PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y CONTABLES

LA AUDITORÍA INFORMÁTICA COMO UN FACTOR DE ÉXITO EN EL CUMPLIMIENTO DE OBJETIVOS EMPRESARIALES

DISERTACIÓN DE GRADO PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA COMERCIAL

OSWALDO VLADIMIR BRAVO ARELLANO

DIRECTOR: ING. CHRISTIAN FAJARDO

QUITO, 2010

DIRECTOR DE DISERTACIÓN:

Ing. Christian Fajardo

INFORMANTES:

Ec. Marco Naranjo

Ing. Jorge Altamirano

DEDICATORIA

A todas las personas que me apoyaron en mis largos años de estudio, a todos mis compañeros de trabajo con quienes muchas veces compartimos más tiempo que con nuestros familiares, a Deloitte por toda la enseñanza y experiencia recibida, a toda la profesión de Auditoría a quienes espero este trabajo les sirva de guía en el cumplimiento de sus tareas asignadas y cubra sus expectativas.

Saludos Cordiales.

Oswaldo

AGRADECIMIENTO

Quiero agradecer a la Universidad y sus profesores, por el apoyo en estoy años de formación, los cuales se ven ya reflejados en mis actividades laborales, a mi Padre, Madre y hermanos que me enseñaron los valores básicos de la vida que me permiten hoy ser feliz, a mi querida Esposa que en estos 6 años ha sido un apoyo incondicional en el cumplimiento de mis metas y objetivos, y no puedo olvidar a mi Dios, Jehová, quien me ha dado el conocimiento, la fuerza, el ánimo necesarios para superarme.

Sin el apoyo de todas las personas mencionadas este trabajo no se hubiera concluido con éxito.

Gracias a todos nuevamente

Oswaldo

ÍNDICE

RESUMEN EJECUTIVO

La auditoría de sistemas actualmente se la ve como un tema técnico que se la debe dejar a especialistas de sistemas, sin embargo los controles que deben ser probados como parte de la revisión del control interno de las empresas, cada vez son más complejos y por ende están soportados en procesos automatizados, esta circunstancia obliga a que los auditores financieros deben conocer en una grado importante sobre los sistemas de información, sus componentes, su funcionamiento y como pueden ellos satisfacer su escepticismo profesional referente a la confiabilidad del control interno de las empresas en las cuales trabajan.

La encuesta realizada a las 25 empresas más grandes de Quito, nos dan una clara referencia que hay mucho por hacer, ya que la mayoría de estas, pertenecientes a sectores industriales y comerciales, pese a utilizar herramientas tecnológicas en sus procesos de negocio y algunos muy complejos, no cuentan con una función de auditoría de sistemas permanente que les apoye en garantizar que los controles automáticos están funcionando correctamente. Las instituciones financieras y empresas de telecomunicaciones, son las que por su estilo de negocio y por exigencias de los entes de control cuentan con estructuras solidas en este aspecto.

El modelo desarrollado busca que la brecha de conocimiento de los auditores financieros con temas de tecnología se cierre, por lo menos a un nivel que les permita dar una opinión razonable sobre el control interno de las diferentes empresas, además de dejarles un

modelo basado en las mejores prácticas de seguridad y control como lo son Cobit, ITIL y la ISO 27000.

Además, este trabajo es una invitación a todos los profesionales que trabajan en el sector de auditoría, a que no vean los controles automatizados y los sistemas de información como una caja negra en la cual no deben involucrarse, al contrario veámoslo como un mundo fascinante en el que debemos ingresar nos guste o no nos guste, el adelanto tecnológico nos está obligando a que debamos tener claros estos conceptos y más aún saber cómo debemos tratarlos.

Los riesgos que vienen atados a este cambiante mundo son altos y nosotros como responsables de asegurar que el control interno de una organización este marchando de acuerdo a las intenciones de la gerencia y al cumplimento de regulaciones de los entes de control, tenemos una gran responsabilidad, la misma que solo podremos cumplir rompiendo paradigmas y preparándonos para enfrentar esta carrera rumbo a la tecnificación de los procesos de todas las compañías de nuestro medio.

