definiciones de la misma manera.

Precisión, significa que la información es válida. Estas definiciones pueden ser razonables y aceptables únicamente si se encuentran correctamente documentadas.

La siguiente tabla ilustra el significado de la síntesis del riesgo, se encuentra medido bajo los valores de “bajo”, “medio” y “alto” en cada eje que permite un mapeo adecuado de la probabilidad e impacto de cada riesgo. Ver tabla 5.3.

Tabla 5.3. Categorización del riesgo con base a probabilidad e impacto.

Factor de Riesgo		**Impacto**		
Probabilidad de ocurrencia		Alto	Medio	Bajo
	Muy probable	Muy fuerte	Fuerte	Decisión por el caso
	Probable	Muy fuerte	Fuerte	Decisión por el caso
	Poco probable	Decisión por el caso	Decisión por el caso	Ninguno

5.5.3.9 Mitigación del Riesgo

La mitigación de riesgos se ha vuelto significativamente prioritaria para el proceso SOX. Mientras que el énfasis para un auditor SOX 404 es en controles, lograr un nivel razonable de aseguramiento también requiere procesos de seguridad que deben ser revisados. Estos procesos incluyen:

- Análisis y evaluación de riesgos
- Procesos de administración de seguridad
- Monitoreo de los sistemas computacionales
- Monitoreo de las comunicaciones
- Seguridad física: acceso a servidores, equipos, personas, etc.
- Personal de seguridad
- Procedimientos de seguridad
- Cultura de seguridad

El auditor TI debe reconocer que la mitigación de riesgos debe ser antes de iniciar la auditoria SOX 404. Así mismo, el auditor debe apreciar que el marco de administración de riesgos va más allá de un marco de control interno al evaluar riesgos no financieros.

Es por ello que el marco de referencia COSO ha cambiado a COSO´s Enterprise Risk Management lo cual intenta asegurar la confiabilidad de los reportes internos y externos, incluyendo cumplimiento de regulaciones. Este nuevo marco incluye el concepto de “objetivos estratégicos” basados en el apetito del riesgo, que gobierna la gran mayoría de las decisiones.

El marco también define dos categorías de controles de sistemas de información: controles generales y controles de aplicación.

Los controles generales incluyen: administración de la tecnología, infraestructura, seguridad y adquisición, desarrollo y mantenimiento de software. Los controles de aplicación se enfocan en la integridad y disponibilidad de la información, tales como detección de errores, pruebas de datos, pruebas lógicas y aceptación de usuarios a esas pruebas.

La auditoría, la cual es desarrollada como parte de la evaluación de controles, provee contexto, historia, conocimiento de amenazas y riesgos, e identificación de controles usados para mitigar esas amenazas y riesgos subsecuentes. A corto plazo, el proceso de mitigación de riesgos provee una estructura para identificar controles mitigantes. Ver la Fig. 5.6.

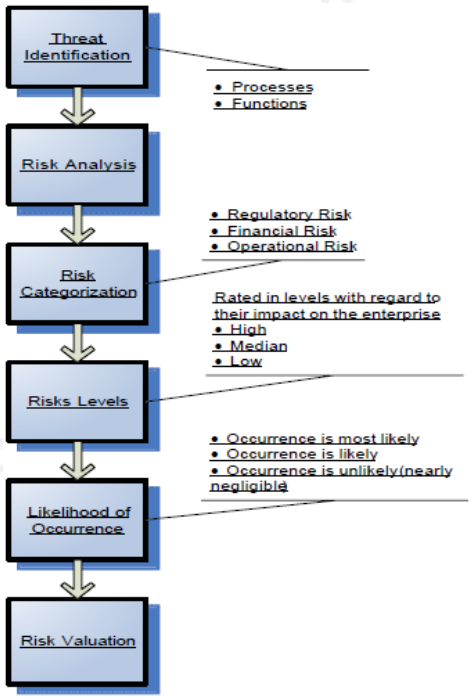

Fig. 5.6. Proceso de Mitigación de Riesgos.

.El impacto inmediato bajo una auditoría SOX es determinar la naturaleza de las pruebas y el tamaño de las muestras usadas para ellas. Ver la tabla 5.4 para validar el tamaño de la muestra con base a la naturaleza del control y la frecuencia.

Tabla 5.4. Naturaleza de las pruebas para obtención de muestras.

Muestras de las pruebas iniciales			
Naturaleza del Control	Frecuencia del Control	Tamaño de muestras	
		Riesgo Bajo-Medio	Riesgo Alto
Manual	Muchas veces al día	25	45
Manual	Diario	15	25
Manual	Semanal	5	8
Manual	Mensual	2	3
Manual	Trimestral	1+1	2+1
Manual	Anual	1	1
Controles Automáticos		Probar una sola muestra	

5.5.3.10 Controles

Los controles son la respuesta a los riesgos identificados. Dos clases de controles son establecidos en el proceso SOX. Estos son los controles clave y generales. Están diseñados de manera que los controles sean suficientes para:

- Prevenir fraudes, mal uso y pérdida de información financiera.
- Permitir detección rápida cuando los incidentes ocurran, y
- Promover acción efectiva para limitar los efectos de tales incidentes.

Los controles clave o generales se derivan de las “mejores prácticas” de TI y que convergen a la iniciativa SOX.

La auditoría SOX 404 debe recordar que una de las ideas clave de SOX es que el acceso a la información debe ser limitada a “la necesidad de saber”. El auditor SOX 404 puede probar la calidad de los controles determinando a través de las políticas, procedimientos o procesos son:

- Estandarizados a través de la compañía.
- Administrados centralmente.
- Controlados centralmente.
- Repetibles.

5.5.3.10.1 Controles Clave

Los controles clave son generalmente definidos por la literatura como los controles que son fundamentales para asegurar que los valores del estado de resultados son correctos y confiables. Por lo tanto, toda transacción monetaria debe ser inicializada, autorizada, implementada, documentada, controlada, reportada y validada por controles clave. Si uno de estos controles es basado en IT, entonces debe ser cubierta por una auditoría SOX 404.

Un ejemplo de control clave, es un disparador/monitoreo en la base de datos que asegure que la adición de una entrada en la tabla de cuentas x cobrar crea automáticamente un registro en el libro mayor. La auditoría SOX permitirá asegurar que ese “disparador” tiene un código de programación correcto y que solamente sea cambiado por personal autorizado. Revisión de códigos, diseños, pruebas unitarias y pruebas de aceptación de usuarios son ejemplos de maneras en que los reportes son calificados como confiables.

5.5.3.10.2 Controles Generales

Los controles generales son generalmente definidos por la literatura como los controles que son aplicables en todos los sistemas TI y que son esenciales para asegurar la integridad, confiabilidad y calidad de los sistemas. Ejemplos de controles generales incluyen:

- Seguridad física.
- Operaciones.
- Seguridad Lógica.
- Recuperación y respaldos.

- Políticas de recuperación de desastres.
- Niveles de servicio.
- Control de Cambios en aplicaciones o software.
- Pruebas.
- Administración del cambio en configuración.

Desde el punto de vista del auditor de TI, es preferible que los controles sean automatizados, desde que la automatización hace más difícil para personas manipular el control maliciosamente. La automatización de controles debe incluir:

- Administración centralizada de procesos IT.
- Versiones centralizadas de políticas y procedimientos.
- Procedimientos de recuperación y respaldo usando códigos, técnicas de clúster, software especializado, etc., así como transferencia de los procesos al hardware de respaldo, cuando el principal falla.
- Procedimientos de autenticación y control de acceso usando servicios de directorio como LDAP o Directorio Activo.
- Procesos de detección y prevención de intrusos usando servicios como IDS/IPS.
- Procesos de antivirus usando software como McAfee o Symantec.
- Procesos de administración del cambio en activos IT.

Si la compañía está desarrollando software, el auditor SOX debe asegurarse que:

- Se encuentra implementado un proceso “SDLC” (Systems Development Life Cycle) para el diseño, desarrollo e instalación para todas las aplicaciones.
- Los estándares de códigos son respetados y revisados conforme a procedimientos.
- Todos los cambios son aprobados, documentados y probados antes de su implementación.
- Procedimientos de administración de incidentes con personal capacitado para atender esos incidentes.
- Un inventario centralizado de activos de infraestructura de IT (PC´s, firewalls, servidores, routers, hubs, etc.).

La granularidad de la expansión de los controles generales depende del tipo de industria. Como resultado, una compañía de manufactura puede tener un número significativo de controles diferentes que una compañía proveedora de Internet.

5.5.3.10.3 Controles de Aplicación

SAP y otros sistemas ERP permiten configurar controles críticos del negocio. Esto es, un parámetro que es colocado por el ser humano, tal como un estatus “activo” o “inactivo”, límites, entre otros. El auditor TI debe probar los parámetros como se explica en el siguiente ejemplo:

Proceso: Cuentas x Pagar
Riesgo: Los desembolsos son fraudulentos
Control: El sistema realiza una comparación de tres maneras donde coincide la factura, la orden de compra y la entrada de mercancía.

En este ejemplo, los controles de aplicación estarán configurados en el ERP para las cuentas x pagar, activando la opción del 3-way match (control configurable en SAP que permite validar que los pagos, recepción de mercancía y pedidos de compra coinciden en cantidades e importes) para forzar de manera automática la comparación entre la factura, la orden de compra y la entrada de mercancía antes de permitir el pago.

5.5.4 Documentación

Las narrativas de auditoría, han sido desarrolladas como parte de la evaluación de controles, provee una descripción de las amenazas, después los riesgos que confrontan el sistema y finalmente los controles que deberían implementarse para mitigar el riesgo.

Esta sección describe una metodología para documentar, el recorrido y probar los controles en una auditoría SOX 404.

El auditor TI probará la eficacia de los controles desarrollando una narrativa de los procesos críticos. Estos procesos son normalmente operaciones, seguridad física, acceso lógico, aplicaciones y recuperación y respaldos. Otros procesos pueden ser añadidos o eliminados dependiendo de los requerimientos del negocio.

Para controles clave y generales los métodos más comunes incluyen entrevistas para asegurar que los procedimientos están siendo llevados a cabo y unas pruebas que aseguren que la documentación y registros se mantienen. El tamaño de la muestra refleja los objetivos y constantes de la mitigación del riesgo.

Para cada control, el auditor TI necesita probar que las políticas, procedimientos y procesos son: creados, aprobados, implementados, monitoreados para consistencia, reportados en una frecuencia, no como un reporte de una sola vez y modificados incluyendo un listado de cambios.

La metodología ilustrada utiliza controles de aplicación en SAP o un software ERP similar. La documentación del control esta referenciada en las narrativas de los procesos, los recorridos y las matrices de pruebas.

Para SOX, los controles de aplicación mitigan los riesgos asociados con los procesos de negocio que el ERP tiene automatizado. Esos controles de aplicación son generalmente configurados, programados o de acceso lógico; los cuales son descritos en las siguientes secciones.

5.5.4.1 Narrativa del control

La narrativa del proceso de cuentas por pagar debe describir que la aplicación realiza de manera sistemática el 3-way match (control automático en SAP que compara la compra, entrada de mercancía y la cuenta por pagar) para prevenir desembolsos no autorizados. La discusión no necesita incluir discusiones de los parámetros específicos de este control.

5.5.4.2 Recorrido del Control

Un recorrido (walkthrough) provee una confirmación del diseño del proceso de los controles clave que han sido documentados en la narrativa y se encuentran operando.

Para asegurar este control, se debe evaluar la configuración en la aplicación y documentar el resultado. Este debe incluir evidencia del parámetro (ej. Reporte del sistema o una impresión de pantalla).

5.5.4.3 Pruebas del Control

El recorrido es, básicamente, una prueba completa de los controles de aplicación desde que se valida que el parámetro está correcto.

Para asegurar que no existe un hueco en la documentación de pruebas, todavía debería buscar una estrategia de pruebas definidas para evaluar el control, pero sin re-realizar la prueba, preferentemente referir al recorrido. Pruebas adicionales deben validar que el control opera en un periodo de tiempo.

Es útil para el auditor TI SOX 404 recordar que la clave detrás del acto es tener a las compañías con los controles suficientes para prevenir fraudes, mal uso de los activos o pérdida de información financiera, controles que permiten una detección rápida cuando ocurre algún problema y que los procedimientos realmente limitan los efectos de tales problemas.

El auditor TI debería probar como mínimo los siguientes controles:

- ***Aprovisionamiento de usuarios***. Asegurar que a los nuevos usuarios solamente se asignen privilegios autorizados, creando un rol para cada tipo de usuario. Deberían existir "checklist" que cuenten con la estandarización de los procesos a manera de prevenir que a los usuarios se le asignen privilegios incorrectos.
- ***Terminación de accesos***. Asegurar que los usuarios que se retiran de la compañía, son removidos de todos los sistemas.
- ***Autenticación***. Uso de un LDAP (Lightweight Directory Access Protocol) centralizado, un repositorio Active Directory o un sistema de administración de identidad para el establecimiento de roles y privilegios.
- ***Privilegios mínimos***. Aplicados cuando son asignados permisos dentro del sistema operativo, aplicaciones y bases de datos. A cualquier individuo, únicamente se deben asignar los permisos requeridos para realizar sus actividades.
- ***Separación de funciones, privilegios y derechos***. Dentro de cualquier sistema contable, un usuario no debe estar involucrado en todo el ciclo financiero dentro de los sistemas.
- ***Administración del cambio.*** Revisión de procesos formales que aseguren que cualquier cambio no autorizado no puede ser implementado en el sistema por personal ajeno a los cambios.

