PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

METODOLOGÍA PARA LA AUDITORÍA INTEGRAL DE LA GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

Tesis para optar por el Título de Ingeniero Informático, que presenta el Bachiller:

Emigdio Antonio Alfaro Paredes

ASESOR: Abraham Eliseo Dávila Ramón

Lima, Octubre 2008

TESIS: METODOLOGÍA PARA LA AUDITORÍA INTEGRAL DE LA GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN

RESUMEN

De la revisión de la literatura sobre estándares internacionales de calidad relacionados a la gestión de tecnología de información (COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000 (ITIL), PMBOK, ISO/IEC 27001, IEEE 1058-1998, ISO 9001:2000 e ISO 19011:2002), MoProSoft 1.3, y las normas relacionadas a la auditoría informática en el Estado Peruano, se concluye que no existe una metodología para la auditoría integral de la gestión de la tecnología de información. Los enfoques actuales están basados sobre el proceso general de auditoría sumándoles las inclusiones no integradas de los diversos estándares de calidad internacional, o las normas vigentes para las entidades que son sujetas de evaluación en una auditoría. El objetivo de la tesis fue el desarrollo de una metodología para la auditoría integral de la gestión de la tecnologías de información (MAIGTI), con un enfoque de procesos, basado en estándares de calidad internacionales.

MAIGTI enlaza los diversos conceptos de COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000 (ITIL), Y PMBOK, sobre la base de una simplificación del proceso general de auditoría descrito en la norma ISO 19011:2002, y sobre la base de una adaptación del esquema de procesos de la ISO 9001:2000 (ISO, 2000). MAIGTI comprende los siguientes elementos: (a) objetivo (la finalidad de la auditoría), (b) alcance (detalle de lo que está incluido y lo que no está incluido como parte de la auditoría), (c) entradas (requerimientos de información), (d) proceso de MAIGTI (evaluaciones a realizar) y (e) salidas (papeles de trabajo e informe de auditoría). Asimismo, cada uno de los procedimientos para la evaluación de los principales objetivos de control dentro de los subprocesos de MAIGTI, comprende la siguiente estructura: (a) objetivo (la finalidad del procedimiento de auditoría), (b) alcance (detalle de lo que está incluido y lo que no está incluido como parte de la auditoría a realizarse a través del procedimiento), (c) entradas (requerimientos de información para ejecutar el procedimiento de auditoría), (d) proceso (detalle de los pasos a seguir en el procedimiento de auditoría), y (e) salidas (hallazgos evidenciados como resultado de la ejecución del proceso). En los procedimientos descritos en el anexo 1, se ha detallado como salidas, algunos hallazgos posibles que se derivan como resultado de la experiencia de las aplicaciones de MAIGTI en auditorías realizadas por el autor de la tesis.

MAIGTI ha sido aplicada principalmente a 2 empresas de seguros y de manera parcial 8 entidades más, auditadas por el autor de la tesis, siendo aplicable para entidades usuarias de tecnología de información. Se recomienda ampliar MAIGTI o crear otra metodología, para la auditoría integral de la gestión de tecnología de información en entidades proveedoras de servicios de tecnología de información.

A mis padres Emigdio y Hortensia, por su incansable apoyo incondicional.

A mi esposa Miriam por su aliento que me ha permitido lograr mis objetivos.

A la memoria de mi hijo Emigdio, quien me dio los mejores cinco años de mi vida.

A todos mis profesores, en especial a mi Asesor, Mg. Abraham Dávila, quien con sus valiosos aportes, me ha permitido lograr esta tesis.

ÍNDICE

LISTA DE FIGURAS

INTRODUCCIÓN

La diversidad de estándares internacionales para la gestión de las tecnologías de información ha aumentado en los últimos años, siendo el COBIT el estándar internacional más completo, el cual incluye objetivos de control específicos considerando el ciclo de calidad de Deming (Plan, Do, Check , Act), para los diversos aspectos relacionados a la gestión de las tecnologías de información: gestión de procesos relacionados con la infraestructura de tecnología de información, gestión de proyectos de infraestructura de tecnología de información, gestión de proyectos de desarrollo de sistemas de información, y gestión de requerimientos relacionados a los sistemas de información en producción; organizados en los grandes temas: Planificación y Organización; Adquisición e Implementación; Entrega de Servicios y Soporte; y Monitoreo y Control. Sin embargo, pese a su existencia, no se dispone de procedimientos específicos dentro del marco de una metodología para el desarrollo de auditorías de la gestión de tecnologías de información, aunque existen algunos procedimientos aislados que han propuesto algunas organizaciones como ISACA, orientados principalmente a la auditoría de aspectos técnicos. Además, en la gestión de tecnología de información comúnmente se cometen muchos errores que en su conjunto estarían impidiendo o retrasando el logro de los objetivos organizacionales con los consecuentes perjuicios en las organizaciones usuarias de las tecnologías de información, de todo sector económico y tamaño. Por ello se hace necesario mejorar el proceso de evaluación de la gestión informática en los diversos tipos de organizaciones, siendo

este el primer paso para que se pueda realizar una planificación estratégica de tecnología de información integrada a las demás funciones de la organización.

La presente tesis contribuye a la solución de este problema a través de una propuesta metodológica alineada a los estándares internacionales más importantes para la auditoría de la gestión de las tecnologías de información, mejorándose el proceso general de la auditoría, enlazándolo e integrándolo con estándares internacionales (COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000 y PMBOK) de manera que se logren evaluaciones integrales mucho más acertadas y se contribuya al logro de los objetivos organizacionales. Esta metodología propuesta fue probada en dos de las empresas de seguros más importantes del Perú y ya ha sido validada y corregida, siendo un aporte importante para mejorar la gestión informática en las organizaciones peruanas. Fue aplicada también de manera parcial, en otras entidades en las cuales el autor de la tesis realizó auditorías de la gestión informática.

1. GENERALIDADES

En este capítulo se definirá el problema a cuya solución se pretende contribuir con el desarrollo de la presente tesis, se definirá una serie de términos que ayudarán a comprender mejor los diversos aspectos del documento de tesis, se explicará qué es la gestión de la tecnología de información, los problemas que se presentan en la gestión de la tecnología de información, el estado del arte en cuanto a estándares para la auditoría de la gestión informática, se describirá la solución propuesta para mejorar la auditoría de la gestión de la tecnología de información, y se detallará las actividades del proyecto de tesis.

1.1. DEFINICIÓN DEL PROBLEMA

Las organizaciones emprenden grandes inversiones en tecnología de información, muchas veces sin evaluar el impacto que realmente tienen en la generación de valor de las mismas. Existen diversas normas dictadas por organismos supervisores como la Contraloría General de la República y la Superintendencia de Banca, Seguros y AFP, así como diversos estándares de calidad que han sido propuestos por diversas entidades a nivel mundial. Estas normas si bien nos ilustran de manera amplia, técnica y ordenada sobre los elementos a tener en cuenta para una adecuada gestión informática, no nos orientan de manera específica sobre los procedimientos a seguir para una evaluación integral de la

gestión informática orientada al logro de los objetivos de un Plan Estratégico Organizacional (que se miden sobre la base de indicadores de gestión y resultados a alcanzar establecidos para toda la organización), lo que sería el primer paso a seguir, si queremos lograr una planificación estratégica de la tecnología de información, orientada hacia el logro de los objetivos organizacionales.

La presente tesis pretende cubrir este vacío de conocimiento proponiendo una metodología para la auditoría integral de la gestión de la tecnología de información (MAIGTI), que permita enlazar los diversos conceptos propuestos por los más importantes estándares de calidad internacionales, y de esa manera, permita contribuir a la generación de valor de las organizaciones que la utilicen.

1.2. MARCO CONCEPTUAL

Esta sección nos mostrará una serie de definiciones importantes para la comprensión del documento, nos explicará qué es la gestión de la tecnología de información, y los problemas que se presentan en sus procesos.

1.2.1. DEFINICIONES DE TÉRMINOS

A continuación se definirá una serie de términos importantes para la correcta comprensión del documento: auditoría, evaluación del proceso de software, método, metodología, procedimiento, proceso, proceso de software, y tecnología de información.

AUDITORÍA

ISO (2002) a través de la norma ISO 19011:2002 indicó las siguientes definiciones para los términos: Criterio de Auditoría, Evidencia de Auditoría, Auditoría y Hallazgos de Auditoría, las cuales se muestran a continuación:

A. Criterio de Auditoría es un conjunto de políticas, procedimientos o requisitos.

B. La Evidencia de auditoría comprende registros, declaraciones de hechos o cualquier otra información que son pertinentes para los criterios de auditoría y que son verificables.

C. La Auditoría es un proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría.

D. Los Hallazgos de Auditoría son los resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría. Los hallazgos de auditoría pueden indicar tanto conformidad o no conformidad con los criterios de auditoría como oportunidades de mejora.

Paulk et al. (1993) indicaron que Auditoría es una evaluación independiente de un resultado o conjunto de resultados, para determinar la conformidad con las especificaciones, estándares, acuerdos contractuales, u otro criterio. Piattini & Del Peso (1998) explicaron lo siguiente:

"Conceptualmente la auditoría, toda y cualquier auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y cumple las condiciones que le han sido prescritas". (p. 4)

Según la NTP-ISO/IEC 12207:2006 (INDECOPI, 2006), el proceso de Auditoría es un proceso para determinar el cumplimiento con los requerimientos, planes y contrato, según aplique. Se indica además que este proceso puede ser empleado por cualesquiera de las dos partes, donde una de ellas (la auditora) audita los productos software o actividades de la otra parte (la auditada). Según ISACA (2008), la auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

EVALUACIÓN DEL PROCESO DE SOFTWARE

Paulk et al. (1993) definieron la Evaluación del Proceso de Software como una evaluación de un equipo entrenado de profesionales de software para determinar el estado del actual proceso de software de la organización, y sus problemas más prioritarios.

Pressman (1998) explicó que la medición permite que gestores y profesionales mejoren el proceso del software en los aspectos siguientes: (a) ayudan en la planificación, seguimiento, y control de un proyecto de software; y (b) evalúan la calidad del producto (software) que se produce. Pressman (1998) indicó también que las medidas de los atributos específicos del proceso, del proyecto, y del producto se utilizan para calcular las métricas del software, las cuales se pueden analizar para proporcionar indicadores que guían acciones de gestión y técnicas.

MÉTODO

Paulk et al. (1993) indicaron que Método es un conjunto de reglas y criterios razonablemente completo que establece una manera precisa y repetible de ejecutar una tarea y lograr un resultado deseado.

METODOLOGÍA

Paulk et al. (1993) indicaron que Metodología es una colección de métodos, procedimientos y estándares que define una síntesis integrada de aproximaciones de ingeniería para el desarrollo de un producto.

PROCEDIMIENTO

Paulk et al. (1993) indicaron que un Procedimiento es una descripción escrita de un curso de acción a ser tomado para la ejecución de una tarea dada.

PROCESO

Paulk et al. (1993) indicaron que un Proceso es una secuencia de pasos para ejecutar un propósito dado.

Oktaba et al. (2005) indicaron que un Proceso es un conjunto de prácticas relacionadas entre sí, llevadas a cabo a través de roles y por elementos automatizados, que utilizando recursos y a partir de insumos producen un satisfactor de negocio para el cliente.

PROCESO DE SOFTWARE

Paulk et al. (1993) indicaron que un Proceso de Software es un conjunto de actividades, métodos, prácticas y transformaciones que la gente usa para desarrollar y mantener software y los productos asociados (por ejemplo: planes de proyecto, documentos de diseño, código, casos de prueba, y manuales de usuario).

Jacobson, Booch, & Rumbaugh (2000) indicaron que un proceso define quien está haciendo qué, cuando y cómo alcanzar un objetivo (construir un producto software o mejorar uno existente, para el caso de la ingeniería de software). Jacobson, Booch, & Rumbaugh (2000) explicaron también que un proceso efectivo proporciona normas para el desarrollo eficiente de software de calidad, captura y presenta las mejores prácticas que el estado actual de la tecnología permite, y debería ser capaz de evolucionar durante muchos años. Jacobson, Booch, & Rumbaugh (2000) definieron el proceso de desarrollo de software, de la siguiente manera:

"Proceso de negocio o caso de uso de negocio, de un negocio de desarrollo de software. Conjunto total de actividades necesarias para transformar los requisitos de un cliente en un conjunto consistente de artefactos que representan un producto software y - en un punto posterior en el tiempo - para transformar cambios en dichos requisitos en nuevas versiones del producto software" (p. 431).

TECNOLOGÍA DE INFORMACIÓN

A continuación se tratará de definir con precisión el concepto "Tecnología de información" (TI). Diversos autores han propuesto conceptos sobre TI:

A. Morton (1988) definió TI como un ente que comprende 5 componentes básicos: computadoras, tecnología de comunicaciones, estaciones de trabajo, robótica y circuitos de computadoras.

B. Huber (1990) definió TI como un dispositivo para transmitir, manipular, analizar o explotar información, en el cual una computadora digital procesa información integral a comunicaciones de usuarios y tareas de decisión.

C. Lau et al. (2001) indicaron que desde inicios de los 1970s, las aplicaciones de computadoras estuvieron orientadas a automatización de oficina y soporte a decisiones, tales como: procesamiento de palabras, hojas de cálculo, y sistemas de información gerencial. Ahora se ha cambiado el énfasis de computación mono usuario a colaboración y conexión (Chatterjee, 1991).

Según el IT Governance Institute (2008), una aplicación de tecnología de información es una funcionalidad electrónica que congrega partes de procesos de negocio con soporte de tecnología de información. Además, según el IT Governance Institute (2008), un servicio de tecnología de información es una provisión diaria de aplicaciones de tecnología de información y soporte para su uso, incluyendo *help desk*, provisión y movimiento de equipos, y autorizaciones de seguridad.

Sumando los conceptos de los diversos autores, el término tecnología de información comprende tanto al *hardware* de computadoras, redes y comunicaciones, así como al software de base (sistemas operativos, servidores *proxy*, manejadores de bases de datos, servidores web, etc.) y los sistemas de información (sistemas que soportan procesos relacionados al manejo de la información en las organizaciones), así como los servicios relacionados, que se usan en las organizaciones para el logro de sus objetivos, tanto dentro de ellas como en sus interrelaciones con otros miembros de las cadenas de suministros con las cuales realizan transacciones.

1.2.2. GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

La gestión de tecnología de información consiste en la aplicación de los procesos de la administración (planificación, ejecución, seguimiento y control) a los diversos

aspectos relacionados a los bienes y servicios de tecnología de información. Incluye los siguientes aspectos: gestión de procesos relacionados con la infraestructura de tecnología de información, gestión de proyectos de infraestructura de tecnología de información, gestión de proyectos de desarrollo de sistemas de información, y gestión de requerimientos relacionados a los sistemas de información en producción.

Piattini & Del Peso (1998) explicaron que el control interno informático debe estar comprendido dentro de las labores del área encargada de la gestión de tecnología de información, y que el control interno informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares, y normas fijadas por la Dirección de Organización y/o la Dirección de Informática, así como los requerimientos legales.

1.2.3. PROBLEMAS EN LA GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN

El IT Governance Institute desarrolló junto con PriceWaterHouse Coopers Corporation, el IT Governance Global Status Report 2008 (IT Governance Institute, 2008), sobre la base de una muestra de 749 entrevistas a los gerentes generales, gerentes de informática, gerentes de operaciones, gerentes financieros y auditores internos, con respecto a diversos puntos relacionados a la gestión de la tecnología de información en sus organizaciones. La muestra de entrevistados incluyó personas de 23 países de organizaciones de diversos sectores económicos y cantidad de empleados. Los resultados demostraron que la madurez del gobierno de tecnología de información en el año 2007 estuvo en 2.67 en promedio (considerando niveles de madurez análogos al CMM, del 1 al 5).

En el IT Governance Global Status Report 2008, se indicaron los problemas manifestados por los entrevistados en orden descendente de importancia, los cuales fueron los siguientes: (a) insuficiente cantidad de personal, (b) problemas de entrega de servicios, (c) inadecuadas habilidades en el personal de tecnología de información, (d) altos costos de la tecnología de información versus el retorno de la inversión, problemas con proveedores, (e) falta de agilidad para la solución de problemas, (f) problemas con la documentación y la gestión del conocimiento, (g) falta de enlace entre la estrategia de tecnología de información y la estrategia de la organización, (h) inadecuado plan de recuperación de desastres, (i) problemas de

almacenamiento de la información, (j) incidentes operacionales serios debido a la tecnología de información, (k) no se cumplen los requerimientos planeados inicialmente, y (l) problemas de seguridad de la información. Los más grandes obstáculos para la mejora de la gestión de tecnología de información, señalados por los entrevistados, fueron los siguientes: (a) presupuestos y retorno de la inversión esperado, (b) falta de conocimiento y entendimiento del gobierno de tecnología de información, (c) personal, (d) problemas de planificación, (e) otros, (f) falta de apoyo de la alta gerencia, (g) procedimientos de trabajo, (h) no hay una visión clara de las metas más importantes, (i) falta de apoyo de otras gerencias, (j) falta de comunicación entre el área de tecnología de información y las otras áreas, y (k) legislación. Algunos indicadores a resaltar en el estudio, son los siguientes:

- Sólo el 20% realiza una gestión activa del retorno de la inversión de la tecnología de información. 22% está en proceso de implementación de este aspecto.

- Sólo el 25% mide el rendimiento de la gestión de tecnología de información. 29% está en proceso de implementación de este aspecto.

- Sólo el 30% realiza una gestión formal del riesgo de tecnología de información. 32% está en proceso de implementación de este aspecto.

- Sólo el 23% ha alineado la estrategia de tecnología de información a la estrategia de la organización. 32% está en proceso de implementación de este aspecto.

Alfaro (2007), enunció algunos errores comunes en los proyectos de desarrollo o implantación de sistemas de información en el Perú, los cuales se presentan a continuación:

A. El desarrollo o implantación del sistema de información se toma como un proyecto aislado del Plan Estratégico de la empresa, en el caso que la empresa tenga un plan estratégico.

B. No se hace participar al usuario en la definición de los requerimientos del sistema de información.

C. El usuario, pese a ser convocado, toma a la ligera su responsabilidad en la definición de los requerimientos. Después, los cambia continuamente cuando el desarrollo o la operación del sistema de información está en marcha.

D. El personal de Informática que toma los requerimientos no conoce de los procesos de gestión a los cuales darán soporte los sistemas de información que se desarrollarán.

E. El proveedor del sistema de información trata de minimizar los cambios con respecto a las características que se tiene que personalizar. Sugiere comúnmente que la empresa cambie sus procesos de acuerdo a la configuración estándar de su producto.

F. Se personaliza el producto del proveedor, de acuerdo a los requerimientos de la empresa; sin embargo, estos requerimientos cambian continuamente dado que la gerencia no tiene clara su estrategia o los procesos para llevarla a cabo.

G. No se sigue los procesos formales del Ciclo de Vida del Software, pese a que es parte de la formación académica estándar que se recibe en los institutos y universidades del Perú, en las carreras de Computación, Informática o Sistemas. Dentro de estos procesos del ciclo de vida del software que comúnmente no se desarrollan o se desarrollan mal, tenemos los siguientes:

   a) Diseño de Planes de Pruebas. No se elaboran documentos en los cuales esté detallada la secuencia de pruebas completa con datos de entrada y datos de salida esperados como resultado, en cada una de las pantallas de los módulos de un sistema de información.

   b) Ejecución de las pruebas. Comúnmente vemos que el usuario es quien realiza las pruebas. El proveedor del sistema de información no realiza las pruebas y el personal de Informática de la empresa cliente tampoco las realiza (porque asume que las pruebas las realizará el usuario) y el usuario realiza las pruebas a la ligera y no detecta los errores sino hasta que usa el sistema en el ambiente de producción (ambiente de software donde está el sistema de información con datos reales).

c) Diseño de Planes de Integración. Se implantan los módulos por partes, con la consecuente programación de interfaces que no estaban planeadas desde un inicio. Estas interfaces comúnmente fallan. Es común que recién cuando el sistema de información está implantado, nos damos cuenta que era necesario que interactúe con otros sistemas de información de la empresa tanto enviando datos hacia esos sistemas como recibiendo datos de ellos.

d) Diseño de Planes de Migración. No se hace un diseño de cómo migrarán los datos de los sistemas de información antiguos hacia los nuevos sistemas de información. En muchos casos se indica al usuario que los datos anteriores los vean en el antiguo sistema y los datos nuevos los vean en el nuevo sistema.

Rubinstein (2007) explicó que el Standish Chaos Report reveló que el 35% de los proyectos fueron exitosos (cumplieron alcance, tiempo y costo) en USA en el año 2006, a diferencia del 16.2% que se obtuvo en el año 1994. Asimismo, se redujo la tasa de proyectos que fueron cancelados de 31.1% en el año 1994 a 19% en el año 2006. Rubinstein (2007) indicó también que la cantidad de proyectos descritos como *desafiados* (exceso grande en tiempo y costos, o que no cubrían las necesidades) bajó de 52.7% en 1994 a 46% en el 2006. Lamentablemente, no se dispone de estudios similares en nuestro país para hacer un comentario estadístico acerca del éxito en la implantación de los sistemas de información en el Perú.

Alfaro (2008) desarrolló una investigación sobre la base de los procesos de selección relacionados a la implementación de las normas técnicas peruanas de gestión de tecnología de información: NTP-ISO/IEC 12207 y NTP-ISO/IEC 17799, en las entidades del Estado Peruano. Como resultado de la investigación se obtuvo que sólo 4.39% de las 1026 entidades usuarias de tecnología de información en el Estado Peruano (según cifras del INEI del año 2002), habrían realizado acciones para la implementación de las normas técnicas peruanas de gestión de tecnología de información. Sólo 1.27% habría logrado implementar la NTP-ISO/IEC 12207, y sólo 1.27% habría logrado implementar la NTP-ISO/IEC 17799. En total se habría invertido S/. 2’760,718 nuevos soles, en servicios de asesoría, consultoría (diagnóstico, plan de implementación, políticas y procedimientos), personal de apoyo, y capacitación, entre otros.

Laudon & Laudon (2008) explicaron que muchas empresas se muestran renuentes a invertir demasiado en la seguridad porque no está directamente relacionada con los ingresos por ventas; pero, la protección de los sistemas de información es crucial para el funcionamiento del negocio. Resaltaron además la importancia de los activos de información (impuestos, información financiera, registros médicos, evaluaciones de desempeño laboral, etc.). También explicaron que los aspectos éticos de los sistemas de información han cobrado nueva importancia por el surgimiento de Internet y el comercio electrónico, y resaltaron la importancia de la seguridad de los individuos y de la sociedad. Laudon & Laudon (2008) indicaron:

"Internet y las tecnologías para las empresas digitales facilitan más que nunca la recopilación, integración, y distribución de la información, y desencadenan nuevas preocupaciones del uso apropiado de la información del cliente, la protección de la privacidad personal, y la protección de la propiedad intelectual" (p. 128).

Alfaro (2007) describió también características típicas en los sistemas de información de una empresa, antes de tomar la decisión de la implantación de un sistema de información ERP (Enterprise Resources Planning), las cuales describen parte de la problemática de la entrega de servicios informáticos para las diversas áreas usuarias:

A. Los sistemas de información no se interrelacionan entre sí. Se debe mirar la información en un sistema, anotarla en un cuaderno o exportarla a una hoja de cálculo y luego recién se puede ingresar los datos correctos en otro sistema. No interactúan los sistemas de información de las áreas de Ventas, Producción, Almacenes, Contabilidad, etc.

B. Existen muchos errores en la información. Frecuentemente salen errores en las pantallas del sistema al momento de ingresar la información. Esos errores se comunican al área de Informática; pero, no se corrigen o si se corrigen, luego encontramos errores similares o diferentes en otras pantallas.

C. Las pantallas del sistema no son amigables. Se tienen que hacer muchos pasos o entrar a varias ventanas para ingresar la información. Además, si se equivocan en ingresar la información en una pantalla, ocurre un error y tienen que salir del sistema de información e ingresar nuevamente. En algunos casos,

además se debe reinicializar la computadora para que pueda funcionar nuevamente el sistema de información.

D. Diversidad de plataformas tecnológicas. Comúnmente en las organizaciones, conviven varias plataformas tecnológicas con las cuales se ha desarrollado sistemas de información (tanto a nivel de la base de datos, como en las herramientas y lenguajes de programación). Se puede observar bases de datos en Oracle, SQL Server, Access, DB2, Informix, DBFs, Archivos Binarios, Archivos de Texto Secuenciales, etc. También se puede observar los lenguajes de programación siguientes: Cobol, Visual Cobol, Visual Basic, Visual FoxPro, FoxPro for Windows, FoxPro, Power Builder, ASP, JSP, PHP, etc. En las empresas comúnmente vemos que la elección de la plataforma tecnológica estuvo en función de lo que sabían las personas que estaban encargadas del desarrollo, las cuales no fueron constantes en el puesto a lo largo de la historia de la empresa.

E. No se tiene documentación de los sistemas de información actuales. No se tiene documentación técnica ni documentación de usuario que permita dar un rápido mantenimiento a los sistemas de información actuales de la empresa. Los programadores no dejaron documentados sus programas ni se tiene manuales técnicos con los cuales se pueda entender las decenas de miles de código de los programas que dejaron.

F. Los sistemas de información actuales son muy lentos. Ocurren demoras considerables en la búsqueda y registro de información, retrasándose el trabajo del personal de las diversas áreas de la empresa. En muchos casos, la tecnología que se usa, no permite administrar eficientemente el volumen de datos que se tiene en las diversas tablas del sistema de información.

Cabe señalar además que comúnmente se carece de o se tiene mal diseñados los siguientes planes relacionados a la Gestión de la Tecnología de Información: Plan de Continuidad de Negocio, Plan de Contingencias de Informática, Plan de Seguridad de la Información, Plan de Mantenimiento (Preventivo y Correctivo), Plan de Licenciamiento de Software, Plan de Capacitación, Planificación de Labores de Rutina, Planes de Compras, Planes de Proyectos, etc. Dado que los planes estaban mal diseñados o se carecía de ellos, en la práctica, su ejecución también presentó una serie de deficiencias o carencias, las cuales se presentan en un número tan

grande en las empresas, que los informes de auditoría al respecto de cada uno de estos temas (en su conjunto), podrían llenar varias decenas o quizás hasta centenas de páginas.

1.3. ESTADO DEL ARTE

La Gestión de la Tecnología de Información, ha evolucionado muy rápido en las últimas décadas, desde su aparición. Ya no es suficiente que se comprenda los procesos de desarrollo de sistemas de información, o los procesos de construcción o mantenimiento de infraestructura de tecnologías de información. Ahora las gerencias de tecnología de información, deben alinearse a los sistemas de gerencia modernos (los sistemas de gestión de la calidad), basados en el ciclo de Deming (Plan, Do, Check, Act). Estos sistemas de gerencia modernos, tienen impacto en la cultura organizacional, la estructura organizacional, los procesos, las políticas, los procedimientos y las instrucciones; no sólo de personal relacionado con la gestión de la tecnología de información, sino también con sus usuarios.

En el Perú, esto recién ha empezado desde hace pocos años. En el Estado Peruano se inició la aplicación de la NTP-ISO/IEC 12207:2004 “Procesos del Ciclo de Vida del Software” (INDECOPI, 2004) en Julio del 2006. Esta norma ya ha sido actualizada y ahora se tiene la NTP-ISO/IEC 12207:2006 (INDECOPI, 2006). Además se tiene la NTP-ISO/IEC 17799:2004 (INDECOPI, 2004), que si bien se titula “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”, en la práctica es una norma que regula los procesos y proyectos que se realizan en áreas de gestión de infraestructura de tecnologías de información (comúnmente llamadas “Soporte Técnico”). A esto se suma las normas de control interno gubernamental para los sistemas informáticos de Contraloría General de la República, que se tiene desde el año 1998 (Contraloría General de la República, 1998) y que ha sido mejorada teniéndose una actualización (Contraloría General de la República, 2006).

En la actualidad, cuando se realiza auditorías informáticas en entidades del Estado Peruano (a través de Auditoría Interna, Auditorías Externas o Auditorías de Contraloría General de la República), se debería tener como objetivos de control, los establecidos en las normas de control interno de Contraloría General de la

República, la NTP-ISO/IEC 12207:2006, la NTP-ISO/IEC 17799:2007, así como normas relativas a la tenencia de software pirata, transparencia, y elaboración de planes estratégicos de Informática y planes operativos de Informática, entre otras.

En las entidades del sector privado supervisadas por la SBS (Superintendencia de Banca, Seguros y Administradoras de Fondos de Pensiones), las auditorías informáticas se rigen por la Circular G-105-2002/SBS (Riesgos de Tecnología de Información). La SBS supervisa en la práctica a: bancos, seguros, administradoras de fondos de pensiones, empresas financieras, edypymes, cajas de ahorro y crédito, y empresas que envían y reciben dinero. Los objetivos de control de la Circular G-105-2002/SBS (Superintendencia de Banca, Seguros y AFP, 2002) comprenden en gran parte los objetivos de control de la NTP-ISO/IEC 17799:2004.

En el contexto internacional existen las normas y/o modelos siguientes: COBIT (ISACA, 1998; ISACA, 2006), CMM (Capability Maturity Model), PMBOK, ISO/IEC 12207 (Procesos del Ciclo de Vida del Software), ISO/IEC 17799 (Código de Buenas Prácticas de la Gestión de la Seguridad de la Información), ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información), ISO/IEC 20000 (Modelo de Gestión de Servicios de Tecnología de Información) o ITIL (Information Technology Infrastructure Library), entre otras, las cuales pueden ser aplicadas a las entidades privadas que deseen implementarlas por razones de mercado, seguridad, mejora en calidad de servicio, costos, etc.

Si bien las normas internacionales son muy amplias; en la actualidad, se carece de una metodología integradora que permita enlazarlas en un todo coordinado que ayude a la gestión informática al logro de los objetivos organizacionales. No se dispone a la fecha, de una metodología que permita enlazar el lenguaje de la gestión de la tecnología de información con la metodología genérica de la auditoría ya sea privada o pública, sumándose a las buenas prácticas internacionales de calidad.

A continuación se hará una breve descripción de los estándares internacionales de calidad más importantes, relacionados con la gestión de las tecnologías de información. Además de los estándares que han servido de base para el desarrollo de la metodología propuesta por la presente tesis (COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000 y PMBOK), se explicará brevemente los alcances de ISO/IEC 27001, CMM, IEE 1058-1998, ISO 19011:2002, MoProSoft 1.3 (Modelo de

Procesos de la Industria del Software versión 1.3), y el Modelo de un Sistema de Gestión de Calidad basado en Procesos de la norma ISO 9001:2000.

1.3.1. COBIT

COBIT es un estándar propuesto por ISACA (Information Systems Audit and Control Association). COBIT significa *Control Objectives for Information and related Technologies* (Objetivos de Control para las Tecnologías de Información y relacionadas).

Es el estándar más completo. Agrupa los diversos conceptos expresados en las normas descritas previamente: ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 27001, ISO/IEC 20000, CMM y PMBOK. Permite una evaluación integral y coordinada de los diversos elementos que forman parte de la gestión de la tecnología de información (desarrollo de sistemas de información, e infraestructura de tecnología de información), integrada a la gestión estratégica de la organización.

ISACA (1998) indicó que COBIT comprende los siguientes grupos de objetivos de control:

A. Planificación y Organización.

Entre los objetivos de control de este grupo tenemos:

a) Plan de Informática alineado al Plan Estratégico de la Organización.
b) Planes de Proyectos.
c) Plan de Seguridad.
d) Plan de Contingencias.
e) Plan de Capacitación.
f) Plan de Licenciamiento de Software.
g) Planes de Mantenimiento Preventivo y Correctivo.
h) Plan de Calidad.
i) Presupuestos.
j) Estructura Organizacional.
k) Recursos Disponibles.
l) Metodologías de Trabajo.

B. Adquisición e Implementación

Entre los objetivos de control de este grupo tenemos:

a) Adquisiciones de tecnologías de información y afines: equipos de cómputo, equipos de red, licencias de software, sistemas de información, etc.
b) Propuestas Técnicas.
c) Propuestas Económicas.
d) Evaluaciones de Proveedores.
e) Contratos.
f) Desarrollo de tecnologías de información de base.
g) Desarrollo de sistemas de información.
h) Cumplimiento de metodologías y la documentación respectiva.

C. Entrega de Servicios y Soporte.

Entre los objetivos de control de este grupo tenemos:

a) Entrega de servicios de Desarrollo e Implantación de Sistemas de Información.
b) Evaluación de posibles soluciones de lo desarrollado o comprado e implantado.
c) Medidas de seguridad.
d) Nivel de satisfacción de los usuarios con respecto al servicio otorgado.
e) Entrega de servicios de Soporte Técnico.
f) Infraestructura de Tecnologías de Información: Hardware y Software de Base, así como servicios relacionados.

D. Monitoreo y Control

Entre los objetivos de control de este grupo tenemos:

a) Seguimiento de los planes.
b) Evaluación Interna del desempeño.
c) Certificaciones o acreditaciones independientes de control y seguridad.
d) Provisión de auditoría Independiente.

Si bien en la práctica COBIT es considerado un buen estándar para la auditoría informática, unido al ciclo de calidad de Deming (*Plan, Do, Check, Act*) podría ser el mejor sistema de gestión para la tecnología de información.

1.3.2. ISO/IEC 12207

ISO/IEC 12207 Procesos del Ciclo de Vida del Software, es una norma que provee una serie de objetivos de control para la gestión de los proyectos de desarrollo de software. Para un desempeño ideal de las áreas de desarrollo de sistemas de información, esta norma debe unirse a ISO/IEC 2000 (ITIL).

Los Grupos de Procesos incluidos en la norma NTP-ISO/IEC 12207:2006 son los siguientes:

A. Procesos Principales

Este grupo de procesos incluye:

a) Adquisición
b) Suministro
c) Desarrollo
d) Operación
e) Mantenimiento.

B. Procesos de Apoyo

Este grupo de procesos incluye:

a) Documentación
b) Gestión de la Configuración
c) Aseguramiento de la Calidad
d) Verificación
e) Validación
f) Revisión Conjunta
g) Auditoría

h) Solución de Problemas.

C. Procesos Organizativos

Este grupo de procesos incluye:

a) Infraestructura
b) Mejora de procesos
c) Recursos Humanos.

Cabe resaltar que comúnmente se conocía como Ciclo de Vida del Software, a los procesos de desarrollo (identificación de necesidades, planificación, análisis, diseño, programación, integración, pruebas e implantación) y mantenimiento. Este norma complementa muy bien la ingeniería del software con procesos de gestión con el enfoque de calidad de Deming (Plan, Do, Check, Act).

1.3.3. ISO/IEC 17799

ISO/IEC 17799 "Código de Buenas Prácticas de Gestión de Seguridad de la Información", en la práctica es una norma que provee una serie de objetivos de control para la gestión de procesos y proyectos de infraestructura de tecnología de información (áreas comúnmente llamadas "Soporte Técnico"). También incluye secciones relacionadas a la seguridad en el desarrollo de sistemas de información y a la gestión de la continuidad del negocio. ISO/IEC 17799 incluye los siguientes grupos de objetivos de control:

A. Política de Seguridad

Entre los objetivos de control de este grupo tenemos:

a) Documento de Política de Seguridad de la Información.
b) Revisión y Evaluación.

B. Aspectos Organizativos de la Seguridad

Entre los objetivos de control de este grupo tenemos:

a) Estructura para la Seguridad de la Información: Comité, Recursos, Responsabilidades, Asesoría de Expertos, Colaboración entre organizaciones y Evaluación Independiente.
b) Seguridad en los accesos de terceras partes.
c) Outsourcing.

C. Clasificación y Control de Activos

Entre los objetivos de control de este grupo tenemos:

a) Responsabilidades sobre los activos.
b) Clasificación de la Información.

D. Seguridad Ligada al Personal

Entre los objetivos de control de este grupo tenemos:

a) Seguridad en la Definición del Trabajo y Recursos
b) Formación y capacitación en seguridad de la información
c) Respuesta ante incidencias y malos funcionamientos de la seguridad

E. Seguridad Física y del Entorno

Entre los objetivos de control de este grupo tenemos:

a) Áreas Seguras
b) Seguridad de los equipos
c) Controles Generales

F. Gestión de Comunicaciones Y Operaciones

Entre los objetivos de control de este grupo tenemos:

a) Procedimientos y Responsabilidades de Operación
b) Planificación y Aceptación del Sistema
c) Protección contra software malicioso
d) Gestión Interna de Respaldo y Manipulación
e) Gestión de redes
f) Uso y seguridad de los medios de información
g) Intercambio de Información y Software

G. Control de Accesos

Entre los objetivos de control de este grupo tenemos:

a) Requisitos de negocio para el control de accesos.
b) Gestión de acceso a usuarios.
c) Responsabilidades de los usuarios.
d) Control de acceso a la red.
e) Control de acceso al sistema operativo.
f) Control de acceso a las aplicaciones.
g) Seguimiento de accesos y usos del sistema.
h) Informática móvil y teletrabajo.

H. Desarrollo y Mantenimiento de Sistemas

Entre los objetivos de control de este grupo tenemos:

a) Requisitos de seguridad en los sistemas.
b) Seguridad de las aplicaciones.
c) Controles criptográficos.
d) Seguridad de los archivos del sistema.
e) Seguridad en los procesos de desarrollo y soporte.

I. Gestión de la Continuidad del Negocio

Entre los objetivos de control de este grupo tenemos:

a) Planificación.
b) Prueba.
c) Mantenimiento y reevaluación de los planes de continuidad.

J. Cumplimiento

Entre los objetivos de control de este grupo tenemos:

a) Cumplimiento de los requisitos legales.
b) Revisiones de la política de seguridad y la conformidad técnica.
c) Consideraciones sobre la auditoría de sistemas.

Para un desempeño ideal de las áreas de gestión de infraestructura de tecnología de información, esta norma debe unirse a ISO/IEC 20000 (ITIL Information Technology Infrastructure Library).

1.3.4. ISO/IEC 20000 (ITIL)

Para un desempeño ideal de las áreas de Informática, las normas ISO/IEC 12207, ISO/IEC 17799 e ISO/IEC 27001 deben unirse a ISO/IEC 20000, la cual es equivalente al estándar BS15000 o ITIL *Information Technology Infrastructure Library*, el cual provee de una metodología para la gestión de los requerimientos de desarrollo que tienen que ver con los sistemas en producción (los sistemas que ya están utilizando los usuarios de las diversas áreas de la organización).

La siguiente figura muestra el marco referencial en el que se ubica ITIL.

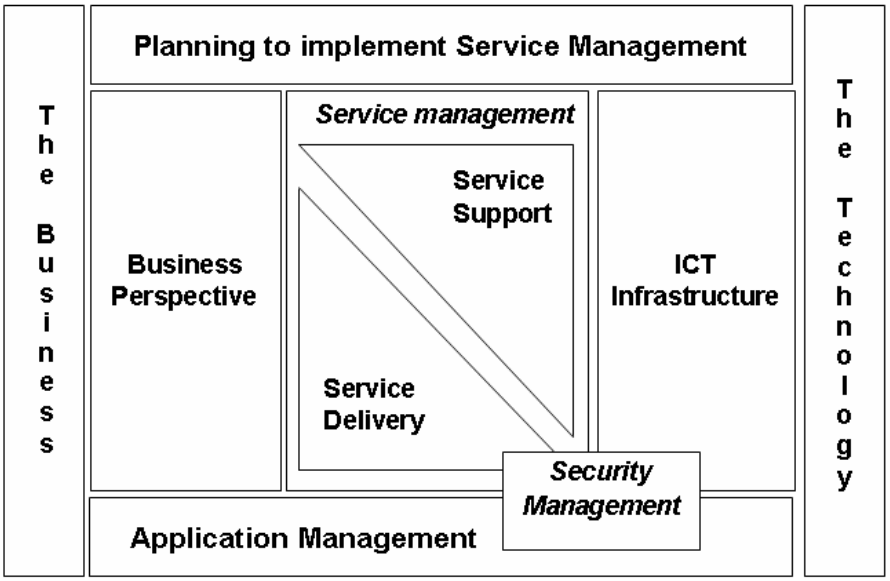


Figura 1-1 Kemmerling & Pondman (2004). ITIL Framework.

Una organización que ha adoptado las buenas prácticas de la gestión de servicios de tecnología de información de ITIL, mejora significativamente la velocidad de atención de requerimientos de desarrollo de sistemas de información, para los sistemas que ya están en producción y que no signifiquen el desarrollo de nuevos proyectos. También ordena la gestión de requerimientos de servicios informáticos en producción (desarrollo de sistemas de información y soporte técnico) en un sólo ente llamado *service desk* (mesa de servicio). Sin embargo, es necesario precisar que se debe mejorar la calidad de los procesos intrínsecos del ciclo de vida del software para evitar que ITIL se convierta en la automatización de correcciones de errores que nunca debieron presentarse.

Cabe resaltar además que quienes se certifican con ITIL son las personas, no las organizaciones en las cuales dichas personas aplican las buenas prácticas de la gestión de servicios de tecnología de información (ITIL Foundation, 2008).

A continuación se detalla la gestión de la atención de requerimientos de ITIL:

A. Previamente a la atención, se ha definido o desarrollado:

a) Niveles de servicio.
b) Criterios para determinar qué requerimientos se pueden atender por el operador que atiende en el *service desk* (ente que canaliza los diversos requerimientos tanto que tengan que ver con procesos de desarrollo de sistemas de información como procesos de gestión de infraestructura de tecnología de información) en un tiempo determinado (15 minutos por ejemplo).
c) Criterios para determinar qué requerimientos se pueden atender en caja rápida y en qué tiempo (en menos de 4 horas por ejemplo).
d) Criterios para determinar los siguientes niveles de servicio en función de la complejidad y naturaleza del requerimiento, además de las competencias de los recursos disponibles.
e) Un sistema de información para soporte de transacciones y para la gestión del conocimiento de las transacciones registradas en el *service desk*. Esto incluye evaluaciones del servicio que debe realizar la persona que lo ha recibido.

Comúnmente los criterios están en función del perjuicio que podría ocasionar la ausencia de los servicios de tecnología de información, afectándose a:

a) Clientes Externos y Clientes Internos.
b) Sólo Clientes Externos.
c) Sólo Clientes Internos.

B. Todos los requerimientos de atenciones sobre las tecnologías de información en producción, se realizan a través del *service desk*, ya sea por teléfono, sistema de información o correo electrónico. Los requerimientos al inicio son considerados “incidentes”; es decir, interrupciones a la operación normal de los servicios de tecnología de información.

C. Los requerimientos reportados son ingresados a la Gestión de Incidentes, de acuerdo a los niveles de servicio previamente definidos.

D. La Gestión de Problemas aparece para solucionar las causas de incidentes comunes que han sido registrados en el *Service Desk*. Ello a su vez, generará nuevos requerimientos.

E. La Gestión de Incidentes o la Gestión de Problemas pueden provocar:

   a) Que se inicie la Gestión de Cambios (cualquier cambio por mínimo que parezca debe ser registrado con los correspondientes efectos en la Gestión de Versiones y la Gestión de Configuraciones).
   b) Que se inicie la Gestión de Versiones (gestión de versiones de documentos, código fuente, ejecutables, etc.).
   c) Que se inicie la Gestión de Configuraciones (configuraciones en hardware, software de base y sistemas de información).

1.3.5. PROJECT MANAGEMENT BODY OF KNOWLEDGE

El PMBOK Project Management Body Of Knowledge, o Guía de los Fundamentos de la Dirección de Proyectos, es un compendio de los diversos conceptos y metodologías de la gestión de proyectos, agrupados bajo un enfoque de procesos. El PMBOK fue propuesto por el PMI Project Management Institute. El PMBOK permite la comprensión de la Gestión de Proyectos, a través de la interacción de los grupos de procesos y las áreas de conocimiento que propuso el PMI.

Project Management Institute (2004) propuso los siguientes Grupos de Procesos:

A. Inicio
B. Planificación
C. Ejecución
D. Seguimiento y Control
E. Cierre

Project Management Institute (2004) propuso las siguientes Áreas de Conocimiento:

A. Integración
B. Alcance
C. Tiempo
D. Costo
E. Calidad
F. Recursos Humanos
G. Comunicaciones
H. Riesgos
I. Adquisiciones

El enfoque de procesos del PMI permite establecer para cada proceso de cada grupo de procesos: sus entradas, sus salidas, así como las herramientas y técnicas diversas. El aporte significativo que da el PMI a la Gestión de Proyectos, además del enfoque de procesos, radica en que agrega más áreas de conocimiento a las típicamente conocidas: alcance, tiempo, costo y calidad.

La Gestión de Proyectos bajo el enfoque PMI, el cual no sólo es aplicable a proyectos de tecnologías de información sino a todos los proyectos, permite un cambio cultural al integrar la gestión dentro y fuera del equipo desarrollador del proyecto en la organización. Tiene impactos en el equipo de usuarios, en el equipo del proveedor, así como un equipo auditor del proyecto.

PMBOK no restringe el uso de determinadas herramientas y técnicas, sino que sugiere algunas como ampliamente aceptadas y da cierta libertad al gerente de proyecto para que determine aquellas que serán de provecho para su gestión. La certificación del PMI es la llamada PMP *Project Management Professional*, la cual certifica a las personas que deseen mejorar sus conocimientos de gestión de proyectos; sin embargo, no se certifica a la organización en sí.

1.3.6. ISO/IEC 27001

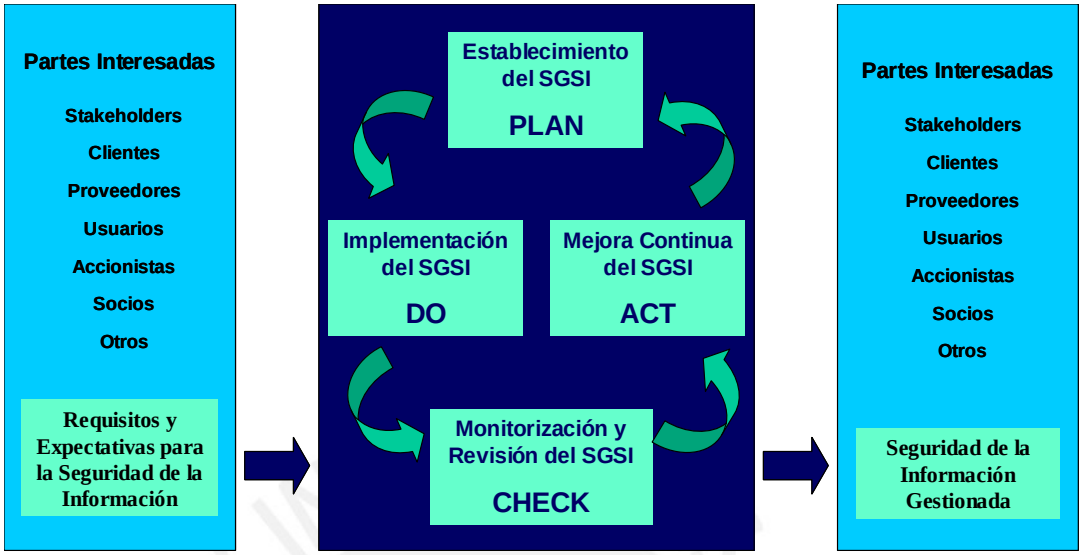


Figura 1-2 Alexander (2007). Naturaleza de la Norma ISO/IEC 27001:2005.

