Revista Tecnológica ESPOL, Vol. xx, N. xx, pp-pp, (Julio,2009)

"DISEÑO DE CONTROLES DE APLICACIÓN GENERALES EN LA IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN"

Adriana Salvador Guncay[1], Alice Naranjo[2]
Auditora en Control de Gestión[1], Máster en Auditoría de Sistemas[2]
Instituto de Ciencias Matemáticas
Escuela Superior Politécnica del Litoral
Campus "Gustavo Galindo V."
Km. 30.5 vía Perimetral
Apartado postal 09-01-5863. Guayaquil, Ecuador
asalvado@espol.edu.ec, bnaranjo@espol.edu.ec

Resumen

El presente artículo resume el diseño de controles de aplicación generales en la implementación de sistemas de información, el cual consistió en establecer los controles que se requieren en el proceso de implementación de los sistemas de información, tomando en cuenta los parámetros que establecen ciertas normas y/o estándares internacionales tales como: COSO, SAC, ISO 17799 y COBIT; y se utilizaron los más aplicables a la implementación de los sistemas de información, luego de la respectiva revisión de cada norma.

De esta manera se pudo establecer cada proceso a seguir, determinando los objetivos de control y las políticas aplicables a los mismos, mediante la elaboración de un manual que debe seguir cada empresa que requiere implementar un sistema de información eficaz y eficientemente; determinando los riesgos que se presentan en el transcurso de la implementación, sabiendo que deben mitigarse mediante la aplicación de los controles establecidos en el manual elaborado teniendo como referencia los procesos del estándar internacional COBIT.

Palabras Claves: controles, implementación, sistemas de información, normas, estándares.

Abstract

The present article summarizes the design of controls of application generals in the implementation of the information systems, which consisted on the controls that are required in the process of the implementation of the information systems, taking in it counts the parameters that establish certain standards such international standard y/o as: COSO, SAC, ISO 17799 and COBIT; and the most applicable were used to the implementation of the information systems, after the respective revision of each norm.

Of this way each process it could establish to continue, determining the objectives of control and the applicable politicians to the same ones, by means of the elaboration of a manual that should follow each company that requires to implement an information systems effective and efficient; determining the risks that are presented in the course of the implementation, knowing that they should be mitigated by means of the application of the controls settled down in the elaborated manual having like reference the processes give the international standard COBIT.

1. Introducción

La elaboración de un manual en el cual se establezcan los controles de implementación de los sistemas de información, es muy necesario en las empresas modernas y competitivas ya que mediante la utilización del mismo, los gerentes e implementadores podrán tener una idea clara de cómo se debe instalar y dejar en funcionamiento del sistema, tomando en cuenta los controles que se requieren para salvaguardar la información de dicho sistema.

Mediante el presente artículo se tendrá una idea clara de cómo establecer los controles preventivos, detectivos y correctivos mínimos que se deben aplicar en la implementación de Sistemas de Información, cómo ayudar a incrementar la efectividad de los Sistemas de Información en la operación de la empresa mediante el establecimiento de controles, reducir o eliminar los riesgos a los que está expuesta la información del sistema mediante la correcta utilización de controles.

2. Contenido

2.1. Antecedentes de los Sistemas de Información

Un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio.

En los años 50's aparecen las primeras computadoras, con esta nueva tendencia los sistemas de información que se realizaban de forma manual en las empresas, empezaron a realizarse de forma automatizada.

En los años 60's por el uso de sistemas de información computacionales sin los controles necesarios, se empezaron a detectar fraudes financieros; como desvíos de dinero en los sistemas financieros informáticos por los que se implementan medidas de control para disminuir este tipo de riesgos.

En los años 80's muchas empresas construyeron sus sistemas de información en forma incremental. Pensaron en soluciones individuales a problemas inmediatos. Generaron Sistemas de información con capacidades poco coordinadas.

A finales de los años 90's hasta la actualidad se incrementó la implantación de ERP's para simplificar y estandarizar la infraestructura de la información. Surgió la necesidad de acceder a información fiable para mejorar las interacciones y comunicaciones con clientes y proveedores. Se desea mejorar los procesos del negocio gracias a una mejor disponibilidad y calidad de datos e información del funcionamiento de la empresa.