5.5.5 Reporte a la Administración

El reporte a la administración sobre los hallazgos de TI, son parte de un reporte más largo. El auditor TI realiza las siguientes contribuciones:

- Índice de papeles de trabajo.
- Memorándum de las deficiencias que fueron encontradas y la remediación necesaria, si no se encontró ninguna deficiencia, el memo debe describirlo.
- Documentación de las pruebas, resultados, o cualquier otro documento que impacte en los hallazgos de la auditoría.
- Recomendaciones y Hallazgos.

Ejemplo Índice:

- Narrativa TI.
- Plan de Pruebas Operaciones y resultados.
    - Sistema Operativo Pruebas.
    - Impresiones de Pantalla al sistema operativo.
- Plan de Pruebas Seguridad física y resultados.
    - Seguridad física pruebas.
    - Documentación soporte, políticas y procedimientos.

CAPÍTULO 6
AUDITORÍA COMPAÑÍA "X"

En el presente capítulo, se describe paso a paso el trabajo desarrollado durante la auditoría de esta importante compañía.

Haciendo énfasis en cada una de las pruebas ejecutadas a fin de validar la eficacia de su operación.

El caso de estudio presentado en esta sección es conducido extensivamente desde los papeles de trabajo de la auditoría realizada para la compañía mencionada.

Es importante considerar que algunos de los conceptos mencionados durante el capítulo anterior no es necesario ejecutarlos al 100% para poder obtener un resultado, esto es por cuestión de presupuesto y tiempos de entrega acordados con la compañía, sin embargo, cabe resaltar que aquellos que no son cubiertos en su totalidad, son aquellos en los que su ejecución total no es de alto impacto y que el porcentaje ejecutado es suficiente para obtener resultados satisfactorios.

6.1 Preparación

Las operaciones de la compañía “x” están agendadas para ser auditadas por sus auditores externos. Bajo las previsiones de SOX, los auditores externos deben mantener su independencia y no pueden proveer otro servicio. Por lo tanto, la empresa “x” ha contratado a Deloitte para conducir la auditoría interna SOX para identificar cualquier deficiencia y programar una remediación para corregirlas.

6.1.1 Alcance

La administración ha definido varios objetivos para la auditoría interna, uno es el identificar cualquier deficiencia SOX que pueda existir y contar con una remediación antes de la llegada de los auditores externos. Un segundo objetivo es minimizar o eliminar la posibilidad de que los auditores externos cuenten con deficiencias y finalmente reducir el costo de las actividades SOX al mínimo.

Las tecnologías de información de la empresa “x” centralizadas en México están caracterizadas por lo siguiente:

- Desde la fundación de la compañía, las funciones de TI habían sido administradas desde Estados Unidos, sin embargo, debido a la crisis del país, la compañía se vio obligada a cerrar subsidiarias, entre ellas la que controlaba la operación, por tal motivo y por decisión del corporativo en Canadá, desde Marzo 2011, estas funciones son administradas por un equipo especializado en la ciudad de México.

- La administración de seguridad de la red, sistemas operativos y bases de datos son tareas de la compañía “y”, líder global de servicios outsourcing de procesos y tecnología con amplia experiencia en el sector salud.

- El tamaño y alcance de las actividades de TI son pequeñas en comparación con el tamaño del grupo.

- El ERP SAP es el sistema que se encuentra en los servidores productivos y que administra cada una de las compañías del grupo, cada adquisición, que se hace se

integra a este sistema. La última adquisición fue una compañía mexicana que se incluyó a SAP en marzo del 2011.

- A pesar de que la administración y operación de toda Latinoamérica (Brasil, Panamá, Argentina y México) se lleva desde México, los servidores donde se encuentra la aplicación SAP, están alojados en Orange County, California en USA.

6.1.2 Regulaciones a la medida

La compañía “x” ha decidido adoptar el marco de referencia COBIT 4.1. Sin embargo, como un apoyo para la compañía, Deloitte ha decidido realizar una auditoría que incluya a COSO de manera que los resultados sean más satisfactorios y completos para reducir el número de riesgos.

6.2 Identificación

Como parte de la planeación de la auditoría es importante identificar el ambiente de tecnología y el personal que opera dentro de la compañía.

6.2.1 Estructura Organizacional

La compañía “x” en México cuenta con un área de Sistemas que se especializa y da servicio al personal en lo siguiente:

- Administración de la seguridad en SAP: control de acceso, roles y perfiles, y configuración, entre otros.
- Operaciones: respaldos, trabajos programados, DRP/BCP.
- Soporte a usuarios.
- Control de cambio en la aplicación.

Cuentan con personal clave de cada proceso para dar soporte en la operación.

Finalmente, cuentan con 2 personas de la compañía “y” en sitio que pudieran apoyar en cualquier contingencia en la infraestructura de la compañía “x”. Ver Fig. 6.1.

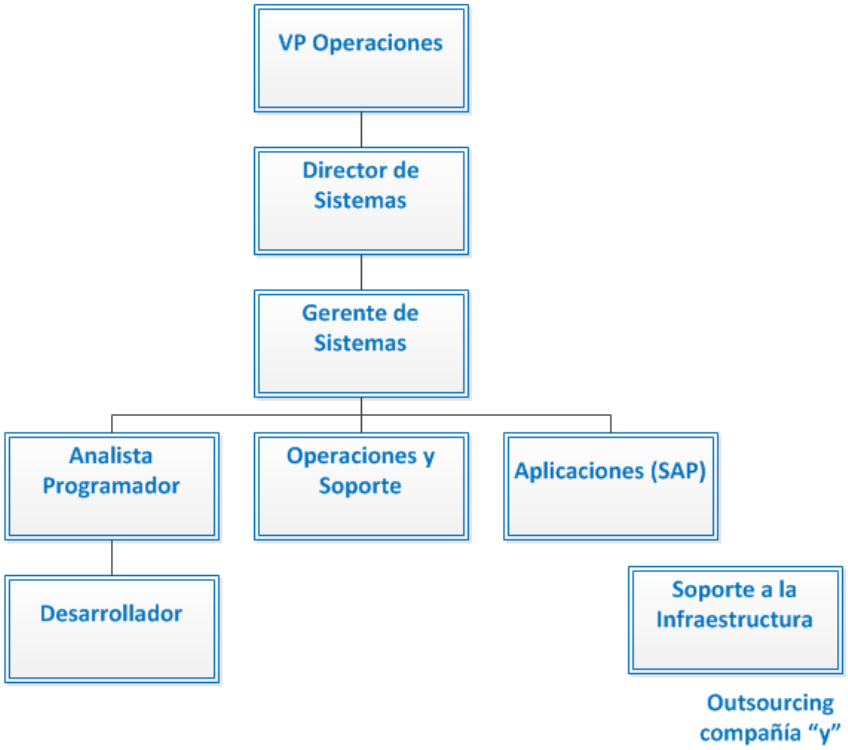

Fig. 6.1. Estructura Organizacional en la compañía “x”

Así mismo, la estructura de reporteo, personal y la segregación de funciones fueron analizadas para validar que se encuentren segregadas adecuadamente. Como resultado de la revisión, se identificó una adecuada segregación de responsabilidades. La tabla siguiente muestra la segregación de actividades que existe en el área de Tecnología donde no encontramos un conflicto sobre las actividades desempeñadas por cada uno de ellos. Ver Tabla 6.1.

Tabla 6.1. Actividades ejecutadas por el personal de TI de la compañía “x”.

Proceso	Estructura Organizacional					
	Gerente de Sistemas	Analista Programador	Basis	Operaciones y Soporte	Desarrollador	Documentador
Seguridad SAP						
Aprovisionamiento de roles a usuarios			✓			
Bloqueo/desbloqueo de usuarios			✓			
Altas y bajas de usuario			✓			
Segregación de funciones			✓			
Aprobación a la seguridad*	✓					
Operaciones						

Respaldos		✓				
Monitoreo de fallas en el sistema y trabajos programados (jobs)		✓				
Creación de Transportes		✓	✓		✓	
Revisión de transportes						✓
Liberación de transportes**		✓	✓			
Soporte a usuarios						
Levantamiento de tickets	✓	✓	✓	✓	✓	✓
Seguimiento a tickets	✓	✓		✓		
Solución a tickets		✓	✓	✓		
Control de cambios						
Requerimiento						✓
Análisis de Impacto y Beneficios						✓
Diseño		✓			✓	
Pruebas en ambientes no productivos						✓
Aceptación de pruebas	✓					
Liberación de las pruebas***	✓					

* La aprobación a las altas, bajas y modificaciones; segregación de funciones se requiere la aprobación del Jefe de Área, Control Interno y del Gerente de Sistemas.
** La regla de la liberación de transportes es cuando el Analista Programador crea el transporte solo puede ser liberado por el Basis y viceversa.
***La liberación de las pruebas son en conjunto entre el dueño del proceso (BPO), Gerente de Sistemas y Control Interno.

6.2.2 Ambiente de Procesamiento

El ambiente de procesamiento representa el alcance de la auditoría, el ambiente de procesamiento deberá ser seleccionado con base en el procesamiento de información contable. La tabla 6.2 muestra este ambiente en la compañía “x”

Tabla 6.2. Ambiente de Procesamiento bajo alcance en la compañía “x”

Aplicativo	Sistema Operativo	Bases de Datos
SAP ECC 6.0	Unix HP-UX 11.23	Oracle 10.02

6.3 Evaluación

A través de esta etapa será posible encontrar los riesgos existentes en el área de tecnología de la compañía “x”.

6.3.1 Amenazas y evaluación de riesgos

Las entrevistas con el personal de la compañía “x” han revelado que solamente un pequeño número de amenazas y/o vulnerabilidades son consideradas para crear un plan de mitigación. Las potenciales amenazas, probabilidad de ocurrencia y un relativo impacto de la compañía han sido desarrolladas en la siguiente tabla. Ver tabla 6.3.

Tabla 6.3. Clasificación de Amenazas en la compañía “x”

Amenaza Potencial	Probabilidad de Ocurrencia	Impacto
Errores y omisiones		
Pérdida de información sensitiva	Bajo	Alto
Destrucción de Información	Bajo	Medio
Fraudes y robos		
Robos	Bajo	Medio
Fraudes	Medio	Alto
Espionaje Industrial	Medio	Alto
Ataques internos		
Recursos mal utilizados por personal interno	Bajo	Bajo
Liberaciones no autorizadas	Bajo	Medio
Acceso a la información confidencial	Bajo	Medio
Ataques externos		
Robos por usuarios no autorizados	Bajo	Medio
Acceso no autorizado a recursos de telecomunicaciones	Medio	Medio
Destrucción de información (virus, códigos maliciosos, etc.)	Bajo	Medio
Hackers	Medio	Medio
Infraestructura		
Desastres naturales	Bajo	Alto
Interrupciones a la comunicación	Alto	Alto

En resumen, la compañía “x” no se ve a sí misma, como un objetivo para un fraude. Dos debilidades son identificadas por el personal:

- Poco control para la Segregación de Funciones, en cuanto a los accesos en los procesos.
- La posibilidad de ataques externos por los enlaces entre las diferentes compañías del grupo (No administrado en México).
- Interrupción en las comunicaciones (No administrado en México).

6.3.2 Mitigación de Riesgos

Con base en las reuniones sostenidas entre el equipo de TI de la compañía “x” y los auditores SOX de Deloitte se ha determinado un número de mitigación de riesgos que ya se encuentran operando desde antes del inicio de la auditoría. El más importante, desde el punto de vista del equipo TI de la compañía “x”, es la seguridad de acceso dentro de SAP, así como la estabilidad y el conocimiento que tienen dentro del sistema. Otra cuestión que agradece el Gerente de Sistemas es el outsourcing de la compañía “y” sobre la infraestructura (decisión corporativa) que mantienen control en la gestión de bases de datos, sistema operativa, control de cambios en hardware, monitoreo de niveles óptimos y sobre todo el monitoreo de la red que detecta cualquier intruso.

Es importante mencionar que la compañía “y” cumple con las necesidades SOX que investigó y requirió la compañía “x” para la formalización del contrato de outsourcing, ya que por ley, la empresa outsourcing no se encuentra liberada de esas obligaciones, por el contrario se vuelven más estrictas. En opinión de la compañía “x”, el modelo de riesgos incorporado a la compañía es tradicional pero cumple con el control, implementación y monitoreo que requieren para la mitigación de riesgos. Ese nivel de detalle está reflejado en su apetito de riesgo que consideran suficiente para asegurar que el riesgo no se materialice. La tabla siguiente muestra la implementación de controles. Ver Tabla 6.4.