Alexander (2007) indicó que el ISO/IEC 27001:2005 se ha desarrollado como modelo para el establecimiento, la implementación, la operación, el monitoreo, la revisión, el mantenimiento y la mejora de un Sistema de Gestión de Seguridad de la Información para cualquier clase de organización. El diseño y la implantación se encuentran influenciados por las necesidades, los objetivos, los requisitos de seguridad, los procesos, los empleados, el tamaño, los sistemas de soporte y la estructura de la organización. Está basada en el ciclo de Deming (Plan, Do, Check, Act), como se muestra en la figura anterior.

Alexander (2007) explicó que entre los puntos considerados en la norma tenemos: control de documentos, control de registros, responsabilidad gerencial, provisión de recursos, capacitación, conocimiento y capacidad, revisión gerencial, auditorías internas, mejora continua, acción correctiva y acción preventiva. Esta norma toma como referencia los objetivos de control de la norma ISO/IEC 17799, la cual fue explicada previamente.

1.3.7. CAPABILITY MATURITY MODEL

El SEI *Software Engineering Institute* desarrolló el CMM *Capability Maturity Model*, el cual permite identificar el estado de madurez de la gestión de los procesos de desarrollo de software. En la práctica, este modelo no ha sido empleado solamente a procesos de software, sino también a los procesos de gestión organizacionales en general, y a los procesos de gestión de proyectos en particular.

El CMM es el estándar de calidad exigido en el mundo desarrollado para las empresas de desarrollo de software. Paulk et al. (1993) indicaron los niveles de madurez del CMM: (a) Nivel 1, Inicial; (b) Nivel 2, Repetido; (c) Nivel 3, Definido; (d) Nivel 4, Administrado; y (e) Nivel 5, Optimizado. Los 5 niveles del CMM, se muestran en la siguiente gráfica:

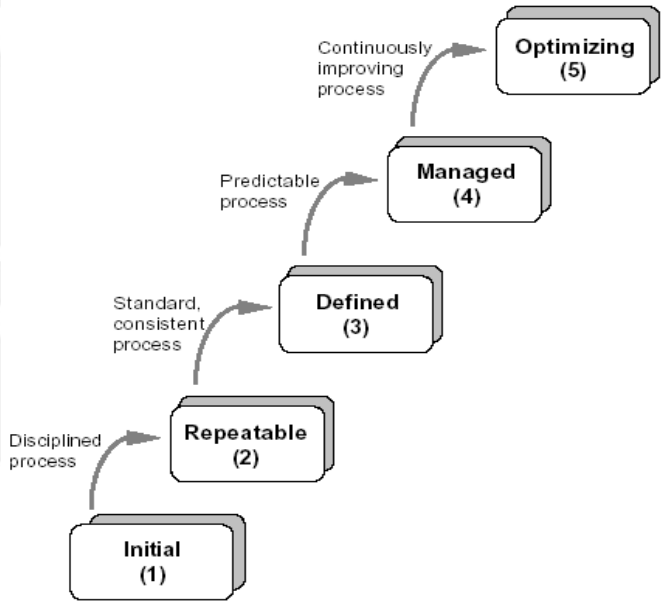


Figura 1-3 Paulk et al. (1993). Key Practices of the Capability Maturity Model Version 1.1. The Five Levels of Maturity of CMM.

1.3.8. IEEE 1058-1998

La norma IEEE 1058 (IEEE, 1998) indicó los siguientes componentes del Plan de Proyecto de Software:

Title Page
Signature Page
Change History
Preface
Table of Contents
List of Figures
List of Tables
1. Overview
    1.1 Project Summary
        1.1.1 Purpose, Scope and Objectives
        1.1.2 Assumptions and Constraints
        1.1.3 Project Deliverables
        1.1.4 Schedule and Budget Summary.
    1.2 Evolution of the Plan
2. References
3. Definitions
4. Project Organization
    4.1 External Interfaces
    4.2 Internal Structure
    4.3 Roles and Responsibilities
5. Managerial Process Plans
    5.1 Start-up Plan
        5.1.1 Estimation Plan
        5.1.2 Staffing Plan
        5.1.3 Resource Acquisition Plan
        5.1.4 Project Staff Training Plan
    5.2 Work Plan
        5.2.1 Work Activities
        5.2.2 Schedule Allocation
        5.2.3 Resource Allocation
        5.2.4 Budget Allocation
    5.3 Control Plan
        5.3.1 Requirements Control Plan
        5.3.2 Schedule Control Plan
        5.3.3 Budget Control Plan
        5.3.4 Quality Control Plan
        5.3.5 Reporting Plan
        5.3.6 Metrics Collection Plan
    5.4 Risk Management Plan
    5.5 Closeout Plan
6. Technical Process Plans
    6.1 Process Model
    6.2 Methods, tools, and techniques
    6.3 Infrastructure Plan
    6.4 Product Acceptance Plan
7. Supporting Process Plans
    7.1 Configuration Management Plan
    7.2 Verifications and Validation Plan
    7.3 Documentation Plan
    7.4 Quality Assurance Plan
    7.5 Reviews and audits
    7.6 Problem Resolution Plan
    7.7 Subcontractor Management Plan
    7.8 Process Improvement Plan
8. Additional Plans
Annexes
Index.

Figura 1-4 IEEE (1998). Format of a Software Project Management Plan.

Como puede observar en la figura 1.6, los diversos elementos del Plan de Proyecto de Software, están comprendidos en los objetivos de control de la ISO/IEC 12207 (ver sección 1.3.2) y el PMBOK (ver sección 1.3.6). Por ello, si bien el formato de la figura anterior, sugerido en la norma IEEE Std 1058-1998 (IEEE, 1998), es bastante completo, su alcance estaría incluido en la ISO/IEC 12207 y PMBOK.

1.3.9. ISO 19011:2002

La ISO 19011:2002 (ISO, 2002) indica el siguiente diagrama de flujo del proceso para la Gestión de un Programa de Auditoría (Directrices para la auditoría de los sistemas de gestión de calidad y/o ambiental):

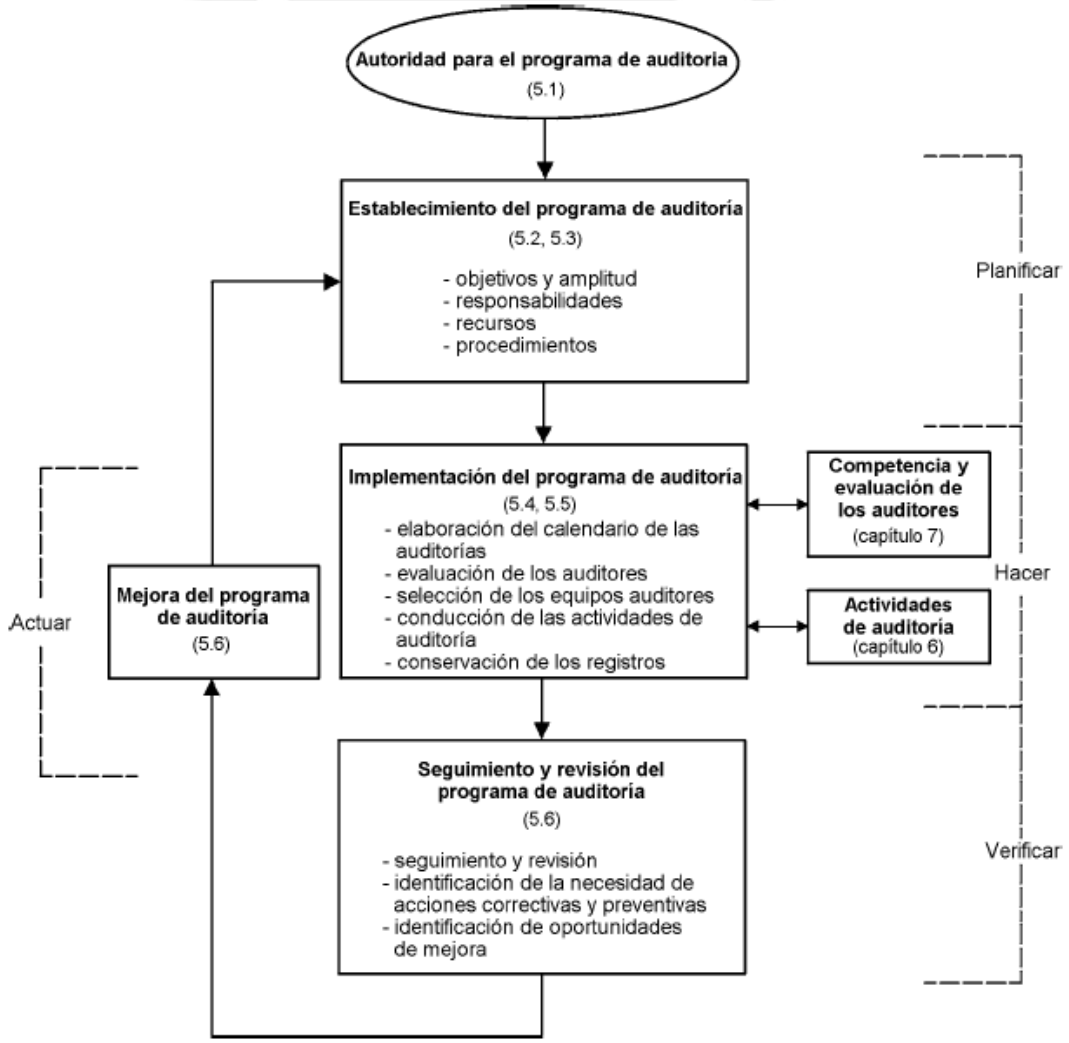


Figura 1-5 ISO (2002). Diagrama de flujo del proceso para la Gestión de un Programa de Auditoría

Como se puede observar en la figura 1.7, el flujo del proceso es similar a lo que se presenta en auditorías en el sector privado como en el sector gubernamental. Dentro de este esquema, se enmarcan también las auditorías de la gestión de tecnología de información, de manera genérica, tomando como referencias aisladas los objetivos de control especificados en los estándares internacionales de calidad y las normas de control interno específicas, ya sean de la propia institución o aplicables por organismos supervisores.

1.3.10. MoProSoft 1.3

MoProSoft 1.3 (Otkaba et al., 2005) incluye parámetros bajo el enfoque de procesos para la gestión de proyectos de software. MoProSoft tiene aspectos relacionados con ISO 9001:2000, CMM v.1.1, e ISO/IEC TR 15504-2:1998.

Las categorías de procesos de MoProSoft 1.3 incluyen:

A. Gestión del Negocio. Otkaba et al. (2005) indicaron que el proceso de Gestión de Negocio se compone de la planificación estratégica, la preparación para la realización de la estrategia, y la valoración y mejora continua de la organización.

B. Gestión de Procesos. Otkaba et al. (2005) explicaron que el proceso de Gestión de Procesos se compone de las siguientes actividades: la planificación de procesos, la preparación a la implantación, y la evaluación y control de procesos.

C. Gestión de proyectos. Otkaba et al. (2005) indicaron que la Gestión de Proyectos se ocupa de los proyectos externos, internos y de las oportunidades de proyectos de la organización.

D. Gestión de recursos. Otkaba et al. (2005) explicaron que el proceso de Gestión de Recursos se compone de las siguientes actividades: la planificación, seguimiento y control de recursos, e investigación de tendencias tecnológicas, apoyadas con tres subprocesos: (a) Recursos Humanos y Ambiente de Trabajo, (b) Bienes, Servicios e Infraestructura, y (c) Conocimiento de la Organización.

E. Administración de proyectos específicos. Otkaba et al. (2005) explicaron que la Administración de Proyectos Específicos aplica conocimientos, habilidades, técnicas y herramientas, a cada una de las siguientes actividades del proyecto: planificación y realización.

F. Desarrollo y mantenimiento de software. Otkaba et al. (2005) indicaron que El proceso de Desarrollo y Mantenimiento de Software se compone de uno o más ciclos de desarrollo. Cada ciclo está compuesto de las siguientes fases: inicio, requerimientos, análisis y diseño, construcción, integración y pruebas, y cierre.

MoProSoft 1.3 no nos proporciona una metodología para la auditoría integral de la gestión de tecnologías de información, siendo su enfoque basado principalmente en procesos de desarrollo de sistemas de información.

1.3.11. Modelo de un Sistema de Gestión de Calidad basado en Procesos

El Modelo de un Sistema de Gestión de Calidad basado en procesos de la norma "ISO 9001:2000 Sistemas de Gestión de la Calidad: Requisitos" (ISO, 2000), se muestra en la siguiente figura:

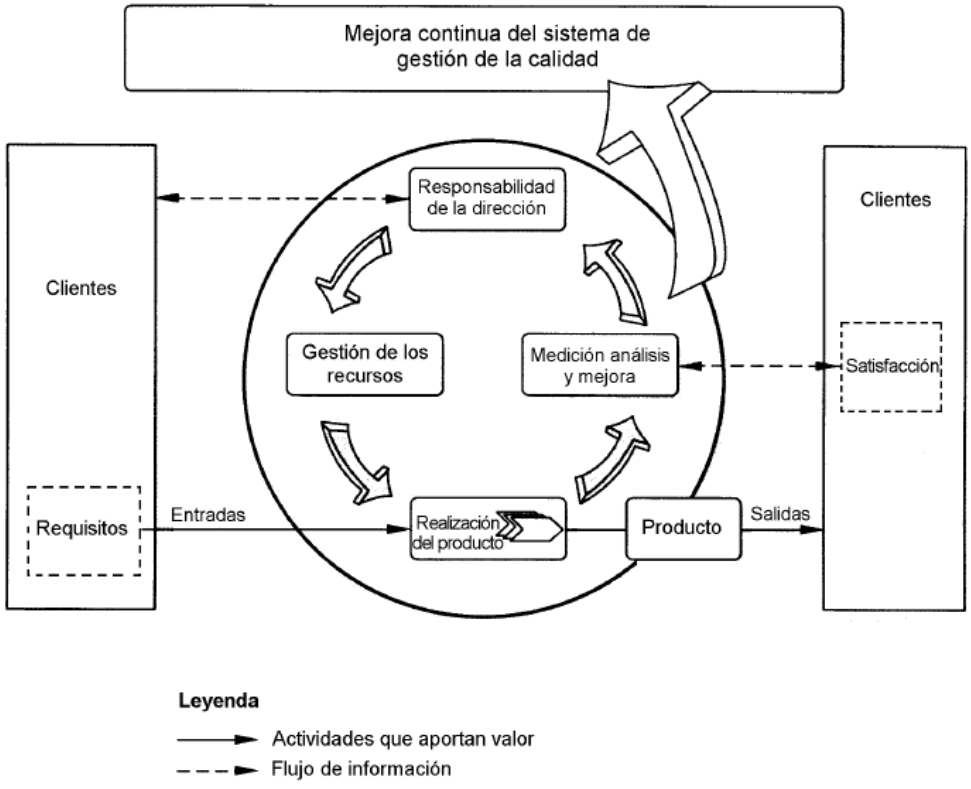


Figura 1-6 ISO (2000). Modelo de un Sistema de Gestión de Calidad basado en procesos

Como se observa en la figura, la norma indica las entradas (Requisitos de Clientes), las salidas (la satisfacción de los clientes a través de los productos), así como el proceso (responsabilidad de la dirección; gestión de los recursos; realización del producto; y medición, análisis y mejora).

1.4. DESCRIPCIÓN Y SUSTENTACIÓN DE LA SOLUCIÓN

En la NTP-ISO/IEC 12207:2006 (INDECOPI, 2006) se explica algunos requisitos previos y tareas a ser desarrolladas para la ejecución de una auditoría. Entre los requisitos previos se describe lo siguiente: (a) establecimiento de hitos para la realización de auditorías; (b) el personal auditor no debería tener responsabilidad directa sobre lo auditado; (c) acuerdos sobre los recursos necesarios para la auditoría; (d) agenda, procedimientos, y criterios de entrada y salida; (e) registro de problemas detectados durante la auditoría; (f) documentación y comunicación de resultados a la parte auditada; y (g) acuerdos sobre resultados y responsabilidades sobre cualquier problema encontrado. Entre las tareas a realizar en la auditoría, se indica que se debería asegurar lo siguiente: (a) la codificación de los productos software refleja la documentación del diseño; (b) los requerimientos prescritos por la documentación de las revisiones de aceptación y pruebas, son los adecuados para la aceptación de los productos software; (c) los datos de las pruebas cumplen con la especificación; (d) los productos software han sido adecuadamente probados y cumplen sus especificaciones; (e) los informes de pruebas son correctos y las discrepancias entre los resultados reales y los esperados se han resuelto; (f) la documentación de usuario cumple con las normas especificadas; (g) las actividades se han llevado a cabo de acuerdo con los requerimientos aplicables, planes y contrato; y (h) los costos y plazos se adhieren a los planes establecidos.

Además, según la NTP-ISO/IEC 12207:2006 (INDECOPI, 2006), como resultado de la implementación exitosa del proceso de auditoría, se tendría lo siguiente: (a) desarrollo y ejecución de una estrategia de auditoría; (b) determinación de la conformidad de productos y/o servicios o procesos de trabajo de software relacionados con los requerimientos, planes y acuerdos según la estrategia de la auditoría; (c) conducción de la auditoría por una parte independiente apropiada; (d) identificación de problemas durante una auditoría, y (e) comunicación a los responsables para la resolución y acción correctiva.

En la NTP-ISO/IEC 17799:2007 (INDECOPI, 2007), se indica que se deberían establecer controles para salvaguardar los sistemas operativos y las herramientas de auditoría durante las auditorías del sistema, y que se debe evitar el mal uso de las herramientas de auditoría. En la NTP-ISO/IEC 17799:2007 en la sección 15.3 se detalla además, una serie de consideraciones con respecto a los controles y a la protección de las herramientas de auditoría de sistemas. En el sitio web de ISACA se puede observar lineamientos, estándares y algunos procedimientos de auditoría enfocados a aspectos técnicos.

Como se puede observar, los estándares IEEE 1058:1998, ISO/IEC 12207, e ISO/IEC 17799, y la organización ISACA nos dan una serie de criterios a tener en cuenta para la auditoría de la gestión de tecnología de información; pero, no nos dan procedimientos enmarcados en una metodología que permita auditar de manera integral la gestión de la tecnología de información, alineada al logro de objetivos estratégicos organizacionales. Si no se tiene una metodología integral, no se puede llegar a un análisis profundo que nos permita encontrar las causas de los problemas y por ende, nos permita realizar un diagnóstico que realmente sirva para realizar una planificación estratégica de tecnología de información alineada a la planificación estratégica organizacional, y las auditorías podrían verse limitadas a la evaluación de decenas o cientos de aspectos aislados cuya solución realmente no beneficiaría de la mejor manera a la organización. Por lo expuesto, en la revisión de literatura realizada, no se ha encontrado una metodología similar, orientada a la auditoría de la gestión integral de la tecnología de información en una organización, con la excepción del uso del proceso general de auditoría de la ISO 19011:2002 o similares, teniendo en cuenta los objetivos de control de las normas gubernamentales o los estándares internacionales de calidad relacionados a la gestión de tecnología de información.

MAIGTI enlazará los diversos conceptos de las buenas prácticas del gobierno corporativo de la gestión de las tecnologías de información (COBIT Control Objectives for Information and related Technologies de ISACA Information Systems Audit and Control Association), la gestión de los procesos del ciclo de vida de desarrollo de software (ISO/IEC 12207), las buenas prácticas de la gestión de la seguridad de la información (ISO/IEC 17799), la gestión de servicios de tecnología de información (ISO/IEC 20000 o ITIL, Information Technology Infrastructure Library), así como la gestión de proyectos del Project Management Institute (PMBOK Project Management Body Of Knowledge), sobre la base de una

simplificación del proceso general de auditoría descrito en la norma ISO 19011:2002, y sobre la base de una adaptación del esquema de procesos de la ISO 9001:2000 (ISO, 2000). Se usarán estos estándares por las siguientes razones:

a) COBIT da un marco para la evaluación basado en el ciclo de calidad de Deming (Plan, Do, Check, Act).

b) Los estándares ISO/IEC 12207, ISO/IEC 17799 e ISO/IEC 20000, se complementan entre sí, no existiendo cruces entre ellos, sino interrelaciones muy útiles.

c) Si bien PMBOK no es un estándar propio de tecnología de información, contiene una serie de aspectos muy importantes con respecto a la gestión de proyectos alineados a la estrategia organizacional, además de complementar algunos aspectos de las normas citadas previamente, y hacer referencia a metodologías de gestión de proyectos en relación a tiempo y costos, entre otros aspectos, que son muy útiles para la gestión de proyectos de tecnología de información.

d) La existencia de estándares es tan diversa, que se hace necesario una metodología unificada para que la auditoría pueda estandarizarse.

1.5. PLAN DEL PROYECTO

Las tareas realizadas como parte de la presente tesis fueron las siguientes:

A. Recopilación de la bibliografía relacionada con los estándares de calidad internacionales: COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000 y PMBOK.

B. Elaboración de la metodología para la auditoría integral de la gestión informática.

C. Aplicación de la metodología para la auditoría integral de la gestión informática en dos empresas de seguros.

D. Afinamiento de la metodología.

E. Aplicación de la metodología afinada.

F. Evaluación de los resultados. Se evaluó el impacto resultante de la aplicación de la metodología para la auditoría integral de la gestión informática en las dos empresas de seguros.

La metodología fue elaborada y aplicada por el autor de la tesis, siendo el único auditor encargado de realizarla directamente, en las dos empresas de seguros mencionadas.

2. DESARROLLO DE LA METODOLOGÍA

2.1. PROCESO DE DESARROLLO DE LA METODOLOGÍA

El proceso seguido para el desarrollo de la metodología fue el siguiente:

A. Para cada una de las áreas temáticas del COBIT (Planificación y Organización, Adquisición e Implementación, Entrega de Servicios y Soporte, y Monitoreo y Control), se revisó los diversos objetivos de control propios del COBIT, y luego se revisó los objetivos de control del PMBOK, ISO/IEC 12207, ISO/IEC 17799 e ISO/IEC 20000, que pudieran complementarlos.

B. Luego, aplicando el procedimiento general de una auditoría de la ISO 19011:2002, se enlazaron al mismo, las evaluaciones de los diversos objetivos de control identificados, bajo la perspectiva del ciclo de Deming (Plan, Do, Check, Act), dentro del marco referencial de las áreas temáticas de COBIT.

C. Finalmente, se determinaron y se elaboraron los procedimientos que deberían ser enlazados al proceso general para la auditoría de la gestión informática, los cuales a su vez comprendieron la evaluación de diversos conjuntos de objetivos de control cuya agrupación facilita el seguimiento, control y/o supervisión.

2.2. ARQUITECTURA DE LA METODOLOGÍA

El siguiente gráfico, expresa la estructura de MAIGTI (metodología propuesta para la auditoría integral de la gestión informática):

Figura 2-1 Estructura de MAIGTI - Metodología para la Auditoría Integral de la Gestión de la Tecnología de Información

La figura 2.1 representa la estructura de objetivos de control que compone la metodología propuesta, la cual a su vez está enmarcada en el modelo de procesos, sobre la base del proceso general de auditoría de la ISO 19011:2002, como se ve en la figura 2.2.

La metodología resultante en la figura 2.2, comprende los siguientes elementos: objetivo (la finalidad de la auditoría), alcance (detalle de lo que está incluido y lo que no está incluido como parte de la auditoría), entradas (requerimientos de información), proceso de MAIGTI (evaluaciones a realizar) y salidas (papeles de trabajo e informe de auditoría). Asimismo, cada uno de los procedimientos para la evaluación de los principales objetivos de control dentro de los procesos 5.1, 5.2, 5.3 y 5.4, comprende la siguiente estructura: objetivo (la finalidad del procedimiento de auditoría), alcance (detalle de lo que está incluido y lo que no está incluido como parte de la auditoría a realizarse a través del procedimiento), entradas (requerimientos de información para ejecutar el procedimiento de auditoría), proceso (detalle de los pasos a seguir en el procedimiento de auditoría), salidas (hallazgos evidenciados como resultado de la ejecución del proceso). En los procedimientos descritos en el anexo 1, se ha detallado como salidas, algunos hallazgos posibles que se derivan como resultado de la experiencia de las aplicaciones de MAIGTI en auditorías realizadas por el autor de la tesis.

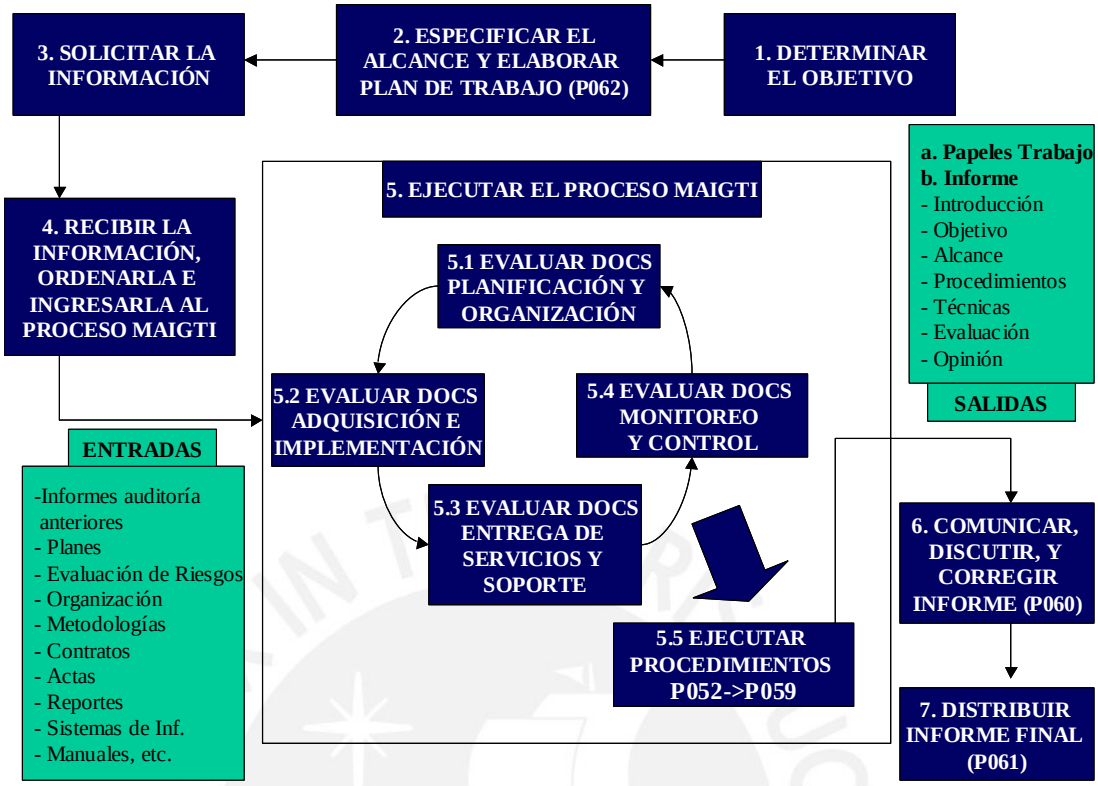


Figura 2-2 MAIGTI. Metodología para la Auditoría Integral de la Gestión de Tecnología de Información.

Para explicar el enfoque de procesos aplicado para la ejecución de cada procedimiento, se detallará a continuación, el procedimiento P029: Procedimiento para la auditoría de los contratos para la compra de sistemas de información, con su objetivo, alcance, entradas, proceso, y salidas. Luego se mostrará un ejemplo de contrato a auditar y finalmente se mostrará un ejemplo de observación o hallazgo resultante.

P029: Procedimiento para la auditoría de los contratos para la compra de sistemas de información

Objetivo

Analizar y evaluar los contratos para las compras de bienes o servicios de sistemas de información en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

Alcance

El alcance del procedimiento incluye:

A. Revisión de procedimientos relativos a la generación de contratos para las compras de sistemas de información (SI).

B. Revisión física de las cotizaciones y evaluaciones previas a los contratos para las compras de SI.

C. Revisión física de los contratos para las compras de SI.

D. Análisis de la generación de valor de los contratos.

El alcance del procedimiento no incluye:

A. Análisis y Evaluación de propuestas no contempladas como parte del análisis para la generación del contrato.

Entradas

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Procedimientos para la generación de contratos para la compra de SI.
B. Cotizaciones finales para la compra de SI.
C. Evaluaciones de las cotizaciones finales para la compra de SI.
D. Contratos y adendas de contratos para las compras de SI.

Proceso

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar los procedimientos relativos a la generación de contratos para la compra de SI. De no existir procedimientos formales, indagar cuál es el procedimiento o los procedimientos reales para la compra de SI.

C. Revisar las cotizaciones y evaluaciones para la compra de SI. Ver procedimiento P026.

D. Revisar los contratos para la compra de SI. Verificar que se solicite como mínimo lo siguiente:

a) Datos básicos iniciales del contrato:
   - Título del Contrato. En la parte superior de la primera hoja del contrato.
   - Datos del Contratante: nombre completo o razón social, RUC, dirección y alias.
   - Datos del Representante Legal del contratante: nombre completo, DNI y datos de la inscripción en registros públicos. De ser un contrato con una organización con representante legal de otro país, indicar también la nacionalidad o carnet de extranjería.
   - Datos del Contratado: nombre completo o razón social, RUC, dirección y alias.
   - Datos del Representante Legal del contratado: nombre completo, DNI y datos de la inscripción en registros públicos. De ser un contrato con una organización con representante legal de otro país, indicar también la nacionalidad o carnet de extranjería.

b) Generalidades.
c) Objeto del Contrato.
d) Especificaciones técnicas de lo solicitado.
e) Metodología.
f) Plan de Trabajo.
g) Entregables y fechas de entrega.
h) Niveles de servicio.
i) Condiciones de hardware mínimas para el funcionamiento del SI.
j) Vigencia del contrato.
k) Costo total y forma de pago.
l) Confidencialidad.
m) Garantías.
n) Limitaciones.

o) Penalidades.
p) Jurisdicción en caso de desacuerdos.
q) Cláusulas de protección contra riesgos (riesgos de operación, riesgos financieros, etc.).
r) Firmas y sellos de los representantes legales.

E. Analizar la generación de valor del contrato. Ver procedimiento P059.

Salidas

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no evalúa varios proveedores al momento de realizar una compra.

B. En los contratos no se indica detalladamente las especificaciones técnicas de lo que se va a entregar, ni se hace referencia a propuestas técnicas donde se encuentre ese detalle.

C. No se hace contratos para la compra de SI.

D. Se determina que gana el contrato, una propuesta para la compra de SI que no fue ponderada como ganadora.

E. No se incluye cláusulas que permitan a la organización, tener una protección ante la quiebra o retiro del mercado del proveedor; por ejemplo, pudiendo acceder al código fuente de su aplicación y a toda la documentación técnica en caso suceda la quiebra o retiro del mercado del proveedor.

A continuación se mostrará el ejemplo de contrato a auditar:

CONTRATO Nº 124-2006-EL PROVEEDOR

Conste por el presente documento, el contrato se desarrollo de sistemas de información de la empresa CLIENTE DE DESARROLLO DE SISTEMAS DE INFORMACIÓN, debidamente representada por su Gerente General, el Sr. Juan Pérez García, identificado con DNI 12345678, a quien en adelante se le llamará EL CLIENTE, con la EMPRESA PROVEEDORA DE DESARROLLO DE SISTEMAS DE INFORMACIÓN, debidamente representada por su Gerente General, el Sr. Carlos Luna Mendoza, identificado con DNI 87654321, a quien en adelante se le llamará EL PROVEEDOR, ambas empresas inscritas en el Registro de Personas Jurídicas de Lima y Callao.

CLÁUSULA 1: OBJETO DEL CONTRATO

Desarrollar un sistema de información que cubra las transacciones de la empresa para los procesos administrativo-financieros para EL CLIENTE, por parte de EL PROVEEDOR.

CLÁUSULA 2: ALCANCE DEL SERVICIO

El sistema administrativo financiero a desarrollar abarcará los procesos siguientes:

a) Tesorería: caja, bancos, cuentas por cobrar y cuentas por pagar.
b) Presupuestos: presupuesto de ingresos y presupuesto de egresos.
c) Contabilidad: registro de libros contables y emisión de estados financieros.
d) Recursos Humanos: registro de datos de trabajadores, así como el pago de planillas de personal obrero, personal empleado y funcionarios.
e) Reportes.

CLÁUSULA 3: TIEMPO DEL SERVICIO

El sistema se deberá desarrollar en 4 meses, y tendrá las siguientes etapas: (a) análisis y diseño, (b) programación, y (c) instalación y puesta en marcha.

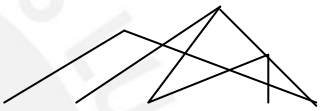
CLÁUSULA 4: INVERSIÓN Y FORMA DE PAGO

La inversión por el servicio asciende a US$ 50,000 y será abonado de la siguiente manera:

a) 20% a la firma del contrato.
b) 20% al terminar la etapa de análisis y diseño.
c) 30% al terminar la etapa de programación.
d) 30% cuando el sistema esté instalado en las computadoras de los usuarios.

Las partes firman en señal de conformidad con las cláusulas del presente contrato, a los 20 días del mes de Julio del 2006.

EL CLIENTE



EL PROVEEDOR

Luego de la aplicación del procedimiento, la redacción del hallazgo sería como se muestra a continuación:

El contrato para la compra del desarrollo del sistema administrativo financiero, no está elaborado adecuadamente

El contrato para la compra del desarrollo del sistema de información administrativo financiero, celebrado con la EMPRESA PROVEEDORA DE DESARROLLO DE SISTEMAS DE INFORMACIÓN, presenta las siguientes deficiencias:

A. Falta completar datos básicos del contrato:
   a) Datos del Contratante: falta dirección y RUC.
   b) Datos del Representante Legal del Contratante: falta número de partida electrónica de la inscripción de poder en registros públicos.
   c) Datos del Contratado: falta dirección y RUC.
   d) Datos del Representante Legal del Contratado: falta número de partida de la inscripción de poder en registros públicos.
B. Falta sección que explique características generales de las partes del contrato.

C. *Las especificaciones técnicas del sistema administrativo financiero a desarrollar son insuficientes para asegurar una adecuada calidad del servicio.*
D. *No se ha desarrollado cláusulas o anexos al contrato, que especifiquen lo siguiente: Metodología, Plan de Trabajo, Entregables y fechas de entrega, Niveles de servicio, Condiciones de hardware mínimas para el funcionamiento del sistema de información, Confidencialidad de la Información, Garantías, Limitaciones, Penalidades, Jurisdicción en caso de desacuerdos, ni Cláusulas de protección contra riesgos (riesgos de operación, riesgos financieros, etc.).*
E. *No tiene firmas ni sellos de los gerentes generales.*

Se ha incurrido a la fecha en costos adicionales de US$ 40,000 sin que el sistema de información esté instalado en los usuarios, y sin que se tenga una planificación del tiempo acordada con el proveedor, dados los adicionales.

La causa de lo ocurrido es la inexistencia de un contrato tipo ni un procedimiento para la elaboración de contratos de compra de desarrollos de sistemas de información.

El efecto ha sido que no se tenga claras las condiciones con el proveedor y haya entregado el software desarrollado sin haberse integrado con el resto de aplicaciones ni migrado los datos del sistema anterior, dado que no estaba especificado en el contrato y en ningún documento consta en requerimiento ni el compromiso del proveedor para realizarlo. Esto ha provocado costos adicionales en el orden de los US$ 40,000 como se ha manifestado y se espera que tenga mayores costos adicionales, en el orden de los US$ 30,000.

El riesgo para la organización es que el sistema administrativo financiero salga a producción sin las debidas especificaciones de calidad, dado que no se ha comprometido al proveedor para que cumpla una metodología de desarrollo de sistemas de información que incluya la planificación y ejecución de pruebas, así como la planificación y ejecución de labores de integración y migración de datos, previas a la implantación del sistema de información. Además, dado que tampoco se ha especificado capacitación para los usuarios y dado que los usuarios no están acostumbrados a utilizar este tipo de sistemas, se demorarían mucho más los registros de transacciones con los consecuentes perjuicios sobre todo para los procesos que están directamente relacionados a la atención a los clientes.

Se recomienda desarrollar un modelo de contrato y un procedimiento para la celebración de contratos con los proveedores de desarrollo de sistemas de información, para proyectos futuros. Para el proyecto actual, se recomienda hacer que el contrato supere las deficiencias indicadas en la presente observación cuanto antes, para luego asignar un responsable de la planificación, ejecución, seguimiento y control del proyecto. Se recomienda además que el área de Auditoría Interna le haga seguimiento a la implementación de estas recomendaciones.

3. DESCRIPCIÓN DE LA METODOLOGÍA

A continuación se describirá MAIGTI, considerando como proceso la gestión integral de la tecnología de información en una organización. Primero se planteará la metodología a través del enfoque basado en procesos teniendo como base el proceso general de auditoría (ver figuras 2.1 y 2.2). Luego se hará una comparación de la metodología MAIGTI con las metodologías existentes.

3.1. PLANTEAMIENTO DE LA METODOLOGÍA

A continuación se explicará los aspectos de los estándares internacionales de la gestión de tecnología de información, que serán utilizados como referencias para los objetivos de control de MAIGTI (en la figura 3.1 se detallarán las interrelaciones de MAIGTI con los 5 estándares internacionales que han servido de base para su construcción):

A. COBIT: Control Objectives for Information and related Technologies. De este estándar se tomará los procesos generales de evaluación, dado que están basados en el ciclo de Deming (Plan, Do, Check, Act). Las cuatro grandes áreas

temáticas del COBIT (Planificación y Organización, Adquisición e Implementación, Entrega de Servicios y Soporte, y Monitoreo y Control) (IT Governance Institute, 2006), serán usadas como marco referencial sobre el cual se enlazarán los aspectos de los estándares internacionales de calidad: ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000, y PMBOK.

B. ISO/IEC 12207: Procesos del Ciclo de Vida del Software (INDECOPI, 2004). De este estándar se tomará los objetivos de control para la auditoría de los procesos del ciclo de vida del software, enmarcados dentro de la planificación de proyectos de desarrollo de sistemas de información, la ejecución de los proyectos de desarrollo de sistemas de información, así como el monitoreo y control de los mismos. Los procesos específicos de la norma que se tomará en cuenta son los siguientes: adquisición, desarrollo, mantenimiento, gestión, y recursos humanos.

C. ISO/IEC 17799: Código de Buenas Prácticas de la Gestión de la Seguridad de la Información (INDECOPI, 2004). De este estándar se tomará los objetivos de control para los temas relativos a la planificación de la seguridad de la información, el plan de continuidad de negocio, aspectos organizativos de seguridad de la información, la entrega de servicios de seguridad lógica, y la entrega de servicios de seguridad física.

D. ISO/IEC 20000: Modelo de Gestión de Servicios de Tecnología de Información (Kemmerling & Pondman, 2004). Se introducirán las buenas prácticas de la gestión de servicios de TI como parte integrante de la gestión de la planificación y organización, la adquisición e implementación, y la entrega de servicios y soporte de TI, principalmente en lo referente a la definición de niveles de servicio y control de cambios.

E. PMBOK: Project Management Body Of Knowledge (Project Management Institute, 2004). De este estándar se tomará los grupos de procesos y áreas de conocimiento como referencia, de manera que se enmarquen los proyectos dentro de los diversos aspectos: integración, alcance, tiempo, costo, calidad, recursos humanos, comunicaciones, riesgos, y adquisiciones. Esto aplicará tanto para los proyectos de desarrollo de sistemas de información como para los proyectos relacionados a la gestión de infraestructura de tecnología de información. Se incluirán estos conceptos dentro de los marcos referenciales de

la Planificación y Organización, Adquisición e Implementación, así como Monitoreo y Control.

F. ISO 19011. Se ha tomado como referencia para procedimientos estrictos de auditoría, lo indicado en la norma ISO 19011:2002.

En la Figura 3.1 se muestra la relación de cada procedimiento de MAIGTI con los estándares internacionales de calidad. Cabe resaltar además, que se ha tomado como referencia, las normas técnicas peruanas, relacionadas a la seguridad eléctrica, NTP 370.052:1999, NTP 370.053:1999, NTP 370.054:1999, y NTP 370.052:1999 (PROCOBRE, 2005). Sería necesario precisar que los temas específicos referidos de estas normas técnicas peruanas, se deberían adaptar a la normatividad vigente en cada país para cada tamaño o tipo de infraestructura de los locales de las organizaciones, si quisiéramos adaptar la metodología propuesta.

La integración de los diversos estándares en un todo coordinado tendrá ventajas sobre la aplicación de auditorías teniendo los estándares dispersos, dado que se podrán interrelacionar y encontrar las causas de los problemas de manera más eficiente y se podrá proponer soluciones concretas para que se mejore la generación de valor de las organizaciones, eliminando o minimizando las causas de los problemas, lográndose así que la mejora de la gestión de la tecnología de información, realmente genere valor de manera rápida e integrada con el Plan Estratégico Organizacional.

Teniendo como base el enfoque basado en procesos (ver figuras 2.1 y 2.2) de MAIGTI, a continuación se detallará lo siguiente: objetivo, alcance, entradas, proceso y salidas.

	ESTÁNDARES INTERNACIONALES DE CALIDAD					
PROCEDIMIENTO	COBIT	ISO/IEC 12207	ISO/IEC 17799	ISO/IEC 20000	PMBOK	ISO 19011
P001	X	X	X	X	X	X
P002	X				X	
P003	X				X	
P004	X				X	
P005	X				X	
P006	X	X			X	
P007	X	X			X	
P008	X		X		X	
P009	X		X		X	
P010	X		X		X	
P011	X		X		X	
P012	X	X			X	
P013	X		X		X	
P014	X		X		X	
P015	X		X		X	
P016	X	X	X		X	
P017	X	X	X		X	
P018	X	X	X		X	
P019	X	X	X		X	
P020	X	X			X	
P021	X		X	X		
P022	X	X	X	X		
P023	X	X	X	X		
P024	X	X			X	
P025	X	X			X	
P026	X	X			X	
P027	X			X	X	
P028	X			X	X	
P029	X			X	X	
P030	X		X			
P031	X	X	X	X		
P032	X		X	X		
P033	X	X	X	X		
P034	X	X				
P035	X	X				
P036	X		X			
P037	X		X			
P038	X		X			
P039	X		X			
P040	X	X	X			
P041	X	X				
P042	X					
P043	X					
P044	X					
P045	X					
P046	X	X	X			
P047	X	X		X		
P048	X	X			X	
P049	X	X			X	
P050	X	X			X	
P051	X		X	X		
P052	X					
P053	X		X			
P054	X		X			
P055	X		X			
P056	X		X			
P057	X		X			
P058	X		X			
P059	X					
P060						X
P061						X
P062						X
P063	X		X			

Figura 3-1 Relaciones de los procedimientos de MAIGTI con los estándares internacionales COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000, PMBOK e ISO 19011.

3.1.1. OBJETIVO

El objetivo de la metodología es evaluar la gestión de la tecnología de información en una organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos relacionados, teniendo como base los estándares internacionales COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000 y PMBOK.

3.1.2. ALCANCE

El alcance de la metodología comprende:

A. Evaluación de la “Planificación y Organización”. Incluye:

   a) Revisión de planes diversos: Plan Estratégico de Tecnología de Información, Plan de Contingencias de Informática, Plan de Continuidad de Negocio, Plan de Capacitación, Plan de Licenciamiento de Software, Plan de Mantenimiento Preventivo, Planes de Proyectos, Plan de Seguridad, Plan de Calidad, Plan de Compras, etc.

   b) Organización del Trabajo: Estructura Organizacional, Recursos Disponibles, Metodologías de Trabajo, Procedimientos, etc.

B. Evaluación de la “Adquisición e Implementación”. Incluye:

   a) Adquisiciones de Tecnologías de Información: equipos de cómputo, equipos de red, licencias de software, sistemas de información, etc. Se revisan tanto las propuestas alternativas como los contratos y anexos a los contratos.

   b) Desarrollos de Tecnologías de Información: desarrollo de tecnologías de información de base y desarrollo de sistemas de información. Se revisa el cumplimiento de la metodología y la documentación respectiva.

C. Evaluación de la “Entrega de Servicios y Soporte”. Incluye:

   a) Entrega de Servicios de Desarrollo e Implantación de Sistemas de Información. Se verifica la evaluación de posibles soluciones, lo

desarrollado o comprado e implantado, medidas de seguridad y el nivel de satisfacción de los usuarios con respecto al servicio otorgado.

b) Entrega de Servicios de Soporte Técnico e Infraestructura de Tecnologías de Información, Hardware y Software de base, así como servicios relacionados.

D. Evaluación del "Monitoreo y Control". Incluye:

a) Seguimiento de los planes.
b) Evaluación Interna del Desempeño.
c) Certificaciones o acreditaciones independientes de control y seguridad.
d) Provisión de Auditoría Independiente.

Cuando ya se ha determinado el alcance (lo que incluirá y lo que no incluirá la auditoría, como materia de evaluación), se debería proceder con la elaboración del Plan de Trabajo de la Auditoría. Esto implica ejecutar el procedimiento P062: Procedimiento para la Elaboración del Plan de Trabajo de la Auditoría.

3.1.3. ENTRADAS

Las entradas de información de la metodología están comprendidas por los documentos que se requiere para iniciar el proceso de auditoría. Se requiere los siguientes documentos realizados o vigentes en el período en evaluación, el período anterior y los documentos a ser aplicados para los períodos siguientes, para cada uno de los grandes temas de revisión: "Planificación y Organización", "Adquisición e Implementación", "Entrega de Servicios y Soporte" y "Monitoreo y Control". Se entiende como período, el tiempo de un año; claro está que el tamaño real del período dependerá de la decisión que tome el área de Auditoría Interna, o el Comité Auditor de la Entidad de Auditoría Externa u Organismo Regulador que desee hacer la auditoría con esta metodología.

A. Para evaluar la "**Planificación y Organización**" se requiere los siguientes documentos:

a) Plan Estratégico de la Organización.
b) Plan Operativo de la Organización.
c) Evaluación de Riesgos de la Organización.
d) Plan Estratégico de Tecnologías de información.
e) Plan Operativo de Tecnologías de información. Está compuesto por:
    i. Planes de proyectos, tanto a nivel técnico como a nivel de gestión.
    ii. Plan de Contingencias de Informática.
    iii. Plan de Continuidad de Negocio.
    iv. Plan de Seguridad de la Información.
    v. Plan de Licenciamiento de Software.
    vi. Plan de Capacitación.
    vii. Plan de Mantenimiento Preventivo de Hardware de Computadoras, Redes y Equipos Relacionados.
    viii. Plan de Mantenimiento Correctivo de Hardware de Computadoras, Redes y Equipos Relacionados.
    ix. Planificación de Labores de Rutina.
    x. Plan de Calidad. Incluye aseguramiento y control de calidad.
    xi. Plan de Compras.
f) Manual de Organización y Funciones.
g) Reglamento de Organización y Funciones.
h) Currículum vitae actualizado de todo el personal que cumple funciones relacionadas a las Tecnologías de información. Incluye: personal por quinta categoría, personal por cuarta categoría y personal colocado por proveedores.