INTRODUCCIÓN

El presente trabajo pretende informar al lector acerca de la importancia de la Auditoría Informática dentro de una organización.

Debido al crecimiento constante de las diferentes industrias, se hace cada vez más necesario estar al día con la tecnología para evaluarla y decidir cuál es aplicable al negocio. Es innegable que hoy por hoy la tecnología es un factor extremadamente relevante en el éxito o fracaso de cualquier organización. Debido a que la tecnología se desarrolla a una velocidad vertiginosa los riesgos asociados crecen de la misma forma.

Los sistemas informáticos se han convertido en la herramienta más versátil para el manejo de uno de los recursos más importantes con los que cuenta la compañía, los datos. Debido a su importancia existe la Auditoría informática.

Este trabajo tiene como objetivo dar a conocer el importante papel que cumplen los sistemas de información y la tecnología en general en el desarrollo y crecimiento de una empresa, los peligros que pueden correr los datos al no contar con los controles suficientes para asegurar los mismos y conocer las características y los beneficios que proporciona la Auditoría Informática, como un factor de éxito en el cumplimiento de los objetivos empresariales.

1 LA FUNCIÓN DE AUDITORÍA INFORMÁTICA FACTOR DE ÉXITO EN LA LAS EMPRESAS ACTUALES

1.1 CRECIMIENTO DEL APOYO TECNOLÓGICO A LOS PROCESOS DE NEGOCIO

Anteriormente la información no era considerada un recurso importante en la organización, esto se debía a que no existía la tecnología adecuada para integrar la información de las diferentes áreas de la empresa de manera que se pueda tener datos actualizados en el momento que se requiera, hoy en día gracias a los pasos agigantados que ha dado la tecnología en su crecimiento es posible contar con todo tipo de sistemas y equipos que permitan obtener información consolidada de la empresa para conocer la situación actual de la misma e incluso realizar proyecciones para tomar decisiones oportunas que beneficien al negocio.

Existen muchos casos de compañías que han incorporado sistemas y equipos de gran tecnología y han logrado obtener notable ventaja competitiva frente a otra compañías que se han quedado atrás en el tema tecnología.

La tecnología no solo ha intervenido en todos los procesos de la entidad para mejorarlos y optimizarlos sino que han creado nuevos procesos con la finalidad de brindarle valor agregado al cliente, de aquí nace por ejemplo el conocido término *e-commerce* tan común hoy en día. Otro concepto muy utilizado en la actualidad es

SIG (Sistemas de Información Gerencial), sistemas enfocados a ayudar en la toma de decisiones.

En la actualidad las tecnologías están presentes en toda la cadena de valor de la organización y son un pilar fundamental para la toma de decisiones.

La probabilidad de errores es mínima cuando se han automatizado los procesos, debido a que los mismos se comportan siempre de igual forma, además gracias a los sistemas de información se pueden obtener datos detallados de cada proceso de la empresa, esta información es utilizada en beneficio de la organización para conocer la situación actual de la misma y así poder realizar proyecciones, de esta manera se podrá obtener una ventaja competitiva frente a las demás empresas de la industria.

La tecnología ha intervenido de varias formas dentro de los negocios, a continuación identificamos las principales:

- Apoyo en la toma de decisiones.
- Creación de ventajas competitivas.
- Facilita la integración de los procesos del negocio.
- Apoyo en la estrategia de negocio.

Es importante que los altos mandos de la organización tengan claro las ventajas de la implantación de tecnologías en el negocio, ya que estas se alinean con las estrategias de la organización.

- **Apoyo en la toma de decisiones.-** Con respecto al apoyo que ofrecen los sistemas de información en la toma de decisiones es importante mencionar que existen dos formas básicas de apoyo:

  - Proporcionando información válida, coherente y real de la situación de la empresa, sea esta acerca de procesos del negocio, información de los clientes, estadística de ventas, etc.