Tabla 6.4. Controles implementados para amenazas

Amenaza Potencial	¿Controles Implementados?	¿Monitoreo ?
Errores y omisiones		
Pérdida de información sensitiva	Sí	Sí
Destrucción de Información	Sí	Sí
Fraudes y robos		
Robos	Sí	Sí
Fraudes	Sí	Sí
Espionaje Industrial	Sí	Sí
Ataques internos		
Recursos mal utilizados por personal interno	Sí	Sí
Liberaciones no autorizadas	Sí	Sí
Acceso a la información confidencial	Sí	Sí
Ataques externos		

Robos por usuarios no autorizados	Sí	Sí
Acceso no autorizado a recursos de telecomunicaciones	Sí	Sí
Destrucción de información (virus, códigos maliciosos, etc.)	Sí	Sí
Hackers	Sí	Sí
Infraestructura		
Desastres naturales	Sí	Sí
Interrupciones a la comunicación	Sí	Sí

6.3.3 Controles Clave

Los controles clave de la compañía “x” se encuentran mapeados en una matriz de riesgos y controles que el corporativo tiene definido por país, por cada compra del ramo o fusiones pactadas, estas matrices deben actualizarse para así cubrir los riesgos de cada una de ellas.

Esta “actualización” la realiza la alta dirección en conjunto con Deloitte USA, por lo que una vez finalizadas estas matrices son enviadas a las oficinas de Deloitte de cada país para que esos controles sean probados por cada oficina.

Para la compañía “x”, según las indicaciones de Deloitte USA, solicitaron probar 31 controles clave acordes a COBIT y que cumplen con la regulación SOX.

6.4 Narrativa de Controles

Las operaciones de TI de la compañía “x” que incluyen cualquier soporte respecto al sistema SAP como accesos, soporte en fallas o control de cambios es administrado por el equipo centralizado de TI.

Con respecto a las operaciones que se encuentran administrado por la compañía “y” incluye: soporte al hardware y software, monitoreo de LAN/WAN, correo electrónico, recuperación de los servicios, infraestructura remota, helpdesk. Estos servicios se encuentran en contratos formales.

Las entrevistas con el Gerente de Sistemas de la compañía “x” revelaron información básica, que después fue inspeccionado en documentación. Las operaciones y soporte así como el hosting de servidores y equipos son auditados contra ISO 9001:2000.

Como parte del proceso de “recorrido” en los procesos de TI se incluye la revisión de políticas y procedimientos donde se confirme que son acordes a las operaciones y tecnología que se encuentran actualmente en la compañía “x”. Las narrativas y controles son divididos en 3 grandes dominios: Operaciones, Seguridad de Accesos/lógica y Control de Cambios. Estas 3 áreas son la estructura básica organizacional requerida para documentar y realizar las pruebas correspondientes.

6.4.1 Operaciones

Las operaciones de TI relacionadas al ERP SAP se encuentran centralizadas en México. Dos pruebas fueron solicitadas para el aseguramiento del control en este dominio.

*6.*4.1.1 Trabajos Programados (Jobs)

El soporte y mantenimiento de los trabajos programados (jobs) en el ambiente productivo es llevado a cabo por el personal basis (personal a cargo del soporte SAP) de la compañía “x”, de acuerdo a lo confirmado con el Gerente de Sistemas. El proceso de calendarización detalla el procesamiento de trabajos en línea (procesos batch) y en línea del ambiente productivo, incluyendo el monitoreo y las acciones correctivas en caso de excepciones. El proceso incluye como los trabajos son programados, que aprobaciones requiere, que procedimientos son requeridos, las herramientas requeridas para el procesamiento y el escalamiento ante cualquier excepción.

La autorización de cambios en la calendarización es responsabilidad del dueño del proceso, gerente de sistemas y del gerente de operaciones. La herramienta primaria que soporta a la calendarización del trabajo programado es la que contiene SAP de fábrica.

Únicamente el personal basis, puede programar, modificar o borrar cualquier trabajo programado. Todos los requerimientos de cambios en ellos (nuevos, modificados o eliminados) deben ser solicitados a través del sistema HelpDesk. Los trabajos programados son ligados al user ID de la persona que podrá ejecutar el job para así identificar el usuario que lo ejecuta.

El control evaluado sobre los accesos para ejecutar trabajos programados se muestra en la siguiente tabla. Ver Tabla 6.5.

Tabla 6.5. Prueba a evaluar sobre los usuarios con permisos para ejecutar jobs

CONTROL CO.04
Access to Change Jobs & Job Schedules System administrative privileges to modify scheduled batch processing and periodic scheduled background jobs are restricted and access to execute batch and background jobs under another account ID is restricted to authorized system administrators.

*6.*4.1.2 Monitoreo de Procesamiento

El Personal de Operaciones y el Analista Programador diariamente a través de la consola de operaciones de SAP conocida como “Solution Manager” realizan un monitoreo de las fallas en el procesamiento de SAP tales como: errores de procesamiento (ABAP dumps), bloqueos, fallas de autorización, uso de memoria y de base de datos. La herramienta le da la facilidad de registrar cualquier eventualidad para dar seguimiento a cada caso.

Además como un extra, la herramienta manda correos electrónicos al personal, conteniendo información sobre jobs abortados para que sean atendidos de manera inmediata en caso de ser urgentes. Como procedimiento, por cada job abortado o error de procesamiento es obligatorio que el personal levante un ticket que incluya la solución dada para mantener un rastro del incidente. En el ticket se documenta la solución.

En ocasiones los errores de procesamiento se deben al ingreso erróneo en algún campo por parte del usuario final, por lo que únicamente se le explica al personal la forma de la captura para que no vuelva a ocurrir en un futuro.

A pesar de que los jobs son controlados por el personal correspondiente, no existe un monitoreo sobre los usuarios que ejecutan los jobs para confirmar que corresponden a usuarios autorizados por el dueño del proceso.

El control evaluado sobre el monitoreo de trabajos programados se muestra en la siguiente tabla. Ver Tabla 6.6.

Tabla 6.6. Prueba a evaluar sobre el monitoreo de trabajos programados

CONTROL CO.06
Monitoring of Jobs Monitoring of jobs occurs on a daily basis. Exceptions to normal processing are escalated in a timely manner (i.e., within two business days).

6.4.2 Seguridad de Acceso

La seguridad de accesos/lógica asegura que los elementos de seguridad de acceso sean reforzados. Así mismo garantiza que únicamente personal autorizado cuente con el acceso a los datos, recursos, objetos, tablas y aplicaciones dentro del sistema.

Otra cuestión que ayuda a asegurar que el personal realice las actividades definidas en sus privilegios (ej. Leer, ejecutar, investigar, escribir, actualizar) en objetos y recursos específicos.

El personal responsable de la administración, control, monitoreo y reporte de la seguridad lógica es responsabilidad del personal Basis (encargado de monitorear el performance del aplicativo SAP)

Los accesos (acceso inicial, transferencias, cambios y terminaciones) para empleados, proveedores y otros terceros son controlados en todo el trayecto. Es inherente que cualquier acceso al sistema requiera de herramientas que administre el acceso (control de passwords).

El trayecto del alta incluye:

- Acceso usuario final –Correo electrónico/ Internet/ Intranet.
- Acceso a la red.
- Acceso a la aplicación SAP.

El acceso al sistema operativo y bases de datos no es necesario para trabajar en el aplicativo.

*6.*4.2.1 Segregación de Funciones

El objetivo del esquema de seguridad en SAP es el asegurar un ambiente estable, confiable y seguro para permitir el acceso con privilegios limitados. El enfoque primario es otorgar controles de acceso mandatorios y discrecionales.

En la compañía "x", cualquier nuevo empleado, reingreso o personal que cambio de área es analizado por Control Interno para analizar conflictos de segregación de funciones, este análisis es realizado a través del sistema de gestión de accesos llamado Access Control, que permite analizar, autorizar (Workflow configurado) y documentar la existencia de conflictos.

Para definir si existen conflictos, la herramienta permite realizar una simulación sobre los roles que se van añadir al usuario y si existe algún conflicto (según a una matriz de reglas cargada en la herramienta) notifica para que sea documentado. Así mismo fue creado un formato que es firmado por Control Interno donde se anexan las impresiones de pantalla de la simulación. El control evaluado sobre la revisión de Segregación de Funciones se muestra en la siguiente tabla. Ver Tabla 6.7.

Tabla 6.7. Prueba a evaluar sobre la revisión de Segregación de Funciones.

CONTROL UA.03
SAP Segregation of Duties New and changed user accounts and roles are reviewed by business process owners for segregation of duties (SOD) conflicts.

6.4.2.2 Altas y modificaciones de usuarios en sistema

Un buen procedimiento de altas y cambios de usuario asegura que los usuarios cuenten con un acceso autorizado, seguro y con privilegios discriminatorios, que les permiten únicamente realizar sus actividades.

En la compañía “x”, cualquier alta de un nuevo empleado o transferencias de área que requieran acceso a SAP, cualquier aprovisionamiento de roles en usuarios y modificación de roles deben ser aprobados vía Workflow (flujo de autorización electrónico) por el dueño del proceso.

La notificación del ABC (Altas, bajas y cambios de usuario) es creada en el sistema de mesa de ayuda por el personal de servicio y soporte y después es enviada a todas las áreas correspondientes para que realicen su actividad correspondiente.

Entre las actividades de alta se encuentran:

- Alta en red.
- Creación de correo electrónico.
- Alta en SAP.
- Aprovisionamiento de roles (según el área).
- Instalación de software especializado.
- Auto, teléfono, radio y cualquier otro dispositivo necesario para sus labores.

Dentro del flujo de aprobación en el ticket se encuentran el área de sistemas, el dueño del proceso, control interno, recursos humanos entre las áreas más importantes.

El control evaluado sobre la aprobación de altas y cambios de funciones se muestra en la siguiente tabla. Ver Tabla 6.8.

Tabla 6.8. Prueba a evaluar sobre la aprobación de altas y cambios de funciones.

CONTROL UA.02
Business Process Owner Approval Granting access, access changes (e.g., transfers, promotions, etc.) to company significant systems must be approved by appropriate business process owner.

6.4.2.3 Bajas de usuarios en sistema

Las bajas de usuario en los sistemas informáticos son importantes de cumplir en tiempo con el fin de evitar que se registre un acceso posterior del usuario (una vez fuera de la compañía) y pudiera realizar algún tipo de afectación con intención. En la compañía “x”, una vez que el empleado ha decidido renunciar o es despedido, el área de Recursos Humanos (RH) dispara la notificación vía el sistema de tickets de mesa de ayuda al área de sistemas para que pueda realizar la baja de los diferentes recursos informáticos.

El personal basis tiene como procedimiento que el usuario en SAP debe bloquearse de inmediato y de no ser posible, tener como máximo 5 días hábiles desde la notificación de RH para bloquear el user ID, remover todos los roles y asignar al usuario a un grupo de usuarios llamado “TERMINATED” que permite ubicar todos los usuarios que ya no laboran en la compañía. Los user ID no se eliminan y solamente se bloquean para poder mantener rastro de las actividades realizadas por el usuario.

El control evaluado sobre la desactivación de usuarios en sistema se muestra en la siguiente tabla. Ver Tabla 6.9.

Tabla 6.9. Prueba a evaluar sobre la desactivación de usuarios en el sistema.

CONTROL UA.05
Access Revocation IT disables user accounts within 5 business days of termination (including permanent and temporary personnel).

Para el seguimiento y control de las bajas, mensualmente, el área de Recursos Humanos envía un reporte de bajas de empleados para que Sistemas se asegure que las cuentas de los usuarios se encuentran deshabilitadas.

El control evaluado sobre el aviso de bajas y desactivación en el sistema se muestra en la siguiente tabla. Ver Tabla 6.10.

Tabla 6.10. Prueba a evaluar sobre el aviso de bajas de usuarios en sistema.

CONTROL UA.29
Termination Review Management receives a monthly termination report from HR and reviews to ensure user accounts were disabled.

6.4.2.4 Usuarios genéricos

Un usuario genérico, es un usuario que no pertenece físicamente a una sola persona. Estos usuarios son utilizados para la gestión de procesos complejos como el diccionario de datos, modificación de estructuras, actualizaciones del sistema, conexiones remotas y cambios de emergencia hablando desde el punto de vista tecnológico. Para la parte de los procesos de negocio, también existen usuarios genéricos que son utilizados para la comunicación (interface) entre dos sistemas distintos, ejecución de un job o uso de un escáner para las etiquetas que contienen los códigos de barra en los productos.

El documentador extrae un listado de usuarios de SAP del ambiente productivo de manera trimestral donde revisa la cantidad de usuarios genéricos existentes. El uso de estos usuarios debe ser autorizado a través del sistema de mesa de ayuda, justificando su uso. Por lo cual el documentador, revisa que todos los usos que se les dieron a estos usuarios sean autorizados. El control evaluado sobre la revisión de usuarios genéricos se muestra en la siguiente tabla. Ver Tabla 6.11.

Tabla 6.11. Prueba a evaluar sobre la revisión de usuarios genéricos.

CONTROL UA.13
Generic Accounts Generic and system user id's are reviewed quarterly to ensure appropriateness

Los usuarios genéricos también se relacionan a los super usuarios que se encuentran por defecto en el sistema SAP. Los superusuarios encontrados en este sistema son: DDIC, SAPCPIC, SAP* y EARLYWATCH.
Estos usuarios gestionan todo el sistema desde las conexiones hasta la base de datos por lo tanto cuentan con privilegios amplios que si son asignados a los usuarios finales podría correrse un riesgo importante en la integración y confidencialidad de la información. Es recomendable que estos usuarios sean bloqueados (en caso de no utilizarse) y que sus contraseñas sean cambiadas periódicamente en todos los mandantes, ya que de fábrica estas contraseñas son conocidas por el dominio público.