B. Para evaluar la “Adquisición e Implementación” se requiere los siguientes documentos:

a) Inventario en unidades y en valores del hardware de tecnologías de información.
b) Inventario en unidades y en valores del software de base.
c) Inventario en unidades y en valores de los intangibles correspondientes a sistemas de información, ya sean desarrollados o comprados a terceros.
d) Cotizaciones para las compras de software de base (sistemas operativos, administradores de bases de datos, protección contra intrusos, protección ante correos no deseados, servidores web, servidores para realizar copias de respaldo, software de oficina, servidores de correo, clientes de correo,

etc.). Considérese como software de base a todo software que no sea sistema de información.

e) Cotizaciones para las compras de sistemas de información.
f) Cotizaciones para las compras de hardware de computadoras, redes y servicios relacionados.
g) Contratos de compra de hardware.
h) Contratos de compra de todas las licencias de software de base.
i) Contratos de compra de todos los sistemas de información cuya propiedad intelectual pertenece a proveedores.
j) Contratos de seguros relativos a las tecnologías de información.
k) Metodología de Desarrollo de Sistemas de Información.
l) Metodología o Procedimiento para la Compra de Hardware.
m) Metodología o Procedimiento para la Compra de Software de Base.
n) Metodología o Procedimiento para la Compra de Sistemas de Información.
o) Metodología para la atención de requerimientos de Hardware de los usuarios.
p) Metodología para la atención de requerimientos de Software de Base de los usuarios.
q) Metodología para la atención de requerimientos de Sistemas de Información de los usuarios.
r) Manuales Técnicos de todo el Hardware comprado o construido.
s) Manuales Técnicos de todo el Software de Base comprado o desarrollado.
t) Manuales Técnicos de todos los sistemas de información que se usan en la organización. Esto incluye tanto los sistemas de información hechos a través de proveedores como desarrollos internos.
u) Manuales de Usuario de todo el Hardware comprado o construido.
v) Manuales de Usuario de todo el Software de Base comprado o desarrollado.
w) Manuales de Usuario de todos los sistemas de información que se usan en la organización. Esto incluye tanto los sistemas de información hechos a través de proveedores como desarrollos internos.

C. Para evaluar la “Entrega de Servicios y Soporte”, se requiere los siguientes documentos:

a) Esquema de la Red de la Oficina Principal y las sucursales.
b) Listado de accesos de todos los usuarios sobre los sistemas de información.
c) Listado de accesos de todos los usuarios sobre carpetas de los servidores.

d) Detalle de la Arquitectura de la red de tecnologías de la información.
e) Manuales de Procedimientos.
f) Formularios de control de entregables de proyectos y requerimientos.

D. Para evaluar el “Monitoreo y Control”, se requiere los siguientes documentos:

a) Informes de auditorías internas anteriores.
b) Informes de auditorías externas anteriores.
c) Certificaciones de calidad.
d) Evaluaciones de desempeño del área responsable de la gestión de tecnologías de información.
e) Evaluaciones de desempeño del personal.
f) Formularios de control de cambios en proyectos.
g) Formularios de control de riesgos en proyectos.
h) Formularios de seguimiento de avances de proyectos.
i) Actas y formularios de seguimiento y verificación de labores de desarrollo de sistemas de información: solicitud de requerimientos, aprobación de requerimientos, formularios de conformidad de servicio, etc.
j) Actas de seguimiento y verificación de las labores de soporte técnico.

3.1.4. PROCESO

La siguiente gráfica resume el Proceso MAIGTI, identificando sus subprocesos con los procedimientos asociados:

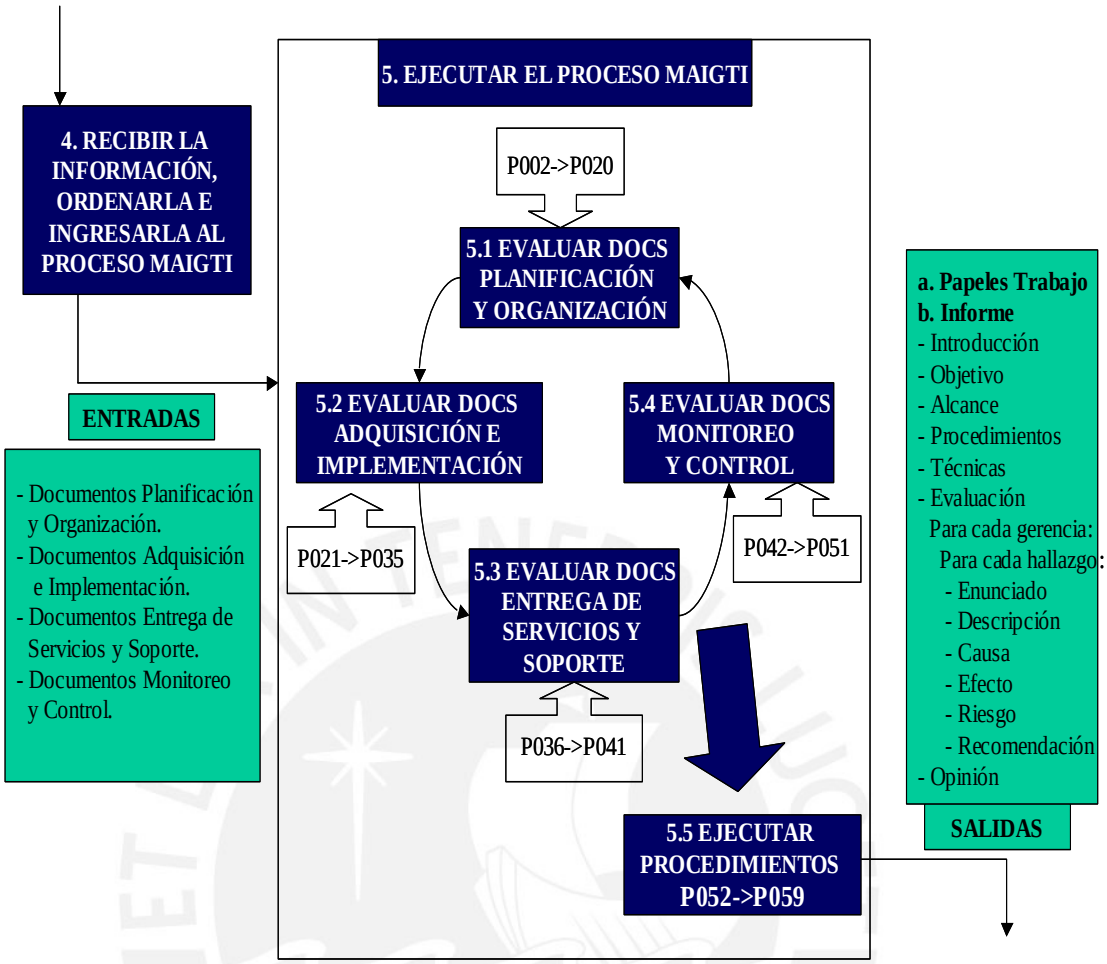


Figura 3-2 El Proceso MAIGTI

Las actividades que comprenden el Proceso MAIGTI, son las siguientes:

A. Solicitar la documentación requerida. Para esta labor, la Gerencia de Auditoría Interna o el Supervisor del Equipo de Auditoría asignado, hará los requerimientos de información indicados en la sección 3.1.3 del presente documento al área que realice la Gestión de la Tecnología de Información. Esta actividad debe realizarse por lo menos con 15 días de anticipación a la fecha programada para la revisión de los documentos.

B. Evaluar los documentos recibidos. Los documentos recibidos deberán ser revisados de acuerdo a cada caso en el orden siguiente:

a) Evaluar los documentos del período anterior al período en evaluación.
b) Evaluar los documentos del período en evaluación.

c) Evaluar los documentos a ser aplicados para el período siguiente al período en evaluación.

Para revisar los documentos de cada período se debe proceder en el orden siguiente:

a) Evaluar los documentos de “Planificación y Organización”. Esto implica ejecutar los procedimientos P002 al P020, del anexo 1.
b) Evaluar los documentos de “Adquisición e Implementación”. Esto implica ejecutar los procedimientos P021 al P035, del anexo 1.
c) Evaluar los documentos de “Entrega de Servicios y Soporte”. Esto implica ejecutar los procedimientos P036 al P041, del anexo 1.
d) Evaluar los documentos de “Monitoreo y Control”. Esto implica ejecutar los procedimientos P042 al P051, del anexo 1.

C. Entrevistar de manera presencial a los usuarios de diversas áreas de la empresa, incluyendo personal con rango gerencial y personal sin rango gerencial. Esto implica ejecutar el procedimiento P052 del anexo 1.

D. Entrevistar y realizar verificaciones presenciales con personal que realiza labores relacionadas con la gestión de la infraestructura de tecnologías de Información.

a) Obtener la lista de correos, teléfonos, anexos y cargos de las personas que trabajan en la gestión de la infraestructura de tecnologías de información.

b) Visitar y revisar las instalaciones de la red eléctrica. Esto implica ejecutar el procedimiento P053 del anexo 1.

c) Visitar y revisar la seguridad de acceso al centro de cómputo principal. Esto implica ejecutar el procedimiento P054 del anexo 1.

d) Visitar y revisar las instalaciones del centro de cómputo principal. Esto implica ejecutar el procedimiento P055 del anexo 1.

e) Visitar y revisar la seguridad de acceso al centro de cómputo alterno. Esto implica ejecutar el procedimiento P056 del anexo 1.

f) Visitar y revisar las instalaciones del centro de cómputo alterno. Esto implica ejecutar el procedimiento P057 del anexo 1.

g) Revisar el cableado de redes de datos. Revisar ubicación de “switches” o “hubs”, así como las condiciones del cableado coaxial, UTP o fibra óptica. Esto implica ejecutar el procedimiento P058 del anexo 1.

E. Entrevistar y realizar verificaciones presenciales con personal que realiza labores relacionadas con la gestión del desarrollo de sistemas de información.

F. Obtener la lista de correos, teléfonos, anexos y cargos de las personas que trabajan en la gestión del desarrollo de sistemas de información.

G. Entrevistar al personal que dirige los proyectos y al personal que realiza los desarrollos de sistemas de información. Esto implica ejecutar el procedimiento P059 del anexo 1.

H. Elaborar el Informe Preliminar. Esto implica ejecutar el procedimiento P060 del anexo 1.

I. Revisar el Informe Preliminar.

a) Verificar que el informe tenga los puntos que exige el organismo regulador o la casa matriz, en caso exista un formato estándar.
b) Verificar que se haya cumplido el procedimiento.
c) Verificar la redacción del informe.
d) Verificar la ortografía del informe.
e) Solicitar entrevistas con el personal que realiza la Gerencia de Tecnología de Información para verificar que las observaciones sean correctas.

J. Corregir el Informe Preliminar y lograr el Informe Final.

K. Enviar, Sustentar y Corregir el Informe Final. Esto implica ejecutar el procedimiento P061 del anexo 1.

3.1.5. SALIDAS

Las salidas de MAIGTI son las siguientes:

A. Papeles de Trabajo.

B. Informe Final de Auditoría de la Gestión de la Tecnología de Información. Este informe comprenderá la siguiente estructura:

a) Introducción
b) Objetivo
c) Alcance
d) Procedimientos de auditoría
e) Técnicas de auditoría
f) Evaluación

Para cada Gerencia que resulte responsable

Para cada hallazgo

La estructura será la siguiente:

- Enunciado
- Descripción
- Causa
- Efecto
- Riesgo
- Recomendaciones
- Comentario de la Gerencia

g) Opinión.

La cantidad de hallazgos posibles durante el desarrollo de la metodología es muy grande. Probablemente encontraremos la ausencia de documentación de los planes, metodologías de desarrollo, información sobre requerimientos de los proyectos, manuales de procedimientos, manuales técnicos y manuales de usuario de los sistemas de información. En los casos en que se encuentran los planes, comúnmente no tienen un detalle suficiente para realizar el seguimiento de manera directa, dejándose muchos vacíos de temas no definidos que hacen que los proyectos se retrasen mucho más.

Además, comúnmente se observa la falta de satisfacción del usuario por los servicios de desarrollo de sistemas y soporte técnico. Esta falta de satisfacción se debe principalmente a la falta de velocidad en la atención de los requerimientos o que los requerimientos nunca fueron atendidos. También se observa el continuo gasto excesivo en proyectos que no se definieron bien, no se probaron bien y que finalmente demoraron y costaron mucho más de lo esperado.

En los procedimientos referenciados en la sección 3.1.4, y que se encuentran en el anexo 1, se podrá observar las salidas específicas para cada evaluación de los diversos objetivos de control tomado sobre la base de los estándares internacionales que conforman la base de la metodología. Las salidas enunciadas en cada procedimiento han sido recopiladas de las experiencias del autor de la tesis desarrollando auditorías informáticas en diversas entidades del Estado y privadas.

3.2. COMPARACIÓN CON METODOLOGÍAS EXISTENTES

Como se ha explicado en la Sección 1.4, en la revisión de literatura realizada, no se ha encontrado una metodología similar a MAIGTI, con la excepción del uso del proceso general de auditoría indicado en la ISO 19011:2002 (ISO, 2002) teniendo en cuenta los objetivos de control de las normas gubernamentales o los estándares internacionales de calidad relacionados a la gestión de tecnología de información.

Además, como se ha indicado en la sección 2.2, MAIGTI es similar al proceso general de la auditoría, dado que está basada en ese proceso (ver figura 2.2); sin embargo, de la experiencia de la aplicación de MAIGTI, la integración de los diversos estándares internacionales mencionados (ver figura 2.1), magnifica el impacto positivo en la evaluación de la gestión de la tecnología de información, a diferencia de las referencias incompletas de objetivos de control mencionados en normas (dado que son cientos de objetivos de control), lo cual comúnmente hace que no se logre esa visión integral que se requiere para un adecuado diagnóstico de la gestión informática.

Las ventajas de la aplicación de MAIGTI (en comparación con el proceso general de auditoría indicado en la ISO 19011:2002) son las siguientes:

A. Reduce la subjetividad al momento de determinar las observaciones a la gestión de las tecnologías de información, dado que se tienen listas de verificación concretas, las cuales no son tan dispersas o no se presentan en tanta cantidad como los objetivos de control de los estándares internacionales de la gestión de la tecnología de información.

B. Permite identificar claramente las causas de los problemas relacionados a la gestión informática, dado que se puede analizar las interrelaciones de los diversos entes involucrados.

C. Permite cuantificar los impactos de los problemas y sus causas, así como cuantificar los riesgos asociados a las ineficiencias en la gestión de las tecnologías de información.

D. Dado que se enfoca en identificar las causas de manera más precisa, se puede realizar un adecuado diagnóstico y recomendaciones concretas para que se eliminen o mitiguen las causas.

E. Luego de su aplicación, la gerencia de las tecnologías de información, se enfoca mejor hacia los puntos que requieren su atención, buscándose el mejor impacto en la generación de valor de la organización.

Las desventajas de la aplicación de MAIGTI (en comparación con el proceso general de auditoría indicado en la ISO 19011:2002) son las siguientes:

A. Al inicio trae conflictos con las áreas auditadas (las áreas de Informática), dado que se evalúa con estándares internacionales y se percibe como injusta, dado que no se les mide a todos los gerentes con la misma forma de evaluación. Esto sucede con mayor énfasis cuando las organizaciones no tienen procesos formales de planificación estratégica (formulación, implementación y evaluación), y por lo tanto es lógico que se perciba como injusto que a un gerente de informática se le evalúe por no planificar estratégicamente sus actividades si no se tiene estrategias de marketing, ventas, operaciones,

finanzas, etc., claramente definidas; además, las otras áreas (áreas usuarias de tecnología de información), tienen menor nivel de planificación de actividades que las áreas de informática, dada la menor complejidad de algunas áreas usuarias.

B. Su aplicación es cara, dado que requiere personal con competencias en lo referente a gerencia (personal que haya tenido la experiencia de ser gerente), y procesos relacionados a la gestión informática intrínseca (experiencia administrando o realizando labores de desarrollo de sistemas de información y/o soporte técnico), además de conocimientos sobre procesos de sistemas de gestión y estándares internacionales de la calidad.

C. Su aplicación tomaría más tiempo que la metodología existente (proceso general de la auditoría que referencia objetivos de control aislados), dado que la misma es incompleta (si quisiéramos evaluar la gestión integral de la tecnología de información en una organización) sin los objetivos de control de los diversos estándares internacionales juntos, ocasionándose que se revisen de manera no optimizada, los objetivos de control comunes entre ellos.

4. PRUEBA DE LA METODOLOGÍA

4.1. ESTRATEGIA DE PRUEBAS

La aplicación de MAIGTI se realizó en 2 empresas de seguros (están entre las más importantes del Perú), en los años 2006, 2007 y 2008, con un alcance a nivel nacional. Estas empresas tienen diversidad de plataformas tecnológicas y la suficiente complejidad en sus procesos y recursos, para poder apreciar con detalle la aplicación de los diversos puntos que comprenden la metodología. Cabe resaltar que esta metodología también se ha aplicado de manera parcial (dada la menor complejidad de sus áreas de tecnología de información) a las auditorías informáticas realizadas por el autor de la tesis en las siguientes organizaciones: dos institutos de investigación del Estado Peruano, dos municipalidades, una empresa de envío y recepción de dinero, una empresa de generación eléctrica, y una empresa de producción y comercialización de combustibles. También ha sido aplicada parcialmente (en lo referente a planificación), a una auditoría de una estrategia nacional multisectorial, de una oficina nacional del Estado Peruano.

La Estrategia de Pruebas de MAIGTI fue la siguiente:

A. En el primer trimestre del 2006, se desarrollaron los 63 procedimientos incluidos en MAIGTI. Luego en el segundo trimestre del 2006, los procedimientos

desarrollados se aplicaron a la auditoría de la gestión de tecnología de información en 2 empresas de seguros. Los tiempos se cumplieron conforme a lo previsto (3 meses).

B. Durante la ejecución de los procedimientos, se fueron identificando una serie de errores en redacción y formato. Asimismo, se fueron identificando algunos elementos que hacían falta en las listas de verificación, principalmente en lo referente al Plan de Seguridad de la Información.

C. Luego de la ejecución de los procedimientos en las 2 empresas de seguros (durante el segundo trimestre del 2006), se tomó nota de los hallazgos y se agregó a las secciones de hallazgos posibles.

D. Durante el tercer trimestre del 2006, se fueron complementando los aspectos relacionados al Plan de Seguridad de la Información (aspectos de seguridad lógica y física), con la información gratuita publicada en el sitio web de ISACA (ISACA, 2006).

E. Durante el cuarto trimestre del 2006 se corrigió la redacción, formato y sección de hallazgos posibles, de todos los procedimientos incluidos en MAIGTI.

F. Durante los años 2007 y 2008, se siguió mejorando la redacción de los procedimientos y las secciones de hallazgos posibles, considerando los hallazgos encontrados en otras auditorías realizadas por el autor de la tesis en las 2 empresas de seguros y en las otras 6 entidades indicadas al inicio de esta sección.

4.2. ANÁLISIS DE RESULTADOS

Como resultado de la experiencia de la aplicación de MAIGTI, se deduce que es aplicable a cualquier tipo de organización usuaria de tecnologías de información, ya sea grande, mediana, o pequeña, en cualquier sector económico. MAIGTI no ha sido probada en organizaciones proveedoras de servicios informáticos como: empresas proveedoras de outsourcing integral de la gestión informática, empresas

proveedoras de servicios de aplicaciones (Application Services Providers), empresas de desarrollo de software, etc.

Los resultados de la aplicación de la metodología fueron los siguientes:

A. Se identificaron los diversos problemas y sus causas, de manera integral.
B. Se identificaron los riesgos potenciales y se cuantificó su impacto.
C. Se pudo hacer un diagnóstico preciso de la realidad y recomendaciones concretas para mejorar la gestión informática de ambas organizaciones.
D. Se pudo contribuir a la mejora de los resultados financieros de ambas empresas, dado que se contribuyó a la solución de problemas en procesos y proyectos críticos que tenían impacto en clientes externos y clientes internos.

5. OBSERVACIONES, CONCLUSIONES Y RECOMENDACIONES

5.1. OBSERVACIONES

Las observaciones principales a la metodología se muestran a continuación:

A. Es vital que se realice un trabajo muy intenso para que se pueda convencer a las organizaciones para la adopción de MAIGTI, dado que comúnmente las organizaciones no tienen una gestión de tecnología de información alineada a estándares internacionales.

B. La aplicación de la metodología podría convertirnos a los auditores informáticos en personas mucho menos populares, dado que al inicio debido a la inadecuada cultura de calidad de muchas organizaciones en países en vías de desarrollo, podrían tomar las observaciones como si se tratara de un tema personal, teniendo en cuenta además, que al resto de áreas de la organización no se les evalúa con el mismo rigor.

C. Se requiere personal muy capacitado (con experiencia gerencial en los diversos tipos de procesos o proyectos de tecnología de información, o por lo menos con

experiencia en la ejecución de los mismos y con conocimiento de sistemas de gestión de calidad) para aplicar la metodología. Si no se consigue el personal correcto, podría caerse en subjetividades que distorsionarían los objetivos y los posibles beneficios de la aplicación de la metodología.

D. Difícilmente las áreas de Informática auditadas van a querer aceptar que se les califique con un sistema de evaluación más riguroso; sin embargo, en el caso de las áreas de Informática, es vital que esto se realice dado que integra las diversas operaciones del negocio, y si no se mejora significativamente su gestión, no se podrían lograr los objetivos organizacionales en el largo plazo.

5.2. CONCLUSIONES

Las conclusiones de la presente tesis son las siguientes:

A. Se ha logrado una metodología para la auditoría integral de la gestión de tecnología de información con las siguientes características:

   a) Tiene en cuenta los principales objetivos de control de los estándares internacionales para la gestión de tecnología de información: COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000, así como el estándar internacional para la gestión de proyectos (PMBOK) y el estándar de ISO para los procesos de auditoría (ISO 19011).
   b) Está basada en un enfoque de procesos.
   c) Evalúa el ciclo de Calidad de la Gestión: Planificar, Hacer, Evaluar y Actuar (Ciclo de Deming: Plan, Do, Check, Act).

B. La decisión de aplicar estándares internacionales de calidad para la auditoría de la gestión de tecnología de información, puede partir del área de Auditoría Interna, y no necesariamente de la Gerencia General o el Directorio. Por ello es muy importante tener personal de auditoría muy competente para ayudar al logro de los objetivos organizacionales.

5.3. RECOMENDACIONES PARA TRABAJOS FUTUROS

Las siguientes son las recomendaciones para trabajos futuros relacionados con la metodología:

A. Se debe mantener una conducta y lenguajes muy alturados y sobre todo, tener mucho cuidado en no fallar en la aplicación de la metodología, para poder obtener el respeto de las áreas auditadas y sean menos reacias a su aceptación.

B. MAIGTI deberá complementarse cada vez que se cambien los procesos de la gestión informática debido a las mejoras en la tecnología: protocolos de seguridad en transacciones electrónicas, herramientas de seguridad de la información, mayor preponderancia de aplicaciones en equipos móviles, certificaciones de calidad internacionales relacionadas a la gestión informática, etc.; sin embargo, la estructura se mantendría sin cambios sustanciales.

C. Un posible siguiente paso, sería validar la metodología propuesta (mejorarla o desarrollar una nueva) para empresas proveedoras de servicios informáticos: empresas proveedoras de outsourcing integral de la gestión informática, empresas proveedoras de servicios de aplicaciones (Application Services Providers), empresas de desarrollo de software, etc.

BIBLIOGRAFÍA

A. Alexander A. (2007). *Diseño de un Sistema de Gestión de Seguridad de la Información: Óptica ISO/IEC 27001:2005*. Bogotá: Alfa Omega Colombiana.

B. Alfaro E. A. (2007). *Los ERPs ¿Generan o Destruyen Valor?*. Trujillo: Universidad César Vallejo – Congreso Internacional de Ingeniería de Sistemas.

C. Alfaro, E. A. (2008). *Avance en la Implementación de las Normas Técnicas Peruanas de Gestión de Tecnología de Información*. Congreso Internacional Sudamericano de Ingeniería de Sistemas, Computación e Informática XII: Arequipa.

D. Andreu, R.; Ricart, J.; & Valor, J. (1991). *Estrategia y Sistemas de Información* (1st ed.). USA: McGraw Hill.

E. Chatterjee P. (1991). ULSI: market opportunities and manufacturing challenges, Digest. IEEE International Election Device Meeting, pag. 117.

F. Contraloría General de la República (1998). *Normas de Control Interno para el Sector Público* (1st ed.). Lima: Contraloría General de la República.

G. Contraloría General de la República (2006). *Normas de Control Interno*. Lima: Contraloría General de la República.

H. David, F. (2000). *Strategic Management: Concepts and Cases* (8va ed.). USA: McGraw Hill.

I. Haag, S.; Cummings, M.; & Dawkins J. (2000). *Management Information Systems for the Information Age* (1st ed.). USA: McGraw-Hill.

J. Huber, G. P. (1990). A theory of effects of advanced information technologies on organizational design, intelligence and decision making. *Academy of Management Review*, 15, pag. 47-71.

K. IEEE (1998). IEEE Standard for Software Project Management Plans. New York: IEEE.

L. INDECOPI (2004). *TECNOLOGÍA DE LA INFORMACIÓN Procesos del Ciclo de Vida del Software* (1st ed.). Lima: Comité de Reglamentos Técnicos y Comerciales de INDECOPI.

M. INDECOPI (2006). *TECNOLOGÍA DE LA INFORMACIÓN Procesos del Ciclo de Vida del Software* (2nd ed.). Lima: Comité de Reglamentos Técnicos y Comerciales de INDECOPI.

N. INDECOPI (2004). *TECNOLOGÍA DE LA INFORMACIÓN Código de Buenas Prácticas para la Gestión de la Seguridad de la Información* (1st ed.). Lima: Comité de Reglamentos Técnicos y Comerciales de INDECOPI.

O. INDECOPI (2007). *TECNOLOGÍA DE LA INFORMACIÓN Código de Buenas Prácticas para la Gestión de la Seguridad de la Información* (2nd ed.). Lima: Comité de Reglamentos Técnicos y Comerciales de INDECOPI.

P. Information Systems Audit and Control Association (1998). COBIT Objetivos de Control (2da ed.).

Q. ISACA (2008). Information Systems Audit and Control Association. Retrieved October 16th 2008, from: http://www.isaca.org/Template.cfm?Section=Downloads3&Template=/ContentManagement/ContentDisplay.cfm&ContentID=19227.

R. ISO (2000). ISO 9001:2000 Sistemas de Gestión de la Calidad: Requisitos (1st ed.). Suiza: ISO.

S. ISO (2002). ISO 19011:2002 Directrices para la auditoría de los sistemas de gestión de calidad y/o ambiental (1st ed.). Suiza: ISO.

T. IT Governance Institute (2006). COBIT 4.0. USA: IT Governance Institute.

U. IT Governance Institute (2008). The Val IT Framework 2.0 Extract. USA: IT Governance Institute.

V. ITIL Foundation (2008). ITIL Foundation Exam Practice. Retrieved May 9th 2008 from http://www.itsmexams.com/?gclid=CIC8jbS2q5MCFQRJFQodKi303g.

W. Jacobson, I., Booch, G., & Rumbaugh J. (2000). *El Proceso Unificado de Desarrollo de Software*. Pearson Educación: Madrid.

X. Kemmerling G. & Pondman D. (2004). Gestión de Servicios TI, una introducción a ITIL. Holanda: Van Haren Publishing.

Y. Lau T., Wong Y. H., Chan K. F., & Law M. (2001). Information Technology and the work environment – does IT change the way people interact at work?. *Human Systems Management*, 20, pag. 267-279.

Z. Laudon K. C., & Laudon J. P. (2008). *Sistemas de Información Gerencial - Administración de la Empresa Digital*. Pearson Educación: México.

AA. Morton M. S. (1988). Information Technology and Corporate Strategy. *Planning Review*, pag. 28-31.

BB. Otkaba, H.; Alquicira, C.; Su, A.; Martínez, A.; Quintanilla, G.; Ruvalcaba, M.; López, F.; Rivera, M. E.; Orozco, M. J.; Fernández, Y.; Flores, M. A. (2005). Modelo de Procesos para la Industria de Software – MoProSoft – Por niveles de capacidad de procesos Versión 1.3.

CC. Paulk M. C., Weber C. W., García S. M., Chrissis M. B., & Bush M. (1993). *Key Practices of the Capability Maturity Model Version 1.1*. CMU/SEI-93-TR-0.25.

DD. Piattini, M., & Del Peso, E. (1998). *Auditoría Informática - Un Enfoque Práctico*. Alfaomega: Bogotá.

EE. Pressman, R. S. (1998). *Ingeniería de Software - Un enfoque práctico*. McGraw-Hill: Madrid.

FF. PROCOBRE (2005). Mallas de Tierra. Accedido: 20 de Diciembre del 2005, de: http://www.procobre.org/archivos/peru/mallas_detierra_en_edificaciones.pdf.

GG. Project Management Institute. (2004). *Guía de los Fundamentos de la Dirección de Proyectos* (3th ed.). Pennsylvania: PMI Publications.

HH. Rubinstein, D. (2007). Standish Group Report: Three's Less Development Chaos Today. Software Development Times, 169(1), 1.

II. Superintendencia de Banca y Seguros (2002). Circular Nº G-105-2002/SBS Riesgos de Tecnologías de Información (1st ed.). Lima: Superintendencia de Banca y Seguros.

JJ. Turban, E., King, D., Lee, J., Warketin, M., & Chung, H. M. (2002). Electronic Commerce 2002 A Managerial Perspective (2da. ed.). USA: Prentice Hall.

ANEXO 1 – PROCEDIMIENTOS DE LA METODOLOGÍA PARA LA AUDITORÍA INTEGRAL DE LA GESTIÓN INFORMÁTICA

A continuación se detallan los procedimientos que están comprendidos como parte de la metodología para la auditoría integral de la gestión informática propuesta en el presente documento:

- P002: Procedimiento para la auditoría de la Planificación Estratégica.
- P003: Procedimiento para la auditoría de los Planes Operativos.
- P004: Procedimiento para la auditoría de la Evaluación de Riesgos.
- P005: Procedimiento para la auditoría de la Planificación Estratégica de Tecnologías de Información.
- P006: Procedimiento para la auditoría de los Planes de Proyecto de Desarrollo de Sistemas de Información.
- P007: Procedimiento para la auditoría de los Planes de Proyecto de Compra de Sistemas de Información.
- P008: Procedimiento para la auditoría del Plan de Contingencias de Informática.
- P009: Procedimiento para la auditoría del Plan de Continuidad de Negocio.
- P010: Procedimiento para la auditoría del Plan de Seguridad de la Información.
- P011: Procedimiento para la auditoría del Plan de Licenciamiento de Software.
- P012: Procedimiento para la auditoría del Plan de Capacitación.
- P013: Procedimiento para la auditoría del Plan de Mantenimiento Preventivo de Hardware de Computadoras, Redes y Equipos Relacionados.
- P014: Procedimiento para la auditoría del Plan de Mantenimiento Correctivo de Hardware de Computadoras, Redes y Equipos Relacionados.
- P015: Procedimiento para la auditoría de la Planificación de Labores de Rutina relacionadas con las Tecnologías de Información.
- P016: Procedimiento para la auditoría del Plan de Calidad.
- P017: Procedimiento para la auditoría del Plan de Compras de Tecnologías de Información.
- P018: Procedimiento para la auditoría del Reglamento de Organización y Funciones.
- P019: Procedimiento para la auditoría del Manual de Organización y Funciones.
- P020: Procedimiento para la Evaluación del Currículum Vitae del personal de Tecnología de Información.
- P021: Procedimiento para la auditoría del Inventario de Hardware de Tecnología de Información.
- P022: Procedimiento para la auditoría del Inventario de Software de Base.
- P023: Procedimiento para la auditoría del Inventario de Sistemas de Información.
- P024: Procedimiento para la auditoría de las Solicitudes y Evaluaciones de Cotizaciones para las compras de hardware de computadoras, redes y equipos relacionados.
- P025: Procedimiento para la auditoría de las Solicitudes y Evaluaciones de Cotizaciones para las compras de software de base.
- P026: Procedimiento para la auditoría de las Solicitudes y Evaluaciones de Cotizaciones para las compras de sistemas de información.
- P027: Procedimiento para la auditoría de los contratos de compra de bienes y servicios, de hardware de computadoras, redes y equipos relacionados.
- P028: Procedimiento para la auditoría de los contratos para la compra de software de base.

- P029: Procedimiento para la auditoría de los contratos para la compra de sistemas de información.
- P030: Procedimiento para la auditoría de los contratos de seguros para las tecnologías de información.
- P031: Procedimiento para la auditoría de la metodología de desarrollo de sistemas de información.
- P032: Procedimiento para la auditoría de la metodología para la atención de requerimientos de soporte técnico.
- P033: Procedimiento para la auditoría de la metodología para la atención de requerimientos de desarrollo de sistemas de información.
- P034: Procedimiento para la auditoría de la documentación de los manuales técnicos de los sistemas de información.
- P035: Procedimiento para la auditoría de la documentación de los manuales de usuario de los sistemas de información.
- P036: Procedimiento para la auditoría de la arquitectura de la red de tecnologías de información.
- P037: Procedimiento para la auditoría de la seguridad de acceso a los sistemas de información.
- P038: Procedimiento para la auditoría de la seguridad de acceso a las carpetas en los servidores.
- P039: Procedimiento para la auditoría de los manuales de procedimientos de soporte técnico.
- P040: Procedimiento para la auditoría de los manuales de procedimientos de desarrollo de sistemas de información.
- P041: Procedimiento para la Revisión de los Formularios de Control de Entregables de Proyectos y Requerimientos de Desarrollo de Sistemas de Información.
- P042: Procedimiento para el Seguimiento de Informes de Auditoría Interna.
- P043: Procedimiento para el Seguimiento de Informes de Auditoría Externa.
- P044: Procedimiento para la auditoría de las Certificaciones de Calidad de Tecnología de Información.
- P045: Procedimiento para la auditoría de la Evaluación de Desempeño del Área de Tecnología de Información.
- P046: Procedimiento para la auditoría de la Evaluación de Desempeño del Personal de Tecnología de Información.
- P047: Procedimiento para la Revisión de los Formularios de Control de Cambios en Proyectos de Compra o Desarrollo de Sistemas de Información.
- P048: Procedimiento para la Revisión de los Formularios de Control de Riesgos en Proyectos de Compra o Desarrollo de Sistemas de Información.
- P049: Procedimiento para la Revisión de los Formularios de Seguimiento de Avances en Proyectos de Compra o Desarrollo de Sistemas de Información.
- P050: Procedimiento para la auditoría del Control de Calidad de los Requerimientos de Compra o Desarrollo de Sistemas de Información.
- P051: Procedimiento para la auditoría del Control de Calidad de los Requerimientos de Soporte Técnico.
- P052: Procedimiento para Entrevistar a los usuarios de Tecnologías de Información.
- P053: Procedimiento para la auditoría de las Instalaciones Eléctricas de los Equipos de Cómputo y Redes.
- P054: Procedimiento para la auditoría de la Seguridad de Acceso al Centro de Cómputo Principal.
- P055: Procedimiento para la auditoría de las Instalaciones del Centro de Cómputo Principal.
- P056: Procedimiento para la auditoría de la Seguridad de Acceso al Centro de Cómputo Alterno.

- P057: Procedimiento para la auditoría de las Instalaciones del Centro de Cómputo Alterno.
- P058: Procedimiento para la auditoría del Cableado de Redes de Datos.
- P059: Procedimiento para la auditoría del Cálculo de la Generación de Valor de los Proyectos.
- P060: Procedimiento para la Elaboración del Informe Preliminar.
- P061: Procedimiento para el Envío, Sustentación y Corrección del Informe Final.
- P062: Procedimiento para la Elaboración del Plan de Trabajo de la Auditoría.
- P063: Procedimiento para la Medición de la Resistencia de la Puesta a Tierra.

P002: PROCEDIMIENTO PARA LA AUDITORÍA DE LA PLANIFICACIÓN ESTRATÉGICA

OBJETIVO

Analizar y evaluar el proceso de Planificación Estratégica de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión del proceso de Conformación del Equipo de la Planificación Estratégica.
B. Revisión del proceso de Selección de la Metodología para la Planificación Estratégica.
C. Revisión del Aprendizaje de la Metodología para la Planificación Estratégica.
D. Revisión del proyecto de Elaboración del Plan Estratégico.
E. Revisión del proceso de planificación del Proyecto de Elaboración del Plan Estratégico.
F. Análisis y evaluación de la ejecución del Proyecto de Elaboración del Plan Estratégico.
G. Revisión de la ejecución del Plan Estratégico.
H. Revisión del proceso de evaluación del Plan Estratégico.

El alcance del procedimiento no incluye:

A. Evaluación de los planes operativos de la organización.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Lista de personas que participan o han participado en el proceso de Planificación Estratégica con sus respectivos teléfonos, anexos y correos para contactarlos.
B. Presupuesto de Ingresos y Egresos.

C. Estados Financieros.
D. Metodología para la Planificación Estratégica.
E. Plan Estratégico de la Organización.
F. Plan Estratégico de cada una de las áreas.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el proceso de Conformación del Equipo de la Planificación Estratégica. Verificar que el equipo esté conformado por personal de todas las gerencias, tanto los gerentes de línea como los gerentes intermedios, así como personal sin rango gerencial directamente involucrado en procesos con el cliente o en procesos con los proveedores.

C. Revisar el proceso de Selección de la Metodología para la Planificación Estratégica. Verificar lo siguiente:

   a) La metodología a utilizar debe ajustarse a las necesidades de la organización. Por ejemplo, usar metodologías que en realidad son modelos matemáticos que son aplicables a realidades diferentes a la nuestra, no sería una elección adecuada.
   b) La metodología a emplear debe permitir que la organización identifique sus problemas, proponga los cambios a futuro y administre cómo hacerlos en la práctica.
   c) La metodología a utilizar debe incluir la participación de personal operativo de diversas áreas, además de los gerentes.

D. Revisar el Aprendizaje de la Metodología para la Planificación Estratégica elegida. Verificar lo siguiente:

   a) El equipo de Planificación Estratégica de la organización, debe tener aprendida la metodología de Planificación Estratégica seleccionada antes de comenzar con el proyecto de Elaboración del Plan Estratégico.
   b) Si el equipo de Planificación Estratégica está conformado también por personal de una empresa proveedora, debe tener las competencias necesarias para dirigir o colaborar con la organización en dicho proceso. Para ello se deberá hacer la evaluación respectiva.

E. Revisar el proyecto de Elaboración del Plan Estratégico.

F. Revisar el proceso de planificación del Proyecto de Elaboración del Plan Estratégico. Verificar lo siguiente:
   a) Que los horarios para el desarrollo de las actividades del proyecto permitan que esté el mayor número de personas.
   b) Que el diagrama de Gantt inicial del proyecto incluya todas y cada una de las etapas formales de la metodología elegida.
   c) Que el diagrama de Gantt inicial del proyecto incluya la elaboración de los planes para cada una de las áreas funcionales de la organización resultante al final del proceso de planificación estratégica.

G. Analizar y evaluar la ejecución del Proyecto de Elaboración del Plan Estratégico. Verificar lo siguiente:

a) Las actas de reuniones del proyecto.
b) Resultado de cada reunión para la elaboración del Plan Estratégico.
c) Diagramas de Gantt con todos los cambios.
d) Elaboración de Planes Estratégicos para cada una de las áreas.
e) Determinación de indicadores de gestión para la organización en su conjunto.
f) Determinación de indicadores de gestión para cada una de las áreas, de manera alineada con los indicadores de la organización en su conjunto.
g) Elaboración de procesos para la evaluación de la estrategia.

H. Revisar la ejecución del Plan Estratégico. Verificar que las actividades desarrolladas por la organización se ajusten a los procesos estratégicos delineados por el Plan Estratégico.

I. Revisar el proceso de evaluación del Plan Estratégico. Verificar que se esté ejecutando el proceso de evaluación y las actas en que conste las decisiones que se haya tomado para corregir las desviaciones de lo planificado, o en su defecto, las evidencias que demuestran que sí se tomaron acciones correctivas.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un Plan Estratégico.

B. El Plan Estratégico es de conocimiento sólo del dueño, presidente del directorio o gerente general, y se va soltando por pequeñas partes la información para que las áreas realicen sus planes. No se llega a entregar o decir verbalmente el Plan Estratégico por temor a que lo sepa la competencia o porque no se ha dedicado el tiempo para documentarlo o estructurarlo correctamente.

C. El Plan Estratégico es encargado a una empresa proveedora y es un documento que sólo sirve para cumplir con tenerlo y evitar que auditoría observe que no se tiene.

D. El Plan Estratégico es un conjunto de ideas sueltas que no integran las labores de las diversas áreas de manera armoniosa.

E. El Plan Estratégico es un conjunto de ideas sueltas que no sirven de mucho para estructurar los planes operativos.

F. El proceso de Planificación Estratégica demora demasiado. Incluso en organizaciones grandes, este proceso no debería demorar más de 4 meses.

G. Los procesos y proyectos descritos en el Plan Estratégico carecen de un análisis de generación de valor.

P003: PROCEDIMIENTO PARA LA AUDITORÍA DE LOS PLANES OPERATIVOS

OBJETIVO

Analizar y evaluar el proceso de elaboración de los planes operativos de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión del proceso de conformación del equipo en cada área para la elaboración de los planes operativos.

B. Verificación de los planes operativos, para saber si están alineados al plan estratégico de la organización.

C. Verificación de los planes operativos, para saber si incluyen todos los procesos y proyectos principales de cada área de la organización.

D. Verificación del establecimiento de presupuestos y cronogramas claros para cada uno de los proyectos que se van a ejecutar.

El alcance del procedimiento no incluye:

A. Evaluación detallada de cada una de las actividades de cada uno de los proyectos planteados.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Lista de personas que participan o han participado en el proceso de elaboración de planes operativos con sus respectivos teléfonos, anexos y correos para contactarlos.
B. Presupuesto de Ingresos y Egresos.
C. Estados Financieros.
D. Plan Estratégico de la Organización.
E. Plan Estratégico de cada una de las áreas.
F. Metodología para la Planificación Operativa.
G. Plan Operativo.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el proceso de conformación de los equipos para la elaboración de los planes operativos. Verificar que el equipo incluya el personal clave de cada gerencia, tanto los gerentes principales como los gerentes intermedios.

C. Verificar que los planes operativos estén alineados al plan estratégico de la organización. Para ello se debe verificar que cada uno de los procesos o actividades principales ayuden ya sea de manera directa o indirecta al logro de los planes estratégicos. Si no se alinean, habrá que observarlos en ese sentido.

D. Verificar que se haya cumplido la metodología establecida por la organización para la elaboración de planes operativos.

E. Verificar que los planes operativos incluyan todos los procesos y proyectos principales de cada área de la organización. Esta parte indica procesos de seguros; sin embargo, dependiendo de cada organización, habría que reemplazar los procesos por los que correspondan:

   a) Planeamiento.
      - Elaboración del Plan Estratégico.
      - Evaluación del Plan Estratégico.
      - Elaboración del Presupuesto.
      - Seguimiento al Presupuesto.

   b) Organización y Métodos
      - Elaboración de organigramas.
      - Elaboración de políticas.
      - Elaboración de los manuales de procedimientos.

   c) Marketing.
      - Investigación de Mercados.
      - Servicio al Cliente.
        - Atención de consultas.
        - Atención de Reclamos.
      - Publicidad
      - Promociones.

   d) Ventas.
      - Canales de Distribución.
      - Bonos e Incentivos.
      - Comisiones.

   e) Operaciones de Seguros.
      - Primas Directas
        - Suscripción de Primas Directas.
        - Emisión de Coberturas Provisionales.
        - Inspección por solicitudes de primas directas.
        - Emisión de Primas Directas.

- Aprobación de Primas Directas.
- Distribución de Documentos de Primas Directas.

- Coaseguros Cedidos / Primas
  - Aceptación de Coaseguros Cedidos.
  - Generación de la Nota Técnica o Planilla de Cesión.

- Coaseguros Recibidos / Primas
  - Aceptación de Coaseguros Recibidos.
  - Generación de la Nota Técnica o Planilla de Cesión.

- Reaseguro de Primas.
  - Generación de contratos de reaseguros.
    - Generación de contratos proporcionales.
    - Generación de contratos no proporcionales.
  - Generación de la Nota Técnica o Planilla de Cesión.

- Siniestros Directos.
  - Recepción de la denuncia del siniestro.
  - Inspección o ajuste.
  - Recepción de los documentos de inspección.
  - Provisión de la reserva por el siniestro.
  - Contabilización de la provisión de la reserva por el siniestro.
  - Liquidación de Siniestros Directos.
  - Contabilización de la Liquidación de Siniestros Directos.
  - Pago de Siniestros Directos.
  - Contabilización del Pago de Siniestros Directos.

- Coaseguros Cedidos / Siniestros
  - Generación de la Planilla de Siniestros.
  - Pago de Siniestros de Coaseguros Cedidos.
  - Generación de la Nota Técnica o Planilla de Cesión.

- Coaseguros Recibidos / Siniestros.
  - Generación de la planilla de siniestros de coaseguros recibidos.
  - Generación de la Nota Técnica o Planilla de Cesión.

- Reaseguro de Siniestros.
  - Evaluación de la Calidad de los Reaseguradores.
  - Cumplimiento de la política de reaseguros de la empresa.
  - Cumplimiento de las normas de contratación de reaseguradores.
  - Generación de la planilla de siniestros.
  - Generación de la Nota Técnica o Planilla de Cesión.
  - Presentación de Información.

- Constitución de Reservas Técnicas.
  - Constitución de Reservas Técnicas de Primas.
  - Constitución de Reservas Técnicas de Siniestros.

- Constitución del Patrimonio de Solvencia.

- Constitución del Fondo de Garantía.

f) Inversiones.
- Cumplimiento del Plan de Inversiones.

- Cumplimiento del Reglamento de Inversiones Elegibles.
- Cobertura de Oligaciones Técnicas.
- Valorización de Inversiones.
- Registro contable de las inversiones.
- Constitución de provisiones.
- Presentación de Información.
  - Presentación de Información a la gerencia general.
  - Presentación de Información al directorio.
  - Presentación de Información a la SBS.
  - Presentación de Información a CONASEV.

g) Recursos Humanos.
- Reclutamiento.
- Selección.
- Contratación.
- Capacitación.
- Evaluación de Desempeño.
- Compensaciones.
- Asistencia Social.

h) Administración y Finanzas.

- Compras.
  - Solicitud de cotizaciones a proveedores.
  - Evaluación de cotizaciones de proveedores.
  - Determinación de la cotización ganadora.
  - Solicitudes de compra.
  - Aprobaciones de las solicitudes de compra.
  - Generación de órdenes de compra.
- Tesorería.
  - Caja.
  - Bancos.
  - Cobranzas.
    - Elaboración de la Política de Cobranzas.
    - Zonificación.
    - Custodia.
    - Distribución.
    - Generación de la planilla de primas por cobrar bajo régimen general.
    - Registro contable de la planilla de primas por cobrar bajo régimen general.
    - Liquidación de Cobranzas.
    - Resolución del contrato de seguros por falta de pago.
  - Pagos.
    - Elaboración de Planillas de Pagos.
    - Pagos a brokers.
    - Pagos a coaseguradores.
    - Pagos a reaseguradores.
    - Pagos a proveedores.
    - Pagos a personal.
    - Pagos de impuestos y contribuciones.
- Contabilidad.
  - Elaboración de Modelos de Asientos Contables.
  - Registro de Transacciones.
  - Cálculo de Impuestos y Contribuciones.