  - Tomando decisiones por ellos mismos, los sistemas son parametrizables y se los puede configurar de tal forma que ingresando ciertos criterios, dé un resultado u otro, por ejemplo aceptación de crédito de un cliente, el cliente puede ingresar sus datos personales y si cumple con los requisitos el sistema le puede confirmar si recibe el crédito o no, de esta manera se ahorra tiempo y por lo tanto dinero al dejar que el sistema de información tome ciertas decisiones básicas.

- **Creación de ventajas competitivas.-** Los Sistemas de Información son una herramienta muy útil en la creación de ventajas competitivas de la organización, esto se puede lograr de tres formas:

  - Creando liderazgo en costos, un Sistema bien utilizado puede proporcionar ventajas a nivel de costos de producción si es parametrizado de forma correcta, además con la implementación de un Sistema de Información se abaratan costos de operaciones pues se utilizan menos recursos para llevar a cabo los procesos del negocio.

- Provee productos o servicios novedosos y atractivos a los clientes, un Sistema de Información puede proveer las herramientas necesarias para identificar las necesidades de los clientes, un ejemplo de esto son los CRM (*Customer Relationship Management*) modelo de gestión enfocado al cliente.

- Enfocarse en un mercado específico, esta es otra manera de crear ventajas competitivas, cuando una organización se orienta a un mercado específico, se desarrollan productos y servicios exclusivamente para el mercado seleccionado.

- **Facilita la integración de los procesos del negocio.-** Las tecnologías de la información se han involucrado en los procesos del negocio a tal punto que no solo afectan la forma en la que ellos operan sino también permiten una perfecta integración entre ellos, es por esto que las altas gerencias de la organización se han dado cuenta que las tecnologías no solo son responsabilidad del departamento de sistemas.

Debido al gran aporte que hacen las tecnologías de la información a la cadena de valor del negocio, hoy en día son consideradas un recurso más de la organización del cual no se puede prescindir.

1.2 IMPORTANCIA DE LA AUDITORÍA INFORMÁTICA EN LAS EMPRESAS ACTUALES

En la actualidad la informática es un recurso más de la organización, tan importante como el capital o el recurso humano, pues sin ellas las organizaciones no podrían mantenerse en el mercado.

Debido a la gran importancia que ha ganado la informática con el pasar de los años se desarrolló la necesidad de crear una función especializada para garantizar que los procesos de tecnología se están ejecutando correctamente, gracias a esto actualmente, existe la auditoría informática la que se focaliza en una evaluación de la eficiencia y eficacia de la tecnología implantada en una organización.

La palabra auditoría viene del latín *auditorius* y de esta proviene auditor, que tiene la virtud de oír. Sin embargo con el pasar de los años este concepto simple ha variado y se ha extendido, hoy podemos decir que la auditoría es un análisis profundo y a detalle pero no mecánico que persigue el objetivo de evaluar y mejorar la eficacia y eficiencia de una organización.

La auditoría informática se encarga de velar por la correcta utilización de los recursos tecnológicos para que estos se alineen con los objetivos micros y macros de la organización, es importante mencionar que para poder llevar a cabo la auditoría informática es necesario conocer a fondo la empresa y sus procesos ya que los Sistemas informáticos se acoplan al negocio.

Por esta razón los sistemas informáticos al igual que los demás recursos de la empresa deben someterse a controles y evaluaciones constantes, a continuación se detalla varias razones por las cuales es importante realizar una auditoría informática:

- Las computadoras y los Centros de Proceso de Datos se convirtieron en blancos apetecibles no solo para el espionaje, sino para la delincuencia y el terrorismo.

- Las computadoras creadas para procesar y difundir resultados o información elaborada pueden producir resultados o información errónea si dichos datos son, a su vez, erróneos. Este concepto obvio es a veces olvidado por las mismas empresas que terminan perdiendo de vista la naturaleza y calidad de los datos de entrada a sus Sistemas Informáticos, con la posibilidad de que se provoque un efecto cascada y afecte a Aplicaciones independientes.