El control evaluado sobre la revisión de usuarios genéricos de fábrica se muestra en la siguiente tabla. Ver Tabla 6.12.

Tabla 6.12. Prueba a evaluar sobre la revisión de contraseñas en usuarios de fábrica.

CONTROL UA.14
SAP Default Passwords The default SAP R/3 passwords for SAP*, DDIC, SAPCPIC, and EarlyWatch (in client 066) are changed and specific user logins to these accounts are approved.

6.4.2.5 Recertificación de usuarios

La recertificación de usuarios es un proceso que permite analizar a través de todos los privilegios asignados a cada empleado, que sean acordes a las actividades de la persona.

Muchas veces son asignados privilegios, de manera temporal por enfermedad, ausencia o renuncia del responsable original, a otra persona que realice esas actividades, sin embargo, posteriormente no se remueven esos accesos.

En la compañía “x”, el personal basis extrae semestralmente un reporte de todos los roles asignados por usuario para que el dueño del proceso analice y compruebe que esos privilegios son correctos para su personal y acordes a sus responsabilidades. Los accesos inapropiados son comunicados de nueva cuenta al personal basis para que remueva los accesos en el sistema.

El control evaluado sobre la revisión de recertificación de usuarios se muestra en la siguiente tabla. Ver Tabla 6.13.

Tabla 6.13. Prueba a evaluar sobre la ejecución de recertificación de usuarios.

CONTROL UA.09
Application Access Re-certification Application owners (and supervisors for SAP) review and recertify user access privileges to ensure access is appropriate given the employee's job requirements.

6.4.2.6 Seguridad SAP

Como se había mencionado el esquema de seguridad en SAP asegura que los usuarios únicamente cuenten con el acceso suficiente para sus responsabilidades.

En la compañía “x”, los roles están construidos de manera que no permiten el acceso a actividades diferentes de sus responsabilidades.

Esas responsabilidades incluyen la gestión del módulo base de SAP: mantenimiento a roles/perfiles de seguridad, monitoreo del performance, monitoreo del espacio en base de datos, alta y bajas de usuarios, uso de comandos del sistema operativo a través de SAP ECC, mantenimiento de parámetros, creación y ejecución de programas, mantenimiento de tablas, uso de objetos, creación y liberación de transportes (permitiendo controlar los cambios) y el control del mandante (que permite realizar modificaciones masivas, cambios en configuración) se asignan solamente a personal autorizado.

En la compañía “x”, todas estas actividades de administración se encuentran restringidas al personal autorizado. La tabla 6.14 indica las funciones administrativas y operativas que deben encontrarse asignadas solamente a personal clave.

Tabla 6.14. Prueba a evaluar sobre los permisos de funciones críticas en el área de sistemas

CONTROL UA.21
SAP User Administration SAP End user and profile administration functions are restricted to appropriate personnel based on job responsibilities.
CONTROL UA.22
SAP External OS Commands The ability to execute external OS commands in SAP is restricted to appropriate personnel based on job responsibilities.
CONTROL UA.23
SAP Data Dictionary The ability to make changes to the SAP R/3 Data Dictionary is restricted to appropriate personnel based on job responsibilities
CONTROL UA.24
SAP Lock Objects The ability to manage SAP R/3 lock objects is restricted to appropriate personnel based on job responsibilities.
CONTROL UA.25
SAP Profile Parameters The ability to maintain SAP R/3 profile parameters is restricted to appropriate personnel based on job responsibilities.
CONTROL UA.26
SAP Program Execution The ability to directly execute SAP R/3 programs is restricted to appropriate personnel based on job responsibilities.
CONTROL CC.10
Program Change Technical Review (QA) Management performs a review of all changes promoted to the production environment to ensure a person independent of the development moved the changes to production.
CONTROL CC.07
Modify SAP Production Programs The ability to directly modify SAP programs in the production environment is restricted to appropriate personnel based on job responsibilities.
CONTROL CC.08
Modify SAP Production Tables The ability to directly modify SAP table data is restricted to appropriate personnel based on job responsibilities.

CONTROL CC.09
Workbench Organizer The ability to modify the SAP R/3 Workbench Organizer and Transport System and to perform transports is restricted to appropriate personnel based on job responsibilities.
CONTROL CC.06
Modify Client Maintenance Settings The ability to modify the SAP client maintenance settings and the global system change option is restricted to appropriate personnel based on job responsibilities.

6.4.3 Seguridad Lógica

La seguridad lógica se refiere a la seguridad en el uso del software y los sistemas, la protección de los datos, procesos y programas.

*6.*4.3.1 Parámetros de Contraseñas

Una estructura apropiada de las contraseñas y buen uso son obligatorios por SAP. Los parámetros de passwords son definidos a nivel sistema operativo (Windows 2000, 2003 a través del directorio activo) y además también deben ser definidos por default en SAP.
El alta de cuenta y la asignación del password se construyen en cuanto a las mejores prácticas y son comunicadas al usuario vía los procedimientos establecidos.

Las reglas del password aplican para todos los usuarios que se encuentran en el ambiente, a pesar de su rol. Las mejores prácticas y que se encuentran aplicadas en SAP cuentan entre otros con los siguientes parámetros:

Password Life Span = NN días. Los usuarios deben cambiar su password en su primer acceso al sistema y después cambiarlo después de NN días.
Minimum Password Length = N. Caracteres con Valores alfanuméricos que deben ser colocados para cumplir con el mínimo del longitud del password.
Password Alpha/Numeric = Al menos N letras, N letras mayúsculas, N letras minúsculas, N dígitos y N alfanuméricos.
Account Lockout = La cuenta se bloquea después de N intentos fallidos
Lockout Duration = Hasta que se desbloquea por empleados de soporte o se desbloquea en automático después de cierto tiempo.
Auto Logout = NNNN segundos. El sistema desconecta en automático la sesión del usuario después de cierto tiempo de inactividad.

El control evaluado sobre la revisión de parámetros del sistema se muestra en la siguiente tabla. Ver Tabla 6.15.

Tabla 6.15. Prueba a evaluar sobre los parámetros del sistema

CONTROL UA.12
Password Configurations Password controls exist to authenticate a user's identity before he/she has access to the network, application, database and operating system resources as per the SOPs.
CONTROL UA.17
SAP Profile Parameters SAP ECC profile parameters are appropriately configured.

*6.*4.3.2 Fire-Fighters

Los fire fighters son una herramienta web (propia de SAP) que permite mantener registro de toda actividad hecha por un super usuario.

Los usuarios finales o claves podrían solicitar el uso de algún superusuario por problemas de emergencia en la operación y que no puede continuar si este no es resuelto, para ello y para que el usuario no ejecute alguna actividad no autorizada de manera intencional, se asigna un usuario fire fighter para mantener log de toda actividad realizada por el usuario. Es recomendable que el fire fighter se asigne solo bajo situaciones de emergencia ya que habilita a los usuarios a realizar funciones que no están incluidas en sus roles asignados.

En la compañía, todas las solicitudes de acceso con privilegios amplios se gestionan a través del sistema de tickets de la mesa de ayuda para poder dar seguimiento. Las solicitudes deben ser aprobadas por los dueños del proceso antes de que se pueda asignar. Si en los accesos solicitados intervienen diferentes procesos, se requiere la aprobación de los distintos dueños de proceso. Una vez que se cuenta con la aprobación, el personal basis crea el rol y le coloca una vigencia (considerada por el usuario para realizar sus actividades). Por procedimiento, el usuario debe avisar sobre su finalización para que sea eliminado el rol asignado al usuario.

Después de la finalización, el área de sistemas envía al dueño del proceso, el log de actividades hecho por el usuario para que identifique cualquier anomalía, el área de sistemas revisa por su parte que no haya realizado ninguna afectación en tablas o sistemas.

El control evaluado sobre la aprobación de uso de Fire Fighter y revisión de las transacciones realizadas se muestra en la siguiente tabla. Ver Tabla 6.16.

Tabla 6.16. Prueba a evaluar sobre el uso de Fire-Fighters en el sistema.

CONTROL UA.19
SAP FF Access - Approval Firefighter access requests are required and must be authorized by the BPO and IT Management (or designee).
CONTROL UA.20
SAP FF Access - Audit Logging Firefighter access is only granted on a temporary basis and the activities performed while using the firefighter role are logged (through a configuration in SAP). All logs are permanently kept within SAP and sent to the BPO and IT Management (or designee) for review.

*6.*4.3.3 Perfiles amplios

Los perfiles amplios configurados en SAP permiten contar con un acceso total en el sistema. Estos perfiles son SAP_ALL y SAP_NEW, el primero permite el acceso total incluyendo modificaciones en tablas y ejecución de programas; el segundo permite la ejecución de nuevos desarrollos.

Estos perfiles normalmente se asignan de manera simultánea para realizar cualquier actividad en el sistema. En la compañía “x”, estos perfiles no se asignan a ningún usuario final (incluso a los administradores del sistema).

El control evaluado sobre la asignación de perfiles amplios en el sistema, se muestra en la siguiente tabla. Ver Tabla 6.17.

Tabla 6.17. Prueba a evaluar sobre la asignación de perfiles amplios en el sistema.

CONTROL UA.27
SAP_ALL and SAP_NEW The SAP_ALL and SAP_NEW profiles are restricted to appropriate personnel based on their job responsibilities.

*6.*4.3.4 Usuario SAP*

El sistema SAP ECC cuenta con un súper usuario por default en todos los mandantes de SAP, cuando el sistema es instalado, sin embargo, SAP* no requiere de un registro maestro de usuarios. Es por ello que si el usuario SAP* es eliminado y si algún usuario se registra con la contraseña conocida, contaría con los siguientes atributos:

- El usuario no está sujeto a chequeos de autorización, por lo tanto cuenta con todas las autorizaciones en el sistema.
- El usuario cuenta con el password “PASS”, el cual no puede ser cambiado.

Por lo tanto este usuario debe ser controlado de la siguiente forma: creación del registro maestro en todos los mandantes, crear un nuevo password y cambiarlo con periodicidad, borrar todos los perfiles que contenga y controlar el parámetro que regenera su contraseña.

En la compañía “x”, el personal Basis se asegura que el uso de este usuario esté justificado y autorizado para cuestiones de emergencia.

El control evaluado sobre la seguridad del usuario SAP*, se muestra en la siguiente tabla. Ver Tabla 6.18.

Tabla 6.18. Prueba a evaluar sobre la seguridad del usuario SAP* en el sistema.

CONTROL UA.28
SAP* Secured SAP R/3 super user ID SAP* has been adequately secured.

6.4.4 Control de Cambios

Los cambios en SAP de la compañía “x” son administrados conforme a los procedimientos de calidad de la compañía. Las responsabilidades de aprobación también se mencionan en ellos. El manual define los lineamientos de la compañía para implementar cambios en la tecnología de información en los ambientes de producción y de pruebas.

El alcance incluye la administración de cambios en la instalación, modificación y suspensión del uso de servidores, aplicaciones, bases de datos y software de infraestructura de los sistemas de cómputo de producción soportados por el área de TI.

El proceso de implementación de cambios en SAP de un cambio normal, se ilustra en la siguiente Fig. 6.2.