- Arqueo de Fondo Fijo y Caja Princiipal a nivel nacional.
- Generación de libros contables.
- Generación de estados financieros.
- Presentación de Información.
  - Presentación de Información a la Gerencia General.
  - Presentación de Información al Directorio.
  - Presentación de Información a CONASEV.
  - Presentación de Información a la SBS.

- Archivo.
- Mantenimiento.
- Almacén.
- Vigilancia.

i) Asesoría Legal.

j) Tecnología de la Información
- Desarrollo de Sistemas.
- Infraestructura de Tecnología de Información.

F. Verificar que se haya elaborado presupuestos y cronogramas claros para cada uno de los proyectos y procesos que se van a ejecutar. Debe incluirse tanto presupuestos de ingresos como presupuesto de egresos además de cronogramas de ejecución de las actividades de los proyectos que se van a desarrollar con su respectiva asignación de responsabilidades. En el caso de los procesos se debe detallar la organización del trabajo y los horarios en los cuáles se van a desarrollar las actividades con su respectiva asignación de responsabilidades.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene planes operativos.

B. Los planes operativos se van haciendo en el transcurso del tiempo de ejecución de la estrategia.

C. Los planes operativos son muy cortos. No se detallan los procesos y actividades a realizar para lograr los objetivos de los planes estratégicos.

D. Los planes operativos no detallan los presupuestos de ingresos y egresos, ni los cronogramas de ejecución con su respectiva asignación de responsabilidades.

E. Los planes operativos carecen de un análisis de generación de valor de los proyectos y procesos involucrados.

F. Los planes operativos se desarrollan sólo para el corto plazo, sin considerar el mediano y largo plazo.

P004: PROCEDIMIENTO PARA LA AUDITORÍA DE LA EVALUACIÓN DE RIESGOS

OBJETIVO

Analizar y evaluar el proceso de evaluación de riesgos de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión del proceso de conformación de los equipos para la evaluación de riesgos.

B. Revisión de la metodología para la evaluación de riesgos.

C. Revisión de los documentos resultado de la evaluación de riesgos.

D. Revisión de las respuestas de las gerencias para evitar o minimizar los riesgos identificados.

E. Verificación de cronogramas y asignación de recursos y responsabilidades en las diversas gerencias, para evitar o minimizar los riesgos, de acuerdo al punto anterior.

El alcance del procedimiento no incluye:

A. Evaluación de errores pasados que no tengan consecuencias futuras.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Lista de personas que participan o han participado en el proceso de evaluación de riesgos con sus respectivos teléfonos, anexos y correos para contactarlos.
B. Plan Estratégico de la Organización.
C. Plan Estratégico de cada una de las áreas.
D. Plan Operativo de cada una de las áreas.
E. Metodología para la Evaluación de Riesgos.
F. Documento de Evaluación de Riesgos.
G. Respuestas de las gerencias ante la evaluación de riesgos.
H. Cronogramas y asignación de recursos y responsabilidades.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el proceso de conformación de los equipos para la evaluación de riesgos. Se deberá tener tanto un equipo correspondiente a la Unidad de Riesgos, un equipo correspondiente al proveedor (en caso que sea una empresa consultora la que realice la evaluación de riesgos) y un equipo o persona correspondiente a cada una de las gerencias de la organización. Verificar que los equipos incluyan a personal clave de cada gerencia, tanto los gerentes principales como los gerentes intermedios.

C. Verificar que se haya cumplido la metodología establecida por la organización para la evaluación de riesgos.

D. Verificar que el resultado de la evaluación de riesgos, incluya los riesgos que se ha podido identificar en el área de Auditoría Interna, además de los riesgos siguientes:

   a) Riesgos de mercado.
   b) Riesgos legales.
   c) Riesgos de liquidez.
   d) Riesgos de operación.
   e) Riesgos de crédito.
   f) Riesgos de reputación o imagen.
   g) Riesgos de lavado de activos.
   h) Riesgos ambientales.
   i) Riesgo estratégico, etc.

   Por cada riesgo identificado se debe especificar por lo menos cualitativamente (si se puede es mejor hacerlo cuantitativamente) lo siguiente:

   a) Probabilidades de ocurrencia (alta, media, baja ó numéricamente).
   b) Impacto (Costos de no protegernos contra ese riesgo).
   c) Costos de protegernos contra ese riesgo.

E. Verificar que se haya elaborado presupuestos y cronogramas claros para cada uno de los proyectos y procesos que se van a ejecutar, luego de la evaluación de riesgos. Debe incluirse tanto presupuestos de ingresos como presupuesto de egresos además de cronogramas de ejecución de las actividades de los proyectos que se van a desarrollar con su respectiva asignación de responsabilidades. En el caso de los procesos se debe detallar la organización del trabajo y los horarios en los cuales se van a desarrollar las actividades con su respectiva asignación de responsabilidades.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no realiza evaluaciones de riesgos.

B. Las evaluaciones de riesgos son encargadas a una empresa consultora que entrega un documento netamente académico modificado para la empresa.

C. Las evaluaciones de riesgos no se realizan de manera estricta y sólo sirven para que el organismo regulador no emita sanciones.

P005: PROCEDIMIENTO PARA LA AUDITORÍA DE LA PLANIFICACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar el proceso de elaboración del Plan Estratégico de Tecnologías de información[1] de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión del proceso de conformación del Comité de Tecnología de información[2].

B. Verificación de la alineación del PETI al plan estratégico de la organización.

C. Verificación de la determinación de presupuesto, cronogramas y responsabilidades de ejecución de los procesos y proyectos del PETI.

D. Verificación de la existencia del Análisis de Generación de Valor de cada uno de los proyectos del PETI, así como el PETI en su conjunto.

E. Verificación de la existencia de indicadores de gestión y procesos de evaluación de la estrategia del PETI, alineados a la evaluación de la estrategia global de la organización.

El alcance del procedimiento no incluye:

A. Evaluación detallada de cada una de las actividades de cada uno de los proyectos planteados.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

[1] En adelante se le llamará PETI al Plan Estratégico de Tecnologías de información.
[2] En adelante se le llamará CTI al Comité de Tecnología de información.

A. Lista de personas que participan o han participado en el Comité de Tecnologías de información con sus respectivos teléfonos, anexos y correos para contactarlos.
B. Actas de reuniones del Comité de Tecnología de información.
C. Presupuesto del PETI.
D. Valorización de activos fijos e intangibles relacionados con las tecnologías de información.
E. Plan Estratégico de la Organización.
F. Plan Estratégico de cada una de las áreas.
G. PETI.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el proceso de conformación del CTI[3]. Verificar que el equipo incluya el personal clave de cada gerencia, tanto los gerentes principales como los gerentes intermedios.

C. Verificar que los PETIs estén alineados al plan estratégico de la organización. Para ello se debe verificar que cada uno de los procesos o actividades principales ayuden ya sea de manera directa o indirecta al logro de los planes estratégicos. Si no se alinean, habrá que observarlos en ese sentido. Por ejemplo, no contribuye al logro de los objetivos organizacionales enfocarse en detalles no urgentes relativos a sistemas contables cuando las operaciones no son llevadas adecuadamente y de acuerdo al plan estratégico se debe incrementar la velocidad de la atención al cliente.

D. Verificar que se haya elaborado presupuestos y cronogramas claros para cada uno de los proyectos y procesos que se van a ejecutar en el PETI. Debe incluirse tanto presupuestos, cronogramas de ejecución de las actividades de los proyectos que se van a desarrollar con su respectiva asignación de responsabilidades. En el caso de los procesos se debe detallar la organización del trabajo y los horarios en los cuáles se van a desarrollar las actividades con su respectiva asignación de responsabilidades.

E. Verificación de la existencia del Análisis de Generación de Valor de cada uno de los proyectos del PETI, así como el PETI en su conjunto. El análisis de generación de valor de los proyectos debe someterse al cálculo del valor presente neto a una tasa mínima atractiva de retorno para un flujo neto en un período de evaluación que debe determinarlo el directorio, la gerencia general o ser igual período de evaluación del plan estratégico. La tasa mínima atractiva de retorno debe ser determinada por el directorio o la gerencia general. El valor presente neto debe ser una cantidad positiva y atractiva para la organización. Ver procedimiento P059, en el cual se detalla el cálculo de la generación de valor de los proyectos. La generación de valor del PETI se calculará como la suma del valor presente neto de cada uno de los proyectos.

[3] El CTI es la entidad que debe desarrollar el PETI.

F. Verificación de la existencia de indicadores de gestión y procesos de evaluación de la estrategia del PETI, alineados a los indicadores de gestión para la evaluación de la estrategia global de la organización.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un PETI.

B. Los PETIs se van haciendo en el transcurso del tiempo.

C. Los PETIs son documentos muy cortos. No se detallan los procesos y actividades a realizar para lograr los objetivos de los planes estratégicos.

D. Los PETIs no detallan los presupuestos de ingresos y egresos, ni los cronogramas de ejecución con su respectiva asignación de responsabilidades.

E. Los PETIs carecen de un análisis de generación de valor de los proyectos y procesos involucrados.

F. Los PETIs se desarrollan sólo para el corto plazo, sin considerar el mediano y largo plazo.

P006: PROCEDIMIENTO PARA LA AUDITORÍA DE LOS PLANES DE PROYECTO DE DESARROLLO DE SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar el proceso de elaboración de planes de proyecto de desarrollo de sistemas de información en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión del proceso de conformación del Comité de Usuarios y el Líder de Usuarios, para el proyecto de desarrollo de un sistema de información.

B. Verificación de la alineación del proyecto al PETI y al Plan Estratégico de la organización.

C. Verificación de la existencia del Análisis de Generación de Valor del proyecto.

D. Verificación de la asignación de presupuesto, cronogramas y responsabilidades de ejecución de los proyectos.

E. Verificación de la existencia de indicadores de gestión para la planificación del proyecto.

F. Revisión de la inclusión de actividades formales del ciclo de vida de desarrollo de sistemas en la planificación del proyecto:

El alcance del procedimiento no incluye:

A. Verificación de procesos en proyectos de compra de sistemas de información.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Lista de personas que participan o han participado en la planificación del proyecto de desarrollo del sistema de información con sus respectivos teléfonos, anexos y correos para contactarlos.
B. Plan Estratégico de la Organización.
C. Plan Estratégico de Tecnologías de información.
D. Análisis de Generación de Valor del Proyecto.
E. Comité de Usuarios del Proyecto.
F. Actas de reuniones del Jefe de Proyecto con el Líder de Usuarios.
G. Especificaciones Funcionales y Técnicas del Proyecto.
H. Planes del Proyecto: Plan de Gestión de la Integración, Plan de Gestión del Alcance, Plan de Gestión del Tiempo, Plan de Gestión de los Costos, Plan de Gestión de la Calidad, Plan de Gestión de Recursos Humanos, Plan de Gestión de las Comunicaciones, Plan de Gestión de Riesgos, y Plan de Gestión de las Adquisiciones.
I. Formatos de Control de Cambios del Proyecto.
J. Formatos de Control de Entregables del Proyecto.
K. Formatos de Control de Riesgos del Proyecto.
L. Todos los diagramas de Gantt del proyecto.
M. Presupuesto del proyecto.
N. Indicadores de Gestión del Proyecto.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el proceso de conformación del Comité de Usuarios y el nombramiento del Líder de Usuarios, para el proyecto de desarrollo del sistema de información. Verificar que en el comité de usuarios esté el personal clave que tiene relación con los procesos que serán soportados con el sistema de información. El líder de usuarios, de preferencia, debe ser una persona con rango gerencial (intermedio o de línea), que conozca los procesos que serán soportados con el sistema de información, sus interrelaciones y las interrelaciones que estos tienen con el resto de procesos de la organización.

C. Verificar la alineación del proyecto al PETI y al Plan Estratégico de la organización. El proyecto debe contribuir a la generación del valor de la organización de acuerdo a lo planteado en el PETI y el Plan Estratégico.

D. Verificar la asignación de presupuesto, cronogramas y responsabilidades de ejecución de los proyectos. Tener en cuenta:

   a) Para la verificación de las responsabilidades, se debe revisar la organización del proyecto, la cual debe tener los principios claros de unidad de mando, así como la asignación de la responsabilidad por cada etapa, proceso o módulo de sistema a desarrollar. Las responsabilidades deben estar asignadas tanto para el equipo de desarrollo como para el equipo o comité de usuarios.

   b) En los cronogramas debe aparecer el detalle de las actividades a nivel de horas. Además se debe verificar la sobreasignación de recursos; es decir, que no se crucen actividades en paralelo con la misma persona o equipo de personas. Revisar el enlace de las actividades de manera que no quede ninguna actividad sin enlazar. De esta manera se puede calcular de manera menos irreal la ruta crítica. Considerar además que se debe tener el calendario laboral con las fechas y horas reales de trabajo, además de lo planificado o replanificado.

   c) Verificar que se haya asignado un presupuesto adecuado para cada una de las etapas considerando tanto las inversiones como los gastos adicionales por el proyecto.

E. Verificar la existencia del Análisis de Generación de Valor del proyecto. Debe verificarse que exista el cálculo del valor actual neto por el proyecto. Si el valor actual neto es un número negativo o un número pequeño positivo, observar que se está desarrollando o se ha desarrollado un proyecto que no genera valor o un proyecto que no es atractivo para la organización, respectivamente.

F. Verificar la existencia de indicadores de gestión para el proyecto. Debe definirse indicadores de gestión que permitan al Jefe de Proyecto, tomar acciones correctivas en el momento adecuado. Estos indicadores de gestión deberán estar en función de tiempo, dinero (presupuesto) y nivel de cumplimiento de las especificaciones.

G. Verificar la correcta definición de los planes de gestión del proyecto que sugiere el PMBOK por cada área de conocimiento: integración, alcance, costos, tiempo, calidad, recursos humanos, comunicaciones, riesgos y adquisiciones.

H. Revisar la inclusión de actividades formales del ciclo de vida de desarrollo de sistemas de información, en la planificación del proyecto:

   a) Levantamiento de Información. Revisión de los formatos de entrevistas u otro tipo de información que sirvió de base para elaborar las especificaciones funcionales.

   b) Elaboración de Especificaciones Funcionales y Técnicas. Verificar la inclusión de las siguientes actividades:
      - Revisar el detalle de los requerimientos funcionales y técnicos del sistema de información.
      - Si un sistema de información reemplazará a uno ya existente, revisar las hojas de análisis diferencial y ver que se hayan incluido todas las funcionalidades del sistema ya existente en el nuevo.

c) Planificación.
- Revisión del enlace de las diversas actividades. No deberían quedar actividades sueltas, sin relaciones con otras actividades.
- Revisión de la correcta definición del diagrama de red e identificación de la ruta crítica (de preferencia, la cadena crítica).
- Verificar que las actividades estén definidas a nivel de horas, separando claramente qué persona o grupo de personas las realizará.

d) Capacitación. Verificar la inclusión de las siguientes actividades:
- Capacitación Funcional sobre procesos a ser soportados por el sistema de información.
- Capacitación Técnica (herramientas y lenguajes de programación, herramientas administradoras de bases de datos, configuraciones, etc.). De no estar definida, recomendar la elaboración de librerías de código fuente en esta etapa.

e) Análisis. Verificar la inclusión de las siguientes actividades:
- Análisis de cada uno de los módulos.
- Interrelaciones entre los módulos.
- Elaboración de los diversos diagramas y documentación, de acuerdo a la metodología elegida.

f) Diseño. Verificar la inclusión de las siguientes actividades:
- Elaboración del diseño de interfaces gráficas de usuario.
- Elaboración del diseño de la base de datos.
- Elaboración del diseño de la estructura de los diversos componentes del sistema de información.
- Elaboración de los diversos diagramas y documentación, de acuerdo a la metodología elegida.
- Elaboración de los diversos planes sugeridos por la ISO/IEC 12207:
  - Plan de Pruebas.
  - Plan de Gestión de la Configuración.
  - Plan de Configuración de la Infraestructura.
  - Plan de Aseguramiento de la Calidad.
  - Plan de Control de Calidad.
  - Plan de Revisión Conjunta.
  - Plan de Validación.
  - Plan de Integración del Software.
  - Plan de Instalación del Software.
  - Plan de Migración de Datos.
  - Plan de Retirada del Software.
  - Plan de Formación.
- Elaboración de Manuales Técnicos.

g) Implementación. Verificar la inclusión de las siguientes actividades:
- Elaboración de especificaciones técnicas o seudocódigos.
- Actividades de programación de cada uno de los módulos.

h) Integración y Pruebas. Verificar la inclusión de las siguientes actividades:
- Integración de las diversas aplicaciones.
- Pruebas del Sistema Completo. Estas pruebas las debe realizar tanto personal de sistemas como personal del comité de usuarios. Deben estar incluidas las siguientes pruebas (que deben pertenecer a un Plan de Pruebas):

- ❖ Pruebas de Interfase Gráfica de Usuario.
- ❖ Pruebas de Caja Negra.
- ❖ Pruebas de Caja Blanca.
- ❖ Pruebas de Integración (Ascendente y Descendente).
- ❖ Pruebas de Resistencia o Estrés.
- ❖ Pruebas de Seguridad.
- ❖ Pruebas de Pistas de Auditoría.

i) Implantación. Verificar la inclusión de las siguientes actividades:
- Elaboración de Manuales de Usuario.
- Instalación y Configuración del sistema de información.
- Migración de los datos.
- Capacitación al Usuario.

j) Operación. Verificar la inclusión de actividades de apoyo al usuario, luego que el sistema de información está implantado.

k) Mantenimiento. Verificar la inclusión de actividades de ajuste a los módulos desarrollados.

I. Verificar la inclusión de actividades formales de revisión y corrección errores al final de cada etapa descrita en el punto H.

J. Verificar la inclusión de actividades formales de documentación, por lo menos al final de cada etapa descrita en el punto H.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. No existe un comité de usuarios ni un líder de usuarios formal.

B. Los usuarios no se comprometen con el proyecto.

C. No se elaboran bien las especificaciones funcionales y técnicas del proyecto.

D. No se elaboran planes de pruebas para los proyectos de desarrollo de sistemas de información.

E. No se elaboran planes de migración de datos para los proyectos de desarrollo de sistemas de información.

F. No se elaboran planes de integración, es decir, planes para la elaboración de interfaces del sistema de información a desarrollar con los demás sistemas existentes en la organización.

G. Los planes indicados en los puntos D, E ó F se hacen de manera muy rápida, luego de la etapa de implementación, cuando el problema ya es evidente, ocasionando más problemas por información errada o inconsistente.

H. No se incluyen actividades de capacitación formales con el personal, de manera previa al análisis; es decir, “Se aprende en el camino”. Esto provoca una serie de retrasos en los proyectos que se traducen muchas veces en demoras adicionales del 25% del tiempo total o más.

I. No se ejecutan todas las pruebas necesarias para asegurarnos que el sistema no falle. Esto se debe en gran parte a que no se tiene un plan de pruebas y lo único que queda después es tratar de probar el sistemas de información desarrollado, con las mejoras intenciones. Esto no permite reducir al mínimo la existencia de errores.

J. No se ejecutan pruebas.

K. Las pruebas las ejecuta directamente el usuario cuando el sistema ya está implantado.

L. No se incluyen actividades formales de revisión y corrección de errores.

M. No se incluyen actividades formales de documentación o la documentación es dejada para el final.

N. Las actividades no se detallan al máximo y aparecen definidas en función de días o semanas.

O. No se capacita adecuadamente al usuario sobre las funcionalidades del sistema.

P. No se desarrollan los planes que sugieren las buenas prácticas del PMBOK. En muchos casos ni siquiera los planes indispensables, relacionados al alcance, tiempo y costo.

P007: PROCEDIMIENTO PARA LA AUDITORÍA DE LOS PLANES DE PROYECTO DE COMPRA DE SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar el proceso de elaboración de planes de proyecto de compra de sistemas de información en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión del proceso de conformación del Comité de Usuarios y el Líder de Usuarios, para el proyecto de compra de un sistema de información.

B. Verificación de la alineación del proyecto al PETI y al Plan Estratégico de la organización.

C. Verificación de la existencia del Análisis de Generación de Valor del proyecto.

D. Verificación de la asignación de presupuesto para el proyecto.

E. Verificación de la existencia de cotizaciones previas a la evaluación de la compra del proyecto.

F. Verificación de la existencia y validez de la evaluación de las cotizaciones y la determinación de la empresa ganadora.

G. Verificación de la asignación de cronogramas y responsabilidades de ejecución al proyecto de compra.

H. Verificación de la existencia de indicadores de gestión para la planificación del proyecto.

I. Revisión de la inclusión de actividades formales del ciclo de vida de desarrollo de sistemas en la planificación del proyecto.

El alcance del procedimiento no incluye:

A. Revisión detallada de la metodología de desarrollo de sistemas de información.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Lista de personas que participan o han participado en la planificación del proyecto de compra del sistema de información con sus respectivos teléfonos, anexos y correos para contactarlos.
B. Plan Estratégico de la Organización.
C. Plan Estratégico de Tecnologías de información.
D. Análisis de Generación de Valor del Proyecto.
E. Actas de reuniones del Jefe de Proyecto de la organización con el Líder de Usuarios y con el Jefe de Proyecto del proveedor.
F. Cotizaciones para la evaluación de la compra del proyecto.
G. Evaluación de las propuestas para la compra del proyecto.
H. Contrato para la compra del proyecto.
I. Especificaciones Funcionales y Técnicas del Proyecto.
J. Planes del Proyecto: Plan de Gestión de la Integración, Plan de Gestión del Alcance, Plan de Gestión del Tiempo, Plan de Gestión de los Costos, Plan de Gestión de la Calidad, Plan de Gestión de Recursos Humanos, Plan de Gestión de las Comunicaciones, Plan de Gestión de Riesgos, y Plan de Gestión de las Adquisiciones.
K. Formatos de Control de Cambios del Proyecto.
L. Formatos de Control de Entregables del Proyecto.
M. Formatos de Control de Riesgos del Proyecto.
N. Todos los diagramas de Gantt del proyecto.
O. Presupuesto del proyecto.
P. Indicadores de Gestión del Proyecto.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el proceso de conformación del Comité de Usuarios y el Líder de Usuarios, para el proyecto de compra del sistema de información. Verificar que en el comité de usuarios esté el personal clave que tiene relación con los procesos que serán soportados con el sistema de información. El líder de usuario de preferencia debe ser una persona con rango gerencial (gerente de línea o gerente intermedio), que conozca los procesos que serán soportados con el sistema de información, sus interrelaciones y las interrelaciones que estos tienen con el resto de procesos de la organización.

C. Verificar la alineación del proyecto al PETI y al Plan Estratégico de la organización. El proyecto debe contribuir a la generación del valor de la organización de acuerdo a lo planteado en el PETI y el Plan Estratégico.

D. Verificar la existencia del Análisis de Generación de Valor del proyecto. Debe verificarse que exista el cálculo del valor actual neto por el proyecto. Si el valor actual neto es un número negativo o un número pequeño positivo, observar que se está desarrollando o se ha desarrollado un proyecto que no genera valor o un proyecto que no es atractivo para la organización, respectivamente.

E. Verificar la asignación de un presupuesto adecuado para el proyecto, de acuerdo a sus objetivos y alcances y de acuerdo a cada una de las etapas considerando tanto las inversiones como los gastos adicionales por el proyecto.

F. Verificar la existencia de cotizaciones previas a la evaluación de la compra del proyecto. Considerar que debe existir por lo menos 3 cotizaciones para una transparente evaluación.

G. Verificar la existencia y validez de la evaluación de las cotizaciones y la determinación de la empresa ganadora. Se debe verificar que se haya recibido en su debido momento, las respectivas propuestas técnicas y propuestas económicas de por lo menos tres proveedores lo suficientemente calificados para poder postular. Además se debe verificar que se hayan tenido claros los criterios de evaluación del proveedor antes de realizar la evaluación y que se haya colocado los puntajes correctos a los proveedores y sus propuestas. Finalmente queda revisar que se haya realizado correctamente el cálculo de la sumatoria de los puntajes diversos de la evaluación para determinar la empresa ganadora.

K. Verificar la correcta definición de los planes de gestión del proyecto que sugiere el PMBOK por cada área de conocimiento: integración, alcance, costos, tiempo, calidad, recursos humanos, comunicaciones, riesgos y adquisiciones.

H. Verificar la asignación de cronogramas y responsabilidades de ejecución de los proyectos. Tener en cuenta:

   a) Para la verificación de las responsabilidades, se debe revisar la organización del proyecto, la cual debe tener los principios claros de unidad de mando, así como la asignación de la responsabilidad por cada etapa, proceso o módulo de sistema a desarrollar. Las responsabilidades deben estar asignadas tanto por el equipo de desarrollo como el equipo o comité de usuarios.

b) En los cronogramas debe aparecer el detalle de las actividades a nivel de horas. Además se debe verificar la sobreasignación de recursos; es decir, que no se crucen actividades en paralelo con la misma persona o equipo de personas. Revisar el enlace de las actividades de manera que no quede ninguna actividad sin enlazar. De esta manera se puede calcular de manera menos irreal la ruta crítica. Considerar además que se debe tener el calendario laboral con las fechas y horas reales de trabajo, además de lo planificado o replanificado.

I. Verificar la existencia de indicadores de gestión para el proyecto. Debe definirse indicadores de gestión que permitan al Jefe de Proyecto, tomar acciones correctivas en el momento adecuado. Estos indicadores de gestión deberán estar en función de tiempo, dinero (presupuesto) y nivel de cumplimiento de las especificaciones.

J. Revisar la inclusión de actividades formales del ciclo de vida de desarrollo de sistemas en la planificación del proyecto:

a) Levantamiento de Información. Revisión de los formatos de entrevistas u otro tipo de información que sirvió de base para elaborar las especificaciones funcionales.

b) Elaboración de Especificaciones Funcionales y Técnicas. Verificar la inclusión de las siguientes actividades:
- Revisar el detalle de los requerimientos del sistema.
- Si un sistema de información reemplazará a uno ya existente, revisar las hojas de análisis diferencial y ver que se hayan incluido todas las funcionalidades del sistema ya existente en el nuevo.

c) Planificación.
- Revisión del enlace de las diversas actividades. No deberían quedar actividades sueltas, sin relaciones con otras actividades.
- Revisión de la correcta definición del diagrama de red e identificación de la ruta crítica.
- Verificar que las actividades estén definidas a nivel de horas, separando claramente qué persona o grupo de personas las realizará.

d) Capacitación. Verificar la inclusión de las siguientes actividades:
- Capacitación Funcional sobre procesos a ser soportados por el sistema de información.
- Capacitación Técnica (herramientas y lenguajes de programación, herramientas administradoras de bases de datos, configuraciones, etc.). De no estar definida, recomendar la elaboración de librerías de código fuente en esta etapa. Esto último es aplicable si el proyecto de compra incluye la compra del código fuente del sistema de información y asumiendo que el código fuente será mantenido por personal de la empresa.

e) Análisis. Verificar la inclusión de las siguientes actividades, aplicables si el proyecto de compra incluye desarrollo de nuevas funcionalidades:
- Análisis de cada uno de los módulos.
- Interrelaciones entre los módulos.
- Elaboración de los diversos diagramas y documentación, de acuerdo a la metodología elegida.

f) Diseño. Verificar la inclusión de las siguientes actividades:
- Elaboración del diseño de interfaces gráficas de usuario.
- Elaboración del diseño de la base de datos.
- Elaboración del diseño de la estructura de los diversos componentes del sistema de información.
- Elaboración de Planes de Pruebas.
- Elaboración de Planes de Migración de los Datos.
- Elaboración del Plan de Integración. Incluye el diseño de Interfaces con los sistemas con los cuales se integrará el sistema de información en desarrollo.
- Elaboración de los diversos diagramas y documentación, de acuerdo a la metodología elegida.
- Elaboración de los diversos planes sugeridos por la ISO/IEC 12207:
  - Plan de Pruebas.
  - Plan de Gestión de la Configuración.
  - Plan de Configuración de la Infraestructura.
  - Plan de Aseguramiento de la Calidad.
  - Plan de Control de Calidad.
  - Plan de Revisión Conjunta.
  - Plan de Validación.
  - Plan de Integración del Software.
  - Plan de Instalación del Software.
  - Plan de Migración de Datos.
  - Plan de Retirada del Software.
  - Plan de Formación.
- Elaboración de Manuales Técnicos.

g) Implementación. Verificar la inclusión de las siguientes actividades, aplicables si el proyecto de compra incluye desarrollo de nuevas funcionalidades:
- Elaboración de especificaciones técnicas o seudocódigos.
- Actividades de programación de cada uno de los módulos.

h) Integración y Pruebas. Verificar la inclusión de las siguientes actividades:
- Integración de las diversas aplicaciones.
- Pruebas del Sistema Completo. Estas pruebas las debe realizar tanto personal de sistemas como personal del comité de usuarios. Deben estar incluidas las siguientes pruebas (que deben pertenecer a un Plan de Pruebas):
  - Pruebas de Interfase Gráfica de Usuario.
  - Pruebas de Caja Negra.
  - Pruebas de Caja Blanca.
  - Pruebas de Integración (Ascendente y Descendente).
  - Pruebas de Resistencia o Estrés.
  - Pruebas de Seguridad.
  - Pruebas de Pistas de Auditoría.

i) Implantación. Verificar la inclusión de las siguientes actividades:
- Elaboración de Manuales de Usuario.
- Instalación y Configuración del sistema de información.
- Migración de los datos.
- Capacitación al Usuario.

j) Mantenimiento. Verificar la inclusión de actividades de ajuste a los módulos desarrollados.

K. Verificar la inclusión de actividades formales de revisión y corrección errores al final de cada etapa descrita en el punto J.

L. Verificar la inclusión de actividades formales de documentación, por lo menos al final de cada etapa descrita en el punto J.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. No existe un comité de usuarios ni un líder de usuarios formal.

B. Los usuarios no se comprometen con el proyecto.

C. No se elaboran bien las especificaciones funcionales del proyecto.

D. No se elaboran planes de pruebas para los proyectos de compra de sistemas de información.

E. No se elaboran planes de migración de datos para los proyectos de compra de sistemas de información.

F. No se elaboran planes para la elaboración de interfases del sistema de información a comprar con los demás sistemas existentes en la organización.

G. Los planes indicados en los puntos D, E ó F se hacen de manera muy rápida, luego de la etapa de implementación, cuando el problema ya es evidente.

H. No se ejecutan todas las pruebas necesarias para asegurarnos que el sistema no falle. Esto se debe en gran parte a que no se tiene un plan de pruebas y lo único que queda después es tratar de probar las cosas con las mejoras intenciones. Esto no permite reducir al mínimo la existencia de errores.

I. No se ejecutan pruebas.

J. Las pruebas las ejecuta directamente el usuario cuando el sistema ya está implantado.

K. No se incluyen actividades formales de revisión y corrección de errores.

L. No se incluyen actividades formales de documentación o la documentación es dejada para el final.

M. Las actividades no se detallan al máximo y aparecen definidas en función de días o semanas.

N. No se capacita adecuadamente al usuario sobre las funcionalidades del sistema.

O. El número de cotizaciones resulta insuficiente para hacer una adecuada evaluación. A veces se decide por un único proveedor, dado que no se convocó a otros.

P. Las evaluaciones de los proveedores son manipuladas para favorecer a uno de los proveedores.

Q. Los contratos comúnmente están mal diseñados. Faltan una serie de cláusulas que podrían proteger a la organización contra diversos riesgos.

R. Cuando los contratos están bien diseñados, diversas partes del documento no se cumplen: asignación de las personas indicadas originalmente para la consultoría, cobro de penalidades por atrasos, pagos adicionales al proveedor no estipulados en el contrato inicial, etc.

Q. No se desarrollan los planes que sugieren las buenas prácticas del PMBOK. En muchos casos ni siquiera los planes indispensables, relacionados al alcance, tiempo y costo.

P008: PROCEDIMIENTO PARA LA AUDITORÍA DEL PLAN DE CONTINGENCIAS DE INFORMÁTICA

OBJETIVO

Analizar y evaluar el proceso de elaboración y ejecución[4] del Plan de Contingencias de Informática, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión del proceso de conformación del Equipo de Elaboración del Plan de Contingencias de Informática.

B. Verificación de la asignación de presupuesto, cronogramas y responsabilidades para la elaboración del Plan de Contingencias de Informática.

C. Verificación de la alineación del Plan de Contingencias de Informática al Plan Estratégico de la Organización.

D. Revisión del documento de Plan de Contingencias de Informática elaborado.

E. Verificación de la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Contingencias de Informática.

El alcance del procedimiento no incluye:

A. Revisión del Plan de Continuidad de Negocio.

[4] Ejecución. Aquí nos referimos a la ejecución de pruebas y a la ejecución real ante una contingencia (de haberse producido esta contingencia en el período en evaluación).

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Lista de personas que participan o han participado en la elaboración del Plan de Contingencias con sus respectivos teléfonos, anexos y correos para contactarlos.
B. Plan Estratégico de la Organización.
C. Plan Estratégico de Tecnologías de información.
D. Análisis de Generación de Valor del Plan de Contingencias de Informática.
E. Presupuesto detallado para la Elaboración del Plan de Contingencias de Informática.
F. Actas de reuniones del equipo de elaboración del Plan de Contingencias de Informática.
G. Diagramas de Gantt para la elaboración del Plan de Contingencias de Informática.
H. Plan de Contingencias de Informática.
I. Diagramas de Gantt para la ejecución del Plan de Contingencias de Informática.
J. Presupuesto detallado para la ejecución del Plan de Contingencias de Informática.
K. Documento de mejoras propuestas para el Plan de Contingencias de Informática.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el proceso de conformación del Equipo de Elaboración del Plan de Contingencias de Informática. Este equipo debe estar conformado por:

   - Personal clave del área que realiza la gestión de tecnología de información.
   - Personal clave de las áreas cuyos procesos serán soportados durante la contingencia.

C. Verificar la alineación del Plan de Contingencias de Informática al Plan Estratégico de la Organización. Se debe verificar que priorice la cobertura de los procesos para no atrasar la ejecución de los proyectos estratégicos de la organización, además de los procesos principales para que la organización opere en un nivel suficiente.

D. Verificar la asignación de presupuesto, cronogramas y responsabilidades para la elaboración del Plan de Contingencias de Informática.

E. Revisar el documento de Plan de Contingencias de Informática elaborado. Se debe verificar que tenga información con la cantidad y claridad suficientes para una exitosa ejecución ante una contingencia. Revisar que se haya detallado:

   a) Evaluación para priorizar las procesos que serán soportados durante el Plan de Contingencias de Informática.

b) Información General:
   - Objetivo del Plan de Contingencias.
   - Alcance del Plan de Contingencias.
   - Definición de Contingencia.
   - Conceptos de Declaración de Contingencia y Notificación.
     - Criterios para declarar la contingencia.
     - Notificación al Centro de Cómputo Alterno Externo o al personal que administra el Centro de Cómputo Alterno Interno.
     - Notificación a la compañía que almacena las copias de respaldo.
     - Notificación a los proveedores de los equipos y servicios para la recuperación.
     - Notificación al resto de personal de la organización.
     - Notificación a los medios de comunicación.
     - Punto de reunión durante la contingencia. Debe ser diferente a la ubicación de la empresa, lejos del impacto de la contingencia. Pueden ser varios puntos de reunión.

c) Organización del Trabajo para la Ejecución del Plan. Se debe tener las formas de localización (direcciones y teléfonos de casa, oficina, celulares, etc.) de:

   - Equipo gerencial.
   - Equipos de Usuarios.
   - Equipo de Informática.
   - Equipo del área encargada de las comunicaciones.
   - Equipo de seguridad y apoyo a emergencias.

   Para cada equipo se debe tener detallado: objetivos, competencias y responsabilidades antes, durante y después de ocurrida la contingencia.

d) Identificación de Aplicaciones críticas.

e) Procedimientos detallados para llevar a cabo la Ejecución del Plan de Contingencias. Por lo menos debe estar definido:
   - Procedimiento General para la ejecución del Plan de Contingencias.
   - Procedimiento para la Preparación del Centro de Cómputo Alterno para que soporte las operaciones durante la contingencia.
   - Procedimiento para la Identificación, Evaluación y Declaración de Contingencia.
   - Procedimiento para Notificación de Contingencia y Activación de los equipos de trabajo.
   - Procedimiento para el traslado de personal y suministros al Centro de Cómputo Alterno.
   - Procedimiento para la Puesta en Producción del Centro de Cómputo Alterno.
     - Procedimiento para la Recuperación de la Central Telefónica.
     - Procedimiento para la Recuperación de las Tecnologías de información. Hace referencia a:
       - Procedimiento para la Recuperación de las tecnologías de base.
       - Procedimiento para la Recuperación de los sistemas de información.
       - Procedimiento para la Restauración de los Datos.
       - Procedimiento para la Recuperación Manual (data huérfana).
       - Procedimiento para la Sincronización de Datos.
   - Procedimiento para la operación en línea del centro de cómputo alterno.

- Detalle de cómo se realizarán las actividades luego de la operación en línea del centro de cómputo alterno. Debe describirse:
  - Secuencia de actividades dentro de la recuperación.
  - Nombre de actividad. Identifica las actividades por equipo de recuperación.
  - Descripción breve de la actividad a ser ejecutada.
  - Referencias de documentos relacionados con la actividad.
  - Comentario del líder de cada equipo acerca de la ejecución de la tarea al momento de la recuperación.

f) Procedimiento de Pruebas del Plan de Contingencias. Por lo menos debe estar definido:
- Objetivo de las pruebas.
- Participantes.
- Cronograma de ejecución.
- Supuestos.
- Actividades.
  - Coordinación y notificación a equipos.
  - Procesos sin sistemas.
  - Activación del Centro de Cómputo Alterno.
  - Sincronización de información.
  - Procesos con sistemas.
- Cierre de prueba.
- Evaluación de resultados.
- Actualización del Plan de Recuperación.

g) Procedimiento de Mantenimiento del Plan de Contingencias. Por lo menos debe estar definido:
- Método de Administración de Cambios.
- Bitácora de Cambios.

F. Verificar la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Contingencias.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. El Plan de Contingencias de Informática es una copia de un documento netamente académico y no contiene el desarrollo de procedimientos detallados para la ejecución de actividades específicas durante una contingencia.

B. El Plan de Contingencias de Informática es un documento con varias carencias de forma y fondo.

C. La elaboración del Plan de Contingencias de Informática es encargada a una empresa consultora que prepara el documento sin llevar a la realidad los procesos descritos. Comúnmente le hacen correcciones a documentos de otros clientes que tienen en su archivo, y eso lo entregan como Plan de Contingencias de Informática para la empresa.

D. No se prueba el Plan de Contingencias de Informática.

E. Las pruebas del Plan de Contingencias de Informática no se hacen de manera adecuada.

P009: PROCEDIMIENTO PARA LA AUDITORÍA DEL PLAN DE CONTINUIDAD DE NEGOCIO

OBJETIVO

Analizar y evaluar el proceso de elaboración y ejecución[5] del Plan de Continuidad de Negocio de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión del proceso de conformación del Equipo de Elaboración del Plan de Continuidad.

B. Verificación de la asignación de presupuesto, cronogramas y responsabilidades para la elaboración del Plan de Continuidad de Negocio.

C. Verificación de la alineación del Plan de Continuidad de Negocio al Plan Estratégico de la Organización.

D. Revisión del documento elaborado como Plan de Continuidad de Negocio.

E. Verificación de la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Continuidad de Negocio.

El alcance del procedimiento no incluye:

A. Evaluación del Plan de Contingencias de Informática.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Lista de personas que participan o han participado en la elaboración y ejecución del Plan de Contingencias de Informática con sus respectivos teléfonos, anexos y correos para contactarlos.
B. Lista de personas que participan o han participado en la elaboración y ejecución del Plan de Continuidad de Negocio con sus respectivos teléfonos, anexos y correos para contactarlos.
C. Plan Estratégico de la Organización.

[5] Ejecución. Aquí nos referimos a la ejecución de pruebas y a la ejecución real luego de una contingencia (de haberse producido esta contingencia en el período en evaluación).

D. Plan Estratégico de Tecnologías de información.
E. Análisis de Generación de Valor del Plan de Continuidad de Negocio.
F. Presupuesto detallado para la Elaboración del Plan de Continuidad de Negocio.
G. Actas de reuniones del equipo de elaboración del Plan de Continuidad de Negocio.
H. Diagramas de Gantt para la elaboración del Plan de Continuidad de Negocio.
I. Plan de Contingencias de Informática.
J. Plan de Continuidad de Negocio.
K. Diagramas de Gantt para la ejecución del Plan de Contingencias de Informática.
L. Diagramas de Gantt para la ejecución del Plan de Continuidad de Negocio.
M. Presupuesto detallado para la ejecución del Plan de Contingencias de Informática.
N. Presupuesto detallado para la ejecución del Plan de Continuidad de Negocio.
O. Documento de mejoras propuestas para el Plan de Contingencias de Informática.
P. Documento de mejoras propuestas para el Plan de Continuidad de Negocio.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el proceso de conformación del Equipo de Elaboración del Plan de Continuidad de Negocio. Este equipo debe estar conformado por:

- Personal clave del área de tecnología de la información.
- Personal clave de las áreas cuyos procesos serán soportados después de la contingencia.

C. Verificar la alineación del Plan de Continuidad al Plan Estratégico de la Organización. Se debe verificar que priorice la cobertura de los procesos para no atrasar la ejecución de los proyectos estratégicos de la organización, además de los procesos principales para que la organización vuelva a tener por lo menos el nivel de servicio anterior.

D. Verificar la asignación de presupuesto, cronogramas y responsabilidades para la elaboración del Plan de Continuidad de Negocio.

E. Revisar el documento de Plan de Continuidad de Negocio. Se debe verificar que tenga información con la cantidad y claridad suficientes para una exitosa ejecución luego de una contingencia. Revisar que se haya detallado:

a) Identificación de riesgos de la organización. Incluye: riesgos de mercado, riesgos de operación, riesgos de crédito, riesgos financieros, etc.

b) Análisis cualitativo de riesgos.

c) Análisis cuantitativo de riesgos.

d) Determinación de los escenarios de contingencia de los cuales la organización se va a proteger.

e) Verificar que los escenarios de contingencia determinados, cubran los que se requiere de acuerdo a la legislación o normatividad vigente de los organismos reguladores.

f) Verificar que el documento, por cada escenario de contingencia y proceso crítico de negocio a proteger (críticos relacionados a la tecnología de información y críticos no relacionados a la tecnología de información), incluya las estrategias para la continuidad del negocio. Para cada proceso crítico se debe verificar que se haya establecido los tiempos de recuperación: RPO (Recovery Point Objective), RTO (Recovery Time Objective), WRT (Work Recovery Time) y MTD (Maximum Tolerable Downtime).

g) Verificar que se haya desarrollado el Plan de Reanudación de Operaciones.

h) Verificar la documentación de las Pruebas del Plan de Continuidad de Negocio.

i) Verificar que se haya incluido la siguiente información:

- Información General del Plan de Continuidad de Negocio.
  - Organización del Plan
  - Objetivos del Plan
  - Alcances del Plan
  - Procesos y subprocesos de negocio
  - Definición de Contingencia
  - Notificación a los equipos de usuarios.
  - Punto de reunión en situación de contingencia
  - Recursos requeridos para el Plan de Continuidad de Negocio

- Equipos de Trabajo
  - Organización de Equipos de Usuarios para la Recuperación
  - Equipos de Contingencia
    - ✓ Líder de Equipo
      - Objetivo
      - Habilidades Requeridas
      - Nombre y Cargo
      - Responsabilidades antes de la contingencia
      - Responsabilidades durante la contingencia
      - Responsabilidades después de la contingencia
      - Actividades del Líder de Equipo
        - ❑ Notificación de la contingencia
        - ❑ Notificación de retorno a la normalidad de las operaciones
    - ✓ Coordinador de Equipo de Usuarios
      - Objetivo
      - Habilidades requeridas
      - Integrantes
      - Responsabilidades antes de una contingencia
      - Responsabilidades durante la contingencia
      - Responsabilidades después de la contingencia
      - Actividades del Coordinador de Equipo
        - ❑ Activación de los equipos de trabajo / notificación de la contingencia

- Validación de Insumos Requeridos para la Operación en Modalidad de Contingencia

✓ Equipo de Usuarios
- Objetivo
- Habilidades requeridas
- Integrantes
- Responsabilidades antes de una contingencia
- Responsabilidades durante la contingencia
- Responsabilidades después de la contingencia

▪ Ejecución del Plan de Recuperación
➢ Introducción
➢ Actividades del Plan de Recuperación
✓ Enunciado del Proceso 1
✓ Enunciado del Proceso 2
➢ Secuencia de Recuperación considerando los equipos de trabajo habilitados
✓ Notificación de la Contingencia
✓ Activación de los equipos de trabajo / notificación de la contingencia
✓ Validación de Insumos y Suministros para operar en modalidad de contingencia
✓ Operación en Modalidad de Contingencia
- Enunciado del Proceso 1
- Enunciado del Proceso 2

✓ Reingreso de Data Huérfana y Carga de Información
➢ Cronograma de Actividades

F. Verificar la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Continuidad de Negocio.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. El Plan de Continuidad de Negocio es una copia de un documento netamente académico y no contiene el desarrollo de procedimientos detallados para la ejecución de actividades específicas luego de haber pasado la contingencia.

B. Los escenarios de contingencia que cubre el Plan de Continuidad de Negocio, son insuficientes para cubrir las operaciones de negocio, ante catástrofes: incendio del edificio de la compañía, terremotos, etc.

C. El Plan de Continuidad de Negocio es un documento con varias carencias de forma y fondo.

D. La elaboración del Plan de Continuidad es encargada a una empresa consultora que prepara el documento sin llevar a la realidad los procesos descritos. Comúnmente le hacen correcciones a documentos de otros clientes que tienen en su archivo, y eso lo entregan como Plan de Continuidad para la empresa.

E. No se prueba el Plan de Continuidad de Negocio.

F. Las pruebas del Plan de Continuidad de Negocio no se hacen de manera adecuada.

F. Comúnmente es confundido con el Plan de Contingencias de Informática.

P010: PROCEDIMIENTO PARA LA AUDITORÍA DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO

Analizar y evaluar el proceso de elaboración y ejecución del Plan de Seguridad de la Información de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión del proceso de conformación del Equipo de Elaboración del Plan de Seguridad de la Información.

B. Verificación de la asignación de presupuesto, cronogramas y responsabilidades para la elaboración del Plan de Seguridad de la Información.

C. Verificación de la alineación del Plan de Seguridad de la Información al Plan Estratégico de Informática.

D. Revisión del documento del Plan de Seguridad de la Información.

E. Verificación de la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Seguridad de la Información.

F. Verificación de la implementación de las acciones indicadas en el Plan de Seguridad de la Información.

El alcance del procedimiento no incluye:

A. Evaluación de los ataques de intrusos u otros problemas de seguridad de la información que hubieran ocurrido durante el período en evaluación.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Lista de personas que participan o han participado en la elaboración del Plan de Seguridad de la Información con sus respectivos teléfonos, anexos y correos para contactarlos.
B. Plan Estratégico de Informática.