- Un Sistema Informático mal diseñado puede convertirse en una herramienta peligrosa para la empresa: como las máquinas obedecen ciegamente a las órdenes recibidas y la modelización de la empresa está determinada por las computadoras que materializan los Sistemas de Información; la gestión y la organización de la empresa no puede depender de un Software y Hardware mal diseñados.

Incluso por parte de los mismos trabajadores de la compañía se realizan infracciones informáticas, las que son muy perjudiciales para la compañía incluso más que un ataque desde afuera.

La proliferación de las nuevas tecnologías en la empresa conlleva también la proliferación de nuevos peligros. Ya no son sólo los ataques y sabotajes informáticos desde el exterior, sino las infracciones desde dentro, las producidas por los propios empleados y contra las que las organizaciones son al parecer más vulnerables.

Las infracciones más habituales que han sido detectadas por parte de personal de la compañía son las siguientes:

- **Creación de empresa paralela, utilizando activos de la empresa.**

  Consiste en la explotación en una empresa de nueva creación, de la propiedad intelectual o la propiedad industrial de la empresa en la que el empleado labora. Generalmente, el trabajador constituye la nueva compañía antes de solicitar la salida voluntaria y realiza un proceso de traspaso de información mediante soportes informáticos o a través de Internet. Es posible que el trabajador actúe aliado con otros compañeros de la empresa.

- **Daños informáticos y uso abusivo de recursos informáticos.**

  Los daños informáticos se producen generalmente como respuesta a un conflicto laboral o a un despido que el trabajador considera injusto. Consisten en la destrucción, alteración o inutilización de los datos, programas o cualquier otro activo inmaterial albergado en redes, soportes o sistemas informáticos de la empresa. Los casos más habituales son los virus informáticos, el sabotaje y

las bombas lógicas, programadas para que tengan efecto unos meses después de la baja o salida del trabajador. También es habitual el uso abusivo de recursos informáticos, especialmente el acceso a Internet.

- **Información confidencial y datos personales.**

Consiste en el acceso no autorizado y en la posterior revelación a terceros, generalmente competidores o clientes, de información confidencial de la empresa. En algunas ocasiones, la revelación la realizan trabajadores que tienen un acceso legítimo, pero con obligación de reserva, a la información posteriormente divulgada.

- **Amenazas, injurias y calumnias.**

El medio utilizado habitualmente es el correo electrónico corporativo, aunque también se han utilizado cuentas anónimas, e incluso se ha suplantado la identidad de otro trabajador de la misma empresa. En el caso de las amenazas, se busca un beneficio material o inmaterial para el trabajador. Si el beneficio no se produce, el trabajador llevará a cabo la conducta anunciada en el mensaje amenazador. En el caso de las injurias y las calumnias, se busca desacreditar a la empresa, o a alguno de sus directivos. También se han producido insultos a clientes habituales o a clientes potenciales de la empresa con el que el trabajador tenía algún conflicto.

- **Infracción propiedad intelectual e introducción de obras de la empresa en redes públicas.**

  Consiste en la copia de activos inmateriales de la empresa, especialmente obras protegidas por la propiedad intelectual, con el fin de cederlas posteriormente a terceros. En los últimos dos años se han dado casos de difusión a través de Internet, mediante el uso de redes de intercambio de ficheros. De esta manera, una multitud de usuarios acceden de forma gratuita a programas de ordenador desprotegidos, información o contenidos multimedia. Intercambio de obras de terceros a través de redes. Este es el caso más habitual y se detecta generalmente en el curso de una auditoría de seguridad informática, mediante el análisis del caudal de datos transferido por los trabajadores a través de la red corporativa.