Los tipos de Sistemas de Información más frecuentemente usados en las organizaciones son:

1.- Sistemas Transaccionales.- A través de éstos suelen lograrse ahorros significativos de mano de obra, debido a que automatizan tareas operativas de la organización.

2.- Sistemas de Apoyo de las Decisiones.- Suelen introducirse después de haber implantado los Sistemas Transaccionales más relevantes de la empresa, ya que estos últimos constituyen su plataforma de información.

3.- Sistemas Estratégicos.- Su función primordial no es apoyar la automatización de procesos operativos ni proporcionar información para apoyar la toma de decisiones.

3. Fundamentación Normativa y/o Estándares Internacionales

3.1. Normas de control interno COSO

El Control Interno es un proceso integrado a los procesos, y no un conjunto de pesados mecanismos burocráticos añadidos a los mismos, efectuado por el consejo de la administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar una garantía razonable para el logro de objetivos incluidos en las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes, reglamentos y políticas.
- Completan la definición algunos conceptos fundamentales.
- Lo llevan a cabo las personas que actúan en todos los niveles, no se trata solamente de manuales de organización y procedimientos.
- Sólo puede aportar un grado de seguridad razonable, no la seguridad total, a la conducción.

3.2. Normas de control interno SAC

El informe de la SAC define el sistema de mando interior, describe sus componentes, proporciona varias clasificaciones de mandos, describe objetivos del mando y riesgos, y define el papel del auditor interno. El informe proporciona una guía para usar, manejar, y proteger los recursos de tecnología de información.

El informe da énfasis al papel e impacto de los sistemas de información informatizados en el sistema de mando interior. Enfatiza la necesidad de evaluar los riesgos, establecer los costos y beneficios, y para construir los mandos en el sistema en lugar de agregarlos después de la aplicación.

3.3. Estándar de Control de Sistemas COBIT

COBIT se fundamenta en los Objetivos de Control existentes de la Information Systems Audit and Control Foundation (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento.

COBIT es una herramienta para la administración y operación a un nivel superior a los estándares de tecnología para la administración de sistemas de información.

El objetivo principal de COBIT es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de Tecnología de Información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo.

3.4. ISO 17799

La ISO (International Standarization Organization) es la organización internacional encargada de favorecer la normalización en el mundo. La finalidad principal de las normas ISO es orientar, coordinar, simplificar y unificar los usos para conseguir menores costos y efectividad.

Este estándar internacional de alto nivel para la administración de la seguridad de la información, fue publicado por la ISO (International Organization for Standardization) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones.

El ISO 17799, se orienta a preservar los siguientes principios de la seguridad informática:

- **Confidencialidad**.- Asegurar que únicamente personal autorizado tenga acceso a la información.
- **Integridad**.- Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.
- **Disponibilidad**.- Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

4. Manual de Controles de Implementación de Sistemas de Información

4.1. CONTROLES DE: LA ORGANIZACIÓN DE LA IMPLEMENTACIÓN

OBJETIVOS DE CONTROL: Realizar la organización de implementación de sistemas una vez que se haya efectuado satisfactoriamente el diseño, construcción, prueba del mismo y existan las evidencias que respalden dicha acción, así como la autorización del líder del proyecto

POLÍTICAS DE CONTROL:

1. Se debe realizar un plan estratégico para efectuar la implementación del sistema, describiendo el equipo de trabajo, actividades o tareas a realizar y los tiempos de ejecución.
2. El equipo de trabajo del proyecto encargado del desarrollo del plan estratégico del sistema debe ser el responsable de la implementación total del mismo o se debe delegar al equipo implementador que corresponda.

4.2. CONTROLES DE: DEFINICIÓN DE PUESTOS

OBJETIVOS DE CONTROL:

Ubicación del personal, según sus capacidades y conocimientos en los departamentos idóneos.

POLÍTICAS DE CONTROL:

1. Se debe elegir la persona adecuada para cada puesto, teniendo en cuenta la experiencia y conocimientos técnicos necesarios para cada cargo.
2. Se debe asignar las responsabilidades en el uso del sistema, la cual debe estar claramente definida, identificada y autenticada.
3. Se debe efectuar una verificación de los antecedentes personales de los candidatos a cada puesto.