C. Análisis de Generación de Valor del Plan de Seguridad de la Información.
D. Presupuesto detallado para la Elaboración del Plan de Seguridad de la Información.
E. Actas de reuniones del equipo de elaboración del Plan de Seguridad de la Información.
F. Diagramas de Gantt para la elaboración del Plan de Seguridad de la Información.
G. Plan de Seguridad de la Información.
H. Diagramas de Gantt para la ejecución de las acciones del Plan de Seguridad de la Información, con su respectiva asignación de responsabilidades.
I. Presupuesto detallado para la ejecución de las acciones del Plan de Seguridad de la Información.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el proceso de conformación del Equipo de Elaboración del Plan de Seguridad de la Información. Este equipo debe estar conformado por personal asignado especialmente para esa labor por parte del área de Tecnología de la Información; sin embargo, de este equipo el líder es sólo un miembro del Comite de Seguridad de la Información, equipo conformado por personal gerencial de diversas áreas de la organización, capaz de determinar políticas y sanciones ante faltas a la seguridad de la información. El equipo deberá coordinar con las demás áreas de la empresa y con la Unidad de Riesgos.

C. Verificar la asignación de presupuesto, cronogramas y responsabilidades para la elaboración del Plan de Seguridad de la Información.

D. Verificar la alineación del Plan de Seguridad de la Información al Plan Estratégico de Informática. Se debe verificar que priorice la seguridad de los procesos críticos de la organización, colocando las medidas de seguridad máximas para evitar que se lleven la información, teniendo en cuenta los siguientes elementos:

   - *Desventajas competitivas*. Analizar ¿Cuánto daño se podría causar a la organización, si la información cayera en manos del competidor?

   - *Pérdida directa del negocio*. Analizar si se perdería ingresos o utilidades si la información es divulgada, dañada o perdida.

   - *Pérdida o daño en la confianza e imagen pública*. Si la información es divulgada, ¿Cuánto daño provocaría en la confianza del cliente, la imagen pública o la lealtad de los accionistas o proveedores?

   - *Daño en la moral*. Si la información es divulgada o perdida, ¿Cuál sería el impacto en la moral o motivación del personal?

   - *Fraude*. Analizar si ocurre el riesgo de fraude en la manipulación de bienes o fondos, si la información es divulgada o alterada.

- *Decisiones gerenciales equivocadas*. Analizar si se podrían tomar decisiones equivocadas como resultado de errores en cambios de información no autorizados.

- *Interrupción de las operaciones de negocio*. Analizar ¿Qué aplicaciones son básicas para que el negocio no se vea interrumpido?

- *Responsabilidad Legal*. Analizar si la divulgación de información podría resultar en un problema legal, regulatorio o de cumplimiento de obligaciones contractuales.

- *Pérdida de privacidad*. Analizar si el usuario podría sufrir personalmente por pérdida de privacidad o uso no autorizado de su identidad.

- *Riesgo de Seguridad Personal*. Analizar si los registros incorrectos podrían poner en riesgo la salud o la vida de los usuarios.

E. Revisar el documento de Plan de Seguridad de la Información. Verificar que se haya detallado acciones para proteger a la organización de lo siguiente:

a) Seguridad Lógica de la Información.

- Riesgos de la Seguridad por uso inadecuado del equipo de cómputo.
  - "Trojan Horse programs".
  - "Back door and remote administration programs".
  - "Denial-of-Service attacks".
  - Ser intermediario de ataques a otras organizaciones.
  - Compartir redes de Windows no protegidas.
  - Programas con extensiones de archivo ocultas.
  - Protección contra uso inadecuado de código fuente de "Java", "JavaScript" o "ActiveX" por parte de intrusos, tanto en páginas accedidas a través del explorador de Internet como en el correo electrónico.
  - Virus en archivos adjuntos en el correo electrónico.
  - Hurto de identidad e información personal (financiera o no financiera).
  - "Cross-site scripting".
  - "E-mail spoofing".
  - "Chat Clients".
  - "Packet Sniffing".
  - "Tunneling".
  - "Zombies".
  - "Spyware".
  - "Adware".

- Violaciones de Reglas y Regulaciones.
  - Propiedad Intelectual.
  - Uso decente del Internet.
  - Espionaje Industrial.
  - Otras reglas y Regulaciones.

- Accidentes.
  - Problemas en el software de base.
  - Problemas en los sistemas de información.

- Políticas para otorgar accesos (se pueden otorgar de manera lógica) a:
  - Unidades de diskette.
  - Lectoras de CD.
  - Grabadoras de CD.
  - Grabadoras de DVD.
  - Envío de correos a direcciones de otras organizaciones.
  - "Chats".
  - Memorias USB.
  - Correo Electrónico Gratuito u otros correos diferentes al correo oficial de la organización.
  - Carga de archivos en páginas web.
  - Panel de control de las computadoras.
  - Instalación de programas en la computadora por parte del usuario.
  - Visualización de los nombres de las páginas web que están siendo accedidas a través del explorador de Internet.
  - Visualización del código fuente de las páginas web desarrolladas en el explorador de Internet.
  - Carpetas compartidas de los servidores.
  - Software de base usado en la organización.
  - Sistemas de Información de la organización.
  - Revisión periódica de los registros de transacciones para verificar si ocurrieron cambios no autorizados en los accesos otorgados.

- Configuración del "firewall".
  - Restricción de accesos a sitios web no autorizados.
  - Restricción de accesos a FTP.
  - Intentos de ataque de intrusos.
  - Ataques ocurridos y no detectados.
  - Vigencia de las reglas de seguridad definidas.
  - Revisión periódica del registro de transacciones del "firewall".

- Configuración del software "antispam".
  - Claridad de las reglas definidas.
  - Vigencia de las reglas de seguridad definidas.
  - Correos filtrados.
  - Revisión periódica del software "antispam".

- Copias de respaldo de la información.
  - Tiempo de demora de la elaboración de copias de respaldo.
  - Cronograma de elaboración de copias de respaldo.
  - Uso de equipos adecuados para las copias de respaldo.
  - Ubicación adecuada de las copias de respaldo: una copia en un ambiente físico del área de Tecnología de la Información, otra copia en un ambiente físico de otra área y otra copia en un ambiente físico fuera de los locales de la organización. Considerar que deben ubicarse las copias en lugares con las condiciones adecuadas de temperatura y humedad dadas por los fabricantes de los dispositivos de almacenamiento. Si la copia de respaldo se aloja en un proveedor, verificar las instalaciones del proveedor.
  - Tiempo de demora en la restauración de la copia de respaldo en el centro de cómputo alterno.
  - Verificación de las tareas de los backups, para ver si se han realizado correctamente.

- Software para apagado automático de los servidores ante un corte de fluido eléctrico (aunque no es necesario si hay UPS y los vigilantes conmutan al uso de energía eléctrica con un generador, apenas ocurre el problema).

b) Seguridad Física de la Información:

- Acceso de Personas.
  - Identificación de las personas que ingresan a las instalaciones.
  - Escolta de las personas que ingresan a las instalaciones.
  - Claves de seguridad en las puertas de acceso a las oficinas y centros de cómputo.
  - Correcto estado de las puertas de acceso a las oficinas y centros de cómputo.

- Suministro de energía eléctrica de los equipos de cómputo.
  - Estabilización de la línea de voltaje de los equipos de cómputo.
  - Uso de una línea de voltaje para los equipos de cómputo que sea diferente de las líneas de voltaje que se usen para otros fines en la organización.
  - Uso de equipos UPS por lo menos en las salas de cómputo ó uso de generadores de voltaje para dichas instalaciones con procedimientos claros ante una caída del suministro de energía eléctrica.
  - Existencia de un pozo de tierra.
  - Mantenimiento periódico del pozo de tierra.

- Protección contra incendios.
  - Extinguidores para incendios originados por equipos electrónicos.
  - Vigencia de los extinguidores de incendios.
  - Suficiencia en cantidad de extinguidores de incendios.
  - Detectores de humo.
  - Correcto funcionamiento de las alarmas contra incendios.
  - Inexistencia de material inflamable en los centros de cómputo, tales como madera, ropa, cuadernos, etc.

- Condiciones ambientales de las salas de cómputo.
  - Correcto funcionamiento de los equipos de aire acondicionado.
  - Correcto funcionamiento de los medidores de humedad y temperatura.
  - Cableado desordenado con riesgo que lo pisen y se retiren los cables de los “switches”.

- Fallas en Hardware.
  - Fallas en disco.
  - Fallas en la fuente de voltaje de la computadora.
  - Fallas en la tarjeta principal.
  - Otras fallas en el hardware.

- Traslado de Información.
  - Normas sobre el traslado de documentos físicos fuera de los locales de la organización.
  - Normas para el ingreso de dispositivos de memoria dentro de la organización.
  - Normas para la salida de dispositivos de memoria fuera de la organización.

F. Verificar la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Seguridad de la Información. Se debe identificar claramente quién será responsable de la ejecución de las actividades descritas en el plan.

G. Verificación de la implementación de las acciones indicadas en el Plan de Seguridad de la Información. Revisar si ejecutan las acciones quienes deberían realizarlas o si el personal que las realiza o ha realizado, tiene o tenía las competencias necesarias para hacerlo.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un Plan de Seguridad de la Información.

B. El Plan de Seguridad de la Información está enfocado en la Seguridad Lógica; pero, no se han tomado acciones en lo referente a la seguridad física.

C. Las acciones referentes a la seguridad de la información son tomadas para todos los usuarios; excepto, personal del área de Tecnología de la Información, quienes tienen accesos a: chats, correos gratuitos, etc.

D. Las claves de seguridad de acceso a diversas tecnologías de información, son conocidas por personas que no necesitan saberlo ó son cambiadas sin notificar al jefe encargado de ello.

E. Errores en la seguridad física:
- Los extinguidores de incendios no son apropiados para apagar incendios de equipos electrónicos. Ej: extinguidores de chorro de agua en lugar de extinguidores de dióxido de carbono o polvo químico seco.
- Los extinguidores de incendios tienen vencida la fecha de renovación.
- Los detectores de humo no han sido probados o no funcionan.
- Las alarmas contra incendios no han sido probadas o no funcionan.
- Los equipos UPS no protegen un tiempo suficiente como para soportar la carga de todos los servidores ante un corte de energía eléctrica, hasta que conecten el generador.
- Existencia de material inflamable como ropa, cuadernos, etc.
- El equipo de aire acondicionado gotea o hace escarcha.
- Cada cierto tiempo los operadores apagan el aire acondionado cuando trabajan en el mismo ambiente.
- El cableado se encuentra muy desordenado, con riesgo que lo pisen y se salgan los cables de red de los switches y ocurra interrupciones en el sistema para algunos usuarios.
- No existe pISO/IEC técnico o “falso piso” para el cableado.
- Los operadores trabajan en el mismo ambiente físico donde se encuentran los equipos del centro de cómputo.
- Existen problemas eléctricos, sobre todo en edificios antiguos, los cuales afectan al hardware de computadoras, redes y equipos relacionados.

P011: PROCEDIMIENTO PARA LA AUDITORÍA DEL PLAN DE LICENCIAMIENTO DE SOFTWARE

OBJETIVO

Analizar y evaluar el proceso de elaboración y ejecución del Plan de Licenciamiento de Software de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Verificación del Inventario de Licencias de Software de la organización.

B. Revisión del Plan de Licenciamiento de Software.

C. Revisión del análisis de generación de valor del Plan de Licenciamiento de Software.

D. Verificación de la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Licenciamiento de Software.

El alcance del procedimiento no incluye:

A. Evaluación de lo adecuado de la compra del software con licencia. Por ejemplo, si en lugar de comprar licencias era mejor usar software libre (por razones de costos y rendimiento), no es parte del alcance de la actividad, a no ser que el Plan Estratégico de Informática lo especifique explícitamente.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Inventario de Licencias de Software. Incluye software de base y sistemas de información.
B. Plan Estratégico de Informática.
C. Plan de Licenciamiento de Software.
D. Análisis de Generación de Valor del Plan de Licenciamiento de Software.
E. Diagramas de Gantt para la ejecución de las actividades del Plan de Licenciamiento de Software, con su respectiva asignación de responsabilidades.
F. Presupuesto detallado para la ejecución de las actividades del Plan de Licenciamiento de Software.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente el Inventario de Licencias de Software. Realizar lo siguiente:

a) Verificar que todos y cada uno de los software que se usan en la organización estén en la relación. Esto incluye:

- Sistemas operativos en servidores.
- Sistemas operativos en clientes.
- Servidor proxy.
- Servidores de bases de datos.
- Servidores Web.
- Servidores de Correo.
- Clientes de Correo.
- Software para realización de copias de respaldo.
- Software de Oficina.
- Sistemas de Información.
- Software “antispam”.
- Software especializado que administra equipos electrónicos, etc.

b) Verificar que se haya indicado la cantidad de usuarios que cubre la licencia y la cantidad de usuarios que actualmente usa el software. Si es un software libre, software “freeware” o software “shareware”, se debe indicar ello en la relación.

c) Consultar el detalle de uso (relación de usuarios y áreas) de las licencias de software más costosas, aquellas licencias de software que se usen en mayor cantidad, y aquellas licencias de software que en mayor proporción y valor no tengamos licenciadas. La cantidad no es estándar; por lo tanto, usar el razonamiento y la intuición para determinar las cantidades de software a revisar.

C. Revisar detalladamente el Plan de Licenciamiento. Verificar lo siguiente:

a) La alineación del Plan de Licenciamiento de Software con el Plan Estratégico de Informática. Las compras de licencias de software deben tener concordancia con la estrategia de informática de la organización. Por ejemplo, si la estrategia de informática indica la instalación de software libre para uso de oficina como Open Office para ahorrar gastos innecesarios en licencias de este tipo, se entiende que no se debería comprar licencias de MS Office, Lotus Smart Suite u otro software propietario de oficina.

b) En el caso de las compras válidas de licencias de software, considerar que el número de licencias a comprar debe considerar el número de licencias que faltan mas un número de licencias prudencial para proyectar un crecimiento de usuarios de por lo menos un año. De esa manera se podría lograr un precio mejor por la licencia y evitar comprarla de manera individual después (el costo sería mucho mayor).

D. Revisión del análisis de generación de valor del Plan de Licenciamiento de Software. Verificar que el Plan de Licenciamiento realmente genere valor para la organización,

E. Verificar la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Licenciamiento de Software. Revisar la asignación planificada y la asignación real.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un Plan de Licenciamiento de Software.

B. La organización no tiene un inventario actualizado del software que utiliza.

C. El Plan de Licenciamiento de Software está incompleto.

D. No se tiene licencias de la mayoría del software propietario que se usa en la organización.

E. El Plan de Licenciamiento está enfocado en la compra de software que actualmente se usa, sin considerar otras alternativas que costarían menos o no costarían más que la capacitación al personal o quizás unas cuantas horas de búsqueda y lectura de información en Internet (como el uso de software libre).

P012: PROCEDIMIENTO PARA LA AUDITORÍA DEL PLAN DE CAPACITACIÓN

OBJETIVO

Analizar y evaluar el proceso de elaboración y ejecución del Plan de Capacitación para el área de Tecnología de la Información de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Verificación del proceso de elaboración del Plan de Capacitación del área de Tecnología de la Información.

B. Revisión del alineamiento del Plan de Capacitación al Plan Estratégico de Tecnologías de información.

C. Revisión del currículum vitae del personal del área de Tecnología de la Información.

D. Revisión del documento del Plan de Capacitación del área de Tecnología de la Información.

E. Revisión del análisis de generación de valor del Plan de Capacitación del área de Tecnología de la Información.

F. Verificación de la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Capacitación.

El alcance del procedimiento no incluye:

A. Evaluación de lo adecuado de la tecnología o proceso de gestión sobre lo cual se está capacitando.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Inventario de competencias del personal contratado directamente por la organización, o por personal contratado a través de un proveedor.
B. Currículum vitae detallado de todo el personal que labora en el área de Tecnología de la información: Incluye: gerentes, sub-gerentes, jefes de proyecto, analistas funcionales, analistas programadores, programadores y practicantes.
C. Plan de Capacitación del área de Tecnología de la Información.
D. Diagramas de Gantt para la ejecución de las actividades del Plan de Capacitación, con su respectiva asignación de responsabilidades.
E. Presupuesto detallado para la ejecución de las actividades del Plan de Capacitación.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el proceso de elaboración del Plan de Capacitación del área de Tecnología de la Información. Verificar que se haya realizado lo siguiente:

    a) Solicitud a cada jefe de área de las necesidades de capacitación para el período del plan.
    b) Inclusión del personal clave en la capacitación.
    c) Relación de temas en los cuales se necesita capacitar al personal.
    d) Una búsqueda adecuada de organizaciones en las cuales se ofrecen cursos sobre los temas a capacitar. Deben existir varias opciones por cada tema.
    e) Elaboración del documento del Plan de Capacitación.

C. Revisar los currículum vitae del personal del área de Tecnología de la Información, tanto del personal directamente contratado por la organización como del personal contratado a través de un proveedor.

D. Revisar el documento del Plan de Capacitación del área de Tecnología de la Información. Verificar que contenga por lo menos lo siguiente:

a) Un inventario de las competencias[6] del personal, de manera previa a la fecha de vigencia del Plan de Capacitación. De no existir, verificar a través de la entrevista, que por lo menos se haya realizado una consulta de conocimientos o revisión de currículum vitae del personal.

b) Una relación de competencias ideales del personal para el final del período de tiempo que tendrá vigencia el Plan de Capacitación.

c) Una relación de cursos, talleres o conferencias, necesarias para lograr las competencias esperadas, considerando el presupuesto, el tiempo y el personal que se requiera.

d) Presupuesto del Plan de Capacitación.

e) Cronograma y Asignación de Responsabilidades.

E. Revisar el alineamiento del Plan de Capacitación al Plan Estratégico de Informática. El Plan de Capacitación debe estar enmarcado en los lineamientos del Plan Estratégico de Informática tanto en lo referente a la tecnología de información (tanto hardware como software) que regirá en el futuro (teniendo en cuenta también la tecnología actual), como aquellas metodologías de gestión de proyectos y gestión de procesos de desarrollo de tecnologías de información.

F. Revisar el análisis de generación de valor del Plan de Capacitación. Verificar que el Plan de Capacitación realmente genere valor para la organización; es decir, que como resultado de la capacitación, se pueda acelerar la ejecución de procesos críticos con resultados de mejoras en ingresos netos ó evitando que se pierda dinero por riesgos o gastos innecesarios.

G. Verificar la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Capacitación. Revisar la asignación planificada y la asignación real.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un Plan de Capacitación para el área de Tecnología de la Información. Comúnmente lo que hacen es entregar un detalle de las capacitaciones que han recibido en el período en evaluación; sin embargo, estas capacitaciones no estuvieron enmarcadas dentro de un plan.

B. La organización no tiene los currículum vitae actualizados del personal contratado a través de un proveedor.

C. El Plan de Capacitación está enfocado principalmente en capacitar sobre el software que van a usar y no sobre temas de gestión o temas referentes al proceso sobre el cual se va a desarrollar los sistemas de información, lo cual es necesario para los cargos de analistas funcionales, jefes de proyecto, analistas programadores y programadores.

[6] Competencias. Este término refiere a los conocimientos, habilidades y actitudes del personal, necesarias para un adecuado desempeño laboral.

P013: PROCEDIMIENTO PARA LA AUDITORÍA DEL PLAN DE MANTENIMIENTO PREVENTIVO DE HARDWARE DE COMPUTADORAS, REDES Y EQUIPOS RELACIONADOS

OBJETIVO

Analizar y evaluar el proceso de elaboración y ejecución del Plan de Mantenimiento Preventivo de Hardware de Computadoras, Redes y Equipos Relacionados en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Verificación del proceso de elaboración del Plan de Mantenimiento Preventivo del Hardware de Computadoras, Redes y Equipos Relacionados[7].

B. Revisión del alineamiento del PMPHCRER al Plan Estratégico de Informática[8].

C. Revisión del documento del PMPHCRER.

D. Revisión del análisis de generación de valor del PMPHCRER.

E. Verificación de la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del PMPHCRER.

El alcance del procedimiento no incluye:

A. Evaluación del Plan de Mantenimiento Correctivo de Hardware de Computadoras, Redes y Equipos Relacionados.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Inventario del hardware de computadoras, redes y equipos relacionados.
B. Listado del hardware de computadoras, redes y equipos relacionados, que requieran mantenimiento preventivo, clasificado de acuerdo a quien le debe realizar dicho mantenimiento (personal de la organización o un proveedor).
C. Fechas e informes de los últimos mantenimientos preventivos o correctivos que se haya realizado sobre los equipos.
D. Diagramas de Gantt para la ejecución de las actividades del PMPHCRER, con su respectiva asignación de responsabilidades.

[7] En adelante se identificará al Plan de Mantenimiento Preventivo de Hardware de Computadoras, Redes y Equipos Ambientales con las iniciales PMPHCRER.
[8] En adelante se identificará al Plan Estratégico de Informática con las iniciales PEI.

E. Presupuesto detallado para la ejecución de las actividades del PMPHCRER.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Verificar que la lista de equipos para el mantenimiento preventivo estén incluidos en el inventario de equipos total. En la lista de equipos debe estar detallado:

- Equipos que forman parte de la computadora o están directamente conectados a ella: monitores, cases, teclados, mouses, impresoras, scanners, cámaras de computadora, computadoras portátiles, etc.
- Equipos de red: routers, firewalls, switches, hubs, cableado, etc.
- Equipos relacionados a la energía eléctrica: cajas de control de suministro de energía (caja de cuchillas), pozo de tierra, línea de voltaje, tomacorrientes, estabilizadores de voltaje, supresor de picos, UPS, etc.
- Equipos relacionados a las condiciones ambientales: ventiladores de los centros de cómputo, medidores de temperatura, medidores de humedad, etc.
- Equipos relacionados a la protección contra incendios: extinguidores de incendios, detectores de humo, alarma de incendios, etc.
- Equipos relacionados a la seguridad: puertas de acceso con llave, puertas de acceso con clave de seguridad, etc.

C. Verificar la inclusión de todos los equipos que comúnmente requieren mantenimiento preventivo en la lista entregada.

D. Revisar el proceso de elaboración del PMPHCRER. Verificar que se haya realizado lo siguiente:

a) Determinación clara de los criterios para la evaluación y priorización de las necesidades de mantenimiento preventivo.
b) Evaluación de las necesidades de mantenimiento preventivo para el período del plan.
c) Priorización de las necesidades de mantenimiento preventivo para el período del plan.
d) Determinación de qué mantenimientos preventivos serán realizados por personal de la organización o por proveedores.
e) Identificación de varios proveedores alternativos para la ejecución de los mantenimientos preventivos.
f) Elaboración del documento del PMPHCRER.
g) Asignación de presupuesto, cronogramas y responsabilidades para la ejecución de las acciones del PMPHCRER.

E. Revisar el documento del PMPHCRER. Verificar que contenga por lo menos lo siguiente:

a) Listado de equipos que necesitan mantenimiento preventivo.
b) Criterios para evaluar y priorizar las necesidades de mantenimiento preventivo.

c) Evaluación y priorización de las necesidades de mantenimiento preventivo.
d) Presupuesto, Cronograma y Asignación de Responsabilidades.

F. Revisar el alineamiento del PMPHCRER al PEI. El PMPHCRER debe estar enmarcado en los lineamientos del PEI, teniendo en cuenta no sólo la tecnología actual, sino aquellas que serán de mayor beneficio para la organización en el futuro.

G. Revisar el análisis de generación de valor del PMPHCRER. Verificar que el PMPHCRER realmente genere valor para la organización; es decir, que como resultado de la ejecución del plan, se pueda acelerar la ejecución de procesos críticos con resultados de mejoras en ingresos netos ó evitando que se pierda dinero por riesgos o gastos innecesarios.

H. Verificar la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del PMPHCRER. Revisar la asignación planificada y la asignación real.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un PMPHCRER. Comúnmente lo que hacen es entregar un detalle de los mantenimientos realizados en el período en evaluación; sin embargo, estos mantenimientos no estuvieron enmarcados dentro de un plan.

B. La organización no solicita informes de los mantenimientos preventivos realizados a los proveedores.

C. La organización no elabora informes de los mantenimientos preventivos realizados por personal que ha contratado directamente.

D. La organización omite realizar mantenimiento preventivo de algunos equipos críticos.

P014: PROCEDIMIENTO PARA LA AUDITORÍA DEL PLAN DE MANTENIMIENTO CORRECTIVO DE HARDWARE DE COMPUTADORAS, REDES Y EQUIPOS RELACIONADOS

OBJETIVO

Analizar y evaluar el proceso de elaboración y ejecución del Plan de Mantenimiento Correctivo de Hardware de Computadoras, Redes y Equipos Relacionados en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Verificación del proceso de elaboración del Plan de Mantenimiento Correctivo del Hardware de Computadoras, Redes y Equipos Relacionados[9].

B. Revisión del alineamiento del PMCHCRER al PEI.

C. Revisión del documento del PMCHCRER.

D. Revisión del análisis de generación de valor del PMCHCRER.

E. Verificación de la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del PMCHCRER.

El alcance del procedimiento no incluye:

A. Evaluación del Plan de Mantenimiento Preventivo de Hardware de Computadoras, Redes y Equipos Relacionados.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Inventario del hardware de computadoras, redes y equipos relacionados.
B. Listado del hardware de computadoras, redes y equipos relacionados, que requieran mantenimiento correctivo, clasificado de acuerdo a quién le debe realizar dicho mantenimiento (personal de la organización o un proveedor).
C. Fechas e informes de los últimos mantenimientos preventivos o correctivos que se haya realizado sobre los equipos.
D. Diagramas de Gantt para la ejecución de las actividades del PMCHCRER, con su respectiva asignación de responsabilidades.
E. Presupuesto detallado para la ejecución de las actividades del PMCHCRER.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Verificar que la lista de equipos para el mantenimiento correctivo estén incluidos en el inventario de equipos total. En la lista de equipos debe estar detallado:

   - Equipos que forman parte de la computadora o están directamente conectados a ella: monitores, cases, teclados, mouses, impresoras, scanners, cámaras de computadora, computadoras portátiles, etc.

[9] En adelante se identificará al Plan de Mantenimiento Correctivo de Hardware de Computadoras, Redes y Equipos Ambientales con las iniciales PMCHCRER.

- Equipos de red: routers, firewalls, switches, hubs, cableado, etc.
- Equipos relacionados a la energía eléctrica: cajas de control de suministro de energía (caja de cuchillas), pozo de tierra, línea de voltaje, tomacorrientes, estabilizadores de voltaje, supresor de picos, UPS, etc.
- Equipos relacionados a las condiciones ambientales: ventiladores de los centros de cómputo, medidores de temperatura, medidores de humedad, etc.
- Equipos relacionados a la protección contra incendios: extinguidores de incendios, detectores de humo, alarma de incendios, etc.
- Equipos relacionados a la seguridad: puertas de acceso con llave, puertas de acceso con clave de seguridad, etc.

C. Revisar el proceso de elaboración del PMCHCRER. Verificar que se haya realizado lo siguiente:

a) Determinación clara de los criterios para la priorización de las necesidades de mantenimiento correctivo.
b) Priorización de las necesidades de mantenimiento correctivo para el período del plan.
c) Determinación de qué mantenimientos correctivos serán realizados por personal de la organización o por proveedores.
d) Identificación de varios proveedores alternativos para la ejecución de los mantenimientos correctivos.
e) Elaboración del documento del PMCHCRER.
f) Asignación de presupuesto, cronogramas y responsabilidades para la ejecución de las acciones del PMCHCRER.

D. Revisar el documento del PMCHCRER. Verificar que contenga por lo menos lo siguiente:

a) Listado de equipos que necesitan mantenimiento correctivo.
b) Criterios para la priorización de las necesidades de mantenimiento preventivo.
c) Priorización de las necesidades de mantenimiento correctivo.
d) Presupuesto, Cronograma y Asignación de Responsabilidades.

E. Revisar el alineamiento del PMCHCRER al PETI. El PMCHCRER debe estar enmarcado en los lineamientos del PEI, teniendo en cuenta no sólo la tecnología actual, sino aquellas que serán de mayor beneficio para la organización en el futuro.

F. Revisar el análisis de generación de valor del PMCHCRER. Verificar que el PMCHCRER realmente genere valor para la organización; es decir, que como resultado de la ejecución del plan, se pueda acelerar la ejecución de procesos críticos con resultados de mejoras en ingresos netos ó evitando que se pierda dinero por riesgos o gastos innecesarios.

G. Verificar la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del PMCHCRER. Revisar la asignación planificada y la asignación real.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un PMCHCRER. Comúnmente lo que hacen es entregar un detalle de los mantenimientos realizados en el período en evaluación; sin embargo, estos mantenimientos no estuvieron enmarcados dentro de un plan.

B. La organización no solicita informes de los mantenimientos correctivos realizados a los proveedores.

C. La organización no elabora informes de los mantenimientos correctivos realizados por personal que ha contratado directamente.

D. La organización omite realizar mantenimiento correctivo de algunos equipos críticos, los cuales terminan malográndose por esta negligencia.

P015: PROCEDIMIENTO PARA LA AUDITORÍA DE LA PLANIFICACIÓN DE LABORES DE RUTINA RELACIONADAS CON LAS TECNOLOGÍAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar el proceso de elaboración y ejecución de la Planificación de Labores de Rutina relacionadas con las Tecnologías de Información[10] en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Verificación del proceso de elaboración de la PLRTI.

B. Revisión del alineamiento de la PLRTI al PEI.

C. Revisión del documento de la PLRTI.

D. Revisión del análisis de generación de valor de la PLRTI.

E. Verificación de la asignación de presupuesto, cronogramas y responsabilidades para la ejecución de la PLRTI.

El alcance del procedimiento no incluye:

A. Revisión de la planificación de actividades de proyectos.

[10] En adelante se identificará a la Planificación de las Labores de Rutina relacionadas con las Tecnologías de Información con las iniciales PLRTI

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Inventario del hardware de computadoras, redes y equipos relacionados.
B. Inventario de software de base.
C. Inventario de sistemas de información.
D. Listado de Labores de Rutina que se planifican por área.
E. Diagramas de Gantt para la ejecución de las actividades de la PLRTI, con su respectiva asignación de responsabilidades.
F. Presupuesto detallado para la ejecución de las actividades del PLRTI.

PROCESO

Las actividades a realizar para llevar a cabo esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el alineamiento de la PLRTI al PEI. Las actividades del PLRTI deben planificarse sobre la base del PEI y cada uno de los planes relacionados. Por lo tanto, sólo deberían ejecutarse actividades que ayuden de manera directa o indirecta al logro del PEI.

C. Revisar el documento de la PLRTI. Verificar que por lo menos contenga lo siguiente:

   a) Planificación de Labores de Rutina relativas a la Infraestructura de Tecnología de Información o Soporte Técnico. Debe verificarse labores de rutina para:

      i. Help Desk.
         - Consultas de usuarios.
         - Instalación de software de base.
         - Instalación de piezas y equipos de cómputo y red.
         - Atención de fallas en hardware de equipos de cómputo y red.
         - Atención de fallas en software de base instalado.

      ii. Programación de Tareas.
         - Cierres periódicos.
         - Tareas de las bases de datos.
         - Tareas referentes a los servidores de correo.

      iii. Correo.
         - Configuración de cuentas de correo internas.
         - Configuración de cuentas de correo externas.
         - Configuraciones de protección contra virus.
         - Configuraciones de protección contra correos no deseados (spam).
         - Tareas de mantenimiento.

      iv. Seguridad de la Información.
         - Accesos.

- ❖ Accesos Físicos.
- ❖ Accesos Lógicos. Considerar: Sistemas Operativos, Sistemas de Información, Software de Base, Envío de correos Externos, etc.

- ➢ Protección contra intrusos.
- ➢ Protección contra correos no deseados.
- ➢ Protección contra código malicioso: virus, worm, spyware, adware, etc.
- ➢ Copias de respaldo de la información. Incluir:
  - ❖ Bases de datos.
  - ❖ Archivos de usuarios.
  - ❖ Carpetas compartidas en servidores.
  - ❖ Configuraciones de Servidores.
  - ❖ Correo Electrónico.
  - ❖ Software de Base.
  - ❖ Código fuente de desarrollos de sistemas de información, etc.

b) Planificación de Labores de Rutina relativas a los sistemas de información. Revisar que se haya planificado y organizado el trabajo de rutina referente a los requerimientos de correcciones o desarrollo de pequeñas nuevas opciones sobre los sistemas de información existentes.

D. Revisar el análisis de generación de valor de la PLRTI. Verificar que la PLRTI realmente genere valor para la organización; es decir, que como resultado de la ejecución del plan, se pueda acelerar la ejecución de procesos críticos con resultados de mejoras en ingresos netos ó evitando que se pierda dinero por riesgos o gastos innecesarios.

E. Verificar la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del PLRTI. Revisar la asignación planificada y la asignación real.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene una PLRTI.

B. La organización tiene una PLRTI incompleta. Comúnmente se descuida temas referentes a las copias de respaldo.

C. La organización pierde correos electrónicos importantes debido a la inadecuada configuración del software antispam.

D. La organización es atacada constantemente por código malicioso: virus, worm, spyware, adware, etc.

E. La organización está desprotegida de ataques de intrusos. Si se tiene software de protección contra intrusos, comúnmente no está bien configurado o no se revisa constantemente sus archivos de transacciones.

F. Existen usuarios que tienen accesos a opciones no autorizadas.

P016: PROCEDIMIENTO PARA LA AUDITORÍA DEL PLAN DE CALIDAD

OBJETIVO

Analizar y evaluar el proceso de elaboración y ejecución del Plan de Calidad para el área de Tecnología de la Información de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Verificación del proceso de elaboración del Plan de Calidad del área de Tecnología de la Información.

B. Revisión del alineamiento del Plan de Calidad al PEI.

C. Revisión de los currículum vitae del personal del área de Tecnología de Información.

D. Revisión del documento del Plan de Calidad del área de Tecnología de Información.

E. Revisión del análisis de generación de valor del Plan de Calidad del área de Tecnología de Información.

F. Verificación de la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Calidad.

El alcance del procedimiento no incluye:

A. Evaluación de la metodología usada como base para el Plan de Calidad.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Inventario de competencias del personal contratado directamente por la organización o personal contratado a través de un proveedor.
B. CurrÍculum vitae detallado de todo el personal que labora en el área de Tecnología de la información: Incluye: gerentes, sub-gerentes, jefes de proyecto, analistas funcionales, analistas programadores, programadores y practicantes.
C. Plan de Calidad del área de Tecnología de la Información.
D. Diagramas de Gantt para la ejecución de las actividades del Plan de Calidad, con su respectiva asignación de responsabilidades.
E. Presupuesto detallado para la ejecución de las actividades del Plan de Calidad.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el proceso de elaboración del Plan de Calidad del área de Tecnología de la Información. Verificar que se haya realizado lo siguiente:

   a) Solicitud a cada jefe de área de las necesidades de mejora de la calidad de procesos para el período del plan.
   b) Inclusión del personal clave en la capacitación sobre gestión de la calidad.
   c) Relación de temas en los cuales se necesita capacitar al personal.
   d) Una búsqueda adecuada de organizaciones en las cuales se ofrecen cursos sobre los temas a capacitar. Deben existir varias opciones por cada tema.
   e) Elaboración del documento del Plan de Calidad.

C. Revisar los currículum vitae del personal del área de Tecnología de Información, tanto del personal directamente contratado por la organización como del personal contratado a través de un proveedor.

D. Revisar el documento del Plan de Calidad del área de Tecnología de la Información. Verificar que contenga por lo menos lo siguiente:

   a) Un inventario de las competencias del personal, de manera previa a la fecha de vigencia del Plan de Capacitación. De no existir, verificar a través de la entrevista, que por lo menos se haya realizado una consulta de conocimientos o revisión de currículum vitae del personal.

   b) Una relación de competencias ideales del personal para el final del período de tiempo que tendrá vigencia el Plan de Calidad.

   c) Una relación de cursos o conferencias, necesarias para lograr las competencias esperadas, considerando el presupuesto, el tiempo y el personal que se requiera.

   d) Detalle de actividades de Aseguramiento de la Calidad.

   e) Detalle de Actividades de Control de Calidad. Las actividades de aseguramiento y las actividades de control de calidad deben estar inmersas en las actividades de Soporte Técnico y en las actividades de Desarrollo y Mantenimiento de Sistemas de Información.

   f) Presupuesto del Plan de Calidad.

   g) Cronograma y Asignación de Responsabilidades.

E. Revisar el alineamiento del Plan de Calidad al PEI. El Plan de Calidad debe estar enmarcado en los lineamientos del PEI para cada una de las áreas que forman parte del área de Tecnología de la Información.

F. Revisar el análisis de generación de valor del Plan de Calidad. Verificar que el Plan de Calidad realmente genere valor para la organización; es decir, que

como resultado de la ejecución del Plan de Calidad, se pueda acelerar la ejecución de procesos críticos con resultados de mejoras en ingresos netos ó evitando que se pierda dinero por riesgos o gastos innecesarios.

G. Verificar la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Calidad. Revisar la asignación planificada y la asignación real.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un Plan de Calidad para el área de Tecnología de la Información.

B. La organización no tiene los currículum vitae actualizados del personal contratado a través de un proveedor.

C. Se tiene en cuenta en la planificación, las actividades de ejecución de controles de calidad; sin embargo, no se toma en cuenta las actividades de planificación ni ejecución de labores de aseguramiento de la calidad.

P017: PROCEDIMIENTO PARA LA AUDITORÍA DEL PLAN DE COMPRAS DE TECNOLOGÍAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar el proceso de elaboración y ejecución del Plan de Compras de Tecnologías de Información en la organización[11], con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Verificación del proceso de elaboración del PCTI.

B. Revisión del alineamiento del PCTI al PEI.

C. Revisión del documento del PCTI.

D. Revisión del análisis de generación de valor del PCTI.

E. Verificación de la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del PCTI.

[11] En adelante se identificará al Plan de Compras de Tecnologías de Información con las iniciales PCTI.

El alcance del procedimiento no incluye:

A. Evaluación del financiamiento o costos relativos al pago de las compras.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Plan Estratégico de Informática.
B. Planes de Proyecto de desarrollo de sistemas de información.
C. Planes de Proyecto de compra de sistemas de información.
D. Plan de Contingencias de Informática.
E. Plan de Continuidad de Negocio.
F. Plan de Seguridad de la Información.
G. Plan de Licenciamiento de Software.
H. Plan de Capacitación.
I. Plan de Mantenimiento Preventivo.
J. Plan de Mantenimiento Correctivo.
K. Planificación de Labores de Rutina.
L. Plan de Calidad.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el proceso de elaboración del PCTI. Verificar que se haya realizado lo siguiente:

    a) Determinación clara de los criterios para la priorización de las necesidades.
    b) Identificación de necesidades de hardware, software de base, sistemas de información y servicios relacionados, por cada área de la organización y para la organización en su conjunto.
    c) Elaboración del documento del PCTI.
    d) Asignación de presupuesto, cronogramas y responsabilidades para la ejecución de las acciones del PCTI.

C. Revisar el documento del PCTI. Verificar que contenga por lo menos lo siguiente:

    a) Detalle de los bienes a comprar en unidades y en valores, para cada una de las áreas y para la organización en su conjunto.
    b) Detalle de los servicios a comprar en unidades y en valores, para cada una de las áreas y para la organización en su conjunto.
    c) Cronograma y Asignación de Responsabilidades.

D. Revisar el alineamiento del PCTI al PEI. El PCTI debe estar enmarcado en los lineamientos del PEI, teniendo en cuenta no sólo la tecnología actual, sino aquellas que serán de mayor beneficio para la organización en el futuro.

E. Revisar el análisis de generación de valor del PCTI. Verificar que el PCTI realmente genere valor para la organización; es decir, que como resultado de la ejecución del plan, se pueda acelerar la ejecución de procesos críticos con resultados de mejoras en ingresos netos ó evitando que se pierda dinero por riesgos o gastos innecesarios.

F. Verificar la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del PCTI. Revisar la asignación planificada y la asignación real.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un PCTI.

B. La organización tiene un PCTI muy genérico. No se detalla lo que se va a comprar, tanto en unidades como en valores, ni las marcas ni proveedores alternativos a los cuales se les podría comprar.

C. La organización prioriza las compras para el corto plazo, evitando inversiones mayores recuperables en el largo plazo.

P018: PROCEDIMIENTO PARA LA AUDITORÍA DEL REGLAMENTO DE ORGANIZACIÓN Y FUNCIONES

OBJETIVO

Analizar y evaluar el proceso de elaboración y ejecución de lo expuesto en el Reglamento de Organización y Funciones del área de Tecnología de Información de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión detallada del documento del Reglamento de Organización y Funciones del área de Tecnología de Información.

B. Revisión del currículum vitae del personal del área de Tecnología de Información.

C. Revisión del análisis de generación de valor del Reglamento de Organización y Funciones del área de Tecnología de Información.

El alcance del procedimiento no incluye:

A. Revisión del manual de organización y funciones.

B. Revisión de los manuales de procedimientos.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Plan Estratégico de Tecnologías de Información.
B. Currículum vitae detallado de todo el personal que labora en el área de Tecnología de la información: Incluye: gerentes, sub-gerentes, jefes de proyecto, analistas funcionales, analistas programadores, programadores, etc.
C. Reglamento de Organización y Funciones del área de Tecnología de Información.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el documento del Reglamento de Organización y Funciones del área de Tecnología de la Información. Verificar que contenga por lo menos lo siguiente:

   a) Antecedentes. Contiene una explicación genérica del reglamento anterior y los cambios en las necesidades o la evidencia del requerimiento de mejoras para los cambios en el reglamento actual.

   b) Marco Jurídico. Indica la base legal para la elaboración del Reglamento de Organización y Funciones. Incluye: constitución política, leyes, decretos legislativos, resoluciones, oficios, circulares, etc.

   c) Objetivos. Relación de objetivos a cumplir que contribuyen a los objetivos estratégicos de la organización.

   d) Organización. Aquí se detalla tanto el organigrama general como el organigrama detallado de cada una de las áreas.

   e) Perfiles, Atribuciones y Responsabilidades. Aquí se detalla por cada área qué perfiles, atribuciones y responsabilidades tiene cada una de las áreas y puestos que conforman el área de Tecnología de la información.

   Si bien los elementos descritos serían aplicables principalmente en organizaciones del Estado, sería recomendable su adopción en lo pertinente, en organizaciones privadas.

C. Revisar detalladamente los currículum vitae del personal del área de Tecnología de Información, tanto del personal directamente contratado por la organización como del personal contratado a través de un proveedor.

D. Revisar el análisis de generación de valor del Reglamento de Organización y Funciones y su cumplimiento. Verificar que el Reglamento de Organización y Funciones realmente genere valor para la organización; es decir, que como

resultado de su puesta en práctica, se pueda acelerar la ejecución de procesos críticos con resultados de mejoras en ingresos netos ó evitando que se pierda dinero por riesgos o gastos innecesarios.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un Reglamento de Organización y Funciones. Comúnmente elaboran un reglamento interno cuando se procede con la auditoría.

B. La organización no tiene los currículum vitae actualizados del personal contratado a través de un proveedor. Algunas veces ni siquiera tiene actualizados los currículum vitae del personal recientemente contratado.

C. El personal no cubría o no cubre los requerimientos para el puesto al momento de ingresar a la organización o a la fecha.

P019: PROCEDIMIENTO PARA LA AUDITORÍA DEL MANUAL DE ORGANIZACIÓN Y FUNCIONES

OBJETIVO

Analizar y evaluar el proceso de elaboración y ejecución de lo expuesto en el Manual de Organización y Funciones del área de Tecnología de Información de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión detallada del documento del Manual de Organización y Funciones del área de Tecnología de Información.

B. Revisión del currículum vitae del personal del área de Tecnología de Información.

C. Revisión de las funciones reales de cada puesto del área de Tecnología de Información.

D. Revisión del análisis de generación de valor del Manual de Organización y Funciones del área de Tecnología de Información.

El alcance del procedimiento no incluye:

A. Revisión de los manuales de procedimientos.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Plan Estratégico de Tecnologías de información.
B. Currículum vitae detallado de todo el personal que labora en el área de Tecnología de la información: Incluye: gerentes, sub-gerentes, jefes de proyecto, analistas funcionales, analistas programadores, programadores, etc.
C. Reglamento de Organización y Funciones del área de Tecnología de la Información.
D. Manual de Organización y Funciones.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el documento del Manual de Organización y Funciones del área de Tecnología de la Información. Verificar que contenga por lo menos lo siguiente:

   a) Antecedentes. Contiene una explicación genérica de la anterior organización y los cambios en las necesidades o la evidencia del requerimiento de mejoras para los cambios en el manual actual.

   b) Marco Jurídico. Indica la base legal para la elaboración del Manual de Organización y Funciones. Incluye: constitución política, leyes, decretos legislativos, resoluciones, oficios, circulares, etc.

   c) Objetivos. Relación de objetivos a cumplir con el manual, que contribuyen a los objetivos estratégicos de la organización.

   d) Organización. Aquí se detalla tanto el organigrama general como el organigrama detallado de cada una de las áreas.

   e) Funciones. Aquí se detalla por cada área qué funciones generales y específicas realiza cada puesto. Por cada puesto se deberá indicar también a qué gerencia pertenece y a qué puesto reporta directamente.

C. Revisar detalladamente los currículum vitae del personal del área de Tecnología de Información, tanto del personal directamente contratado por la organización como del personal contratado a través de un proveedor.

D. Revisar las funciones reales de cada puesto del área de Tecnología de Información. Verificar que lo que realmente hacen coincida con lo expuesto en el manual de organización y funciones.

E. Revisar el análisis de generación de valor del Manual de Organización y Funciones y su cumplimiento. Verificar que el Manual de Organización y Funciones realmente genere valor para la organización; es decir, que como resultado de su puesta en práctica, se pueda acelerar la ejecución de procesos

críticos con resultados de mejoras en ingresos netos ó evitando que se pierda dinero por riesgos o gastos innecesarios.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un Manual de Organización y Funciones. Comúnmente elaboran un manual sobre la base de los perfiles actuales al momento que se procede con la auditoría.

B. La organización no tiene los currículum vitae actualizados del personal contratado a través de un proveedor. A veces ni siquiera tiene actualizados los currículum vitae del personal recientemente contratado.

C. El personal no cubría o no cubre los requerimientos para el puesto al momento de ingresar a la organización o no los cubre a la fecha.

D. El personal realiza funciones que no le competen.

E. El personal realiza funciones para las cuales no está capacitado.

P020: PROCEDIMIENTO PARA LA EVALUACIÓN DEL CURRÍCULUM VITAE DEL PERSONAL DE TECNOLOGÍA DE LA INFORMACIÓN

OBJETIVO

Analizar y evaluar el currículum vitae del personal del área de Tecnología de la Información de la organización[12], con el fin de identificar la probable pérdida de valor debido a fallas en los procesos de selección de personal.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión detallada del currículum vitae del personal del área de Tecnología de la Información.

B. Verificación del alineamiento del currículum vitae al reglamento de organización y funciones y en su defecto, a las necesidades de la organización para el período en evaluación.