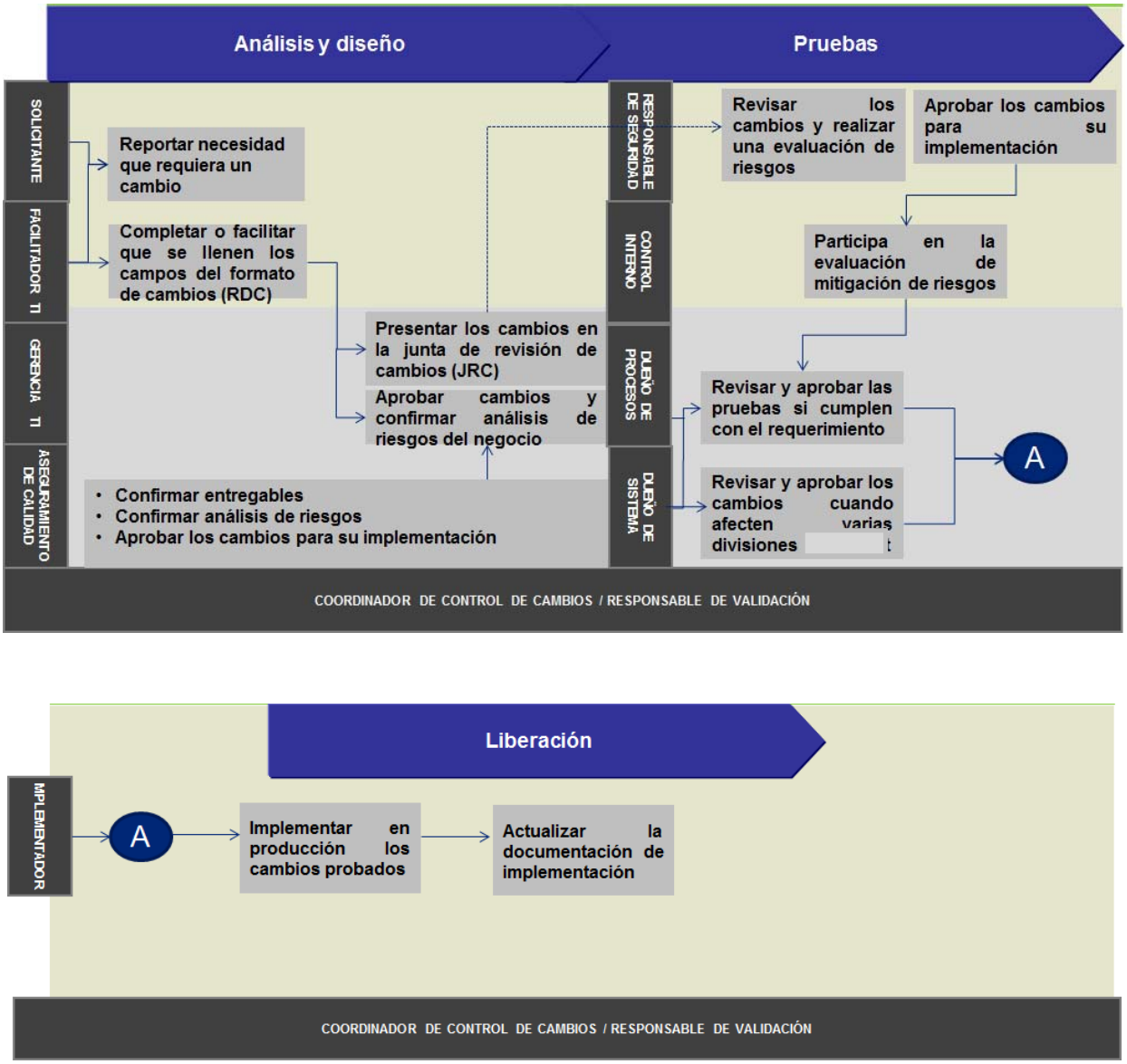

Fig. 6.2. Proceso de Implementación de cambios en la compañía “x”

Existen 2 tipos de control de cambio en la compañía “x”: Normal y de Emergencia.

*6.*4.4.1 Control de Cambio Normal

- El solicitante/facilitador TI debe completar el formato RDC y envía al responsable de validación.
- El responsable de validación revisa que el formato RDC esté completo, una vez que confirma el llenado correcto, asigna un número de control. Envía el formato RDC a aprobación.
- El responsable de seguridad realiza la evaluación de seguridad para cambios en un ambiente de prueba.

- Aseguramiento de Calidad realiza la aprobación después de que el RDC ha sido revisado y completado, asegurando que los documentos requeridos / entregables son correctos.
- Con base a una evaluación de riesgos cuantitativa con un resultado de riesgo importante, el cambio debe ser evaluado por la Junta de Revisión de Cambios (JRC).
- El RDC debe contener la firma de aprobación del Facilitador, Responsable de Validación, Aseguramiento de Calidad, Gerente TI y Dueño del Proceso.
- El facilitador TI entrega el formato al implementador para que realice los cambios en un ambiente de pruebas.
- El Dueño del Proceso (BPO) debe revisar y aprobar el resultado de las pruebas por medio del formato PAU (Aceptación de Pruebas por parte del Usuario) donde debe asegurarse que los resultados de las pruebas corresponden a los requerimientos del negocio. La firma del BPO reconoce la aceptación de todos los entregables.
- Aseguramiento de Calidad también se asegura y aprueba que existen todos los entregables.
- El Responsable de Validación (RV) abre un ticket y asigna al Facilitador de TI un recordatorio con el envío de todos los documentos de implementación completados.
- El RV notifica al solicitante y al BPO sobre la aprobación para proceder a la implementación en el ambiente de producción.
- El Implementador con la aprobación del BPO, realiza el transporte del cambio al ambiente de producción. El desarrollador y el implementador son roles segregados en la aplicación de cambios.
- Si existe una desviación no encontrada durante el plan de proceso de implementación, ésta debe ser archivada en la documentación.

*6.*4.4.2 Control de Cambio de Emergencia

- Personal de TI, responde a la situación de emergencia, solicita la aprobación de la Gerencia de TI, ésta puede ser verbal y debe ser seguida de un correo electrónico enviado al Facilitador de TI, RV y el AC si es requerido.
- El Facilitador TI elabora y prueba (si es posible) la solución requerida usando procedimientos adecuados, abre un ticket con prioridad ASAP referenciando la necesidad para un cambio de emergencia.
- La documentación para el cambio (Forma RDC, Plan de Implementación, PAU pruebas de aceptación de usuario, etc.) es completada (referenciado al número de ticket) y sometida al Coordinador de Control de Cambios dentro de las 48 horas posteriores a la implementación en el ambiente productivo.

- El RV/Gerente TI revisan el formato RDC / documentos entregables (verificar como mínimo, la implementación con las impresiones de pantallas que avala dicha implementación) y deben asegurarse que todo está debidamente documentado y aprobado).
- El RV cierra, registra y archiva el RD y los entregables.

Los controles evaluados para la revisión, aprobación y liberación de requerimientos de cambios se muestran en la tabla 6.19.

Tabla 6.19. Prueba a evaluar sobre el control de cambios en SAP.

CONTROL CC.01
UAT Testing UAT testing is performed and documented for all changes. If UAT is not required, IT management (independent from development) is required to document the rationale behind this decision.
CONTROL CC.02
Approval of Changes All changes are approved by appropriate management prior to release to production (IT and BPO).
CONTROL CC.03
Separate Environments All application changes are developed and tested in a non-production environment and then transported to the production environment.

6.4.4.3 Sistema de Transportes SAP

El sistema de transportes en SAP es de suma importancia, desde el punto de vista de seguridad. A través del mismo se garantiza la separación de los ambientes y el control de cambios.

Las órdenes de transporte son la estructura en la que se almacena la información a transportar, las mismas están constituidas por tareas individuales (pueden tener una sola) las cuales deben asociarse a usuarios individuales, los cuales adjuntaran sus modificaciones en las mismas.

Cuando alguien modifica un objeto en el sistema (**ABAP**, Customizing o algún otro) el tipo de objeto es seleccionado automáticamente y se solicita una orden de transporte la cual se puede crear si posee los permisos.

Hasta ese instante, la orden no ha sido liberada, por lo que para que sea funcional en el ambiente productivo, debe liberarse. En instante, el sistema se encarga de guarda la versión de los objetos involucrados en el directorio correspondiente del sistema operativo. Hay dos tipos de transportes: ***customizing (transportan configuración del sistema) y workbench (transportan códigos de programas).***

Los transportes workbench contienen código del lenguaje de programación ABAP, incluyendo cálculos y reportes. Estos transportes afectan a todos los mandantes configurados.

Los transportes customizing contienen modificaciones a la configuración como cambios en tablas, controles automatizados y flujos de autorización. Estos transportes afectan solo al mandante donde se aplica el cambio. Los riesgos del control de cambios se presentan cuando se cuenta con el acceso a la modificación directamente en el ambiente productivo.

Al considerarse el medio de transporte para los cambios, en la compañía "x", el implementador se asegura de que el cambio cumpla con los procedimientos de calidad para el control de cambios, entre otros aspectos, la revisión incluye: nomenclatura del transporte, objetos transportados, código de acuerdo al estándar, comentarios, modificaciones en configuración, etc.
Los controles evaluados para la revisión de estándares en transportes se muestran en la tabla 6.20.

Tabla 6.20. Prueba a evaluar sobre la revisión de estándares en transportes.

CONTROL CC.04
SAP Program Change Technical Review (QA) On a quarterly basis, management selects a sample of 20 transports migrated into production and performs Technical Review (QA) for adherence to technical and security standards

*6.*4.4.4 Mandante

El mandante constituye el nivel jerárquico superior en el sistema SAP. Las especificaciones que se realizan a los datos que se introducen a este nivel son válidas para todas las sociedades y para todas las estructuras organizativas, evitando tener que introducir la información más de una vez. Cada mandante es una unidad independiente con registros maestros separados y set de tablas.

Los usuarios deben introducir una clave de mandante cuando entran al sistema. De esta forma facilitan al sistema el mandante con el que desean trabajar. Tanto el almacenamiento de todas las entradas efectuadas como el análisis y proceso electrónico de datos se realizan por cliente.

En la compañía "x", la apertura del mandante (que implica cualquier modificación en el sistema) es controlado de manera estricta con acceso muy limitado al personal basis.

Por procedimiento, el mandante únicamente es abierto para cambios de emergencia que deben realizarse directamente en el ambiente productivo.

El control evaluado para la configuración del mandante se muestra en la tabla 6.21.

Tabla 6.21. Prueba a evaluar sobre la revisión de configuración en el mandante.

CONTROL CC.05
SAP Client Maintenance Settings The SAP client maintenance settings and the global change option are configured to prevent development from occurring directly in the production environment. In the event that non-transportable changes are required in the production environment, they are documented and approved consistent with the change management process.

6.5 Documentación

La documentación representa el esfuerzo realizado durante la identificación de riesgos y evaluación de controles, así mismo es la evidencia de lo ejecutado por el auditor.

Cierta evidencia clave que demuestra la evaluación de la auditoría se muestra para confirmación del lector. (*Véase Apéndice A3*).

6.5.1 Matriz de Pruebas

La matriz de pruebas es el resultado de la ejecución de la auditoría, es la prueba de que el auditor externo e interno realizó la evaluación de los controles y sobre la cual se asienta la descripción del control, la prueba a ejecutar, el tamaño de la muestra, el resultado de la prueba y el plan de acción que hará el cliente si es que se identifica que algún control no se encuentre operando de manera efectiva.

El template de pruebas de esta compañía fue elaborado entre las oficinas de Atlanta (al encontrarse el corporativo de la compañía “x” en aquella ciudad) y la de México, donde encontramos toda la operación de Latinoamérica. Esta matriz de pruebas contiene todos los atributos que deben probarse durante la auditoría SOX. (*Véase Apéndice A2*)

En la siguiente tabla se muestra el resultado de las pruebas ejecutadas sobre los controles revisados en el dominio de *Operaciones*, *Seguridad y Control de Cambios*. Ver tabla 6.22.

Tabla 6.22. Matriz de Pruebas ejecutadas en la compañía “x”.

Operaciones					
Control ID	**Control**	**Tamaño muestra**	**Prueba**	**Resultados**	**Plan de acción**
CO.04	**Access to Change Jobs & Job Schedules**	1	Listado de usuarios a transacciones SAP que administran y ejecutan jobs.	Los listados de usuarios muestran que únicamente es personal autorizado	Ninguna deficiencia
CO.06	**Monitoring of Jobs**	25	Solicitar la evidencia de la ejecución de 25 jobs para confirmar su finalización correcta y en caso de falla detectar el monitoreo y solución otorgada al problema.	. **NO SE** encontró un monitoreo a una tabla que permite validar los usuarios que ejecutan los jobs.	**Requerida, Una excepción encontrada** El personal generará diariamente un listado de los jobs críticos, mensualmente revisará que los jobs sean ejecutados por personal autorizado.75
CC.10	**Program Change Technical Review (QA)**.	Todos	Solicitar el listado de transportes creados y liberados para detectar los usuarios involucrados.	Los listados de usuarios muestran que únicamente es personal autorizado.	Ninguna deficiencia
Seguridad de Acceso y lógica					
UA.02	**Business Process Owner Approval**	25	Solicitar el listado de altas y cambios para confirmar autorización del dueño del proceso.	Todos los casos muestran que fueron autorizados por el dueño del proceso.	Ninguna deficiencia
UA.03	**SAP Segregation of Duties**	25	Solicitar el listado de altas y cambios para después confirmar que para los casos seleccionados, las áreas correspondientes revisan la segregación de funciones.	En todos los casos fue validado que se cuenta con una revisión de Control Interno para cada usuario nuevo, promociones, cambios de área o modificación de roles.	Ninguna deficiencia
UA.05	**Access Revocation**	25	Solicitar el listado de bajas para después confirmar que para los casos seleccionados, los accesos fueron deshabilitados sin la posibilidad de accesar al sistema.	Todas las bajas seleccionadas ya no cuentan con acceso a la aplicación ya que tienen el usuario deshabilitado.	Ninguna deficiencia
Control ID	**Control**	**Tamaño muestra**	**Prueba**	**Resultados**	**Plan de acción**
UA.09	**Application Access Re-certification**	1	Solicitar el reporte de revisión de los privilegios por usuario donde fueron detectados accesos	El reporte contiene comentarios del dueño del proceso donde detecta accesos incorrectos, sin	**Requerida, Deficiencia encontrada**