4.3. CONTROLES DE: CAPACITACIÓN

OBJETIVOS DE CONTROL:
Educar a los usuarios mediante capacitación continua, para que conozcan el uso de sistemas de información, creando conciencia institucional respecto a la seguridad y buen uso de los Sistemas de Información.

POLÍTICAS DE CONTROL:
1. El personal deberá tener capacitación permanente pudiendo así aumentar sus habilidades técnicas.
2. Evaluar el desempeño del personal regularmente para determinar si cumple o no con los estándares requeridos en la organización.
3. Los empleados deberán ser asesorados sobre su desempeño en el Sistema de Información cuando sea requerido.

4.4. CONTROLES DE: ACCESO FÍSICO Y LÓGICO

OBJETIVOS DE CONTROL:
Definir la comunidad de usuarios y los roles de los mismos de acuerdo a sus responsabilidades y tareas.

POLÍTICAS DE CONTROL:
1. Se debe elaborar una lista de todos los usuarios que deben tener acceso al sistema con la declaración de los perfiles de seguridad y opciones de menú debidamente autorizadas por su jefe inmediato.
2. Se debe definir la comunidad de usuarios y los roles de los mismos de acuerdo a sus responsabilidades y tareas.

4.5. CONTROLES DE: CONTROLES DE CONVERSIÓN

OBJETIVOS DE CONTROL:
Se debe realizar un proceso de limpieza de los datos antes de la conversión, para garantizar que todos los datos a convertir sean precisos, válidos y estén actualizados.

POLÍTICAS DE CONTROL:
1. Se debe elaborar un plan de conversión que involucre las estrategias y los recursos informáticos necesarios, el tiempo, los costos, la organización del personal que efectuará la conversión y la asignación de responsabilidades.
2. La gerencia usuaria y de sistemas deben dar el visto bueno o la aprobación respectiva al plan de conversión.

4.6. CONTROLES DE: PRUEBAS DE ACEPTACIÓN

OBJETIVOS DE CONTROL: Efectuar pruebas de Aceptación, que consistan en probar con datos reales la información con que el sistema deberá operar.

POLÍTICAS DE CONTROL:
1. La documentación de los programas, el manual del usuario y el manual de operación deben existir antes de ejecutar una prueba de aceptación**.**
2. Se debe concluir las pruebas de aceptación por parte del usuario con la firma del usuario en el requerimiento del sistema con lo cual califica al sistema como apto para entrar en la etapa de paralelo.

4.7. CONTROLES DE: CONTROLES DE AUDITORIA

OBJETIVOS DE CONTROL:
Realizar auditorias internas y/o independientes en intervalos de tiempos determinados para que la empresa se vea beneficiada con mejores recomendaciones para la implementación de los sistemas de información y de esta manera aumentar los niveles de confianza.

POLÍTICAS DE CONTROL:
1. La alta gerencia deberá establecer normas, políticas y estatutos de control en las que se detallen las responsabilidades de quienes realicen las auditorias independientes
2. Los miembros del comité de auditoria deberán ser independientes tanto de la empresa como a los Sistemas de Información por lo que se recomienda contratar los servicios de auditores externos.
3. Se deben desarrollar, documentar, y probar los procedimientos de respaldo de la auditoria del SI.

4.8. CONTROLES DE: CONTROLES DE SEGURIDAD

OBJETIVOS DE CONTROL:
Evaluar la seguridad del Sistema de Información y establecer la confiabilidad de las mismas.

POLÍTICAS DE CONTROL:
1. Se debe designar un responsable de la función de seguridad de los sistemas empresariales.
2. Se deben hacer revisiones de las Capas de la Seguridad Empresarial, aunque si bien éstas se concentran en otros aspectos y no hacen foco en las fases del ciclo de vida de software, de una u otra manera incidirán en la implementación del nuevo SI.

Por ello a través de una lista de chequeo se debe efectuar revisión de estos elementos que indirectamente podrían generar vulnerabilidades en el SI.

4.9. CONTROLES DE: SEGURIDAD EN LA ARQUITECTURA DE LA RED

OBJETIVOS DE CONTROL:
Proteger físicamente el Sistema de Información, controlando los accesos a la red de información.