El alcance del procedimiento no incluye:

A. Evaluación de desempeño del personal.

[12] Aquí se considera tanto a personal propio de la organización como personal colocado por proveedores.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Plan Estratégico de Informática.
B. Currículum vitae detallado de todo el personal que labora en el área de Tecnología de la información: Incluye: gerentes, sub-gerentes, jefes de proyecto, analistas funcionales, analistas programadores, programadores, etc.
C. Reglamento de Organización y Funciones del área de Tecnología de Información.
D. Manual de Organización y Funciones del área de Tecnología de Información.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente los currículum vitae del personal del área de Tecnología de la Información. Verificar que cada currículum vitae contenga lo siguiente:

   a) Datos Personales: nombre completo, dirección, teléfonos de contacto (casa, celular, etc.), estado civil, fecha de nacimiento, etc.

   b) Experiencia Laboral. Listado de lugares y nombres de puestos donde ha laborado el trabajador. Se debe incluir la lista de funciones que realizaba en sus centros de trabajo, así como las herramientas de tecnologías de información que utilizaban o han desarrollado. De ser personal joven, considerar también las prácticas pre-profesionales.

   c) Educación. Considerar la formación técnica o universitaria (pregrado y postgrado) del personal evaluado, así como sus capacitaciones, cursos, talleres, charlas y conferencias a las cuales ha asistido.

C. Verificar el alineamiento del currículum vitae al Reglamento de Organización y Funciones y en su defecto, a las necesidades de la organización para el período en evaluación.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene los currículum vitae actualizados del personal contratado a través de un proveedor. A veces ni siquiera tiene actualizados los currículum vitae del personal recientemente contratado.

B. El personal no cubría o no cubre los requerimientos para el puesto al momento de ingresar a la organización, y tampoco los cubre a la fecha.

P021: PROCEDIMIENTO PARA LA AUDITORÍA DEL INVENTARIO DE HARDWARE DE TECNOLOGÍA DE INFORMACIÓN

OBJETIVO

Analizar y evaluar el Inventario de Hardware de Tecnología de la Información[13] de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión detallada del documento del IHTI.

B. Revisión de procedimientos relativos a altas, bajas y mejoras en el hardware de Tecnología de la Información.

C. Verificación física de los documentos relativos a altas, bajas, cambios y transferencias en el hardware de Tecnología de la Información.

D. Verificación física de una muestra del IHTI.

E. Revisión y Evaluación de la correcta contabilización del IHTI.

F. Evaluación de la probable pérdida de valor por errores u omisiones.

El alcance del procedimiento no incluye:

A. Evaluación del inventario de software.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. IHTI en unidades de todas las oficinas a nivel nacional.

B. IHTI en valores de todas las oficinas a nivel nacional.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente el documento del IHTI. Verificar que se encuentren los siguientes tipos de hardware:

[13] En adelante se le llamará IHTI al Inventario de Hardware de Tecnología de la Información

- Equipos que forman parte de la computadora o están directamente conectados a ella: monitores, cases, teclados, mouses, impresoras, scanners, cámaras de computadora, computadoras portátiles, etc. Considerar además las partes internas: mainboard, tarjeta de red, tarjeta de sonido, tarjeta fax-modem, tarjeta de video, discos duros, unidades de diskette, lectoras de CD, grabadoras de CD, grabadoras de DVD.
- Equipos de red: routers, firewalls, switches, hubs, cableado, etc.
- Equipos relacionados a la energía eléctrica: estabilizadores de voltaje, supresor de picos, UPS, etc.

C. Revisar los procedimientos relativos a altas, bajas, transferencias y cambios en el hardware de Tecnología de Información. Considerar que estos procedimientos deben conducir a que se identifique únicamente a cada movimiento[14] que implique una operación contable, realizado sobre el hardware.

D. Verificar físicamente los documentos relativos a altas, bajas, cambios y transferencias en el hardware de Tecnología de la Información. Revisar que los documentos tengan las respectivas autorizaciones y que se detalle los activos fijos sobre los cuales se está tratando.

E. Verificar físicamente una muestra del IHTI. Tomar una muestra aleatoria estratificada por tipo de equipo y valor y revisar que físicamente se encuentren en las instalaciones de la organización o en aquellas a las cuales la organización haya dispuesto que estén, para beneficio directo o indirecto de esta.

F. Revisar y evaluar la correcta contabilización del IHTI. Verificar que se haya realizado una correcta contabilización en los siguientes casos:
   - Compras.
   - Altas.
   - Bajas.
   - Transferencias.
   - Depreciaciones.
   - Revaluaciones.
   - Ventas.
   - Provisión para desvalorización.
   - Registro en libro auxiliar de activos fijos.

G. Evaluar la probable pérdida de valor por errores u omisiones. Calcular el monto en los equipos que no aparecen, el monto en los equipos que no han sido contabilizados correctamente, etc.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un IHTI detallado ni en unidades ni en valores.

B. La organización tiene un IHTI incompleto.

[14] El término movimiento se refiere a: altas, bajas y cambios.

C. No se contabiliza adecuadamente el inventario. Comúnmente se envía al gasto aquello que debe considerarse como activo fijo.

D. No se conserva adecuadamente los equipos fuera de uso, provocando que se deterioren y ya no sirvan.

P022: PROCEDIMIENTO PARA LA AUDITORÍA DEL INVENTARIO DE SOFTWARE DE BASE

OBJETIVO

Analizar y evaluar el Inventario de Software de Base[15] de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión detallada del documento del ISB.

B. Revisión de procedimientos relativos a altas, bajas y mejoras en el software de base.

C. Verificación física de los documentos relativos a altas, bajas, cambios y transferencias en el software de base.

D. Verificación física de una muestra del ISB.

E. Revisión y Evaluación de la correcta contabilización del ISB.

F. Evaluación de la probable pérdida de valor por errores u omisiones.

El alcance del procedimiento no incluye:

A. Evaluación del Inventario de Sistemas de Información.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. ISB en unidades, de todas las oficinas a nivel nacional.

B. ISB en valores, de todas las oficinas a nivel nacional.

[15] En adelante al Inventario de Software de Base se le llamará ISB. Considérese como software de base a todo software que no sea sistema de información.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente el documento del ISB. Verificar lo siguiente:

a) Existencia de los siguientes tipos de software:
- Sistemas operativos.
- Administradores de bases de datos.
- Software de protección contra intrusos.
- Software de protección ante correos no deseados.
- Servidores web.
- Servidores para realizar copias de respaldo.
- Software de oficina.
- Servidores de correo.
- Clientes de correo.
- Software de Administración de centrales telefónicas.
- Software de Diseño Gráfico.
- Lenguajes de Programación.
- Herramientas de Análisis de Sistemas.
- Herramientas de Diseño de Sistemas, etc.

b) El listado debe indicar claramente el número de licencias que se ha comprado, junto al número de usuarios que realmente las usa, y el número de usuarios que realmente las necesita. Si el software es shareware, freeware o libre, también debe estar indicado en el listado.

C. Revisar los procedimientos relativos a altas, bajas, transferencias y cambios en el software de base. Considerar que estos procedimientos deben conducir a que se identifique únicamente a cada movimiento que implique una operación contable, realizado sobre el software de base.

D. Verificar físicamente los documentos relativos a altas, bajas, cambios y transferencias en el software de base. Revisar que los documentos tengan las respectivas autorizaciones y que se detalle los activos intangibles sobre los cuales se está tratando.

E. Verificar físicamente una muestra del ISB. Tomar una muestra aleatoria estratificada por tipo de software y valor y revisar que físicamente se encuentren en las instalaciones de la organización o en aquellas instalaciones en las cuales la organización haya dispuesto que estén, para beneficio directo o indirecto de esta.

F. Revisar y evaluar la correcta contabilización del ISB. Verificar que se haya realizado una correcta contabilización en los siguientes casos:
- Compras.
- Altas.
- Bajas.
- Transferencias.
- Amortizaciones.
- Revaluaciones.
- Ventas.

- Provisión para desvalorización.
- Registro en libro auxiliar de activos intangibles.

G. Evaluar la probable pérdida de valor por errores u omisiones. Calcular el monto en el software de base que no aparece, el monto en el software de base que no ha sido contabilizado correctamente, el monto en multas y daño a la imagen de la organización que se produciría de ser intervenidos por tener software pirata, etc.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un ISB detallado ni en unidades ni en valores.

B. La organización tiene un ISB incompleto.

C. No se contabiliza adecuadamente el inventario. Comúnmente se envía al gasto aquello que debe considerarse como activo intangible. Dado que no se activa el software, tampoco se amortiza adecuadamente.

D. No se da de baja al software que ya no se usa.

E. Se tiene software pirata en la organización. Además no se tiene identificado cuánto realmente costaría licenciar todo, ni se ha visto cómo evitar su compra a través del uso de software libre o freeware.

P023: PROCEDIMIENTO PARA LA AUDITORÍA DEL INVENTARIO DE SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar el Inventario de Sistemas de Información[16] de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión detallada del documento del ISI.

B. Revisión de procedimientos relativos a altas, bajas y mejoras en los sistemas de información.

C. Verificación física de los documentos relativos a altas, bajas, cambios y transferencias en los sistemas de información.

[16] En adelante al Inventario de Sistemas de Información se le llamará ISI.

D. Verificación física de una muestra del ISI.

E. Revisión y Evaluación de la correcta contabilización del ISI.

F. Evaluación de la probable pérdida de valor por errores u omisiones.

El alcance del procedimiento no incluye:

A. Evaluación del Inventario de Software de Base.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. ISI en unidades, de todas las oficinas a nivel nacional.

B. ISI en valores, de todas las oficinas a nivel nacional.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente el documento del ISI. Verificar lo siguiente:

a) Existencia de los siguientes tipos de sistemas de información:
   - Sistemas de Procesamiento de Transacciones.
   - Sistemas Integrados al Cliente.
   - Sistemas de Información Gerencial.
   - Sistemas de Soporte a Grupos de Trabajo.
   - Sistemas de Soporte a Toma de Decisiones e Inteligencia Artificial.
   - Sistemas de Información Ejecutivos.
   - Sistemas de Información Interorganizacionales.
   - Sistemas de Planificación.

b) El listado debe indicar claramente el número de licencias que se ha comprado, junto al número de usuarios que realmente las usa, y el número de usuarios que realmente las necesita. Si el software es shareware, freeware o libre, también debe estar indicado en el listado. Deberá diferenciar además, los sistemas de información desarrollados de manera interna como aquellos sistemas de información comprados o desarrollados por proveedores.

C. Revisar los procedimientos relativos a altas, bajas, transferencias y cambios en los sistemas de información. Considerar que estos procedimientos deben conducir a que se identifique únicamente a cada movimiento que implique una operación contable, realizado sobre los sistemas de información.

D. Verificar físicamente los documentos relativos a altas, bajas, cambios y transferencias de los sistemas de información. Revisar que los documentos tengan las respectivas autorizaciones y que se detalle los activos intangibles sobre los cuales se está tratando.

E. Verificar físicamente una muestra del ISI. Tomar una muestra aleatoria estratificada por tipo de sistemas de información y valor, y revisar que físicamente se encuentren instalados en los locales de la organización o en aquellos locales en los cuales la organización haya dispuesto que estén, para beneficio directo o indirecto de esta.

F. Revisar y evaluar la correcta contabilización del ISI. Verificar que se haya realizado una correcta contabilización en los siguientes casos:
   - Compras.
   - Altas.
   - Bajas.
   - Transferencias.
   - Amortizaciones.
   - Revaluaciones.
   - Ventas.
   - Provisión para desvalorización.
   - Registro en libro auxiliar de activos intangibles.

H. Evaluar la probable pérdida de valor por errores u omisiones. Calcular el monto en los sistemas de información que no están instalados, el monto en los sistemas de información que no ha sido contabilizado correctamente, el monto en multas y daño a la imagen de la organización que se produciría de ser intervenidos por tener sistemas de información piratas, etc.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un ISI detallado ni en unidades ni en valores.

B. La organización tiene un ISI incompleto. En muchos casos se tiene en unidades y no en valores.

C. No se contabiliza adecuadamente el inventario. Comúnmente se envía al gasto aquello que debe considerarse como activo intangible.

D. No se da de baja a los sistemas de información que ya no se usan.

E. Se tiene sistemas de información piratas en la organización. Además no se tiene identificado cuánto realmente costaría licenciar todo, ni se ha visto cómo evitar su compra a través del uso de sistemas de información basados en software libre o sistemas de información freeware.

P024: PROCEDIMIENTO PARA LA AUDITORÍA DE LA SOLICITUDES Y EVALUACIONES DE LAS COTIZACIONES PARA LAS COMPRAS DE HARDWARE DE COMPUTADORAS, REDES Y EQUIPOS RELACIONADOS

OBJETIVO

Analizar y evaluar las cotizaciones para las compras de Hardware de Computadoras, Redes y Equipos Relacionados[17] en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de procedimientos relativos a la solicitud de cotizaciones para las compras de HCRER.

B. Revisión de procedimientos relativos a la evaluación de las cotizaciones para las compras de HCRER.

C. Revisión física de las cotizaciones para las compras de HCRER.

D. Revisión física de las evaluaciones de las cotizaciones para las compras de HCRER.

El alcance del procedimiento no incluye:

A. Revisión de contratos celebrados a partir de las cotizaciones.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Procedimientos para la solicitud de cotizaciones para la compra de HCRER.
B. Procedimientos para la evaluación de cotizaciones para la compra de HCRER.
C. Cotizaciones finales para la compra de HCRER.
D. Evaluaciones de las cotizaciones finales para la compra de HCRER.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

[17] En adelante se llamará HCRER al Hardware de Computadoras, Redes y Equipos relacionados.

A. Revisar la información indicada en la sección anterior.

B. Revisar los procedimientos relativos a la solicitud de cotizaciones para la compra de HCRER. Verificar que se solicite como mínimo lo siguiente:

   a) Especificaciones técnicas de lo solicitado.
   b) Niveles de servicio.
   c) Entregables y fechas de entrega.
   d) Costo total y forma de pago.
   e) Garantías.

C. Revisar los procedimientos relativos a la evaluación de las cotizaciones para la compra de HCRER. Verificar que se incluya como mínimo lo siguiente:

   a) Evaluación de Propuesta Técnica. Debe considerar ponderaciones para los principales aspectos de la propuesta técnica: especificaciones ténicas, niveles de servicio, entregables y fechas de entrega.
   b) Evaluación de Propuesta Económica. Debe considerar ponderaciones para los principales aspectos de la propuesta económica: costo total (inversiones y gastos) y forma de pago.

D. Revisar físicamente las cotizaciones para la compra de HCRER. Las cotizaciones deben contener por lo menos lo indicado en el punto B.

E. Revisar físicamente las evaluaciones de las cotizaciones para la compra de HCRER. Las evaluaciones de las cotizaciones deben contener lo indicado en el punto C. Además, debe someterse cada alternativa a un análisis de generación de valor.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no evalúa varios proveedores al momento de realizar una compra.

B. En las cotizaciones no se indica detalladamente las especificaciones técnicas de lo que se va a entregar, niveles de servicio, garantías, etc.

P025: PROCEDIMIENTO PARA LA AUDITORÍA DE LAS SOLICITUDES Y EVALUACIONES DE COTIZACIONES PARA LAS COMPRAS DE SOFTWARE DE BASE

OBJETIVO

Analizar y evaluar las cotizaciones para las compras de Software de Base[18] en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

[18] En adelante se llamará SB al Software de Base. SB es todo aquel software diferente a un sistema de información.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de procedimientos relativos a la solicitud de cotizaciones para las compras de SB.

B. Revisión de procedimientos relativos a la evaluación de las cotizaciones para las compras de SB.

C. Revisión física de las cotizaciones para las compras de SB.

D. Revisión física de las evaluaciones de las cotizaciones para las compras de SB.

El alcance del procedimiento no incluye:

A. Revisión de contratos celebrados a partir de las cotizaciones.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Procedimientos para la solicitud de cotizaciones para la compra de SB.
B. Procedimientos para la evaluación de cotizaciones para la compra de SB.
C. Cotizaciones finales para la compra de SB.
D. Evaluaciones de las cotizaciones finales para la compra de SB.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar los procedimientos relativos a la solicitud de cotizaciones para la compra de SB. Verificar que se solicite como mínimo lo siguiente:

    a) Especificaciones técnicas de lo solicitado.
    b) Niveles de servicio.
    c) Entregables y fechas de entrega
    d) Costo total y forma de pago.
    e) Garantías.

C. Revisar los procedimientos relativos a la evaluación de las cotizaciones para la compra de SB. Verificar que se incluya como mínimo lo siguiente:

    a) Evaluación de Propuesta Técnica. Debe considerar ponderaciones para los principales aspectos de la propuesta técnica: especificaciones ténicas, niveles de servicio, entregables y fechas de entrega.

b) Evaluación de Propuesta Económica. Debe considerar ponderaciones para los principales aspectos de la propuesta económica: costo total (inversiones y gastos) y forma de pago.

D. Revisar físicamente las cotizaciones para la compra de SB. Las cotizaciones deben contener lo indicado en el punto B.

E. Revisar físicamente las evaluaciones de las cotizaciones para la compra de SB. Las evaluaciones de las cotizaciones deben contener lo indicado en el punto C. Además, debe someterse cada alternativa a un análisis de generación de valor.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no evalúa varios proveedores al momento de realizar una compra.

B. En las cotizaciones no se indica detalladamente las especificaciones técnicas de lo que se va a entregar, niveles de servicio, garantías, etc.

P026: PROCEDIMIENTO PARA LA AUDITORÍA DE LAS SOLICITUDES Y EVALUACIONES DE COTIZACIONES PARA LAS COMPRAS DE SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar las cotizaciones para las compras de Sistemas de Información[19] en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de procedimientos relativos a la solicitud de cotizaciones para las compras de SI.

B. Revisión de procedimientos relativos a la evaluación de las cotizaciones para las compras de SI.

C. Revisión física de las cotizaciones para las compras de SI.

D. Revisión física de las evaluaciones de las cotizaciones para las compras de SI.

[19] En adelante se llamará SI a los sistemas de información.

El alcance del procedimiento no incluye:

A. Revisión de contratos celebrados a partir de las cotizaciones.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Procedimientos para la solicitud de cotizaciones para la compra de SI.
B. Procedimientos para la evaluación de cotizaciones para la compra de SI.
C. Cotizaciones finales para la compra de SI.
D. Evaluaciones de las cotizaciones finales para la compra de SI.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar los procedimientos relativos a la solicitud de cotizaciones para la compra de SI. Verificar que se solicite como mínimo lo siguiente:

   a) Objetivo y alcance del SI.
   b) Especificaciones técnicas de lo solicitado. Estas especificaciones deberían detalladarse por módulo, sub-módulo y opción del SI.
   c) Metodología de Trabajo.
   d) Niveles de servicio. Debería estar detallada la velocidad del servicio que se tendrá, así como el perfil de personas que colocarán en el proyecto. Es necesario que se solicite también el currículum vitae de las personas que trabajarán en el proyecto.
   e) Entregables y fechas de entrega. Debería entregarse un cronograma detallado de la ejecución del proyecto, por lo menos a nivel de semanas.
   f) Costo total y forma de pago. La cotización debería indicar claramente los pagos a realizar al momento de la entrega de cada etapa.
   g) Garantías.

C. Revisar los procedimientos relativos a la evaluación de las cotizaciones para la compra de SI. Verificar que se incluya como mínimo lo siguiente:

   a) Evaluación de Propuesta Técnica. Debe considerar ponderaciones para los principales aspectos de la propuesta técnica: especificaciones ténicas, metodología de trabajo, niveles de servicio, entregables y fechas de entrega.
   b) Evaluación de Propuesta Económica. Debe considerar ponderaciones para los principales aspectos de la propuesta económica: costo total (inversiones y gastos) y forma de pago.

D. Revisar físicamente las cotizaciones para la compra de SI. Las cotizaciones deben contener lo indicado en el punto B.

E. Revisar físicamente las evaluaciones de las cotizaciones para la compra de SI. Las evaluaciones de las cotizaciones deben contener lo indicado en el punto C. Además, debe someterse cada alternativa a un análisis de generación de valor.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no evalúa varios proveedores al momento de realizar una compra de sistemas de información.

B. En las cotizaciones no se indica detalladamente las especificaciones técnicas de lo que se va a entregar, niveles de servicio, garantías, etc.

C. Los proveedores no presentan ni plantean el uso de una metodología de trabajo en sus propuestas técnicas.

P027: PROCEDIMIENTO PARA LA AUDITORÍA DE LOS CONTRATOS DE COMPRA DE BIENES Y SERVICIOS, DE HARDWARE DE COMPUTADORAS, REDES Y EQUIPOS RELACIONADOS

OBJETIVO

Analizar y evaluar los contratos para las compras de bienes o servicios de Hardware de Computadoras, Redes y Equipos Relacionados[20] en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de procedimientos relativos a la generación de contratos para las compras de bienes o servicios de HCRER.

B. Revisión física de las cotizaciones y evaluaciones previas a los contratos para las compras de bienes o servicios de HCRER.

C. Revisión física de los contratos para las compras de bienes o servicios de HCRER.

D. Análisis de la generación de valor de los contratos.

[20] En adelante se llamará HCRER al Hardware de Computadoras, Redes y Equipos relacionados.

El alcance del procedimiento no incluye:

A. Análisis y Evaluación de propuestas no contempladas como parte del análisis para la generación del contrato.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Procedimientos para la generación de contratos para la compra de HCRER.
B. Cotizaciones finales para la compra de HCRER.
C. Evaluaciones de las cotizaciones finales para la compra de HCRER.
D. Contratos y adendas de contratos para las compras de HCRER.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar los procedimientos relativos a la generación de contratos para la compra de HCRER. De no existir procedimientos formales, indagar cuál es el procedimiento o los procedimientos reales para la compra de HCRER.

C. Revisar las cotizaciones y evaluaciones para la compra de HCRER. Ver procedimiento P024.

D. Revisar los contratos para la compra de HCRER. Verificar que se solicite como mínimo lo siguiente:

   a) Datos básicos iniciales del contrato:
      - Título del Contrato. En la parte superior de la primera hoja del contrato.
      - Datos del Contratante: nombre completo o razón social, RUC, dirección y alias.
      - Datos del Representante Legal del contratante: nombre completo, DNI y datos de la inscripción en registros públicos. De ser un contrato con una organización con representante legal de otro país, indicar también la nacionalidad o carnet de extranjería.
      - Datos del Contratado: nombre completo o razón social, RUC, dirección y alias.
      - Datos del Representante Legal del contratado: nombre completo, DNI y datos de la inscripción en registros públicos. De ser un contrato con una organización con representante legal de otro país, indicar también la nacionalidad o carnet de extranjería.
   b) Generalidades.
   c) Objeto del Contrato.
   d) Especificaciones técnicas de lo solicitado.
   e) Metodología.
   f) Plan de Trabajo.
   g) Entregables y fechas de entrega.

h) Niveles de servicio.
i) Condiciones para el adecuado funcionamiento de los equipos.
j) Vigencia del contrato.
k) Costo total y forma de pago.
l) Confidencialidad.
m) Garantías.
n) Limitaciones.
o) Penalidades.
p) Jurisdicción en caso de desacuerdos.
q) Cláusulas de protección contra riesgos (riesgos de operación, riesgos financieros, etc.).
r) Firmas y sellos de los representantes legales en todas las hojas.

E. Analizar la generación de valor del contrato. Ver procedimiento P059.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no evalúa varios proveedores al momento de realizar una compra.

B. En los contratos no se indica detalladamente las especificaciones técnicas de lo que se va a entregar, ni se hace referencia a propuestas técnicas donde se encuentre ese detalle.

C. No se hace contratos para la compra de hardware.

D. Se determina que gana el contrato, una propuesta para la compra de hardware que no fue ponderada como ganadora.

P028: PROCEDIMIENTO PARA LA AUDITORÍA DE LOS CONTRATOS PARA LAS COMPRAS DE SOFTWARE DE BASE

OBJETIVO

Analizar y evaluar los contratos para las compras de bienes o servicios de software de base en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de procedimientos relativos a la generación de contratos para las compras de bienes o servicios de SB.

B. Revisión física de las cotizaciones y evaluaciones previas a los contratos para las compras de bienes o servicios de SB.

C. Revisión física de los contratos para las compras de bienes o servicios de SB.

D. Análisis de la generación de valor de los contratos.

El alcance del procedimiento no incluye:

A. Análisis y Evaluación de propuestas no contempladas como parte del análisis para la generación del contrato.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Procedimientos para la generación de contratos para la compra de SB.
B. Cotizaciones finales para la compra de SB.
C. Evaluaciones de las cotizaciones finales para la compra de SB.
D. Contratos y adendas de contratos para las compras de SB.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar los procedimientos relativos a la generación de contratos para la compra de SB. De no existir procedimientos formales, indagar cuál es el procedimiento o los procedimientos reales para la compra de SB.

C. Revisar las cotizaciones y evaluaciones para la compra de SB. Ver procedimiento P025.

D. Revisar los contratos para la compra de SB. Verificar que se solicite como mínimo lo siguiente:

   a) Datos básicos iniciales del contrato:
      - Título del Contrato. En la parte superior de la primera hoja del contrato.
      - Datos del Contratante: nombre completo o razón social, RUC, dirección y alias.
      - Datos del Representante Legal del contratante: nombre completo, DNI y datos de la inscripción en registros públicos. De ser un contrato con una organización con representante legal de otro país, indicar también la nacionalidad o carnet de extranjería.
      - Datos del Contratado: nombre completo o razón social, RUC, dirección y alias.
      - Datos del Representante Legal del contratado: nombre completo, DNI y datos de la inscripción en registros públicos. De ser un contrato con una organización con representante legal de otro país, indicar también la nacionalidad o carnet de extranjería.
   b) Generalidades.
   c) Objeto del Contrato.
   d) Especificaciones técnicas de lo solicitado.

e) Metodología.
f) Plan de Trabajo.
g) Entregables y fechas de entrega.
h) Niveles de servicio.
f) Condiciones de hardware mínimas para el funcionamiento del SB.
g) Vigencia del contrato.
h) Costo total y forma de pago.
i) Confidencialidad.
j) Garantías.
k) Limitaciones.
l) Penalidades.
m) Jurisdicción en caso de desacuerdos.
n) Cláusulas de protección contra riesgos (riesgos de operación, riesgos financieros, etc.).
o) Firmas y sellos de los representantes legales en todas las hojas.

E. Analizar la generación de valor del contrato. Ver procedimiento P059.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no evalúa varios proveedores al momento de realizar una compra.

B. En los contratos no se indica detalladamente las especificaciones técnicas de lo que se va a entregar, ni se hace referencia a propuestas técnicas donde se encuentre ese detalle.

C. No se hace contratos para la compra de SB, aunque los montos sean elevados.

D. Se determina que gana el contrato, una propuesta para la compra SB que no fue ponderada como ganadora.

P029: PROCEDIMIENTO PARA LA AUDITORÍA DE LOS CONTRATOS PARA LAS COMPRAS DE SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar los contratos para las compras de bienes o servicios de sistemas de información en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

E. Revisión de procedimientos relativos a la generación de contratos para las compras de SI.

F. Revisión física de las cotizaciones y evaluaciones previas a los contratos para las compras de SI.

G. Revisión física de los contratos para las compras de SI.

H. Análisis de la generación de valor de los contratos.

El alcance del procedimiento no incluye:

B. Análisis y Evaluación de propuestas no contempladas como parte del análisis para la generación del contrato.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

E. Procedimientos para la generación de contratos para la compra de SI.
F. Cotizaciones finales para la compra de SI.
G. Evaluaciones de las cotizaciones finales para la compra de SI.
H. Contratos y adendas de contratos para las compras de SI.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

F. Revisar la información indicada en la sección anterior.

G. Revisar los procedimientos relativos a la generación de contratos para la compra de SI. De no existir procedimientos formales, indagar cuál es el procedimiento o los procedimientos reales para la compra de SI.

H. Revisar las cotizaciones y evaluaciones para la compra de SI. Ver procedimiento P026.

I. Revisar los contratos para la compra de SI. Verificar que se solicite como mínimo lo siguiente:

a) Datos básicos iniciales del contrato:
   - Título del Contrato. En la parte superior de la primera hoja del contrato.
   - Datos del Contratante: nombre completo o razón social, RUC, dirección y alias.
   - Datos del Representante Legal del contratante: nombre completo, DNI y datos de la inscripción en registros públicos. De ser un contrato con una organización con representante legal de otro país, indicar también la nacionalidad o carnet de extranjería.
   - Datos del Contratado: nombre completo o razón social, RUC, dirección y alias.
   - Datos del Representante Legal del contratado: nombre completo, DNI y datos de la inscripción en registros públicos. De ser un contrato con una organización con representante legal de otro país, indicar también la nacionalidad o carnet de extranjería.

b) Generalidades.
c) Objeto del Contrato.
d) Especificaciones técnicas de lo solicitado.
e) Metodología.
f) Plan de Trabajo.
g) Entregables y fechas de entrega.
h) Niveles de servicio.
i) Condiciones de hardware mínimas para el funcionamiento del SI.
j) Vigencia del contrato.
k) Costo total y forma de pago.
l) Confidencialidad.
m) Garantías.
n) Limitaciones.
o) Penalidades.
p) Jurisdicción en caso de desacuerdos.
q) Cláusulas de protección contra riesgos (riesgos de operación, riesgos financieros, etc.).
r) Firmas y sellos de los representantes legales en todas las hojas.

J. Analizar la generación de valor del contrato. Ver procedimiento P059.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

F. La organización no evalúa varios proveedores al momento de realizar una compra.

G. En los contratos no se indica detalladamente las especificaciones técnicas de lo que se va a entregar, ni se hace referencia a propuestas técnicas donde se encuentre ese detalle.

H. No se hace contratos para la compra de SI.

I. Se determina que gana el contrato, una propuesta para la compra de SI que no fue ponderada como ganadora.

J. No se incluye cláusulas que permitan a la organización, tener una protección ante la quiebra o retiro del mercado del proveedor; por ejemplo, pudiendo acceder al código fuente de su aplicación y a toda la documentación técnica en caso suceda la quiebra o retiro del mercado del proveedor.

P030: PROCEDIMIENTO PARA LA AUDITORÍA DE LOS CONTRATOS DE SEGUROS PARA LAS TECNOLOGÍAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar los contratos de seguros para las Tecnologías de Información[21] en la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de procedimientos relativos a la generación de contratos de seguros relativos a las TI.

B. Revisar cotizaciones y evaluaciones para la compra de seguros relativos a las TI.

C. Revisión de los contratos de seguros relativos a las TI.

D. Verificación del cumplimiento de las cláusulas de los contratos de seguros relativos a las TI.

E. Análisis de la generación de valor de los contratos de seguros relativos a las TI.

El alcance del procedimiento no incluye:

A. Análisis y Evaluación de propuestas no contempladas como parte del análisis para la generación del contrato.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Procedimientos para la generación de contratos de seguros relativos a las TI.
B. Contratos y adendas de contratos de seguros relativos a las TI.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

[21] En adelante se le llamará TI a las Tecnologías de Información.

B. Revisar los procedimientos relativos a la generación de contratos de seguros de TI. De no existir procedimientos formales, indagar cuál es el procedimiento o los procedimientos reales para la compra de seguros relativos a las TI.

C. Revisar las cotizaciones y evaluaciones para la compra de seguros relativos a las TI.

D. Revisar los contratos de seguros relativos a las TI. Verificar que se solicite por lo menos los siguientes tipos de coberturas de riesgos:

a) Incendio.
b) Rotura de Maquinaria.
c) Equipos Electrónicos.

La póliza de seguro de equipo electrónico debe contener secciones y cláusulas que contengan la siguiente información:

a) Datos básicos iniciales del contrato:
   - Título del Contrato. En la parte superior de la primera hoja del contrato.
   - Datos del Contratante: nombre completo o razón social, RUC, dirección y alias.
   - Datos del Representante Legal del Contratante: nombre completo, DNI y datos de la inscripción en registros públicos. De ser un contrato con una organización con representante legal de otro país, indicar también la nacionalidad o carnet de extranjería.
   - Datos del Contratado: nombre completo o razón social, RUC, dirección y alias.
   - Datos del Representante Legal del contratado: nombre completo, DNI y datos de la inscripción en registros públicos. De ser un contrato con una organización con representante legal de otro país, indicar también la nacionalidad o carnet de extranjería.
   - Datos del Beneficiario del Seguro (entidad a la cual se le endosa la póliza): nombre completo o razón social, RUC, dirección y alias.

b) Coberturas básicas. Ej: límites de cobertura según lo declarado.

c) Exclusiones Generales. Ej: guerra, invasión, reacción nuclear, acto intencional o negligencia del asegurado, etc.

d) Normas Generales.
   - Bases del Contrato. Ej: sometimiento a las condiciones impresas o mecanografiadas de la póliza, validez de la póliza sólo con la firma de funcionarios autorizados de la empresa de seguros, etc.
   - Plazo para rectificaciones convenidas.
   - Avisos y Comunicaciones. Ej: deben hacerse por escrito, toda comunicación con el corredor de seguros surte efecto en relación al asegurado, etc.
   - Pago de primas y resolución automática por falta de pago.
   - Resolución del Contrato.
   - Gastos que debe asumir el asegurado. Ej: gastos de emisión de la póliza, gastos adicionales para el pago de un siniestro, etc.
   - Predominio de Condiciones y/o Cláusulas. Ej: en caso de dudas prevalecen las condiciones mecanografiadas sobre las condiciones impresas.

- Declaración falsa y/o reticente. Ej: que el asegurado tenga más de un seguro de lo mismo, declaraciones inexactas, mala fe del asegurado al celebrarse el contrato o durante su vigencia, etc.
- Otros seguros. Ej: obligación del asegurado de declarar a la empresa aseguradora los seguros vigente o futuros que contrate referidos al riesgo cubierto.
- Adaptación Automática. Ej: cualquier modificación de las condiciones generales de la póliza que fuera aprobada legalmente y que represente un beneficio para el asegurado, se considerará automáticamente introducida dentro de la póliza, siempre que se produzca dentro del plazo de vigencia de la misma.
- Cláusula de Reclamación Fraudulenta.
- Arbitraje.
- Fuero o Jurisdicción a la que se someten la empresa aseguradora y el asegurado.
- Domicilio.

e) Objeto del Seguro. Ej: el asegurado deberá tomar las precauciones razonables y cumplir con las recomendaciones de la empresa aseguradora para prevenir daño y cumplirá con las recomendaciones del fabricante, la empresa aseguradora podrá inspeccionar en cualquier momento el riesgo, el asegurado deberá notificar cualquier cambio material en el riesgo, etc.

f) Procedimiento para el reclamo del siniestro.

g) Indemnización de los siniestros.
- Daños Materiales.
- Portadores de Datos Externos.
- Incremento en el Costo de Operación.

Para cada uno de los puntos referidos, se debe incluir:

- Alcance de la cobertura.
- Exclusiones Especiales.
- Disposiciones Aplicables. Ej: suma asegurada y base de la indemnización.

h) Cobertura para gastos extraordinarios por tiempo extra, trabajo nocturno, trabajo en días festivos y flete expreso.

i) Celebración de un contrato de mantenimiento.

j) Cobertura de Flete Aéreo.

k) Obligaciones relativas a equipos de climatización.

E. Verificar el cumplimiento de las cláusulas de los contratos de seguros relativos a las TI. Hacer una inspección a las instalaciones eléctricas y electrónicas que se encuentran en la empresa, principalmente a las ubicadas en los centros de cómputo principal y alterno. Ver procedimientos P055 y P057.

F. Analizar la generación de valor del contrato. Ver procedimiento P059.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no contrata seguros referidos a los equipos electrónicos.

B. La organización no cumple con las cláusulas de las pólizas de seguros referidas a los equipos electrónicos, poniéndose en riesgo el cobro del beneficio del seguro si se presentara una contingencia que los dañe.

P031: PROCEDIMIENTO PARA LA AUDITORÍA DE LA METODOLOGÍA DE DESARROLLO DE SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar la metodología de desarrollo de sistemas de información de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de la metodología de desarrollo de sistemas de información.

B. Revisión de la ejecución de la metodología de desarrollo de sistemas de información.

C. Análisis de la pérdida de valor debido a fallas en la metodología, en su ausencia o en su uso.

El alcance del procedimiento no incluye:

A. Revisión del proceso de selección de la metodología de desarrollo.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Listado de todos los manuales técnicos y manuales de usuario de los sistemas de información de la organización con sus respectivos accesos por área y usuario.

B. Acceso a todos los manuales técnicos y manuales de usuario de los sistemas de información de la organización.

C. Documentos sustentatorios del cumplimiento de la metodología.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar la metodología de desarrollo. La organización debe tener definida una metodología de desarrollo de sistemas de información basada en el ciclo de vida de desarrollo de sistemas de información: definición de requerimientos, planificación, análisis, diseño, implementación (codificación y pruebas), integración y pruebas, implantación, operación y mantenimiento. De manera ideal, la metodología debería contener los procesos indicados en la ISO/IEC 12207: procesos organizativos, procesos de apoyo y procesos principales.

C. Revisar la ejecución de la metodología de desarrollo.

- Si se ha usado metodología estructurada (Yourdon):
  - Especificaciones Funcionales y Técnicas. Detalle de la funcionalidad que tendrá el sistema módulo por módulo. Incluir hojas de análisis diferencial.
  - Análisis. Detalle de la definición de estándares para el análisis, los diagramas de contexto, diagrama cero y diagramas de flujos de datos y especificaciones funcionales con su respectivo diccionario de datos.
  - Diseño. Debe incluirse:
    - ✓ Definición de estándares para el diseño.
    - ✓ Detalle de las cartas estructuradas desde el módulo principal hasta los últimos módulos. Debe incluirse las cartas estructuradas con sus respectivos datos, controles y diccionario de datos.
    - ✓ Diseño de la base de datos.
    - ✓ Prototipo del Sistema.
    - ✓ Elaboración de los diversos planes sugeridos por la ISO/IEC 12207:
      - Plan de Pruebas.
      - Plan de Gestión de la Configuración.
      - Plan de Configuración de la Infraestructura.
      - Plan de Aseguramiento de la Calidad.
      - Plan de Control de Calidad.
      - Plan de Revisión Conjunta.
      - Plan de Validación.
      - Plan de Integración del Software.
      - Plan de Instalación del Software.
      - Plan de Migración de Datos.
      - Plan de Retirada del Software.
      - Plan de Formación.
    - ✓ Elaboración de Manuales Técnicos.
  - Implementación. Debe incluirse:
    - ✓ Definición de estándares para la implementación.
    - ✓ Detalle de los seudocódigos de los módulos (por lo menos los más complejos).
    - ✓ Documentación del código fuente.
  - Integración y Pruebas. Debe incluirse: ejecución del plan de pruebas, así como la ejecución en la cual se demuestra que todo funciona correctamente.
  - Implantación. Debe incluirse:

- ✓ Configuración del software de base.
- ✓ Ejecución del Plan de Migración de Datos.
- ✓ Ejecución del Plan de Integración.
- ✓ Instalación del Sistema.
- ✓ Configuración de Parámetros Generales del sistema.
- ✓ Capacitación al Usuario.

❖ Operación. Incluir actividades de soporte al usuario cuando el sistema ya ha sido implantado.

❖ Mantenimiento. Debe incluirse condiciones y nivel de servicio. Verificar además el retorno de la inversión. El mantenimiento debe incluir todos los procesos descritos en esta sección.

➢ Si se ha usado metodología orientada a objetos (UML):

❖ Especificaciones Funcionales y Técnicas. Debe incluirse:
- ✓ Detalle de la funcionalidad que tendrá el sistema módulo por módulo.
- ✓ Diagrama de casos de uso del sistema general. Incluye: casos de uso, secuencia, precondiciones y postcondiciones.

❖ Análisis y Diseño. Debe incluise:
- ✓ Prototipo del Sistema.
- ✓ Diagrama de casos de uso detallados.
- ✓ Diagrama de actividades.
- ✓ Diagrama de clases.
- ✓ Diagrama de estados.
- ✓ Diagrama de secuencias.
- ✓ Diagrama de componentes.
- ✓ Elaboración de los diversos planes sugeridos por la ISO/IEC 12207:
  - Plan de Pruebas.
  - Plan de Gestión de la Configuración.
  - Plan de Configuración de la Infraestructura.
  - Plan de Aseguramiento de la Calidad.
  - Plan de Control de Calidad.
  - Plan de Revisión Conjunta.
  - Plan de Validación.
  - Plan de Integración del Software.
  - Plan de Instalación del Software.
  - Plan de Migración de Datos.
  - Plan de Retirada del Software.
  - Plan de Formación.
- ✓ Elaboración de Manuales Técnicos.

❖ Implementación. Debe incluirse:
- ✓ Definición de estándares para la implementación.
- ✓ Elaboración de seudocódigos.
- ✓ Documentación del código fuente.

❖ Integración y Pruebas. Debe incluise:
- ✓ Configuración del software de base.
- ✓ Ejecución del Plan de Migración de Datos.
- ✓ Instalación del Sistema.
- ✓ Configuración de Parámetros Generales del sistema.
- ✓ Capacitación al Usuario.

❖ Implantación.
- ✓ Configuración del software de base.
- ✓ Ejecución del Plan de Migración de Datos.
- ✓ Instalación del Sistema.
- ✓ Configuración de Parámetros Generales del sistema.

- ✓ Capacitación al Usuario.
- ❖ Operación. Incluir actividades de soporte al usuario cuando el sistema ya ha sido implantado.
- ❖ Mantenimiento. Debe incluirse condiciones y niveles de servicio. Verificar además el retorno de la inversión.

D. Revisar que se haya realizado los registros correspondientes a la gestión cambios, gestión de versiones y gestión de configuraciones.

E. Analizar la pérdida de valor que se podría originar en caso no se tuviera una metodología o no se cumpliera con esta.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no ha definido una metodología formal de desarrollo de sistemas de información.

B. La organización no sigue una metodología formal de desarrollo de sistemas de información en personal contratado directamente, aunque la haya definido.

C. La organización no exige a los proveedores el seguimiento de una metodología formal de acuerdo al ciclo de vida de desarrollo de sistemas de información, aunque la haya definido.

D. Ausencia de tres planes críticos para minimizar las fallas del sistema de información: Plan de Pruebas, Plan de Migración de Datos y Plan de Integración.

P032: PROCEDIMIENTO PARA LA AUDITORÍA DE LA METODOLOGÍA DE ATENCIÓN DE REQUERIMIENTOS DE SOPORTE TÉCNICO

OBJETIVO

Analizar y evaluar la metodología para la atención de requerimientos de soporte técnico de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de la metodología de atención de requerimientos de soporte técnico de la organización, tanto los desarrollados por la organización como los comprados a proveedores.

El alcance del procedimiento no incluye:

A. Evaluación de la metodología de atención de requerimientos de desarrollo de sistemas de información.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Metodología de atención de requerimientos de soporte técnico cuando la realiza personal interno.

B. Metodología de atención de requerimientos de soporte técnico cuando la realiza un proveedor.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente la metodología de atención de requerimientos de soporte técnico, con personal interno o asignado de manera permanente por un proveedor. Debe incluirse los siguientes procesos:

   a) Recibir del requerimiento.
   b) Clasificar el requerimiento.
   c) Definición de criterios para priorizar la atención de requerimientos.
   d) En caso que el requerimiento no lo pueda atender el personal interno, ir al punto C.
   e) Definir procesos para la atención de requerimientos de cada tipo.
   f) Verificar la correcta ejecución de los procesos para la atención de requerimientos de cada tipo.
   g) Si el usuario no da su conformidad, regresar al punto “a”.
   h) Registrar los procesos en la atención de requerimientos de cada tipo.
   i) Consultar al usuario acerca de la calidad de la atención recibida.
   j) Realizar los registros correspondientes a la gestión cambios, gestión de versiones y gestión de configuraciones.
   k) Publicar sus niveles de servicio, así como la satisfacción de los usuarios, periódicamente.

C. Revisar detalladamente la metodología de atención de requerimientos de soporte técnico, con proveedores eventuales. Verificar:

   a) Contactar con proveedores alternativos.
   b) Recibir cotizaciones de varios proveedores.
   c) Evaluar cotizaciones de varios proveedores[22].
   d) Determinar la propuesta ganadora.
   e) Escoltar al personal de proveedor que realizará la atención del requerimiento. Esto se desarrollará en caso que el requerimiento se atienda

[22] Para la auditoría de los puntos “a”, “b” y “c”, ejecutar el procedimiento P024 ó el procedimiento P025.

dentro del local de la organización. De ser un servicio de larga duración, coordinar los pases y restricciones de acceso físico a las instalaciones, del personal del proveedor.

f) Solicitar informe (diagnóstico) antes de la ejecución de la solución.
g) Ejecutar el servicio.
h) Solicitar el informe final, luego de la ejecución de la solución.
i) Verificar la calidad del servicio recibido.
j) Si la calidad del servicio no satisface
    Si lo que falta es leve entonces
        Indicar que se regrese al punto g
    Caso contrario
        Si lo que falta es grave entonces
            Regresar al punto a
            Evaluar daños y acciones administrativas y/o legales
Caso Contrario
    Solicitar la aprobación del requerimiento por parte del usuario
    Si el usuario indica su aprobación entonces
        Solicitar el registro de la aprobación del requerimiento
    Caso Contrario
        Regresar al punto g.
k) Realizar los registros correspondientes a la gestión cambios, gestión de versiones y gestión de configuraciones.

D. Analizar la pérdida de valor que se podría originar por una inadecuada metodología de atención de requerimientos de soporte técnico. Calcular cuánto dinero podría perder la organización si la metodología es inadecuada o no se cumple, ya sea por error, omisión o malicia, así como la probabilidad de que esto ocurra.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. Se tiene requerimientos reconocidos como adecuados; pero, nunca son atendidos.

B. No existen criterios claramente definidos para priorizar la atención de los requerimientos de soporte técnico.

P033: PROCEDIMIENTO PARA LA AUDITORÍA DE LA METODOLOGÍA DE ATENCIÓN DE REQUERIMIENTOS DE DESARROLLO DE SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar la metodología para la atención de requerimientos de desarrollo de sistemas de información de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de la metodología de atención de requerimientos de desarrollo o mantenimiento de los sistemas de información que se encuentran en producción en la organización, tanto los desarrollados por la organización como los comprados a proveedores.

El alcance del procedimiento no incluye:

A. Evaluación de la metodología de atención de requerimientos de soporte técnico.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Metodología de atención de requerimientos de desarrollo o mantenimiento cuando la realiza personal interno.

B. Metodología de atención de requerimientos de desarrollo o mantenimiento cuando la realiza un proveedor.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente la metodología de atención de requerimientos de desarrollo de sistemas de información, con personal interno. Verificar:

   a) Recepción del requerimiento.
   b) Clasificación del requerimiento. Ej: corrección, opción adicional o proyecto.
   c) Criterios para priorizar la atención de requerimientos.
   d) En caso que el requerimiento no lo pueda atender el personal interno, ir al punto “C”.
   e) Definición de procesos para la atención de requerimientos de cada tipo. Debe incluirse los siguientes procesos:
      - Analizar el requerimiento.
      - Elaborar la especificación funcional y técnica para atender el requerimiento.
      - En general, seguir todos los pasos de la metodología de desarrollo de sistemas de información, alineada a lo que se exige en la ISO/IEC 12207. Ejecutar P031 aunque se trate sólo de un mantenimiento.
      - Realizar los registros correspondientes a la gestión cambios, gestión de versiones y gestión de configuraciones.
      - Solicitar al usuario la verificación del requerimiento.
      - Si el usuario verifica que el requerimiento ha sido atendido satisfactoriamente, debe aprobar el requerimiento; caso contrario, volver al paso b).
   f) Registro de los procesos en la atención de requerimientos de cada tipo.