			erróneos o inapropiados con respecto a las responsabilidades del personal por parte del dueño del proceso.	embargo, para algunos casos, los roles no fueron dados de baja según lo confirmado en el sistema.	Asegurar a través de un incidente que sean removidos los accesos
UA.12	**Password Configuration** .	1	Obtener evidencia de los valores de los parámetros de acceso y seguridad encontrados en el aplicativo SAP.	Los usuarios únicamente tienen acceso a nivel aplicativo y los parámetros de acceso y seguridad definidos en el sistema son valores acordes a mejores prácticas.	Ninguna deficiencia
UA.13	**Generic Accounts**	2	Obtener evidencia de los reportes generados donde sea confirmando la revisión de los usuarios genéricos.	Los reportes contienen comentarios sobre el uso de todos los usuarios genéricos. Todos los usuarios genéricos son autorizados.	Ninguna deficiencia
UA.14	**SAP Default Passwords**	1	Obtener evidencia sobre si los súper usuarios cuentan con contraseñas por default.	La evidencia muestra que todos los super usuarios no cuentan con la contraseña por default definida por el sistema.	Ninguna deficiencia
UA.17	**SAP Profile Parameters**	1	Obtener evidencia de los valores de los parámetros de acceso y seguridad encontrados en el aplicativo SAP.	Los usuarios únicamente tienen acceso a nivel aplicativo y los parámetros de acceso y seguridad definidos en el sistema son valores acordes a mejores prácticas.	Ninguna deficiencia
UA.19	**SAP FF Access - Approval**	8	Solicitar las solicitudes de uso de Fire Fighter, para confirmar que el dueño del proceso autorizó en todos los casos.	Los casos seleccionados muestran que la asignación de un rol fire fighter es autorizado por el BPO.	Ninguna deficiencia
UA.20	**SAP FF Access - Audit Jogging**	8	Solicitar las solicitudes de uso de Fire Fighter, para confirmar que en todos los casos fue generado un log con todas las tareas ejecutadas por el usuario, el cual además es validado por el BPO.	Los casos seleccionados muestran que fue generado un log y enviado al BPO para su aprobación sobre las tareas ejecutadas por el usuario al que se le asignó el fire fighter.	Ninguna deficiencia
Control ID	**Control**	**Tamaño muestra**	**Prueba**	**Resultados**	**Plan de acción**
UA.21	**SAP User Administration** .	1	Solicitar el listado de usuarios con acceso a la administración de roles, perfiles y usuarios.	Los listados muestran que únicamente el personal basis (autorizado), son los únicos que cuentan con los	Ninguna deficiencia

				privilegios para la administración de la seguridad.	
UA.22	**SAP External OS Commands** .	1	Solicitar el listado de usuarios con acceso a la ejecución de comandos del sistema operativo a través de la aplicación.	Los listados muestran que únicamente el personal basis (autorizado), son los únicos que cuentan con los privilegios para la ejecución de comandos.	Ninguna deficiencia
UA.23	**SAP Data Dictionary** .	1	Solicitar el listado de usuarios con acceso a la administración del diccionario de datos.	Los listados muestran que únicamente el personal basis (autorizado), son los únicos que cuentan con los privilegios para la administración del diccionario de datos.	Ninguna deficiencia
UA.24	**SAP Lock Objects** .	1	Solicitar el listado de usuarios con acceso al bloqueo de objetos.	Los listados muestran que únicamente el personal basis (autorizado), son los únicos que cuentan con los privilegios para el bloqueo de objetos.	Ninguna deficiencia
UA.25	**SAP Profile Parameters** .	1	Solicitar el listado de usuarios con acceso al mantenimiento de los parámetros del sistema.	Los listados muestran que únicamente el personal basis (autorizado), son los únicos que cuentan con los privilegios para el mantenimiento de los parámetros del sistema.	Ninguna deficiencia
UA.26	**SAP Program Execution** .	1	Solicitar el listado de usuarios con acceso a la creación y ejecución de programas.	Los listados muestran que el personal basis (autorizado), son los únicos que cuentan con los privilegios para la creación y ejecución de programas.	Ninguna deficiencia
UA.27	**SAP_ALL and SAP_NEW** .	1	Solicitar el listado de usuarios que cuentan con la asignación de los perfiles con amplios privilegios.	Los listados muestran que estos perfiles no se asignan a ningún usuario dentro de la compañía.	Ninguna deficiencia
UA.28	**SAP* Secured**	1	Solicitar evidencia sobre la seguridad mantenida sobre el superusuario SAP*	La evidencia muestra que: el usuario SAP* está bloqueado y además no tiene asignado roles y perfiles,	Ninguna deficiencia
UA.29	**Termination Review**	3	Solicitar evidencia de los reportes enviados por HR al personal basis.	La evidencia muestra que para todos los usuarios que fueron reportados como bajas, los user Id’s ya se encuentran deshabilitados.	Ninguna deficiencia

Control de Cambios					
Control	**Control**	**Tamaño**	**Prueba**	**Resultados**	**Plan de acción**

ID		muestra			
CC.01	**UAT Testing**	25	Solicitar el listado de cambios para después confirmar que para los casos seleccionados, se cuente con evidencia de las pruebas realizadas.	En todos los casos fue validado que se cuenta con formatos de las pruebas realizadas en un ambiente distinto a productivo. El formato es firmado y autorizado.	Ninguna deficiencia
CC.02	**Approval of Changes**	25	Solicitar el listado de cambios para después confirmar que para los casos seleccionados, se cuente con evidencia de las aprobaciones de las pruebas antes de la implementación en productivo.	En todos los casos fue validado que se cuenta con formatos de las pruebas realizadas en un ambiente distinto a productivo. El formato es firmado y autorizado.	Ninguna deficiencia
CC.03	**Separate Environments**	25	Solicitar el listado de cambios para después confirmar que para los casos seleccionados, se cuente con evidencia de las pruebas realizadas.	En todos los casos fue validado que se cuenta con formatos de las pruebas realizadas en un ambiente distinto a productivo. El formato es firmado y autorizado. Los transportes son llevados por personal autorizado con la segregación adecuada.	Ninguna deficiencia
CC.04	**SAP Program Change Technical Review (QA)**	25	Solicitar el listado de transportes para después confirmar que para los casos seleccionados, se cuente con una revisión técnica, lógica y de nomenclatura con respecto a los estándares de seguridad.	**NO** en todos los casos se encontró evidencia de la revisión de transportes acordes a los estándares de seguridad.	**Requerida, Deficiencia encontrada.** El personal responsable se asegurará todos los transportes sean revisados.
CC.05	**SAP Client Maintenance Settings**	1	Solicitar evidencia que avale que los mandantes sean asegurados con el fin de evitar cambios no autorizados.	La evidencia muestra que el mandante está cerrado y asegurado para evitar modificaciones no autorizadas.	Ninguna deficiencia
CC.06	**Modify Client Maintenance Settings** .	1	Solicitar el listado de usuarios con acceso a la administración del mandante	Los listados muestran que únicamente el personal basis (autorizado), son los únicos que cuentan con los privilegios para la administración del mandante.	Ninguna deficiencia
CC.07	**Modify SAP Production Programs** .	1	Solicitar el listado de usuarios con acceso a la ejecución de programas	Los listados muestran que únicamente el personal basis (autorizado), son los únicos que cuentan con los privilegios para la ejecución de programas.	Ninguna deficiencia
CC.08	**Modify SAP Production Tables**	1	Solicitar el listado de usuarios con acceso a la modificación de tablas.	Los listados muestran que únicamente el personal basis (autorizado), son los	Ninguna deficiencia

	.			únicos que cuentan con los privilegios para la modificación de tablas.	
CC.09	**Workbench Organizer** .	1	Solicitar el listado de usuarios con acceso a la gestión del sistema de transportes	Los listados muestran que únicamente el personal autorizado puede crear y liberar transportes en el ambiente productivo.	Ninguna deficiencia

6.5.2 Papeles de Trabajo

Los papeles de trabajo de SOX 404 que el Auditor TI considera relevantes, están resumidos en la siguiente tabla. La referencia del papel de trabajo (#) en el índice es el que se refiere al repositorio de papeles. La organización de los papeles se muestra en la siguiente tabla. Ver tabla 6.23.

Tabla 6.23. Papeles de Trabajo de en la compañía “x”

Referencia del Papel	Papel de Trabajo
4000.1	“X” company SOX 2011 ELC Testing Template notes
MEX4000.2	Deficiencies list “x” company
MEX4000.3	Operations Narrative with Controls
CO.04	Access to change Job & Job schedules- *Test Sheet*
CO.06	Monitoring of jobs –*Test sheet*
MEXCO.06.01	Job logs
MEXCO.06.02	Configuration e-mail alerts
MEX4000.4	User Access Narrative with Controls
UA.02	Business Process Owner Approval – *Test sheet*
MEXUA.02.01	Granting access and role changes
UA.03	Segregation of duties –*Test sheet*
MEXUA.03.01	SAP Segregation of duties
UA.05	Access Revocation –*Test sheet*
MEXUA.05.01	User account disabled
UA.09	Application access re-certification –*Test sheet*
MEXUA.09.01	Application access re-certification
UA.12	Password configurations –*Test sheet*
UA.13	Generic accounts –*Test sheet*
MEXUA.13.01	SAP Generic Accounts
UA.14	Default SAP R/3 Passwords for SAP*, DDIC, SAPCPIC and EarlyWatch –*Test sheet*
UA.17	SAP R/3 Profile Parameters –*Test sheet*
UA.19-20	SAP Firefighter Access-Approval and Audit Logging –*Test sheet*
MEXUA.19.01	BPO authorization for fire fighter access request
MEXUA.20.01	BPO fire fighter log review
UA.21	Access to SAP End User and Profile Administration Functions – *Test sheet*
UA.22	Access to Execute External OS Commands –*Test sheet*
UA.23	Access to Modify the SAP R/3 Data Dictionary –*Test sheet*
UA.24	Access to Manage SAP R/3 Lock Objects –*Test sheet*
UA.25	Access to Maintain SAP R/3 Profile Parameters –*Test sheet*
UA.26	Access to Directly Execute SAP R/3 Programs –*Test sheet*
UA.27	Access to SAP_ALL and SAP_NEW Profiles –*Test sheet*

UA.28	SAP* - *Test sheet*
UA.29	Termination review – *Test sheet*
MEX4000.5	Change Control Narrative with Controls
CC.01-03	Change Control - *Test sheet*
MEXCC.01-03.01	Change Control
CC.04	SAP Program Change Technical Review (QA) –*Test sheet*
CC.05	SAP Client Maintenance Settings – *Test sheet*
CC.06	Modify Client Maintenance Settings – *Test sheet*
CC.07	Access to directly modify SAP Programs –*Test sheet*
CC.08	Access to directly modify SAP Table Data –*Test sheet*
MEXCC.08.01	Users with access to modify tables
CC.09	Access to Modify the SAP R/3 Workbench Organizer and Transport System – *Test sheet*
CC.10	Management review of DBA activity – *Test sheet*

6.5.3 Hallazgos

Una vez finalizada la evaluación y documentación de la auditoría, es identificable que la compañía “x” sea una empresa que cuenta con controles adecuados que permiten cumplir con la ley SOX. Sin embargo, se encontraron 3 deficiencias que fueron comunicadas en tiempo, las cuales se describen a continuación. Ver tabla 6.24.

Es importante hacer notar, que las deficiencias fueron comunicadas en una presentación ejecutiva con la administración de TI y Control Interno de la compañía “x”, pudiendo dar tiempo para generar un plan de remediación previo a la llegada de los auditores externos.

Tabla 6.24. Deficiencias encontradas durante la auditoría de la compañía “x”.

Proceso	Actividad de Control	Control COBIT 4.1	Deficiencia	Plan de Remediación	Fecha de Remediación	Impacto
Seguridad de Acceso	UA.09	DS5.4	Con base a la revisión del reporte sobre la recertificación de usuarios, identificamos que los accesos definidos por el dueño del proceso como incorrectos, no son eliminados completamente por el Personal Basis	Al recibir el documento, donde el BPO indique accesos que no autoriza, se creará un incidente en base al procedimiento DIT-010-2 asegurando retirar los accesos no aprobados	Agosto	Medio
Control de Cambios	CC.04	AI7.8	No para todas las órdenes de transporte se encontraron comentarios de cumplimiento con estándares técnicos y de seguridad.	Verificar el texto breve de todas las órdenes de transporte del tipo Customizing. Los transportes workbench se incluyen pantallas en la documentación como evidencia y se revisan estándares.	Julio	Medio
Operaciones	CO.06	DS11.5	No es revisado de	Realizar un listado de	Agosto	Bajo

			manera trimestral la tabla de SAP que permite monitorear que usuario ha ejecutado trabajos críticos.	trabajos críticos ejecutados diariamente por los usuarios. Mensualmente hacer una revisión para asegurar la correcta generación de los mismos.		

CONCLUSIONES DEL PROYECTO

De acuerdo al alcance de los procedimientos realizados desde la etapa de planeación hasta la de reporteo, la auditoría proporciona un grado de confianza sobre el aseguramiento de los controles internos en el ambiente de procesamiento bajo alcance. Los procedimientos de control ejecutados por el personal de Tecnología de la compañía "x" **soporta el procesamiento confiable de información financiera**.

Aún y cuando el procesamiento de la información financiera es confiable en el ambiente de procesamiento, se han encontrado deficiencias mínimas que fueron reportadas a la administración y que estarán siendo remediadas en una fecha definida.