POLÍTICAS DE CONTROL:
1. Se deben cuantificar y prevenir de situaciones de error y deben ser mitigadas.
2. Se deben disponer de mecanismos de recuperación ante problemas graves, y desastres o siniestros.
3. Se debe proteger físicamente a los servidores.
4. Controlar todos los accesos a la red corporativa
5. Revisión de las conexiones de red físicas y lógicas a fin de evitar vulnerabilidades.

4.10. CONTROLES DE: SISTEMAS DE PROTECCIÓN

OBJETIVOS DE CONTROL:
Determinar las herramientas necesarias que se utilizarán para proteger el sistema de información.

POLÍTICAS DE CONTROL:
1. Es necesario activar las opciones de registro de las aplicaciones críticas.
2. Deben realizarse revisiones periódicas de los registros.
3. Debe existir personal calificado para realizar estos análisis.
4. Se debe contar con herramientas para facilitar el análisis de estos logs off-line, así como para la detección de comportamientos anómalos de forma automática y que activen alarmas.

4.11. CONTROLES DE: SEGURIDAD EN SISTEMAS OPERATIVOS

OBJETIVOS DE CONTROL:
Cerrar la mayor cantidad de puertos posibles para salvaguardar la información.

POLÍTICAS DE CONTROL:
1. Se deben cerrar la mayor cantidad de puertos posibles, ya que cualquier puerto abierto es una puerta de entrada
2. Se deben cerrar los puertos no usados.
3. Se debe emplear protección para los puertos usados.
4. Conceder los permisos adecuados en detalles a cada recurso

4.12. CONTROLES DE: CONTROLES EN LA POST-IMPLEMENTACIÓN

OBJETIVOS DE CONTROL:
Verificar que el sistema implantado funcione correctamente, mediante el seguimiento de las operaciones que realiza.

POLÍTICAS DE CONTROL:
1. Se debe ejecutar un seguimiento de los procesos y funciones implementados con el objeto de detectar desviaciones y determinar posibles soluciones para ser consideradas en el momento o en las implementaciones posteriores.
2. En caso de encontrarse falencias significativas, se debe enviar al área de desarrollo las desviaciones o fallas encontradas para que elaboren las modificaciones pertinentes en forma oportuna.
3. Se debe proporcionar el área de mantenimiento o soporte de usuarios todos los elementos necesarios para que puedan hacerse cargo del sistema.

CONCLUSIONES

- Durante los próximos años, los Sistemas de Información cumplirán tres objetivos básicos dentro de las organizaciones:
  1. Automatización de procesos operativos.
  2. Proporcionar información que sirva de apoyo al proceso de toma de decisiones.
  3. Lograr ventajas competitivas a través de su implantación y uso.

- La elaboración del presente manual me ayudó a conocer todas las etapas que intervienen en la implementación de Sistemas de Información.

- Mediante este artículo he presentado los controles necesarios para minimizar los riesgos que pueden aparecer en el momento de implantar un Sistema de Información en una empresa.

RECOMENDACIONES

- Se recomienda aplicar los controles que se requieran en cada etapa del proceso de los sistemas de información según lo establecen los estándares internacionales.

- Los usuarios de los sistemas de información deberán tomar la capacitación necesaria para que conozcan cómo se aplicarán los controles preventivos, detectivos y correctivos en la implementación de sistemas.

- La alta gerencia deberá trabajar en conjunto con el personal de sistemas y de auditoria para conocer cuales serán los controles que deberán aplicarse en la implementación de un nuevo sistema de información con el debido uso y conocimiento del manual realizado.

REFERENCIAS

1. Enciclopedia Autodidáctica Océano, Volumen II (ISBN 84-7764-011-4, Grupo Editorial Océano, 1988)

2. Muñoz Razo Carlos, Auditoría en Sistemas Computacionales (ISBN: 970-17-0405-3, PearsonEducation, México, 2002)

3. Senn James, Sistemas de Información para la Administración (Editorial Ibero América, México, 1992)

4. Senn James, Análisis y Diseño de Sistemas de Información (Editorial Mc. Graw Hill, México, 1992)