C. Revisar detalladamente la metodología de atención de requerimientos de desarrollo de sistemas de información, con proveedores. Debe incluirse:

   a) Contactar con proveedores alternativos.
   b) Recibir cotizaciones de varios proveedores.
   c) Evaluar cotizaciones de varios proveedores[23].

[23] Para la auditoría de los puntos “a”, “b” y “c”, ejecutar el procedimiento P026.

d) Determinar la propuesta ganadora.
e) Escoltar al personal de proveedor que realizará la atención del requerimiento. Esto en caso el requerimiento se atienda dentro del local de la organización. De ser un servicio de larga duración, coordinar los pases y restricciones de acceso físico a las instalaciones, del personal del proveedor.
f) Solicitar informe previo (diagnóstico) a la ejecución de la solución.
g) Ejecutar el servicio.
h) Solicitar el informe final, luego de la ejecución de la solución.
i) Verificación de la calidad del servicio recibido.
j) Si la calidad del servicio no satisface

```
Si lo que falta es leve entonces
        Indicar que se regrese al punto g
Caso contrario
        Si lo que falta es grave entonces
                Regresar al punto a
Caso Contrario
        Solicitar la aprobación del requerimiento por parte del usuario.
        Si el usuario indica su aprobación entonces
                Solicitar la aprobación a la atención del requerimiento
        Caso Contrario
                Regresar al punto g.
```

l) Realizar los registros correspondientes a la gestión cambios, gestión de versiones y gestión de configuraciones.

D. Analizar la pérdida de valor que se podría originar por una inadecuada metodología de atención de requerimientos de desarrollo de sistemas de información. Calcular cuánto dinero podría perder la organización si la metodología es inadecuada o no se cumple, ya sea por error, omisión o malicia, así como la probabilidad de que esto ocurra.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. Se tiene requerimientos reconocidos como adecuados; pero, nunca son atendidos.

B. Se tiene requerimientos reconocidos como adecuados; pero, su atención demora meses o años, dado que no son atendidos con la prioridad debida.

C. No existen criterios claramente definidos para priorizar la atención de los requerimientos.

P034: PROCEDIMIENTO PARA LA AUDITORÍA DE LA DOCUMENTACIÓN DE LOS MANUALES TÉCNICOS DE LOS SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar la documentación de los manuales técnicos de los sistemas de información de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de los manuales técnicos de los sistemas de información de la organización, tanto los desarrollados por la organización como los comprados a proveedores.

B. Verificación del acceso de los usuarios del área de Tecnología de Información, a los manuales técnicos.

C. Revisión del procedimiento para otorgar accesos a los manuales técnicos.

D. Análisis de la pérdida de valor que se podría originar en caso no se tuviera los manuales técnicos.

El alcance del procedimiento no incluye:

A. Revisión de manuales de usuario de los sistemas de información de la organización.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Listado de todos los manuales técnicos de los sistemas de información de la organización con sus respectivos accesos por área y usuario.

B. Acceso a todos los manuales técnicos de los sistemas de información de la organización.

C. Procedimiento para otorgar accesos a los manuales técnicos.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente los manuales técnicos de los sistemas de información de la organización, tanto los desarrollados por la organización como los comprados a proveedores. Verificar lo siguiente:

   a) Existencia de los manuales técnicos.

   b) Por cada manual técnico revisar:

      - Debe existir documentación técnica sobre cada una de las etapas del ciclo de vida de desarrollo de sistemas de información, de acuerdo a la metodología de desarrollo que use la organización o el proveedor (estructurada, orientada a objetos, etc.).

      - Claridad de los textos y herramientas gráficas del documento.

      - Verificar que el manual contenga lo que se establece en el procedimiento P031, para la metodología de desarrollo de sistemas de información.

C. Verificar el acceso de los usuarios a los manuales técnicos. Los usuarios del área de Tecnología de Información necesitan tener el acceso de lectura sobre los manuales técnicos, los cuales comúnmente se encuentran en un directorio compartido o en la Intranet de la organización. De no tener el acceso, por lo menos debe existir una relación de manuales técnicos para que cuando se requiera, el personal del área de Tecnología de Información sepa de su existencia y solicite su acceso.

D. Revisar el procedimiento para otorgar accesos a los manuales técnicos de la organización. El procedimiento debe incluir como mínimo la aprobación del jefe o gerente de área dentro del área de Tecnología de Información.

E. Analizar la pérdida de valor que se podría originar en caso no se tuviera los manuales técnicos de los sistemas de información o se otorgara un acceso indebido. Calcular cuánto dinero podría perder la organización si alguien tuviera acceso a un manual técnico (junto al acceso indebido al sistema de información correspondiente) e hiciera un daño mínimo o un daño total sobre la base de datos, ya sea por error, omisión o malicia, así como la probabilidad de que esto ocurra.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene manuales de técnicos de los sistemas de información desarrollados por personal contratado directamente.

B. La organización no exige a los proveedores de sistemas de información, el desarrollo y entrega de manuales técnicos.

C. Los manuales técnicos son muy simples y no cubren las necesidades de aprendizaje técnico de los sistemas de información.

P035: PROCEDIMIENTO PARA LA AUDITORÍA DE LA DOCUMENTACIÓN DE MANUALES DE USUARIO DE LOS SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar la documentación de los manuales de usuario de los sistemas de información de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de los manuales de usuario de los sistemas de información de la organización, tanto los desarrollados por la organización como los comprados a proveedores.

B. Verificación del acceso de los usuarios a los manuales.

C. Revisión del procedimiento para otorgar accesos a los manuales de usuario.

D. Análisis de la pérdida de valor que se podría originar en caso no se tuviera los manuales de usuario o su acceso.

El alcance del procedimiento no incluye:

A. Revisión de manuales técnicos de los sistemas de información de la organización.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Listado de todos los manuales de usuario de los sistemas de información de la organización con sus respectivos accesos por área y usuario.

B. Acceso a todos los manuales de usuarios de los sistemas de información de la organización.

C. Procedimiento para otorgar accesos a los manuales de usuario.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar los manuales de usuario de los sistemas de información de la organización, tanto los desarrollados por la organización como los comprados a proveedores. Verificar lo siguiente:

   a) Existencia de los manuales de usuario.
   b) Por cada manual de usuario revisar:
      - Suficiencia de las opciones tratadas. Deben estar incluidas todas y cada una de las opciones del sistema de información en el manual de usuario.
      - Claridad de los textos y herramientas gráficas. La explicación sobre el uso de cada opción debe conducir a un autoaprendizaje por parte del usuario. Para ello es necesario que se disponga de herramientas gráficas además de las pantallas del sistema.

C. Verificar el acceso de los usuarios a los manuales. Los usuarios de los sistemas de información necesitan tener el acceso de lectura sobre los manuales de usuario, los cuales comúnmente se encuentran en un directorio compartido o en la Intranet de la organización. De no tener el acceso, por lo menos debe existir una relación de manuales de usuario para que cuando se requiera, el usuario sepa de su existencia.

D. Revisar el procedimiento para otorgar accesos a los manuales de usuario de la organización. El procedimiento debe incluir como mínimo la aprobación del jefe o gerente de área junto a la revisión de la Unidad de Riesgos, en caso exista.

E. Analizar la pérdida de valor que se podría originar en caso no se tuviera los manuales de usuario de los sistemas de información o se otorgara un acceso indebido. Calcular cuánto dinero podría perder la organización si alguien tuviera acceso a un manual de usuario (junto al acceso indebido al sistema de información correspondiente) e hiciera un daño mínimo o un daño total sobre la base de datos, ya sea por error, omisión o malicia, así como la probabilidad de que esto ocurra.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene manuales de usuario de los sistemas de información desarrollados por personal contratado directamente.

B. La organización no exige a los proveedores de sistemas de información, el desarrollo y entrega de manuales de usuario.

C. Los manuales de usuario son muy simples y no cubren las necesidades de aprendizaje de los sistemas de información.

P036: PROCEDIMIENTO PARA LA AUDITORÍA DE LA ARQUITECTURA DE LA RED DE TECNOLOGÍAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar la Arquitectura de la Red de Tecnologías de Información[24] de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión detallada del documento de la ARTI.

B. Verificación física de la ARTI.

C. Evaluación de la probable pérdida de valor por errores en la ARTI.

El alcance del procedimiento no incluye:

A. Evaluación de los sistemas de información que operan sobre la ARTI.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Plan Estratégico de Informática.
B. Documento de la ARTI.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente el documento de la ARTI.

   a) Revisar los siguientes tipos de hardware en los diversos locales en cada edificio, pISO/IEC y oficina (no necesariamente deben estar todos):

      - Equipos de red: routers, firewalls, switches, hubs, cableado, etc. Ej: verificar que el cableado esté colocado ordenadamente en estantes (“racks”) y en pisos técnicos (falsos pisos).

[24] En adelante se le llamará ARTI a la Arquitectura de la Red de Tecnologías de Información

- Puntos de la Red de Datos. Ej: verificar cercanía a motores y puntos conectores a la red de energía eléctrica.
- Velocidad de los enlaces de las redes internas. Ej: 10 Mbps, 100 Mbps o 1000 Mbps.
- Equipos y velocidad de conexión a servicios Internet como línea dedicada o línea RDSI. Ej: 128 Kbps, 256 Kbps, 2 Mbps, etc.
- Equipos Servidores.
- Equipos Clientes.

b) Revisar los siguientes tipos de software de base en los diversos locales en cada edificio, piso, servidor y oficina (no necesariamente deben estar todos):

- Sistemas Operativos.
- Servidores Proxy.
- Servidores Web.
- Servidores de Correo.
- Sistemas Administradores de Bases de Datos.
- Servidores de Aplicaciones.
- Servidores de Archivos.
- Servidores Backup.
- Servidores de Centrales Telefónicas.

C. Verificar físicamente la ARTI. Verificar físicamente que se encuentren todos los componentes descritos en el documento de la ARTI. Comprobar además las velocidades de transmisión indicadas tanto en la red interna como en Internet u otro servicio de red dado por un proveedor.

D. Evaluar la probable pérdida de valor por errores en la ARTI. Calcular el monto en los equipos que no aparecen, software de base que se compró y nunca se usó, servidores que fueron alquilados y no fueron reemplazados cuando pasó la necesidad del alquiler, velocidades de transmisión que no permiten trabajar adecuadamente a los usuarios, etc.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un documento formal sobre la ARTI.

B. La organización tiene un documento incompleto o desactualizado sobre la ARTI.

C. La ARTI tiene tecnologías muy diversas que necesitan la creación y mantenimiento de una serie de interfaces que implican mayor costo y tiempo de procesamiento y desarrollo.

D. La ARTI se vuelve más diversa con cada compra de aplicaciones a un proveedor.

E. Se tiene arquitectura de software propietaria; es decir, la organización debe pagar licencias por la arquitectura de software de base que utiliza, pudiendo usar software libre.

F. Se tiene arquitectura de hardware que condiciona que sólo determinado tipo de software pueda funcionar sobre ella.

P037: PROCEDIMIENTO PARA LA AUDITORÍA DE LA SEGURIDAD DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar la seguridad de acceso a los sistemas de información de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de los accesos del personal sobre las opciones de los diversos sistemas de información.

B. Revisión del procedimiento para otorgar accesos al personal.

C. Verificación aleatoria sobre el permISO/IEC único y exclusivo del personal a las opciones a las cuales se les ha otorgado acceso.

D. Análisis de la pérdida de valor que se podría originar en caso se violase la seguridad de acceso o se otorgara un acceso indebido.

El alcance del procedimiento no incluye:

A. Verificación de la seguridad de acceso a carpetas en servidores.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Listado de todos los accesos de todos los usuarios sobre los sistemas de información.

B. Procedimiento para otorgar accesos a los usuarios.

C. Acceso a todos los sistemas de información que otorgan accesos en la organización, en modo lectura; es decir, acceso sólo a opciones de consulta y reportes.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente los accesos del personal sobre las opciones de los diversos sistemas de información. Por cada área y usuario, revisar la lista de sistemas de información a los cuales puede acceder y por cada sistema de información, la lista de opciones. Verificar si el personal realmente necesita ingresar a un sistema de información u opción.

C. Revisar el procedimiento para otorgar accesos al personal. Verificar que incluya por lo menos lo siguiente:

   a) Autorización del gerente o jefe de área del usuario.
   b) Verificación de la Unidad de Riesgos, si existe.

   Es necesario sentarse con el operador que asigna los accesos y ver con detalle cómo realiza la asignación de accesos en los diversos sistemas de información, a través de ejemplos reales de acuerdo a los requerimientos que tiene pendientes. Observar cualquier tema irregular.

D. Verificar de manera aleatoria el acceso único y exclusivo del personal a las opciones a las cuales se les ha otorgado permiso. Realizar lo siguiente:

   a) Revisar que la pantalla de acceso tenga como mínimo la exigencia de ingresar el nombre de usuario y la clave. El sistema no debe permitir que existan claves vacías ni que se pueda fallar en el ingreso de la clave de manera indefinida (al tercer intento fallido debe evitar que siga intentando).

   b) Tomar una muestra estadística aleatoria y estratificada del personal que tiene acceso a los sistemas de información y luego verificar que sólo tengan acceso a lo asignado, tanto en la aplicación como en la base de datos.

E. Analizar la pérdida de valor que se podría originar en caso se violase la seguridad de acceso a los sistemas de información o se otorgara un acceso indebido. Calcular cuánto dinero podría perder la organización si alguien tuviera acceso a una opción o sistema de información que no debe e hiciera daño mínimo o un daño total sobre la base de datos, ya sea por error, omisión o malicia, así como la probabilidad de que esto ocurra.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. El personal puede ingresar a sistemas de información y opciones a las cuales no debería tener acceso.

B. Diversas personas del área de Tecnología de la Información, manipulan directamente la base de datos.

C. En la práctica, varias personas tienen acceso a asignar usuarios, además de la persona responsable.

D. En el módulo de asignación de accesos, se puede ver la clave de las personas. Además, al tener acceso a la base de datos, también pueden hacer lo mismo.

E. Se tienen que realizar operaciones manuales (con comandos sobre la base de datos) para asignar accesos en algunos casos, dado que falla el programa de asignación de accesos.

F. Los sistemas de información permiten que se ingrese con claves vacías, o claves que son iguales al nombre de usuario.

P038: PROCEDIMIENTO PARA LA AUDITORÍA DE LA SEGURIDAD DE ACCESO A LAS CARPETAS EN LOS SERVIDORES

OBJETIVO

Analizar y evaluar la seguridad de acceso a las carpetas en los servidores de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de los accesos del personal sobre las carpetas en los servidores.

B. Revisión del procedimiento para otorgar accesos al personal.

C. Verificación aleatoria sobre el permISO/IEC único y exclusivo del personal a las carpetas de los servidores, a las cuales se les ha otorgado acceso.

D. Análisis de la pérdida de valor que se podría originar en caso se violase la seguridad de acceso o se otorgara un acceso indebido.

El alcance del procedimiento no incluye:

A. Verificación de la seguridad de acceso a los sistemas de información.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Listado de todos los accesos de todos los usuarios sobre las carpetas de los servidores. En el listado debe indicarse claramente la ruta de red por cada carpeta.

B. Procedimiento para otorgar accesos a los usuarios sobre las carpetas de los servidores.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente los accesos del personal sobre las carpetas de los servidores. Por cada área y usuario, revisar la lista de carpetas a las cuales puede acceder. Verificar si el personal realmente necesita ingresar a una carpeta.

C. Revisar el procedimiento para otorgar accesos sobre las carpetas de los servidores. Verificar que incluya por lo menos lo siguiente:

   a) Autorización del gerente o jefe de área del usuario.
   b) Verificación de la Unidad de Riesgos, si existe.

   Es necesario sentarse con el operador que asigna los accesos y ver con detalle cómo realiza la asignación de accesos de las carpetas, a través de ejemplos reales de acuerdo a los requerimientos que tiene pendientes. Observar cualquier tema irregular.

D. Verificar de manera aleatoria el acceso único y exclusivo del personal a las carpetas a las cuales se les ha otorgado permiso. Para ello es necesario tomar una muestra estadística estratificada del personal que tiene acceso a carpetas y luego realizar lo siguiente:

   Para cada usuario de la muestra, realizar lo siguiente:

   - Ingresar al explorador de archivos[25] en la computadora del usuario.
   - Elegir 3 carpetas al azar, a las cuales el usuario no tenga acceso.
   - Elegir 3 carpetas al azar, a las cuales el usuario tenga acceso.
   - Para cada carpeta elegida en las líneas anteriores, realizar lo siguiente:
     - Ingresar la ruta en la cual se encuentra la carpeta. Pulsar “Enter”.
     - Verificar que el usuario pueda ver el contenido de la carpeta sólo si tiene el acceso.
     - Verificar si el usuario tiene permISO/IEC de lectura o escritura, según sea el acceso.

E. Analizar la pérdida de valor que se podría originar en caso se violase la seguridad de acceso a las carpetas o se otorgara un acceso indebido. Calcular cuánto dinero podría perder la organización si alguien tuviera acceso a una carpeta que no debe e hiciera daño mínimo o un daño total sobre los archivos de la carpeta, ya sea por error, omisión o malicia, así como la probabilidad de que esto ocurra.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

[25] Explorador de Windows en el sistema operativo Windows.

A. El personal usuario puede ingresar a carpetas a las cuales no debería tener acceso.

B. Diversas personas del área de Tecnología de Información, pueden acceder a carpetas a las cuales no deberían tener acceso.

C. En la práctica, varias personas tienen acceso a asignar carpetas, además de la persona responsable.

P039: PROCEDIMIENTO PARA LA AUDITORÍA DE LOS MANUALES DE PROCEDIMIENTOS DE SOPORTE TÉCNICO

OBJETIVO

Analizar y evaluar los manuales de procedimientos de soporte técnico de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Verificación de la existencia de procedimientos en cantidad suficiente para cubrir las principales operaciones de soporte técnico.

B. Revisión del contenido de los procedimientos de soporte técnico.

El alcance del procedimiento no incluye:

A. Evaluación de los manuales de procedimientos de desarrollo de sistemas.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Metodologías.
B. Manuales de Procedimientos.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Verificar el cumplimiento de los procedimientos de acuerdo a la metodología que se tenga como base.

C. Verificar la existencia de procedimientos en cantidad suficiente para cubrir las principales operaciones de soporte técnico. Debe incluirse en el manual, procedimientos para:

a) Help Desk.
- Consultas de usuarios.
- Instalación de software de base.
- Instalación de piezas y equipos de cómputo y red.
- Atención de fallas en hardware de equipos de cómputo y red.
- Atención de fallas en software de base instalado.

b) Programación de Tareas.
- Cierres periódicos.
- Tareas de las bases de datos.
- Tareas referentes a los servidores de correo.

c) Correo.
- Configuración de cuentas de correo internas.
- Configuración de cuentas de correo externas.
- Configuraciones de protección contra código malicioso.
- Configuraciones de protección contra correos no deseados (spam).
- Tareas de mantenimiento.

d) Seguridad de la Información.
- Accesos.
  - Accesos Físicos.
  - Accesos Lógicos. Considerar: Sistemas Operativos, Sistemas de Información, Software de Base, Envío de correos Externos, etc.
- Protección contra intrusos.
- Protección contra correos no deseados.
- Protección contra código malicioso: virus, spyware, adware, worms, etc.
- Copias de respaldo de la información. Incluir:
  - Bases de datos.
  - Archivos de usuarios.
  - Carpetas compartidas en servidores.
  - Configuraciones de Servidores.
  - Correo Electrónico.
  - Software de Base.
  - Código fuente de desarrollos de sistemas de información, etc.

D. Revisar el contenido de los procedimientos de soporte técnico. Verificar que el contenido de cada procedimiento tenga lo necesario para cumplir su objetivo.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene manuales de procedimientos de soporte técnico.

B. Los manuales de procedimientos de soporte técnico están incompletos o no están actualizados.

P040: PROCEDIMIENTO PARA LA AUDITORÍA DE LOS MANUALES DE PROCEDIMIENTOS DE DESARROLLO DE SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar los manuales de procedimientos de desarrollo de sistemas de información de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Verificación de la existencia de procedimientos en cantidad suficiente para cubrir las principales operaciones de desarrollo de sistemas de información.

B. Revisión del contenido de los procedimientos de desarrollo de sistemas de información.

El alcance del procedimiento no incluye:

A. Evaluación de los manuales de procedimientos de soporte técnico.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Metodologías de Desarrollo de Sistemas de Información.
B. Manuales de Procedimientos.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Verificar el cumplimiento de los procedimientos de acuerdo a la metodología que se tenga como base.

C. Verificar la existencia de procedimientos en cantidad suficiente para cubrir las principales operaciones de desarrollo de sistemas de información. Debe incluirse en el manual, procedimientos para:

   a) Priorizar la atención de requerimientos.
   b) Analizar los requerimientos.
   c) Actualizar la base de datos.
   d) Programar nuevas transacciones o modificaciones de transacciones existentes.
   e) Probar los desarrollos.

f) Corregir errores.
g) Aprobar los desarrollos.
h) Liberar nuevas versiones de los programas.
i) En general, se debe verificar que existan los procedimientos suficientes para cubrir las diversas actividades de la metodología de desarrollo de sistemas de información de la organización, la cual debe estar basada como mínimo en los procesos del ciclo de vida del software.

D. Revisar el contenido de los procedimientos de desarrollo de sistemas de información. Verificar que el contenido de cada procedimiento tenga lo necesario para cumplir su objetivo.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene manuales de procedimientos de desarrollo de sistemas de información.

B. Los manuales de procedimientos de desarrollo de sistemas de información están incompletos o no están actualizados.

C. Se tiene metodologías y procedimientos para el desarrollo de sistemas de información bastante buenos; sin embargo, no se cumplen en la práctica.

P041: PROCEDIMIENTO PARA LA REVISIÓN DE LOS FORMULARIOS DE CONTROL DE ENTREGABLES DE PROYECTOS Y REQUERIMIENTOS DE DESARROLLO DE SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar los formularios de control de entregables de proyectos y requerimientos de desarrollo de sistemas de información de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de los formularios de control de entregables de proyectos y requerimientos de desarrollo o mantenimiento de los sistemas de información de la organización, tanto los desarrollados por la organización como los comprados a proveedores.

B. Análisis de la generación de valor relativa a la correcta o incorrecta emisión de los formularios de control de entregables.

El alcance del procedimiento no incluye:

A. Evaluación de formularios de control de entregables referidos a requerimientos de soporte técnico.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Metodología de atención de requerimientos de desarrollo o mantenimiento cuando la realiza personal interno.

B. Metodología de atención de requerimientos de desarrollo o mantenimiento cuando la realiza un proveedor.

C. Formularios de control de entregables de desarrollo o mantenimiento cuando la realiza personal interno.

D. Formularios de control de entregables de atención de requerimientos de desarrollo o mantenimiento cuando la realiza un proveedor.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente el formulario de control de entregables de proyectos y requerimientos de desarrollo de sistemas de información, con personal interno. Verificar que contenga por lo menos los siguientes datos:

   a) Nombre del Proyecto (en caso que el requerimiento sea parte de un proyecto).
   b) Requerimiento.
   c) Fecha de Inicio.
   d) Fecha de Fin.
   e) Aprobación de Control de Calidad del área de Tecnología de la Información.
   f) Aprobación de por lo menos un usuario del requerimiento.
   g) Aprobación de la gerencia o gerencias usuarias del requerimiento.

C. Analizar la generación de valor relativa a la correcta o incorrecta emisión de los formularios de control de entregables. Calcular cuánto dinero ha perdido o podría perder la organización por no controlar adecuadamente los entregables de los proyectos o requerimientos de desarrollo o mantenimiento de sistemas de información.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. Los entregables son aceptados sin ser revisados por el usuario o el área de Tecnología de Información.

B. Los entregables son revisados sin haberse realizado todas las pruebas estándares para el control de calidad.

P042: PROCEDIMIENTO PARA REALIZAR SEGUIMIENTO DE INFORMES DE AUDITORÍA INTERNA

OBJETIVO

Dar las pautas para realizar seguimiento a los informes anteriores de auditoría interna, lo cual se realiza como parte de la labor rutinaria del área de Auditoría Interna.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de los informes de auditoría interna anteriores.

B. Verificación de la inclusión de las observaciones de los informes de auditoría interna anteriores en el seguimiento.

C. Verificación de la inclusión de las observaciones de los informes de auditoría externa (auditores externos u organismos reguladores) anteriores en el seguimiento.

D. Identificación de las observaciones de informes anteriores que a la fecha no hayan sido subsanadas.

E. Realización del seguimiento de las observaciones descritas en el punto C.

El alcance del procedimiento no incluye:

A. Evaluación o juicio de la calidad de los informes pasados.

ENTRADAS

Para realizar esta actividad se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Informes de Auditoría Interna.

B. Informes de Auditoría Externa, tanto de auditores externos como organismos reguladores.
C. Documentación que ha presentado el área auditada para levantar las observaciones descritas en los informes.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente los informes de auditoría interna anteriores.

C. Verificar la inclusión de las observaciones de los informes de auditoría interna anteriores en el seguimiento. Revisar que no sólo estén las observaciones del informe anterior, sino también todas las observaciones que aún no estén subsanadas de informes de mayor antigüedad.

D. Verificar la inclusión de las observaciones de los informes de auditoría externa (tanto de auditores externos como organismos reguladores) anteriores en el seguimiento. Revisar que no sólo estén las observaciones del informe anterior, sino también todas las observaciones que aún no estén subsanadas de informes de mayor antigüedad.

E. Identificar las observaciones de informes anteriores que a la fecha no hayan sido subsanadas. Resaltar aquellas observaciones que la gerencia auditada ha dicho que estarían subsanadas a la fecha de la revisión.

F. Realizar el seguimiento de las observaciones de informes anteriores que a la fecha no hayan sido subsanadas. Revisar detalladamente la información y posteriormente se debe realizar muestreos, inspecciones y entrevistas para constatar las acciones realizadas para subsanar cada observación.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. Las áreas auditadas no han avanzado las acciones para levantar las observaciones.

B. Las áreas auditadas han avanzado parcialmente las acciones para levantar las observaciones.

C. Las áreas auditadas reportan como concluidas, acciones que no se han realizado o se encuentran en proceso.

P043: PROCEDIMIENTO PARA REALIZAR SEGUIMIENTO DE INFORMES DE AUDITORÍA EXTERNA

OBJETIVO

Dar las pautas para realizar seguimiento de informes anteriores de auditoría externa, lo cual se realiza como parte de la labor de auditoría interna.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de los informes de auditoría externa anteriores, tanto de auditores externos contratados como auditores del organismo regulador.

B. Verificación de la inclusión de las observaciones de los informes de auditoría externa anteriores en el seguimiento de los informes de auditoría interna.

El alcance del procedimiento no incluye:

A. Seguimiento de informes de auditoría interna.

ENTRADAS

Para realizar esta actividad se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Informes de Auditoría Externa (de auditores externos u organismos reguladores).
B. Informes de Seguimiento de Auditoría Interna.

PROCESO

A. Revisar la información indicada en la sección anterior.

B. Revisar los informes de auditoría externa anteriores, tanto de auditores externos contratados como auditores del organismo regulador. Resaltar aquellas observaciones que a la fecha de la revisión, la gerencia auditada había indicado que estarían subsanadas.

C. Verificar la inclusión de las observaciones de los informes de auditoría externa anteriores en el seguimiento de los informes de auditoría interna. Verificar que se hayan incluido tanto las observaciones de auditores externos contratados como las observaciones del organismo regulador.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. Las áreas auditadas no han avanzado las acciones para levantar las observaciones.

B. Las áreas auditadas han avanzado parcialmente las acciones para levantar las observaciones.

C. Las áreas auditadas reportan como concluidas, acciones que no se han realizado o se encuentran en proceso.

P044: PROCEDIMIENTO PARA LA AUDITORÍA DE CERTIFICACIONES DE CALIDAD DE TECNOLOGÍA DE INFORMACIÓN

OBJETIVO

Analizar y evaluar las certificaciones de calidad de la organización, relativas a las tecnologías de información, con el fin de identificar la probable pérdida de valor en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Identificación de las certificaciones de calidad relativas a las TI en la organización.

B. Revisión de los requerimientos de cada una de las certificaciones de calidad relativas a las TI en la organización.

C. Evaluación del cumplimiento de los requerimientos que exigen las certificaciones de calidad relativas a las TI.

D. Análisis de generación de valor debido a las certificaciones de calidad relativas a las tecnologías de información.

El alcance del procedimiento no incluye:

A. Evaluación de la conveniencia de la elección de una certificación u otra.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período en evaluación, la siguiente información:

A. Listado de certificaciones de calidad relativas a las TI.

B. Listado de requerimientos de cada una de las certificaciones de calidad relativas a las TI.
C. Manuales de Calidad relativos a las TI.
D. Metodologías relativas a las TI.
E. Manuales de Organización y Funciones relativos a las TI.
F. Manuales de Procedimientos relativos a las TI.
G. En general, solicitar todo documentos elaborado en cumplimiento de los requerimientos de las certificaciones de calidad relativas a las TI.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Identificar las certificaciones de calidad relativas a las TI y su gestión en la organización. Verificar que exista alguna de las siguientes certificaciones de calidad a nivel de la organización o a nivel del personal de áreas relativas a las TI como la Jefatura o Gerencia de Sistemas, el área de Riesgos y el área de Auditoría Interna:

   - Capability Maturity Model - CMM.
   - International Organization for Standardization - ISO. Ej: ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 13236, etc.
   - Information Technology Infrastructure Library – ITIL.
   - Project Management Institute - PMI. Ej: Project Management Professional (PMP).
   - Information Systems Audit and Control Asociation – ISACA. Ej: Certified Information Systems Auditor (CISA), y Certified Information Security Management (CISM).

C. Revisar los requerimientos de cada una de las certificaciones de calidad relativas a las TI que posee la organización. Revisar tanto los documentos como las acciones que exigen las certificaciones de calidad relativas a las TI.

D. Evaluar el cumplimiento de los requerimientos que exigen las certificaciones de calidad relativas a las TI. Evaluar tanto el cumplimiento de los requerimientos, como las acciones que se hayan realizado o se estén realizando para el cumplimiento de dichos requerimientos.

E. Analizar la generación de valor debido a las certificaciones de calidad relativas a las TI. Analizar el incremento o la disminución de valor debido al cumplimiento o la falta de cumplimiento de los requerimientos de las certificaciones de calidad relativas a las TI en la organización.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no está preparada para revalidar la certificación de calidad.

B. La organización tiene una certificación de calidad relativa a las TI; pero, no cumple con los requerimientos que la certificación estipula.

P045: PROCEDIMIENTO PARA LA AUDITORÍA DE LA EVALUACIÓN DE DESEMPEÑO DEL ÁREA DE TECNOLOGÍA DE INFORMACIÓN

OBJETIVO

Analizar y evaluar el proceso de evaluación del desempeño del área de Tecnología de la Información, con el fin de identificar la probable pérdida de valor en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de las evaluaciones de desempeño del área de Tecnología de Información.

B. Revisión de auditorías realizadas al área de Tecnología de la Información.

C. Análisis de la probable pérdida de valor por una inadecuada evaluación de desempeño al área de tecnología de la información.

El alcance del procedimiento no incluye:

A. Revisión de la evaluación de desempeño al personal del área de Tecnología de Información.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Informes de evaluación de desempeño realizadas al área de Tecnología de la Información.

B. Informes de auditoría realizadas al área de Tecnología de Información.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar las evaluaciones de desempeño del área de Tecnología de Información. Verificar que las evaluaciones de desempeño tengan un fuerte componente de la evaluación por parte de los usuarios de los servicios del área de Tecnología de Información y que sea coherente con los logros obtenidos por esta área durante el período en evaluación, de acuerdo a lo que establece el Plan Estratégico de la organización. Revisar además si se ha producido mejoras en el desempeño comparando la información de varios períodos consecutivos.

En general, las evaluaciones de desempeño deben referirse a la eficiencia y la eficacia de la gerencia del área de Tecnología de Información.

C. Revisar las auditorías realizadas al área de Tecnología de la Información. Verificar si las auditorías realizadas cubren los aspectos siguientes:

   a) Planificación y Organización.
   b) Adquisición e Implementación.
   c) Entrega de Servicios y Soporte.
   d) Monitoreo y Control.

D. Analizar la probable pérdida de valor por una inadecuada evaluación de desempeño al área de tecnología de la información.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no realiza evaluaciones de desempeño al área de Tecnología de Información.

B. Las evaluaciones de desempeño al área de Tecnología de Información no reflejan el sentir de los usuarios sobre la calidad del servicio recibido.

C. Las evaluaciones de desempeño y los informes de auditoría no guardan concordancia en cuanto a la eficiencia y la eficacia de la gerencia del área de Tecnología de Información.

D. La organización no realiza auditorías al área de Tecnología de Información.

E. La organización realiza auditorías al área de Tecnología de Información sin ninguna metodología formal. Comúnmente se evalúa la ejecución de las actividades realizadas, sin hacer un análisis de la planificación, la organización, el monitoreo y el control.

P046: PROCEDIMIENTO PARA LA AUDITORÍA DE LA EVALUACIÓN DE DESEMPEÑO DEL PERSONAL DE TECNOLOGÍA DE INFORMACIÓN

OBJETIVO

Analizar y evaluar el resultado de la evaluación de desempeño del personal del área de Tecnología de la Información, con el fin de identificar la probable pérdida de valor en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de las evaluaciones de desempeño al personal del área de Tecnología de la Información.

B. Revisión de los informes de auditoría al área de Tecnología de la Información.

C. Análisis de generación de valor de la evaluación de desempeño del personal del área de Tecnología de la Información.

El alcance del procedimiento no incluye:

A. Revisión de la evaluación de desempeño del área de Tecnología de la Información.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Informes de evaluación de desempeño realizadas al personal del área de Tecnología de Información.

B. Informes de auditoría al área de Tecnología de Información.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar la evaluación de desempeño al personal del área de Tecnología de la Información. Verificar que la evaluación tenga un fuerte componente de calificación de las áreas usuarias de los servicios del personal del área de Tecnología de la Información. La evaluación debe incluir la calificación de: jefes, compañeros de área, clientes de servicio tanto internos como externos y proveedores de bienes o servicios tanto internos como externos. Verificar también si el personal ha mejorado o empeorado su desempeño comparando las evaluaciones realizadas en períodos consecutivos. La evaluación de desempeño debe incluir desarrollo de competencias para la planificación, ejecución, seguimiento y control del trabajo que desempeñas. Las competencias directivas, son mucho más relevantes para personal que tiene recursos humanos a su cargo.

C. Revisar los informes de auditoría al área de Tecnología de la Información. Verificar en especial las observaciones relativas a un mal desempeño específico del personal del área de Tecnología de la Información y verificar además, su concordancia con la evaluación de desempeño realizada.

D. Analizar la generación de valor de la evaluación de desempeño del personal del área de Tecnología de Información. Es necesario evaluar si producto de una evaluación de desempeño, el personal mejoró su desempeño y es necesario calcular cuánto significó en términos monetarios la mejora organizacional producto de dicha evaluación.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no realiza evaluaciones de desempeño sobre el personal del área de Tecnología de Información.

B. Las diversas áreas usuarias colocan una calificación baja o muy baja a la calidad del servicio que ofrece el personal del área de Tecnología de Información.

C. La evaluación de desempeño realizada sobre el personal no coincide con lo expresado en los informes de auditoría.

P047: PROCEDIMIENTO PARA LA REVISIÓN DE LOS FORMULARIOS DE CONTROL DE CAMBIOS EN PROYECTOS DE COMPRA O DESARROLLO DE SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar los formularios de control de cambios de proyectos de compra o desarrollo de sistemas de información de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de la metodología de atención de requerimientos de desarrollo o mantenimiento de los sistemas de información de la organización, tanto los desarrollados por la organización como los comprados a proveedores.

B. Revisión de los formularios de control de cambios funcionales en proyectos.

C. Revisión de los formularios de control de cambios técnicos en proyectos.

D. Asignación de versión al módulo u opción afectada por el cambio solicitado.

E. Análisis de la probable pérdida de valor por la falta de registro de formularios de control de cambios.

El alcance del procedimiento no incluye:

A. Evaluación de la metodología de atención de requerimientos de soporte técnico.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Metodología de atención de requerimientos de desarrollo o mantenimiento cuando la realiza personal interno.
B. Metodología de atención de requerimientos de desarrollo o mantenimiento cuando la realiza un proveedor.
C. Formularios de control de cambios funcionales en proyectos.
D. Formularios de control de cambios técnicos en proyectos.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar la metodología de atención de requerimientos de desarrollo o mantenimiento de los sistemas de información de la organización, tanto los desarrollados por la organización como los comprados a proveedores. Verificar que la metodología contenga el uso de formularios de control de cambios funcionales y cambios técnicos en los proyectos.

C. Revisar de los formularios de control de cambios funcionales en proyectos. Verificar que contenga como mínimo la siguiente información:

   a) Datos Generales del Cambio Solicitado:
      - Nombre del Proyecto
      - Nombre del Documento
      - Versión del Documento
      - Módulo sobre el cual se aplicará el cambio.
      - Nombre de la Opción del Módulo sobre la cual se aplicará el cambio.
      - Transacción sobre la cual se aplicará el cambio.
      - Usuarios Involucrados.
      - Analista Responsable.
      - Programa.
      - Fecha y hora.
   b) Descripción funcional detallada del cambio solicitado.
      - Puntos y/o acuerdos pendientes.
      - Descripción del impacto dentro del sistema. Describir tareas que se tendrá que realizar a consecuencia del cambio.
      - Cambios a realizar en la base de datos.
      - Firma del Analista Asignado.
      - Firma del Usuario Responsable de la solicitud del cambio.

D. Revisar de los formularios de control de cambios técnicos en proyectos. Verificar que contenga como mínimo lo siguiente:

   a) Desarrollador.
   b) Fecha y Hora de los cambios.
   c) Nuevas transacciones o errores corregidos mediante el cambio.
   d) Detalle de los cambios a nivel de aplicaciones en el cliente.
      - Detalle de los cambios en código fuente cliente. Ej: Java Script.
      - Detalle de cambios en imágenes.
      - Detalle de cambios en estilos.
      - Detalle de cambios en textos.
      - Detalle de cambios en efectos visuales, etc.

e) Detalle de los cambios a nivel de aplicaciones en el servidor.
   - Detalle de los cambios en código fuente. Ej: código fuente en servidor web como ASP ó PHP.
   - Detalle de cambios en librerías de código fuente u objetos.
   - Detalle de los cambios en servidor de bases de datos.
     - ✓ Cambios en tablas. Ej: nombre, inclusión, modificación o eliminación de tablas.
     - ✓ Cambios en campos. Ej: nombre, inclusión, modificación o eliminación de campos.
     - ✓ Cambios en procedimientos almacenados ("stored procedures").
     - ✓ Cambios en programas de activación automática ("triggers").
     - ✓ Cambios en reglas.
     - ✓ Cambios en restricciones.
     - ✓ Cambios en definición de usuarios de la base de datos, etc.

F. Asignar versión al módulo u opción afectada por el cambio solicitado. Verificar que se haya llenado la hoja de control de versiones y se haya asignado la versión correcta (un número correlativo o decimales sobre el número existente dependiendo de la importancia de los cambios). La hoja de control de versiones debe contener como mínimo la siguiente información:

a) Datos Generales sobre la Versión:
   - Fecha y hora de la versión.
   - Versión.
   - Base de datos primaria.
   - Idioma.

b) Datos sobre el desarrollo. Considerar el tiempo estimado, el tiempo real y la diferencia entre las fechas y horas de inicio y fin de la versión.

c) Datos sobre las pruebas. Considerar el tiempo estimado, el tiempo real y la diferencia entre las fechas y horas de inicio y fin de la versión.

d) Alcances:
   - Transacción, Reporte o Proceso Batch (en lote).
   - Error.
   - Prioridad de atención del error.
   - Programador Responsable.
   - Reponsable de las pruebas.
   - Tiempo Estimado.
   - Tiempo Real.
   - Indicador de Logro (sí o no).

e) Resultados por cada uno de los recursos participantes:
   - Recurso.
   - Días y horas trabajados.
   - Tipo de desempeño realizado. Ej: alto, medio y bajo.
   - Comentarios del evaluador.
   - Comentarios del evaluado.
   - Firma del evaluador.

f) Comentarios Generales.

G. Analizar la probable pérdida de valor por la falta de registro de formularios de control de cambios. Analizar la probable pérdida de valor por fallas o gastos en exceso.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no documenta los cambios en los proyectos a nivel funcional.

B. La organización no documenta los cambios en los proyectos a nivel técnico.

C. Los cambios registrados no tienen toda la documentación que los sustente.

D. Se realizan muchos cambios sin las respectivas aprobaciones del personal encargado.

P048: PROCEDIMIENTO PARA LA REVISIÓN DE LOS FORMULARIOS DE CONTROL DE RIESGOS EN PROYECTOS DE COMPRA O DESARROLLO DE SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar los formularios de control de riesgos en proyectos de compra o desarrollo de sistemas de información, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de la metodología de atención de requerimientos de desarrollo o mantenimiento de los sistemas de información de la organización, tanto los desarrollados por la organización como los comprados a proveedores.
B. Revisión de los formularios de control de riesgos.
C. Análisis de la generación de valor relativa a la evaluación de riesgos en proyectos de este tipo.

El alcance del procedimiento no incluye:

A. Revisión de la metodología de evaluación de riesgos de la organización.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Metodología de atención de requerimientos de desarrollo o mantenimiento cuando la realiza personal interno.
B. Metodología de atención de requerimientos de desarrollo o mantenimiento cuando la realiza un proveedor.
C. Formularios de control de riesgos de proyectos.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar la metodología de atención de requerimientos de desarrollo o mantenimiento de los sistemas de información de la organización, tanto los desarrollados por la organización como los comprados a proveedores. Verificar que la metodología contenga el uso de formularios de control de riesgos en los proyectos.

C. Revisar los formularios de control de riesgos de proyectos. Verificar que contengan como mínimo la siguiente información:

   a) Riesgo Identificado.
   b) Fecha y hora de identificación.
   c) Causas.
   d) Efectos Probables.
   e) Acciones a realizar para minimizar el riesgo.
   f) Rango de fechas en las cuales se ejecutarán las acciones.
   g) Recursos necesarios para ejecutar las acciones para minimizar el riesgo.
   h) Responsable de la ejecución de las acciones para minimizar el riesgo.
   i) Nombre y Firma del Jefe de Proyecto del área de Tecnología de la Información y el proveedor (en caso exista un proveedor).
   j) Nombre y Firma del Líder de Usuarios.

D. Analizar la probable pérdida de valor por la falta de registro de formularios de control de riesgos. Analizar la probable pérdida de valor por fallas o gastos en exceso.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no realiza procesos de evaluación de riesgos en los proyectos de compra o desarrollo de sistemas de información.

B. La organización no documenta los riesgos en los proyectos de compra o desarrollo de sistemas de información.

C. La organización no realiza acciones para prevenir los riesgos en los proyectos de compra o desarrollo de sistemas de información.

D. La organización identifica los riesgos y propone acciones para mitigar sus efectos; sin embargo, estas acciones no son realizadas y no se hace seguimiento de su realización.

P049: PROCEDIMIENTO PARA LA REVISIÓN DE LOS FORMULARIOS DE SEGUIMIENTO DE AVANCES EN PROYECTOS DE COMPRA O DESARROLLO DE SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar los formularios de seguimiento de avances en proyectos de compra o desarrollo de sistemas de información, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de las metodologías de compra o desarrollo de sistemas de información de la organización.

B. Revisión de los formularios de seguimiento de avances de proyectos.

C. Análisis de la generación de valor relativa al seguimiento de avances en los proyectos.

El alcance del procedimiento no incluye:

A. Evaluación completa de los proyectos de compra o desarrollo de sistemas de información.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Metodología de desarrollo de sistemas de información de la organización.
B. Metodología de compra de sistemas de información de la organización.
C. Formularios de seguimiento de avances de proyectos de compra o desarrollo de sistemas de información.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar las metodologías de compra o desarrollo de sistemas de información de la organización. Verificar que incluyan la elaboración de formularios de seguimiento de avances de proyectos.

C. Revisar los formularios de seguimiento de avances de proyectos. Verificar que cada formato contenga como mínimo la siguiente información:

a) Nombre del Proyecto.
b) Fecha de Emisión del Formato de seguimiento de avances.
c) Rango de fechas del reporte de avance.
d) Actividades.
e) Fechas de inicio y fin planificadas de cada actividad.
f) Fechas de inicio y fin reales de cada actividad.
g) Porcentaje de avance de las actividades.
h) Recursos asignados inicialmente a las actividades.
i) Recursos asignados realmente a las actividades.
j) Nombre y firma del Jefe de Proyecto del área de Tecnología de la Información o el proveedor.

D. Analizar la pérdida de valor que se podría originar por un inadecuado seguimiento de avances en proyectos de compra o desarrollo de sistemas de información. Verificar probables pérdidas por pagos de servicios no efectuados o demoras por asignación de recursos que no eran los adecuados.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no realiza un adecuado seguimiento de avances de proyectos.

B. La organización no registra formularios de seguimiento de avances de proyectos.

C. Se pierde dinero por pagos de actividades que nunca fueron realizadas en los proyectos.

P050: PROCEDIMIENTO PARA LA AUDITORÍA DEL CONTROL DE CALIDAD DE LA ATENCIÓN DE REQUERIMIENTOS DE COMPRA O DESARROLLO DE SISTEMAS DE INFORMACIÓN

OBJETIVO

Analizar y evaluar el control de calidad en la atención de requerimientos de compra o desarrollo de sistemas de información, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de la metodología de atención de requerimientos de desarrollo o mantenimiento de los sistemas de información de la organización, tanto los desarrollados por la organización como los comprados a proveedores.

B. Revisión detallada del proceso de control de calidad inmerso en la metodología de desarrollo de sistemas de información de la organización.

C. Análisis de la generación de valor relativa al control de calidad de la atención de requerimientos de desarrollo de sistemas de información.

El alcance del procedimiento no incluye:

A. Evaluación del control de calidad de la atención de requerimientos de soporte técnico.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Metodología de atención de requerimientos de desarrollo o mantenimiento cuando la realiza personal interno.
B. Metodología de atención de requerimientos de desarrollo o mantenimiento cuando la realiza un proveedor.
C. Documentación del proceso de control de calidad de la atención de requerimientos de desarrollo de sistemas de información.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar la metodología de atención de requerimientos de desarrollo o mantenimiento de los sistemas de información de la organización, tanto los desarrollados por la organización como los comprados a proveedores. Verificar que se incluya procesos de control de calidad dentro de la metodología.