Estos hallazgos serán reportados como parte de la sección 404 de la auditoría SOX que se realiza anualmente para esta compañía.

Se cumplió con los objetivos planteados al contar con una auditoría satisfactoria para el cliente, donde fue posible evaluar los controles y realizar recomendaciones finales para mejorar ese ambiente de control.

CONCLUSIONES PERSONALES

Con base en los logros planteados, se obtuvieron diferentes beneficios personales que fueron cumplidos satisfactoriamente:

- ✓ Fortalecimiento de conocimientos de una auditoría SOX, al ser la tercera que ejecutaba desde mi arribo a Deloitte. Hasta esta oportunidad pude dar seguimiento a un real plan de remediación así como enterarme de la forma en cómo se documenta el reporte para informar a los inversionistas.
- ✓ Aplicación de conocimiento adquirido anteriormente.
- ✓ Conocimiento de herramientas para administración del área de tecnología.
- ✓ Conocimiento de un “real” ambiente de control, al validar que todos los procesos están documentados y existe evidencia para cada uno de ellos.
- ✓ Toma de decisiones sobre reporteo a la dirección debido a que mi gerente no se encontraba disponible.
- ✓ El cliente quedó muy satisfecho con el trabajo elaborado al felicitarnos por la revisión.
- ✓ Este proyecto es un peldaño más para la próxima promoción a nivel gerente.

APÉNDICE

APÉNDICE A1 - Resumen del Acto 2002 de Sarbanes Oxley

Section 101 Establishment; Duties of the Board.
Section 103 Auditing, Quality Control, and Independence Standards and Rules.
Section 102(a) Mandatory Registration
Section 102(f) Registration And Annual Fees.
Section 109(d) Funding; Annual Accounting Support Fee for the Board.
Section 104 Inspections of Registered Public Accounting Firms
Section 105(b) (5) Investigation and Disciplinary Proceedings; Investigations; Use of Documents.
Section 105(c) (2) Investigations and Disciplinary Proceedings; Disciplinary Procedures; Public Hearings.
Section 105(c) (4) Investigations and Disciplinary Proceedings; Sanctions.
Section 105(d) Investigations And Disciplinary Proceedings; Reporting of Sanctions.
Section 106 Foreign Public Accounting Firms.
Section 107(a) Commission Oversight of the Board; General Oversight Responsibility.
Section 107(b) Rules of the Board.
Section 107(d) Censure of the Board and Other Sanctions.
Section 107(c) Commission Review of Disciplinary Action Taken By the Board.
Section 108 Accounting Standards.
Section 201 Services Outside The Scope Of Practice Of Auditors; Prohibited Activities.
Section 203 Audit Partner Rotation.
Section 204 Auditor Reports to Audit Committees.
Section 206 Conflicts of Interest.
Section 207 Study of Mandatory Rotation of Registered Public Accountants.
Section 209 Consideration by Appropriate State Regulatory Authorities.
Section 301 Public Company Audit Committees.
Section 302 Corporate Responsibility for Financial Reports.
Section 303 Improper Influence on Conduct of Audits
Section 304 Forfeiture of Certain Bonuses and Profits.
Section 305 Officer and Director Bars and Penalties; Equitable Relief.
Section 305 Officer and Director Bars and Penalties.
Section 306 Insider Trades During Pension Fund Black-Out Periods Prohibited.
Section 401(a) Disclosures in Periodic Reports; Disclosures Required.
Section 401 (c) Study and Report on Special Purpose Entities.
Section 402(a) Prohibition on Personal Loans to Executives.

Section 403 Disclosures Of Transactions Involving Management And Principal Stockholders.
Section 404 Management Assessment of Internal Controls.
Section 407 Disclosure of Audit Committee Financial Expert.
Section 409 Real Time Disclosure.
Section 501 Treatment of Securities Analysts by Registered securities Associations.
Section 601 SEC Resources and Authority.
Section 602(a) Appearance and Practice Before the Commission.
Section 602(c) Study and Report.
Section 602(d) Rules of Professional Responsibility for Attorneys.
Section 701 GAO Study and Report Regarding Consolidation of Public Accounting Firms.
Title VIII Corporate and Criminal Fraud Accountability Act of 2002.
Title IX White Collar Crime Penalty Enhancements.
Section 1001 Sense of Congress Regarding Corporate Tax Returns.
Section 1102 Tampering With a Record or Otherwise Impeding an Official Proceeding.
Section 1103 Temporary Freeze Authority.
Section 1105 SEC Authority to Prohibit Persons from Serving as Officers or Directors.

APÉNDICE A2 - Template de Pruebas SOX

Company Name:
Business Unit Name
Quarter/Fiscal Year: Trimestre revisado para la auditoría SOX.
Process

Control Activity ID: ID encontrado en los índices de los papeles de trabajo.
Control Owner (s): Persona que ejecuta el control.
Related Systems (s): La aplicación definida para el alcance.
Control Activity: Las actividades que necesitan ser probadas para validar su eficacia.

1. Actividad de Control y referencia al objetivo (ejemplo: 1,3 y 4).
2. Actividad de Control y referencia al objetivo (ejemplo: 2 y 5).

Test Procedure: Describe el método de pruebas (investigación, observación, inspección, etc.) y detalla los procedimientos para la ejecución de las pruebas. Incluye el criterio de selección de muestras, período, método y descripción de la población.

Test Period: Periodo cubierto de la auditoría (ej. Enero-Marzo, Marzo-Julio, etc.).

Testing Technique: Técnica ejecutada para validar la eficacia del control.

1. *Inquiry:* Esta técnica permite realizar una investigación de los controles existentes. Esta técnica se refiere al walkthrough hecho en las entrevistas.
2. *Reperformance:* Esta técnica permite confirmar a la persona que el sistema está realizando correctamente el control. Eje. *Cálculo de importes en facturas.*
3. *Inspection/Examination:* Esta técnica permite inspeccionar la información proporcionada por el cliente.

4. *Observation:* Esta técnica permite por medio de la vista el confirmar la eficacia del control. Esta técnica no es muy común al no mantener evidencia.

Test Results (Supporting docs): Documentación de los resultados de las pruebas, documentación soporte y cualquier hallazgo. En caso de que sea solicitada más de una muestra, se documentan en una tabla para dar seguimiento a todos los casos.

		Testing Attributes			
Sample	**Description**	**A**	**B**	**C**	**Notes**

Testing Attributes
A = Describir los atributos revisados en la prueba.
B = Describir los atributos revisados en la prueba.
C = Describir los atributos revisados en la prueba.

Sample Population: Breve explicación del porqué de la selección de "x" muestras seleccionadas.
Control Frequency
Sample Size

Conclusion Notes: Notas del porqué de la conclusión seleccionada.
Conclusion/Results: Conclusión del resultado de la eficacia del control.

1. **P:Pass:** El control opera eficientemente.
2. **FN: Failed: No Control:** El control no existe.
3. **FE: Failed Exception:** A pesar de que el control existe, hay una actividad de las "n" definidas para la que no se encontró evidencia.
4. **N/A: Not applicable:** No hay conclusión para el control.

Sign Off: Las iniciales y fecha de firma del preparador y los "n" revisores.

Recommendaion (if applicable): Descripción de las acciones correctivas para mitigar la exposición relacionada al control inefectivo. Debe identificarse el plan de acción, la persona responsable de la remediación y la fecha de remediación.

Ejemplo de la matriz de pruebas. Ver la Fig. A2.1

CONTROL ACTIVITY

Business Process Owner Approval
Granting access, access changes (e.g., transfers, promotions, etc.) to company significant systems must be approved by appropriate business process owner.

TEST PLAN & FINDINGS

TEST PROCEDURE:
Inquiry:
Interviewed Martha Vazquez -Testing Analyst (Basis Functions) on 06/23/2011 to confirm that granting access and access changes (e.g., transfers, promotions, etc.) to the company's significant systems are approved by the appropriate business process owner. Per Martha, when a new employee begins work or changes roles at the corporate location, the HR department will send an email request to the IT Helpdesk (ACS) regarding access approval. IT uses an application called Service Center to create tickets for access approval. The e-mail and tickets of approval are attached to the tickets in the Service Center application.

In order to test that new and change users were approved by the business process owners obtained a SAP generated listing of SAP users created or changed access from 1/1/2011 to 6/30/2011. Noted that there were 52 new users in SAP and considering a "high risk" testing, we determined to use a sample size of 'daily' and selected 15 to confirm BPO's approval.

According to Martha Vazquez there was not any changed users during 1/1/2011-6/30/2011 period, all were new users, the ones coming from Tecnofarma and new hires, so, in order to evaluate Business Process Owner approval select changed role samples from that period. Noted that there were 35 changed roles in SAP and considering a "high risk" testing, we determined to use a sample size of 'weekly' and selected 10 to confirm BPO´s approval. Considering new users and changes in roles, we have a total population of 25 to accomplish the

SCOPE		
Test Period	FROM	TO
	01/01/2011	06/30/2011

TESTING TECHNIQUE	
Inquiry	X
Reperformance	
Inspection/Examination	X
Observation	

SAMPLING INFORMATION

SAMPLE POPULATION SOURCE & PERIOD COVERED:

1) Population of new SAP users and changes in roles from 1/1/2011 to 6/30/2011. "Ref. Supporting Docs 2"

2) 15 Service Center tickets for new users and 10 for changes in roles containing Business Process Owner approval "Ref. Supporting Docs 1"

SAMPLING APPROACH	
Control Frequency	Daily
Sample Size	25

CONCLUSION / RESULTS

CONCLUSION NOTES: **Control Operating Effectively**

ASSESSMENT RESULTS	
Conclusion / Results	P: Pass
Test of Design	Adequate with No Exception
Test of Effectiveness	Effective with No Deficiency

D&T REVIEW AND SIGN-OFF

COMMENTS:

D&T REVIEW AND SIGN-OFF		
Sign-Off	INITIAL	DATE
Preparer	CABI	06/28/2011
Reviewer	SRGC	07/14/2011
Reviewer	ICO	07/22/2011

Fig. A2.1 Matriz de pruebas ejecutadas en la compañía “x”

Revisión de muestras. Ver Fig. A2.2

Purpose:	To determine whether granting access, access changes (e.g., transfers, promotions, etc.) to SAP are approved by appropriate business process owner.
Source:	Martha Vazquez -Testing Analyst (Basis Functions)
Description:	Judgementally selected a sample of new users and changes in roles and their corresponding ticket. Verified that access granted were properly approved using Access Enforcer and a CMN or RDC for role changes
Attribute A	Access Enforcer or Service Center ticket for new users and role changes respectively
Attribute B	Business Process Owner approval in Access Enforcer for new users and a CMN or RDC forms for role changes

No.	User Name	Name	Type	Date	BPO Approval	Ticket or Request Number	Attribute A	Attribute B	Notes	Evidence
1	EMENDOZA	MENDOZA MARTINEZ EDGAR	New Account	18-Jan-11	Pablo Briones	2731 -Access Enforcer	Pass	Pass		
2	JCARMONA	CARMONA HERNANDEZ JORGE ABRAHAM	New Account	19-Jan-11	Moises Pelaez, Pablo Briones, Mitchell Paez, Miguel Cote	2733 -Access Enforcer	Pass	Pass		
3	N/A	ALDANA MORALES MIRIAM	New Account	01-feb-11	N/A	N/A	N/A	N/A	The user does not need access to SAP system	
4	LGARCIA	GARCIA GUTIERREZ LUIS RAFAEL	New Account	01-mar-11	Jeronimo Ahedo, Moises Pelaez	3123 - Access Enforcer	Pass	Pass		
5	JSOTO	SOTO HERNANDEZ JACQUELINE SUGEHI	New Account	07-mar-11	Miguel Angel Cote	3149 - Access Enforcer	Pass	Pass		
6	RTIRAPU	TIRAPU PEREZ, IVANNY YEZABETH	New Account	10-feb-11	Moises Pelaez, Mitchell Paez	3035 - Access Enforcer	Pass	Pass		
7	N/A	MENDIVIL MARTIN GERARDO	New Account	22-mar-11	N/A	N/A	N/A	N/A	The user does not need access to SAP system	
8	YMARTINE	MARTINEZ DOMINGUEZ YESSICA	New Account	12-may-11	Miguel Angel Cote	3416 - Access Enforcer	Pass	Pass		
9	OCABRERA	CABRERA ORDOÑEZ OSCAR	New Account	03-jun-11	Alfonso Arellano, Maria Blancas	3537 - Access Enforcer	Pass	Pass		
10	FRODRIGU	RODRIGUEZ HERNANDEZ FELIPE	New Account	30-may-11	Moises Pelaez, Pablo Briones, Mitchell Paez, Javier Rovalo, Jeronimo Ahedo	3483 - Access Enforcer	Pass	Pass		
11	N/A	FLORVILLE CHACON ROSA INES	New Account	14-feb-11	N/A	N/A	N/A	N/A	The user does not need access to SAP system	See UA.02.01 Granting Access and role changes
12	IRIOS	RIOS COTE MARIA ISELA	New Account	28-mar-11	Miguel Angel Cote	3226 - Access Enforcer	Pass	Pass		
13	N/A	SILVA PEREZ SONIA	New Account	25-abr-11	N/A	N/A	N/A	N/A	The user does not need access to SAP system	