C. Revisar detalladamente el proceso de control de calidad inmerso en la metodología de desarrollo de sistemas de información de la organización. Verificar que el proceso de control de calidad incluya como mínimo las siguientes pruebas:

   a) Verificación de las especificaciones funcionales y técnicas. Verificar que las especificaciones funcionales y técnicas del sistema, sean las necesarias para cubrir los requerimientos de los usuarios.

   b) Pruebas de Interfase Gráfica de Usuario. Verificar:
      - Estándares de tamaños y tipos de letra.
      - Estándares de tamaños y colores de formularios.
      - Estándares de tamaños de imágenes.
      - Existencia de ayudas de texto y gráfico.

   c) Pruebas de Caja Negra. Verificar el cumplimiento de las especificaciones funcionales descritas en los formatos de control de cambios, tanto de las modificaciones como los nuevos requerimientos.

d) Pruebas de Caja Blanca. Revisar detalladamente el código fuente de las aplicaciones, objetos, “stored procedures” (procedimientos almacenados) y “triggers” (programas que se activan ante algún evento sobre la base de datos). Verificar que lo revisado cumpla con las especificaciones funcionales y técnicas acordadas.

e) Pruebas de Integración. Verificar que sea posible el acceso sin mensajes de error o problemas de algún tipo, a todas y cada una de las opciones partiendo del módulo más general a la opción más específica (integración descendente) y viceversa (integración ascendente).

f) Pruebas de Resistencia o Estrés. Verificar que las aplicaciones sean eficientes con un volumen de datos de acuerdo a las necesidades actuales y futuras, proyectándonos sobre la base del tiempo de vida del sistema de información.

g) Pruebas de Seguridad. Verificar que sólo personal autorizado tenga acceso a las diversas opciones del sistema.

h) Pruebas de Registro de Pistas de Auditoría. Verificar el registro de por lo menos el usuario, así como la fecha y hora de la última modificación sobre las tablas críticas. Verificar también en aquellas tablas que lo requieran, el registro de movimientos o relación de actualizaciones realizadas, junto al usuario y la fecha y hora de cada una de las modificaciones.

D. Analizar la pérdida de valor que se podría originar por un inadecuado control de calidad de la atención de requerimientos de desarrollo de sistemas de información. Valorizar los costos de los errores cometidos por el inadecuado control de calidad.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no realiza control de calidad en la atención de requerimientos de desarrollo de sistemas de información.

B. La organización realiza un inadecuado control de calidad en la atención de requerimientos de desarrollo de sistemas de información. El control de calidad no sigue ninguna metodología ni se toma en cuenta puntos realmente importantes a evaluar.

P051: PROCEDIMIENTO PARA LA AUDITORÍA DEL CONTROL DE CALIDAD DE LA ATENCIÓN DE REQUERIMIENTOS DE SOPORTE TÉCNICO

OBJETIVO

Analizar y evaluar el control de calidad de la atención de requerimientos de soporte técnico, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de la metodología de atención de requerimientos de soporte técnico, tanto los realizados por la organización como los realizados por proveedores.

B. Revisión detallada del proceso de control de calidad inmerso en la metodología de atención de requerimientos de soporte técnico.

C. Análisis de la generación de valor del control de calidad de la atención de requerimientos de soporte técnico.

El alcance del procedimiento no incluye:

A. Evaluación del control de calidad de la atención de requerimientos de desarrollo de sistemas de información.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Metodología de atención de requerimientos de soporte técnico cuando la realiza personal interno.
B. Metodología de atención de requerimientos de soporte técnico cuando la realiza un proveedor.
C. Documentación del proceso de control de calidad de la atención de requerimientos de soporte técnico.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar la metodología de atención de requerimientos de soporte técnico, tanto los realizados por la organización como los realizados por proveedores. Verificar que tenga inmerso un proceso de control de calidad.

C. Revisar detalladamente el proceso de control de calidad inmerso en la metodología de atención de requerimientos de soporte técnico. Verificar que el control de calidad contenga como mínimo lo siguiente:

   a) Cumplimiento de los requerimientos de correcciones o mejoras estipuladas inicialmente, tanto en funcionalidad, documentación y tiempo de entrega.

   b) Condiciones de finalización según cada tipo de requerimiento. Ej: correcto funcionamiento del software instalado, correcto funcionamiento del hardware instalado, valores apropiados en mediciones eléctricas, restricción real del acceso a determinados dispositivos o servicios tanto dentro como fuera de los locales de la organización, etc.

D. Analizar la pérdida de valor que se podría originar por un inadecuado control de calidad de la atención de requerimientos de soporte técnico. Valorizar los costos de los errores cometidos por un inadecuado control de calidad.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no realiza control de calidad en la atención de requerimientos de soporte técnico.

B. La organización realiza un inadecuado control de calidad en la atención de requerimientos de soporte técnico. El control de calidad no sigue ninguna metodología ni se toma en cuenta puntos realmente importantes a evaluar.

P052: PROCEDIMIENTO PARA ENTREVISTAR A LOS USUARIOS DE LAS TECNOLOGÍAS DE INFORMACIÓN

OBJETIVO

Dar las pautas para la correcta ejecución de entrevistas a los usuarios de las tecnologías de información, las cuales se realizan como parte de la labor de auditoría.

ALCANCE

El alcance del procedimiento incluye:

A. Coordinación de citas para las entrevistas.
B. Desarrollo de las entrevistas.

El alcance del procedimiento no incluye:

A. Evaluación en la computadora del software que utiliza el entrevistado.

ENTRADAS

Para realizar esta actividad se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Organigrama.
B. Lista de teléfonos y anexos de cada uno de los usuarios de las diversas áreas de la organización.
C. Procesos de cada una de las áreas: los que son soportados con sistemas de información, los que son soportados con software de oficina y los que son realizados de manera manual.

PROCESO

A continuación se detalla las actividades a realizar para las entrevistas con los usuarios durante el desarrollo de la auditoría de la gestión de tecnologías de información.

a. Sacar citas con usuarios de cada una de las gerencias en la Oficina Principal.

b. Sacar citas con cada una de las gerencias en las oficinas en provincias. El número de oficinas se determina el acuerdo al alcance de la auditoría.

c. Durante el desarrollo de cada cita:

   i. Tener a la mano el formato de resumen de entrevista.
   ii. Llenar los datos de la cabecera relativos a la entrevista: persona entrevistada, área, cargo, auditor que realiza la entrevista, fecha y hora.
   iii. Reflexionar que debemos mantener en todo instante una actitud totalmente objetiva y no parcializarnos ni a favor ni en contra del área de tecnología de información.
   iv. Llenar la sección “Temas Tratados” del formato de resumen de entrevista teniendo en cuenta las respuestas del usuario por lo siguiente:
      - Velocidad y Calidad del Servicio de Soporte Técnico. Consultar sobre:
        - Las atenciones de requerimientos pendientes.
        - Los requerimientos atendidos en el período en evaluación y períodos anteriores.
        - El servicio de la plataforma tecnológica actual: correo, Intranet, velocidad de Internet, velocidad de uso de los sistemas de información, etc.
      - Velocidad y Calidad del Servicio de Desarrollo de Sistemas de Información. Consultar sobre:
        - Las atenciones de requerimientos pendientes.
        - Los requerimientos atendidos en el período en evaluación y períodos anteriores.
        - El servicio de los sistemas de información actuales.

- Cantidad de trabajo manual que realizan fuera del sistema. Considerar:
  - Verificaciones de listados a mano.
  - Cálculos a mano.
  - Cálculos en hojas de cálculo.
  - Elaboración de documentos en procesadores de texto.

De notar que el entrevistado no conoce el tema, pedir de manera cortés el contacto con aquellos subordinados del entrevistado que sepan sobre el tema. Con los subordinados, repetir este mismo procedimiento (Punto C).

v. Llenar la sección “Acuerdos” sobre la base de:
- Información que el entrevistado ha quedado pendiente de enviar o encargar el envío.
- Indagaciones adicionales que ha sugerido el usuario al auditor, para que sean revisadas con mayor detenimiento.
- Reuniones futuras pactadas con el mismo entrevistado o con sus subordinados.
- Otros acuerdos relacionados con la auditoría a los cuales se haya llegado.
- En caso de no existir acuerdos, colocar la palabra “ninguno”.

SALIDAS

Al desarrollar esta actividad es común escuchar o darnos cuenta de lo siguiente:

A. Los usuarios gerentes comúnmente no están involucrados con los problemas relativos a las tecnologías de información.

B. Los usuarios se quejan de la mala calidad del trato de Soporte Técnico o área de Infraestructura de Tecnología de Información, o porque no les aclaran las dudas correctamente.

C. Los usuarios se quejan de tener requerimientos pendientes de desarrollo desde hace varios años.

D. Los usuarios se quejan que los sistemas de información no cubren sus necesidades para el soporte de las transacciones diarias.

E. Los usuarios se quejan del trato inadecuado ante la solicitud de nuevos requerimientos de opciones de sistemas de información.

F. Los usuarios se quejan que los sistemas de información presentan muchas fallas.

G. Los usuarios se quejan que las correcciones a las fallas demoran mucho en realizarse.

H. Comúnmente cada área maneja entre 15 a 25 reportes en hojas de cálculo, fuera del sistema, lo cual evidencia que los sistemas no están diseñados pensando en el mediano y largo plazo en cuanto a requerimientos futuros de reportes o necesidades de cálculo.

P053: PROCEDIMIENTO PARA LA AUDITORÍA DE LAS INSTALACIONES ELÉCTRICAS DE LOS EQUIPOS DE CÓMPUTO Y REDES

OBJETIVO

Analizar y evaluar las instalaciones eléctricas de los equipos de cómputo y redes de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de medidas y condiciones del pozo de tierra.

B. Revisión de medidas y condiciones de cajas de control de la corriente eléctrica.

C. Revisión de medidas y condiciones de tomacorrientes de equipos de cómputo.

D. Revisión de medidas y condiciones de equipos de suministro de energía eléctrica: UPS y generador.

E. Revisión de la frecuencia de los mantenimientos a las instalaciones de puesta a tierra.

F. Análisis de la pérdida de valor que se podría originar por probables daños en las instalaciones eléctricas.

El alcance del procedimiento no incluye:

A. Revisión técnica detallada de las instalaciones eléctricas.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Listado de personas que tienen relación con el mantenimiento de instalaciones eléctricas o con los proveedores que las realizan, con sus respectivos anexos, teléfonos o correos electrónicos.

B. Normas vigentes para los sistemas de conexión a Tierra. En el caso peruano, se tiene las siguientes normas (PROCOBRE, 2005):

   - NTP 370.052:1999 SEGURIDAD ELÉCTRICA. Materiales que constituyen el pozo de puesta a tierra. Elección de los materiales eléctricos en las instalaciones interiores para la puesta a tierra.

- NTP 370.053:1999 SEGURIDAD ELÉCTRICA. Enchufes y tomacorrientes con protección a tierra para uso doméstico y uso general similar.

- NTP 370.054:1999 SEGURIDAD ELÉCTRICA. Sistema de Puesta a Tierra, Glosario de Términos.

- NTP 370.055:1999 SEGURIDAD ELÉCTRICA. Electrodos de cobre para puesta a tierra.

C. Plano de instalaciones eléctricas de equipos de cómputo. Considerar: pozo de tierra, caja de control de la corriente eléctrica, tomacorrientes de equipos de cómputo y equipos de suministro de energía eléctrica (UPS y generador).

D. Informes técnicos de mantenimientos preventivos y correctivos anteriores.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información solicitada en la sección anterior.

B. Revisar medidas y condiciones del pozo de tierra de acuerdo a las normas vigentes.

a) Verificar el cálculo o la medición de lo siguiente:
   - Resistencia (R_E). Debe ser menor a 5 ohms[26]. Ver procedimiento P063.
   - Voltaje (U_{ST}). Ej: 0.9 V
   - Frecuencia (F_M). Ej: 111 Hz.
   - Resistencia de la Estaca de Voltaje (R^S). Ej: 0.100 K' ohms.
   - Resistencia de la Estaca de Corriente (R_H). Ej: 0.100 K' ohms.
   - Señal de Medición. Ej: 48 VAC.
   - Tamaño del Pozo de tierra. Ej: 2.5 m. alto y 1.0 m. de diámetro.

b) Verificar las condiciones:
   - El terreno o material usado para relleno no debe tener un índice (pH) de acidez, que cause corrosión al electrodo. El pH debe estar entre 6 (ácido) y 10 (alcalino). Si se usa materiales químicos de relleno, verificar que no esté en contra de las leyes de protección al ambiente. No debería usarse como relleno los siguientes materiales: arena, polvo de coque, ceniza, arcilla dura (no es adecuada ya que si es fuertemente compactada puede llegar a ser impermeable al agua y podría permanecer seca) y otros materiales ácidos o corrosivos.
   - Si el terreno tiene poca conductividad eléctrica, verificar que se haya usado como relleno (sólos o combinados) los siguientes materiales: bentonita (montmorillonita sódica, pH 10.5), yeso (sulfato de calcio, pH entre 6.2 y 6.9), sales (gel), etc.
   - Todas las uniones o conexiones bajo tierra deben estar construidas de modo que no se presente corrosión en la unión o conexión. Las conexiones entre los diversos componentes deben ser mecánicamente

[26] Esta única medición no garantiza que el sistema de puesta a tierra está en buenas condiciones. Por ejemplo, puede haber corrosión en los componentes del electrodo o en las uniones.

robustas, tener buena resistencia a la corrosión y baja resistividad eléctrica.
- Uniones o conexiones innecesarias.
- Existencia de corrosión en el recorrido del electrodo enterrado.

C. Revisar medidas y condiciones de cajas de control de la corriente eléctrica. Verificar:

a) El Tablero General de Electricidad debe tener llaves electromagnéticas.
b) Señalización del Tablero General de Electricidad.

D. Revisar medidas y condiciones de tomacorrientes de equipos de cómputo.

a) Los tomacorrientes de los equipos de cómputo deben tener línea a tierra.
b) Los tomacorrientes deben encontrarse sin deterioros físicos.

E. Revisar medidas y condiciones de equipos de suministro de energía eléctrica. Verificar:

a) Estado del UPS.
b) Estado del generador de corriente eléctrica.
c) Cableado no dañado.
d) Cableado aislado de manera que no se afecte con las condiciones del entorno. Debe estar empotrado con canaletas.

F. Revisar la frecuencia de los mantenimientos a las instalaciones de puesta a tierra.

G. Si la oficina se encuentra en lugares donde se dan rayos y truenos, como la Sierra por ejemplo, verificar la correcta instalación de pararrayos.

H. Analizar la pérdida de valor que se podría originar por probables daños en las instalaciones eléctricas. Recopilar además, información sobre los daños ocasionados a los equipos por problemas en las instalaciones eléctricas. De esa manera se tendría también una historia de los gastos en los cuales se ha incurrido.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no tiene un pozo de tierra.

B. La organización no realiza un mantenimiento adecuado al pozo de tierra.

C. La corriente eléctrica para los centros de cómputo no está estabilizada.

D. No se han implantado medidas de prevención contra cortes de energía eléctrica.

E. El Tablero General de Electricidad tiene llaves de cuchilla o mecánicas. Estas llaves tienen plomos en su interior como un elemento de seguridad, no siendo apropiado ante una sobrecarga eléctrica.

P054: PROCEDIMIENTO PARA LA AUDITORÍA DE LA SEGURIDAD DE ACCESO AL CENTRO DE CÓMPUTO PRINCIPAL

OBJETIVO

Analizar y evaluar la seguridad de acceso al centro de cómputo principal de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión del acceso por la puerta principal del edificio donde se encuentra el centro de cómputo principal.

B. Revisión del procedimiento en recepción para otorgar tickets de visitante y permitir el acceso a las instalaciones del edificio.

C. Revisión del acceso al pISO/IEC donde se encuentra el centro de cómputo principal.

D. Revisión del acceso por la entrada al centro de cómputo principal.

E. Análisis de la pérdida de valor que se podría originar en caso se violase la seguridad de acceso.

El alcance del procedimiento no incluye:

A. Revisión técnica de los equipos que sirven de apoyo para la seguridad de acceso.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Listado de personas que tienen relación con el permISO/IEC de acceso a las instalaciones del centro de cómputo, desde los vigilantes que están en la entrada, hasta el acceso a la puerta del centro de cómputo principal.

B. Capacitación otorgada al personal de seguridad en la puerta principal del edificio, referente a los criterios para decidir si se permite o no el ingreso de una persona a recepción.

C. Procedimientos para el personal, relacionados al acceso a las instalaciones, a personas ajenas a la organización.

D. Informes sobre incidentes relativos a la seguridad de acceso.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el acceso por la puerta principal del edificio donde se encuentra el centro de cómputo principal. Verificar lo siguiente:

   a) Criterios impartidos al personal de vigilancia para permitir el acceso de una persona al edificio.
   b) Revisión de bolsas, maletas u otro tipo de objetos en los cuales se pueda transportar armas.
   c) Detección de armas u objetos que pudieran servir para tal fin, sobre el cuerpo de las personas.

C. Revisar el procedimiento en recepción para otorgar tickets de visitante y permitir el acceso a las instalaciones del edificio. Verificar lo siguiente:

   a) Criterios impartidos al personal de recepción para permitir el acceso de una persona al edificio.
   b) Capacitación sobre reconocimiento de documentos de identidad falsos.
   c) Solicitud y custodia de identificación de las personas que van a acceder a las instalaciones del edificio.

D. Revisar el acceso al pISO/IEC donde se encuentra el centro de cómputo principal. Verificar lo siguiente:

   a) Existencia de personal encargado de recepción en el piso.
   b) Criterios impartidos al personal de recepción del pISO/IEC para permitir el acceso a las instalaciones.
   c) Existencia de dispositivo para colocar clave de seguridad para el ingreso.
   d) Estado de la puerta que permite el acceso al pISO/IEC (abierta o cerrada). Verificar esto en varias oportunidades para confirmar si fue una casualidad o es un descuido común el hecho de encontrar la puerta abierta.

E. Revisar el acceso por la entrada al centro de cómputo principal.

   a) Existencia de personal encargado de controlar el acceso.
   b) Criterios impartidos al personal encargado de controlar el acceso para decidir si permite a una persona dicho acceso.
   c) Existencia de dispositivo para colocar clave de seguridad para el ingreso.
   d) Estado de la puerta que permite el acceso al centro de cómputo principal (abierta o cerrada). Verificar esto en varias oportunidades para confirmar si fue una casualidad o es un descuido común, si la encontramos abierta.
   e) Registro de ingreso y salida de personal ajeno al área de Tecnología de Información.

F. Analizar la pérdida de valor que se podría originar en caso se violase la seguridad de acceso. Calcular cuánto dinero podría perder la organización si algún extraño que logre entrar al centro de cómputo principal, hiciera una daño mínimo o un daño total sobre sus instalaciones, así como la probabilidad de que esto ocurra.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. Continuamente se permite el ingreso al edificio a personas ajenas a las labores de la organización. Ejemplos: vendedores de comida, personas que vienen a realizar gestiones de otras organizaciones que se encuentran en el mismo edificio y transitan por pisos que no son los correctos, etc.

B. El personal de recepción sólo entrega el ticket de visitante y no pregunta a quién va a visitar la persona a la cual le entrega el ticket. Generalmente sólo pregunta el piso.

C. Pese a que las puertas tienen dispositivos para colocar claves de seguridad para el ingreso, permanecen abiertas.

D. La puerta de acceso al centro de cómputo no tiene dispositivo para colocar clave de seguridad.

E. No se lleva un registro de quiénes ingresan o salen del centro de cómputo principal, así como la hora en que produjo la entrada o la salida.

P055: PROCEDIMIENTO PARA LA AUDITORÍA DE LAS INSTALACIONES DEL CENTRO DE CÓMPUTO PRINCIPAL

OBJETIVO

Analizar y evaluar el estado de las instalaciones del centro de cómputo principal de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Verificación de la existencia de los equipos de acuerdo al inventario actualizado.

B. Verificación del funcionamiento de los equipos de cada tipo.

C. Verificación del funcionamiento de las tecnologías de información en los servidores.

D. Verificación del cumplimiento de las medidas de seguridad del centro de cómputo.

E. Análisis de la pérdida de valor que se podría originar por los errores u omisiones encontradas.

El alcance del procedimiento no incluye:

A. Revisión técnica de los equipos del centro de cómputo principal.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Inventario actualizado de los equipos del centro de cómputo principal. Debe pedirse que se diferencie los equipos alquilados, prestados o propios.
B. Inventario de tecnologías de información que existen en los servidores del centro de cómputo principal.
C. Reportes de mantenimientos realizados sobre los equipos.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Verificar la existencia de los equipos del centro de cómputo principal, de acuerdo al inventario actualizado. Revisar tanto los equipos alquilados, prestados o propios que se tenga en el centro de cómputo principal.

C. Verificar el funcionamiento de las tecnologías de información en los servidores.

D. Verificar el funcionamiento de los equipos de cada tipo: routers, switches, hubs, cableado, racks, computadoras servidores, equipo de aire acondicionado, alarma contra incendios, equipos de aire acondicionado, UPS, estabilizadores, supresores de picos, etc.

E. Verificar el cumplimiento de las medidas de seguridad del centro de cómputo. Seguir el procedimiento relativo a la seguridad física y la seguridad lógica que se detalla en el documento P010: “Procedimiento para la Auditoría del Plan de Seguridad de la Información”.

F. Analizar la pérdida de valor que se podría originar por los errores u omisiones encontradas. Calcular cuánto dinero podría perder la organización por daños mínimos o máximos sobre el centro de cómputo principal, ya sea por error, omisión o malicia, así como la probabilidad de que esto ocurra.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización tiene equipos que no usa en el centro de cómputo. Ejemplo: computadoras servidores o computadoras de usuarios. Algunas veces usan el centro de cómputo para guardar lo que no sirve, incluyendo material inflamable como maderas, cuadernos, etc.

B. La organización alquila servidores pudiendo ser reemplazados por computadoras fuera de uso.

C. Existen problemas de seguridad de la información diversos. Ver sección "Salidas", en el documento P010: "Procedimiento para la Auditoría del Plan de Seguridad de la Información".

P056: PROCEDIMIENTO PARA LA AUDITORÍA DE LA SEGURIDAD DE ACCESO AL CENTRO DE CÓMPUTO ALTERNO

OBJETIVO

Analizar y evaluar la seguridad de acceso al centro de cómputo alterno de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión del acceso por la puerta principal del edificio donde se encuentra el centro de cómputo alterno.

B. Revisión del acceso al pISO/IEC donde se encuentra el centro de cómputo alterno.

C. Revisión del acceso por la entrada al centro de cómputo alterno.

D. Análisis de la pérdida de valor que se podría originar en caso se violase la seguridad de acceso.

El alcance del procedimiento no incluye:

A. Revisión técnica de los equipos que sirven de apoyo para la seguridad de acceso.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Listado de personas que tienen la función de permitir el acceso a las instalaciones del centro de cómputo alterno, desde los vigilantes que están en la entrada, hasta el acceso a la puerta del centro de cómputo alterno.
B. Capacitación otorgada al personal de seguridad en la puerta principal del edificio, referente a los criterios para decidir si se permite o no el ingreso de una persona.
C. Informes sobre incidentes relativos a la seguridad de acceso.

D. Procedimientos para el personal, relacionados al acceso a las instalaciones, a personas ajenas a la organización.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar el acceso por la puerta principal del edificio donde se encuentra el centro de cómputo alterno. Verificar lo siguiente:

   a) Criterios impartidos al personal de vigilancia para permitir el acceso de una persona al edificio.
   b) Revisión de bolsas, maletas u otro tipo de objetos en los cuales se pueda transportar armas.
   c) Detección de armas u objetos que pudieran servir para tal fin, sobre el cuerpo de las personas.

C. Revisar el acceso al pISO/IEC donde se encuentra el centro de cómputo alterno. Verificar lo siguiente:

   a) Existencia de personal encargado de recepción en el piso.
   b) Criterios impartidos al personal de recepción del pISO/IEC para permitir el acceso a las instalaciones.
   c) Existencia de dispositivo para colocar clave de seguridad para el ingreso.
   d) Estado de la puerta que permite el acceso al pISO/IEC (abierta o cerrada). Verificar esto en varias oportunidades para confirmar si fue una casualidad o es un descuido común.

D. Revisar el acceso por la entrada al centro de cómputo alterno.

   a) Existencia de personal encargado de controlar el acceso.
   b) Criterios impartidos al personal encargado de controlar el acceso para decidir si permite a una persona dicho acceso.
   c) Existencia de dispositivo para colocar clave de seguridad para el ingreso.
   d) Estado de la puerta que permite el acceso al centro de cómputo alterno (abierta o cerrada). Verificar esto en varias oportunidades para confirmar si fue una casualidad o es un descuido común.

E. Analizar la pérdida de valor que se podría originar en caso se violase la seguridad de acceso. Calcular cuánto dinero podría perder la organización si algún extraño que logre entrar al centro de cómputo alterno, hiciera una daño mínimo o un daño total sobre sus instalaciones, así como la probabilidad de que esto ocurra.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. El acceso al local del centro de cómputo alterno es fácil, dado que es un edificio de atención al público. Cualquier persona podría subir por la puerta por la que accede el personal de la organización.

B. Basta con decir que trabajamos en la organización para que nos dejen subir sin problemas por todo el edificio.

C. En el pISO/IEC donde se encuentra el centro de cómputo alterno no existe vigilancia previa al ingreso al centro de cómputo alterno.

P057: PROCEDIMIENTO PARA LA AUDITORÍA DE LAS INSTALACIONES DEL CENTRO DE CÓMPUTO ALTERNO

OBJETIVO

Analizar y evaluar el estado de las instalaciones del centro de cómputo alterno de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Verificación de la existencia de los equipos de acuerdo al inventario actualizado.

B. Verificación del funcionamiento de los equipos de cada tipo.

C. Verificación del funcionamiento de las tecnologías de información en los servidores.

D. Verificación del cumplimiento de las medidas de seguridad del centro de cómputo.

E. Análisis de la pérdida de valor que se podría originar por los errores u omisiones encontradas.

El alcance del procedimiento no incluye:

A. Revisión técnica de los equipos del centro de cómputo alterno.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Inventario Actualizado de los equipos del centro de cómputo alterno. Debe pedirse que se diferencie los equipos alquilados, prestados o propios.
B. Inventario de tecnologías de información que existen en los servidores del centro de cómputo alterno.
C. Reportes de mantenimientos realizados sobre los equipos.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Verificar la existencia de los equipos del centro de cómputo alterno, de acuerdo al inventario actualizado. Revisar tanto los equipos alquilados, prestados o propios que se tenga en el centro de cómputo alterno.

C. Verificar el funcionamiento de los equipos de cada tipo. Por cada tipo de equipo: routers, switches, hubs, cableado, racks, computadoras servidores, equipo de aire acondicionado, alarma contra incendios, equipos de aire acondicionado, UPS, estabilizadores, supresores de picos, etc.

D. Verificar el funcionamiento de las tecnologías de información en los servidores del centro de cómputo alterno. Considerar además del inventario, que las tecnologías de información existentes, deben cubrir las necesidades de la organización ante una contingencia; por ello, el centro de cómputo alterno debe tener por lo menos lo mínimo indispensable para que la organización pueda funcionar, reemplazando al centro de cómputo principal de manera suficiente.

E. Verificar el cumplimiento de las medidas de seguridad del centro de cómputo. Seguir el procedimiento relativo a la seguridad física y la seguridad lógica que se detalla en el documento P010: “Procedimiento para la Auditoría del Plan de Seguridad de la Información”.

F. Analizar la pérdida de valor que se podría originar por los errores u omisiones encontradas, en el centro de cómputo alterno. Calcular cuánto dinero podría perder la organización por daños mínimos o máximos sobre el centro de cómputo alterno, ya sea por error, omisión o malicia, así como la probabilidad de que esto ocurra. Considerar además la pérdida de valor debido a que el centro de cómputo alterno no cumpla su función por no tener los sistemas de información necesarios para cubrir las necesidades de la organización ante una contingencia.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización tiene equipos que no usa en el centro de cómputo. Ejemplo: computadoras servidores y computadoras de usuarios. Comúnmente se usa para guardar cosas que ya no sirven, incluyendo material inflamable como madera, cuadernos, etc.

B. La organización alquila servidores pudiendo ser reemplazados por computadoras fuera de uso.

C. Existen problemas de seguridad de la información. Ver sección 5 “Hallazgos”, en el documento P010: “Procedimiento para la Auditoría del Plan de Seguridad de la Información”.

P058: PROCEDIMIENTO PARA LA AUDITORÍA DEL CABLEADO DE REDES DE DATOS

OBJETIVO

Analizar y evaluar el cableado de redes de datos de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de la ubicación y condiciones del cableado de redes de datos.

B. Revisión de la velocidad de la transmisión por el cableado de redes de datos.

C. Análisis de la pérdida de valor que se podría originar por ubicación o condiciones inapropiadas en el cableado de redes de datos.

El alcance del procedimiento no incluye:

B. Revisión técnica de los equipos a los cuales se conectan los cables de redes de datos.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Plano del cableado de redes de datos de la organización.
B. Informes técnicos de mantenimientos preventivos y correctivos anteriores.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información solicitada en la sección anterior.

B. Revisar la ubicación y condiciones del cableado de redes de datos. Verificar:
   a) Ubicación del Cableado.
      - El cableado no puede estar expuesto a altas temperaturas. Evitar que esté expuesto al sol.
      - El cableado no puede estar cerca de motores ni cables de corriente eléctrica.
   b) Condiciones del Cableado:
      - El cableado no debe estar dañado.
      - El cableado debe estar colocado ordenadamente en canaletas.
      - El cableado debe conectarse ordenadamente a los “racks”,

C. Revisar la velocidad de la transmisión por el cableado de redes de datos. Verificar que la velocidad sea la esperada: 10 Mbps, 100 Mbps, etc; visualizando la velocidad de la transmisión en las computadoras de los usuarios de diversas subredes.

D. Analizar la pérdida de valor que se podría originar por ubicación, velocidad o condiciones inapropiadas en el cableado de redes de datos. Calcular el monto perdido sobre la base de las interrupciones del trabajo del personal debido a la velocidad, las malas condiciones o ubicación del cableado de redes de datos, así como los montos de pago a proveedores por reparaciones de fallas que provocaron problemas mayores por no haber sido detectadas a tiempo.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. El cableado del centro de cómputo se encuentra disperso por el pISO/IEC sin ningún orden, con el consecuente riesgo que el personal lo pise y se puedan generar interrupciones en el servicio para los usuarios de las redes de cómputo.

B. No se usa adecuadamente los “racks”, pese a estar disponibles.

C. El cableado de redes de datos se coloca de manera muy cercana a los cables de corriente eléctrica.

D. El cableado de redes de datos no se encuentra ubicado apropiadamente dentro de canaletas para evitar perturbaciones o ruido en la señal.

E. El cableado está expuesto al sol.

F. La velocidad de la transmisión por el cableado de redes de datos es menor a la esperada. Comúnmente sucede porque las tarjetas de red o los “switches” o “hubs” no han sido actualizados a la velocidad que soporta el cableado.

P059: PROCEDIMIENTO PARA LA AUDITORÍA DEL CÁLCULO DE LA GENERACIÓN DE VALOR DE LOS PROYECTOS

OBJETIVO

Analizar y evaluar la forma en que se realiza el análisis de la generación de valor de los proyectos de la organización.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión del proceso de determinación del período de evaluación del proyecto.
B. Revisión del proceso de determinación de la tasa mínima atractiva de retorno.
C. Revisión del flujo de caja proyectado.

D. Revisión del proceso de cálculo de generación de valor del proyecto del proyecto.

El alcance del procedimiento no incluye:

A. Construcción de alternativas al proyecto en evaluación.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

B. Metodología para el cálculo de la generación de valor de los proyectos.
C. Cálculo de la generación de valor de todos los proyectos.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar la definición del período de evaluación del proyecto. Debe ser una decisión del directorio basada en alguna de las siguientes formas: tiempo de vida de las tecnologías de información del proyecto, período de planificación estratégica de la organización o un tiempo especialmente asignado por el directorio.

C. Revisar la definición de la tasa mínima atractiva de retorno de la inversión que será aplicada al cálculo del valor presente neto del proyecto. Esta tasa deberá ser determinada por el directorio; pero teniendo en cuenta que debe ser superior a las tasas libres de riesgo o riesgo mínimo (tasas por depósito a plazo fijo por ejemplo).

D. Revisar la identificación de los ingresos adicionales por el proyecto. Revisar que los ingresos adicionales se den tanto por el incremento en el margen de contribución (valor de venta menos costos variables) como por los ahorros generados por el proyecto. Considerar como ahorros no sólo los costos que ya no se darán por la mejora en un proceso, sino también el ahorro en multas que se presentarían si no se cumple con entregar un requerimiento o los márgenes que se dejarían de percibir por la inconformidad y retiro de los clientes de la empresa.

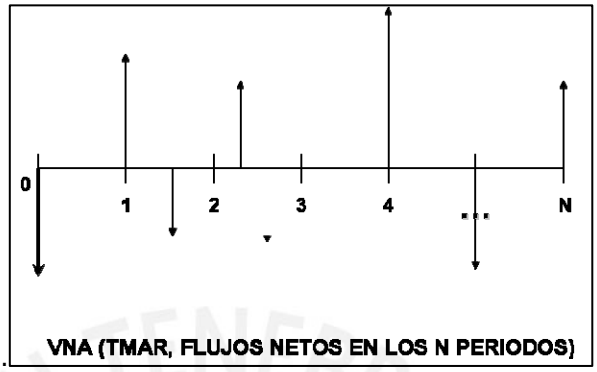
E. Revisar la identificación de los egresos adicionales por el proyecto. Recordar que los egresos adicionales se dan tanto por las inversiones adicionales como por los gastos adicionales debido al proyecto.

F. Revisar el cálculo del flujo neto como la diferencia entre los ingresos adicionales y los egresos adicionales.

G. Revisar el cálculo de la generación de valor del proyecto. En el caso de empresas, la generación de valor se determina mediante el cálculo del valor

actual neto para los flujos netos del período de tiempo indicado, aplicando la tasa mínima atractiva de retorno.

H. Verificar si el proyecto conviene o no conviene. Si el proyecto genera un valor actual neto negativo o un valor actual neto positivo que no es atractivo (unos cuantos soles por ejemplo), no tiene sentido ejecutar el proyecto.



SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. La organización no realiza un análisis de generación de valor antes de ejecutar los proyectos.

B. El análisis de generación de valor se basa en suposiciones sin una adecuada estimación numérica.

P060: PROCEDIMIENTO PARA LA ELABORACIÓN DEL INFORME PRELIMINAR

OBJETIVO

Dar las pautas para realizar el proceso de elaboración del informe preliminar de una auditoría.

ALCANCE

El alcance del procedimiento incluye:

A. Revisión de la normatividad relativa a los informes de auditoría.
B. Revisión del detalle de las actividades comprendidas en la elaboración del informe preliminar.
C. Análisis de generación de valor del informe de auditoría.

El alcance del procedimiento no incluye:

A. Revisión de la planificación de las actividades para la elaboración del informe preliminar.

ENTRADAS

Para realizar esta auditoría, se requiere que la organización provea con respecto al período en evaluación, la siguiente información:

A. Normas externas para la presentación de informes de auditoría.
B. Normas internas para la presentación de informes de auditoría.
C. Estructura para los informes de auditoría que indica la norma.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente las normas relativas a los informes de auditoría, tanto internas como externas.

C. Revisar detalladamente la información solicitada.

D. Realizar la evaluación de la actividad objetivo asignada para la auditoría.

E. Elaborar cada una de las secciones del informe preliminar. Debe incluirse:

a) Avance del informe con los siguientes puntos:

i. Introducción.
ii. Objetivo y Alcance de la Actividad.
iii. Procedimientos y Técnicas de Auditoría.
iv. Evaluación de la Actividad. Para cada gerencia auditada y para cada hallazgo indicar: enunciado del hallazgo, descripción, causa, efecto, riesgo, y recomendaciones.
v. Opinión

En caso que el informe se deba realizar para una entidad del Estado Peruano, se debe tener la siguiente estructura lógica para la redacción de cada hallazgo (observación):

i. Enunciado.
ii. Descripción.
iii. Norma que se está violando.
iv. Causa.
v. Efecto.
vi. Riesgo.
vii. Responsables.
viii. Recomendaciones.

b) Revisar y corregir el avance del informe con el Gerente de Auditoría Interna, o Supervisor de la Auditoría.

F. Analizar la generación de valor del informe de auditoría. Debe analizarse cuánto dinero se está generando para la empresa, ya sea por ingresos netos adicionales o por ahorros por errores en procesos o multas que ya no se

pagarían, gracias a que el informe evidenció esos problemas a tiempo. El dinero que se perdería debe estar colocado como observación.

SALIDAS

Al desarrollar esta auditoría es común encontrar las siguientes observaciones:

A. Las secciones de técnicas y procedimientos no se redactan adecuadamente. Carecen de información suficiente para que el auditor que desee realizar esa auditoría en el futuro, pueda realizar las mismas actividades o proponer mejoras.

B. Los informes demoran mucho en realizarse.

C. Los informes están enfocados en cosas puntuales y no se evalúa el tema como un todo para luego hacer recomendaciones conjuntas.

P061: PROCEDIMIENTO PARA EL ENVÍO, SUSTENTACIÓN Y CORRECCIÓN DEL INFORME FINAL

OBJETIVO

Dar las pautas para realizar el envío, la sustentación y la corrección del informe final de una auditoría.

ALCANCE

El alcance del procedimiento incluye:

A. Envío del informe preliminar.
B. Sustentación del informe preliminar ante la gerencia auditada y la Gerencia General.
C. Corrección del informe final.
D. Envío al Comité de Auditoría y al Directorio de la organización.

El alcance del procedimiento no incluye:

A. Revisión de la planificación de las actividades para la elaboración del informe preliminar.
B. Revisión de las actividades para la elaboración del informe preliminar.

ENTRADAS

Para realizar este proceso, se requiere que la organización provea para el período en evaluación, la siguiente información:

A. Informes Preliminares de auditoría de la gestión de tecnologías de información.

PROCESO

Las actividades a realizar para esta auditoría son las siguientes:

A. Revisar la información indicada en la sección anterior.

B. Revisar detalladamente el informe preliminar y hacer las últimas correcciones necesarias.

C. Enviar a la gerencia auditada, vía correo electrónico y en hojas impresas, el informe preliminar.

D. Solicitar reunión con la gerencia auditada para tratar las observaciones del informe.

E. En la reunión, recibir los comentarios de la gerencia sobre las observaciones realizadas.

F. Retirar o corregir las observaciones que la gerencia auditada haya demostrado que no son correctas.

G. Solicitar y/o Recibir los comentarios de la o las Gerencias Auditadas, o que resulten responsables de las observaciones encontradas.

H. Enviar el informe preliminar corregido (con lo comentarios de la Gerencia Auditada) a la Gerencia General con copia a la gerencia auditada.

I. Solicitar reunión con la Gerencia General y la gerencia auditada.

J. En la reunión, recibir los comentarios de la gerencia auditada y la Gerencia General.

K. Retirar o corregir las observaciones que la gerencia auditada y la Gerencia General demuestren que no son correctas.

L. Enviar el informe final (informe preliminar corregido) al Comité de Auditoría con copia a la gerencia auditada y la Gerencia General, tanto por correo electrónico como en hojas impresas.

M. Solicitar que se coloque en agenda del Comité de Auditoría, la discusión del informe entregado.

N. Discutir en el Comité de Auditoría y/o el Directorio, el informe final. Enviar a los organismos supervisores, en caso lo indique la legislación vigente que regula a la entidad supervisada.

SALIDAS

Al desarrollar este procedimiento es común encontrar las siguientes observaciones:

A. No se indica cuánto dinero ha perdido la organización, debido a los errores u omisiones ocurridos.

B. No se indica cuánto dinero perdería la organización debido a los errores u omisiones ocurridos.

P062: PROCEDIMIENTO PARA LA ELABORACIÓN DEL PLAN DE TRABAJO DE LA AUDITORÍA

OBJETIVO

Dar las pautas para la correcta elaboración del plan de trabajo para la realización de una auditoría en la organización.

ALCANCE

El alcance del procedimiento incluye:

A. Solicitud de información.
B. Preparación de cronograma de trabajo.
C. Identificación de hallazgos comunes.

El alcance del procedimiento no incluye:

A. Procedimientos detallados para el uso de herramientas de planificación.

ENTRADAS

Para realizar esta actividad, se requiere que la organización provea la siguiente información:

A. Documentos físicos que las áreas auditadas deben entregar.
B. Documentos electrónicos que las áreas auditadas deben entregar o que el área de Tecnología de Información debe entregar.
C. Acceso a tecnologías de información.
D. Informes de auditorías internas y externas anteriores.

PROCESO

A continuación se detalla las actividades a realizar la preparación del plan de trabajo:

A. Solicitar información para la auditoría. Responsable: auditor. Tiempo de Ejecución: por lo menos 15 días útiles antes de comenzar el trabajo de auditoría.

B. Elaborar el cronograma de trabajo.

   Aquí se debe detallar claramente las actividades a realizar, junto a *la duración en horas*, la fecha y hora de inicio y fin de cada actividad y quién será responsable de ejecutarlas.

El Cronograma de Trabajo detallado debe entregarse de manera *trimestral*. Para elaborarlo deberá tomar una plantilla de cronograma en la herramienta Microsoft Project. Las actividades a colocar en el Plan de Trabajo deben adecuarse a cada auditoría; sin embargo, de manera genérica debería incluir en el orden indicado, lo siguiente:

a) Solicitud de información para la auditoría. Ver punto A.

b) Avance de las siguientes secciones del informe:

i. Introducción.
ii. Objetivo y Alcance de la Actividad.
iii. Procedimientos y Técnicas de Auditoría.

- Responsable: Auditor.
- Duración Máxima: 1 día útil.

c) Revisión de avance del informe con el Gerente de Auditoría Interna, o el Jefe de Comisión de Auditoría.

- Responsables: Gerente de Auditoría Interna y Auditor.
- Duración Máxima: 1 día útil.

d) Revisión de la información solicitada por el auditor. Aquí se debe detallar paso a paso cuando se va a revisar cada tipo o bloque de información solicitada.

- Responsable: Auditor.
- Duración Máxima: 10 días útiles. Eventualmente, bajo aprobación del Gerente de Auditoría Interna o el Jefe de Comisión de Auditoría, el tiempo podría extenderse.

e) Elaboración del Informe Preliminar.

- Responsable: Auditor.
- Duración Máxima: 5 días útiles. Eventualmente, bajo aprobación del Gerente de Auditoría Interna o el Jefe de Comisión de Auditoría, el tiempo podría extenderse.

f) Verificación de las observaciones encontradas en el Informe Preliminar (sin entrega del informe) con personal del área auditada.

- Responsable: Auditor.
- Duración Máxima: 1 día útil.

g) Revisión del Informe Preliminar con Gerente de Auditoría Interna o el Jefe de Comisión de Auditoría.

- Responsable: Auditor.
- Duración Máxima: 2 días útiles.

h) Envío por correo electrónico del Informe Preliminar al gerente del área auditada.

- Responsable: Secretaria y/o Auditor.
- Duración Máxima: 1 día útil.

i) Reunión con gerente del área auditada para realizar las verificaciones finales del Informe Preliminar.

- Responsables: Gerente de Auditoría Interna (o Jefe de Comisión de Auditoría) y Auditor.
- Duración Máxima: 1 día útil.

j) Elaboración del Informe Final. Realizar las correcciones que sean necesarias en el informe preliminar, de acuerdo a la reunión con el gerente del área auditada.

- Responsables: Gerente de Auditoría Interna (o Jefe de Comisión de Auditoría) y Auditor.
- Duración Máxima: 1 día útil.

k) Entrega del Informe Final. Se entregará al gerente del área auditada y al Gerente General.

- Responsable: Secretaria.
- Duración Máxima: 1 día útil.

l) Revisión del Informe Final. Se revisará el informe con el gerente del área auditada y el Gerente General.

- Responsables: Gerente de Auditoría Interna (o Jefe de Comisión de Auditoría) y auditor.
- Duración Máxima: 1 día útil.

m) Correcciones al Informe Final (de ser necesarias).

- Responsables: Gerente de Auditoría Interna (o Jefe de Comisión de Auditoría) y auditor.
- Duración Máxima: 1 día útil.

C. Identificar hallazgos comunes. Aquí se debe especificar qué hallazgos comúnmente se encuentra en el desarrollo de la auditoría. Esto se debe desarrollar de manera previa a la auditoría, colocando lo aprendido a través de la experiencia de informes de auditorías internas y externas anteriores, experiencia del auditor y experiencia del Gerente de Auditoría Interna (o Jefe de Comisión de Auditoría).

SALIDAS

Al desarrollar esta actividad es común darnos cuenta de lo siguiente:

A. Se realiza un plan de trabajo poco detallado.

B. No se incluyen todas las actividades necesarias para el desarrollo de cada auditoría.

C. No se cumplen los plazos previstos para la auditoría.

P063: PROCEDIMIENTO PARA LA MEDICIÓN DE LA RESISTENCIA DE LA PUESTA A TIERRA

OBJETIVO

Dar las pautas para la correcta medición de la resistencia de la puesta a tierra en una instalación eléctrica relativa a los equipos de cómputo y redes de datos.

ALCANCE

El alcance del procedimiento incluye:

A. Pasos detallados para la medición de la resistencia de la puesta a tierra.

El alcance del procedimiento no incluye:

A. Revisión de la construcción de la puesta a tierra.

ENTRADAS

Para realizar este procedimiento, se requiere que la organización provea con respecto al período anterior al período en evaluación, el período en evaluación y los períodos próximos, la siguiente información:

A. Informes elaborados en los mantenimientos de los tableros de control de la energía eléctrica y los mantenimientos del pozo de tierra. Considerar tanto mantenimientos preventivos como correctivos.

B. Plano de instalaciones eléctricas de equipos de cómputo. Considerar: pozo de tierra, caja de control de la corriente eléctrica, tomacorrientes de equipos de cómputo y equipos de suministro de energía eléctrica (UPS y generador).

PROCESO

Las actividades a realizar son las siguientes:

A. Revisar la información solicitada en la sección anterior.

B. Desenergizar la instalación.

C. Desconectar el electrodo a tierra del sistema eléctrico[27].

D. De no ser posible desenergizar la instalación y desconectar de manera completa el electrodo de tierra, seguir los siguientes pasos:

[27] De no ser así, se podría generar una diferencia de potencial peligrosa para el personal que elabora las mediciones.

a) Asignar a un responsable de las actividades de medición.

b) Proveer un medio de comunicación constante (radio o teléfono portátil) a todos los que participan en la prueba.

c) Proveer guantes y calzado adecuado al personal y verificar que los usen.

d) Usar doble interruptor con aislamiento apropiado para conectar los cables al instrumento de medición.

e) Usar placa metálica para asegurar una equipotencial en la posición de trabajo. La placa debe ser lo suficientemente grande para incluir al instrumento, al interruptor y al operador durante la prueba. Se debe tener un terminal instalado de modo que la placa pueda conectarse al electrodo.

f) Suspender la prueba durante una tormenta eléctrica u otras condiciones severas de clima.

E. Realizar la medición.

SALIDAS

Al desarrollar este procedimiento, es común encontrar las siguientes fuentes de error:

A. Colocar la estaca de corriente demasiado cerca del electrodo bajo prueba.

B. Colocar la estaca de voltaje demasiado cerca del electrodo de prueba[28].

C. No considerar metales enterrados que se ubican paralelos a la dirección de la prueba.

D. Usar cable con aislamiento dañado.

[28] La teoría indica que en terreno uniforme basta una lectura colocando la estaca de voltaje a una distancia del electrodo en prueba igual al 61.8% de la distancia entre el electrodo en prueba y el electrodo de corriente (PROCOBRE, 2005).