Fig. A2.2 Revisión de muestras para calificación de atributos

APÉNDICE A3 - Documentación clave de la auditoría

Control del Mandante (Ver Fig. A3.1)

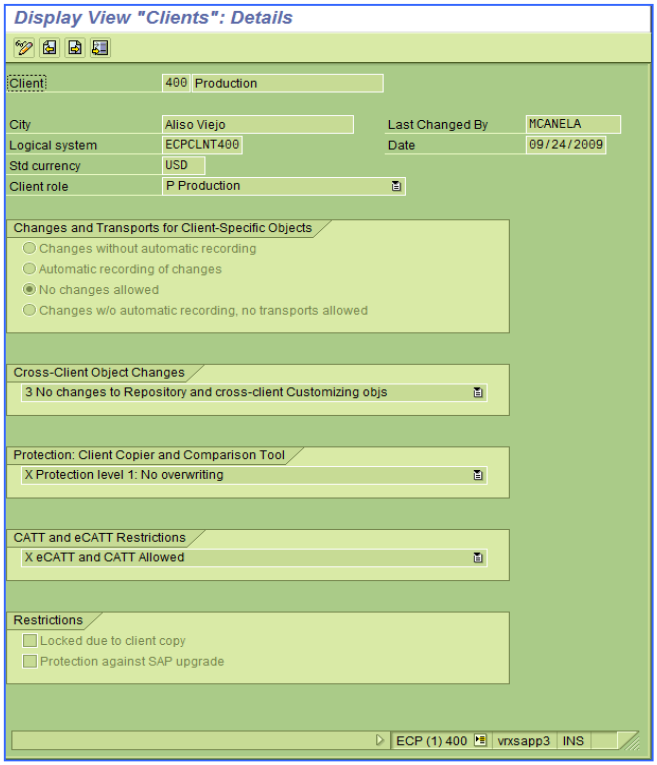

Fig. A3.1 Revisión de configuración del mandante

Parámetros del sistema (Ver Fig. A3.2)

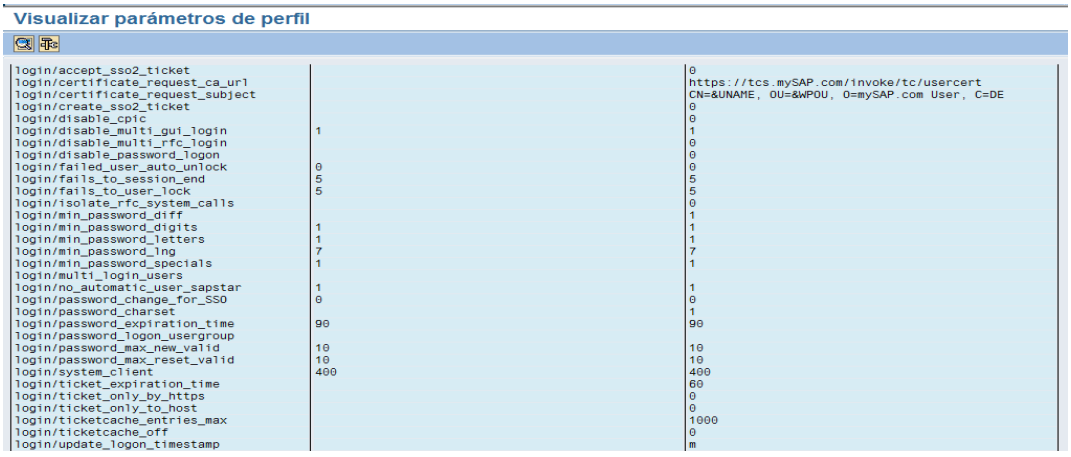

Fig. A3.2 Revisión de parámetros del sistema

Control SAP* (Ver Fig. A3.3)

Fig. A3.3 Revisión de configuración del usuario SAP*

Deshabilitar un usuario (Ver Fig. A3.4)

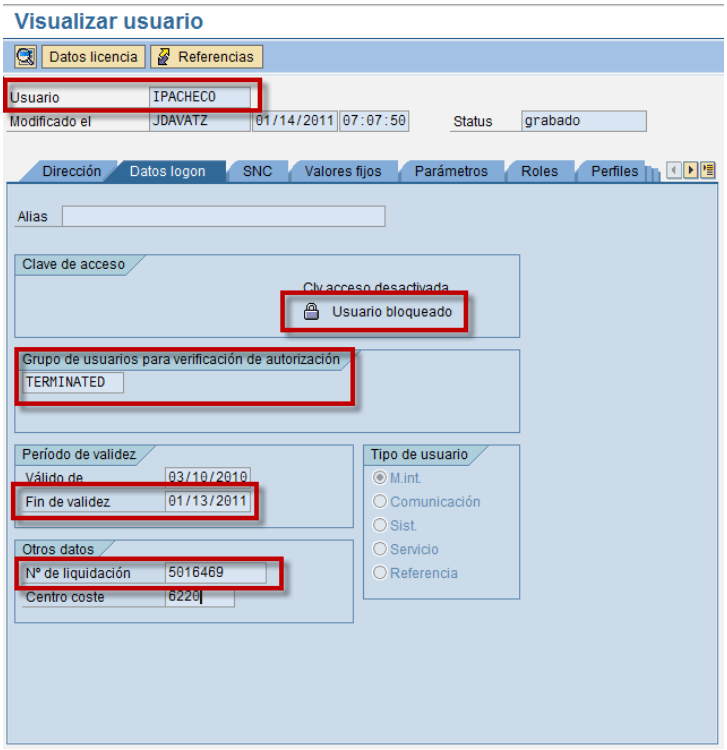

Fig. A3.4 Revisión de deshabilitación de usuario en SAP

GLOSARIO DE TÉRMINOS

En el presente capítulo, se describe se describe la definición de los conceptos mencionados a lo largo de los seis capítulos que conforman este informe de actividades

A

ABAP (Advanced Business Application Programming)
Lenguaje de programación orientado a objetos, propiedad de SAP, que se utiliza para programar la mayoría de los productos de la compañía. Utiliza sentencias de SQL para conectarse rápidamente a cualquier base de datos.

Actividad de control
Normas y procedimientos (actividades necesarias para implementar las políticas), cuyo fin es asegurar el cumplimiento de las directrices establecidas por la dirección para controlar los riesgos.

AICPA (American Institute of Certified Public Accountants)
Instituto compuesto de contadores para la elaboración de marcos de referencia especializados en la evaluación de controles en el negocio.

Amenaza
Cualquier cosa que puede aprovechar una vulnerabilidad. Cualquier causa potencial de un incidente puede ser considerada una amenaza.

Auditoría
Es una función de la dirección cuya finalidad es analizar y evaluar el control interno de las organizaciones para garantizar la integridad de su patrimonio, la confiabilidad de la información y la eficacia en los sistemas de gestión.

B

BCP (Business Continuity Plan)
Plan diseñado para mantener la operación de un negocio en caso de que se presente una contingencia por fallo en el sistema.

C

Control Automático
Controles que existen dentro o que son soportados por el uso de un sistema o aplicación.

Control Interno
Proceso diseñado y efectuado por los encargados del gobierno, la administración y demás personal para proporcionar seguridad razonable sobre el logro de confiabilidad de los informes financieros, eficiencia y eficacia de las operaciones y cumplimiento con leyes y regulaciones.

COSO (Committee of Sponsoring Organizations of the Treadway Commission)
Marco de referencia utilizado para el desarrollos y guía de la administración de riesgos empresariales, control interno y detección de fraudes.

COBIT (Control Objectives for Information and Related Technology)
Conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información, (ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute).

CEO (Chief Executive Officer)
Persona encargada de la administración, coordinación y dirección de la operación íntegra de una empresa. Es el contacto directo con comités y accionistas de la empresa.

CFO (Chief Financials Officer)
Persona encargada de la administración, coordinación y dirección de las finanzas de una empresa. Esta figura reporta al CEO.

D

Diseño
Es la acción de validar que el control creado mitigue el riesgo a través de acciones que digan qué, cómo, cuándo y cada cuanto se lleva a cabo el control.

DRP (Disaster Recovery Plan)
Plan diseñado para mantener el sistema o aplicación de una compañía en caso de que se presente una contingencia que inhabilite su uso.

E

Eficacia Operativa
Es la acción de validar que el control creado opere de manera eficiente en un periodo de tiempo que permita concluir en que el control proporcione una seguridad razonable.

ERS (Enterprise Risk Services)
Área de la compañía Deloitte que ofrece apoyo en servicios relacionados con riesgos tecnológicos y de negocio.

Evidencia
Se llama evidencia de auditoría a " Cualquier información que utiliza el auditor para determinar si la información cuantitativa o cualitativa que se está auditando, se presenta de acuerdo al criterio establecido".

F

Fraude
Acción contraria a la verdad y a la rectitud, que perjudica a la organización contra quién se comete.

H

Hallazgo
Diferencias significativas encontradas en el trabajo de auditoría con relación a lo normado o a lo presentado por la gerencia.

I

Implementación
Es la acción de corroborar que el diseño establecido sea empleado y/o ejecutado por la administración.

ISACA (Information Systems Audit and Control Association)
Asociación encargada de definir los marcos de referencia que establecen un ambiente de control adecuado para los sistemas de información.

J

JRC (Junta de Revisión de Cambios)
Es el comité encargado de autorizar los cambios sugeridos en el formato RDC.

O

Objetivos de Control
Es un conjunto de actividades que tiene por objeto la medida y evaluación de la eficacia de los controles.

P

PAU (Pruebas de aceptación de Usuario)
Formato que utiliza la compañía “x” para que el usuario apruebe los cambios realizados a la funcionalidad del sistema.

Papeles de Trabajo
Son los archivos que maneja el auditor y que contienen todos los documentos que sustentan su trabajo efectuado durante la auditoria.

Personal Basis
Personas encargadas del aseguramiento en la operación del sistema SAP a nivel base de datos, aplicación y sistema operativo.

Prueba de Control
Una actividad mediante la cual, se pretende comprobar la existencia/ausencia en el cumplimiento/deficiencia de un control previamente identificado.

R

RDC (Request for Changes)
Formato utilizado para la compañía “x” que establece el inicio del ciclo de cambios, el cual debe ser firmado por las personas involucradas para proceder con el cambio.

Riesgo
La posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. El riesgo se mide en términos de impacto y probabilidad.

Riesgo de Control
Es la posibilidad de que los procedimientos de control interno incluyendo a la unidad de auditoría interna, no puedan prevenir o detectar los errores significativos de manera oportuna. Este riesgo si bien no afecta a la entidad como un todo, incide de manera directa en los componentes.

Riesgo Inherente
Es la posibilidad de que existan errores o irregularidades en la gestión administrativa y financiera, antes de verificar la eficiencia del control interno diseñado y aplicado por el ente a ser auditado. Este riesgo tiene relación directa con el contexto global de una institución e incluso puede afectar a su gestión.

Riesgo Residual
El nivel remanente del riesgo después de que se han tomado medidas de tratamiento del riesgo.

RV (Responsable de Validación)
Figura de la compañía “x” que debe dar el visto bueno sobre el cambio presentado en el formato de cambios RDC

S

SAP (Sistemas, Aplicaciones y Productos)
Sistema ERP, creado en Alemania, que gestiona la totalidad de la operación de una compañía. El sistema mantiene actualizado en línea toda la información financiera y de logística a través de la comunicación entre sus distintos módulos.

SDLC (Systems Development Life Cycle)
Metodología utilizada por la compañía “x” para el desarrollo de sistemas. Se compone de distintas fases desde el diseño hasta la liberación en el ambiente productivo.

Seguridad
Aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sean de manera personal, grupal o empresarial.

SOX (Sarbanes-Oxley)
Ley establecida en Estados Unidos que establece la responsabilidad de mantener una estructura adecuada de control interno. Esta ley debe ser cumplida por aquellas compañías que cotizan en la bolsa de valores de los Estados Unidos de Norteamérica.

T

TR (Technology Risk)
Subárea perteneciente a ERS de la compañía Deloitte que se encarga de ofrecer servicios relacionados a riesgos de tecnología de las compañías.

TI (Tecnologías de Información)
Herramientas y métodos empleados para recabar, retener, manipular o distribuir información.

V

Vulnerabilidad
Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza

FUENTES DE INFORMACIÓN

1. Metodología Deloitte, sitio intranet (consultado el 09/10/2011 a las 10:00:30 pm)

2. Herramientas internas Deloitte:
   - ✓ Industry Print
   - ✓ Rack
   - ✓ Infobase

3. http://www.deloitte.com/mx (consultado el 10/10/2011 a las 9:30:50 pm)

4. http://www.coso.org (consultado el 16/03/2012 a las 6:30:35 pm)

5. http://www.isaca.org (consultado el 16/03/2012 a las 6:00:59 pm)

6. http://www.aicpa.org (consultado el 19/03/2012 a las 7:30:43 am)

7. http://www.seguridadsap.com (consultado el 10/04/2012 a las 8:12:15 pm)

8. http://www.sox-online.com (consultado el 10/04/2012 a las 9:00:09 pm)

9. www.acs-inc.com (consultado el 10/04/2012 a las 11:30:05 pm)