- **Infracción de derechos de propiedad industrial.**

  El caso más habitual ha sido la infracción de marcas de la empresa mediante el registro del nombre de dominio por parte del trabajador. En algunos casos, se ha creado una página web con contenidos ofensivos para conseguir un mayor efecto nocivo para la empresa o para obtener una suma de dinero por la transferencia.

  Ante la aparición de esta clase de situaciones, ¿cuál ha sido la estrategia de respuesta de las empresas? La mayoría de las empresas prefieren encomendar la investigación de los posibles actos desleales de un trabajador a un equipo

interno, generalmente formado por miembros del departamento de RRHH y del departamento de sistemas.

Cuando se toma la decisión de llevar la infracción a los tribunales, la obtención de las evidencias electrónicas se encarga a un tercero, con el fin de conseguir mayor objetividad y valor probatorio. El procedimiento de recopilación de las evidencias debe respetar los derechos del trabajador para que sea válido judicialmente. Una investigación se inicia a partir de las sospechas e indicios generados por la propia conducta del trabajador, por un consumo de recursos poco usual o por el descubrimiento de los efectos de la infracción.

Estos son solo algunos de los varios inconvenientes que puede presentar un Sistema Informático, por eso, la necesidad de la **Auditoría de Sistemas.**

- **Objetivos de la Auditoría Informática.**

La Auditoría Informática se puede definir como el conjunto de procedimientos y técnicas cuya finalidad es evaluar y controlar un sistema informático con el fin de constatar si sus actividades son correctas, de acuerdo a las normativas informáticas y generales prefijadas en la organización y a las mejores prácticas de seguridad y control.

La Auditoría Informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde la

entrada de datos, procedimientos, controles, archivos, seguridad, obtención y salida de información.

Esta es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.

La auditoría del sistema de información en la empresa, a través de la evaluación y control que realiza, tiene como objetivo fundamental mejorar la rentabilidad, la seguridad y la eficacia del sistema de información.

Los principales objetivos que tiene la auditoría Informática son:

- El control de la función informática.

- El análisis de la eficiencia de los sistemas informáticos.

- La verificación del cumplimiento de la Normativa general de la empresa en este ámbito.

- La revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

- **Alcance de la Auditoría Informática.**

Las organizaciones actuales han sufrido un cambio importante en sus procesos de negocio al considerar a la información como un recurso de importancia estratégica. Ello requiere, que igual que para el resto de los activos de la empresa los requisitos de eficacia y eficiencia, dentro de un marco de riesgos controlados, se apliquen a los Sistemas y Tecnologías de la Información.

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada por personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

La función que tiene la auditoría de sistemas es la responsabilidad de la evaluación de la cobertura de los riesgos inherentes a los procesos de la información así como de la evaluación de esos procesos, sistemas, tecnologías utilizadas y servicios asociados para su desarrollo y mantenimiento óptimo, como medio para la consecución de los objetivos de las organizaciones.

El alcance de la auditoría informática debe definir el ambiente y los límites en que se va a llevar a cabo la auditoría. En la etapa de planificación de la auditoría, el auditor de sistemas debe determinar el alcance de la auditoría y al

final de la misma debe quedar constancia del alcance que tuvo la auditoría en el informe final.

Es importante mencionar que al momento de definir el alcance de la auditoría se debe tener presente los objetivos de la auditoría pues el alcance está estrechamente relacionado con los mismos.

- **Características de la Auditoría Informática.**

La auditoría informática es recoger, organizar y evaluar evidencias para determinar si un sistema de información tiene los controles necesarios para salvaguardar la información que maneja.

Una persona capacitada debe estar a cargo de realizar esta función tan importante en el área tecnológica de una compañía. El rol del auditor informático solamente está basado en la verificación de controles, evaluación del riesgo de fraudes y el diseño y desarrollo de exámenes que sean apropiados a la naturaleza de la auditoría asignada, y que deben detectar:

- Irregularidades que puedan tener un impacto sobre el área auditada o sobre toda la organización.

- Debilidades en los controles internos que podrían resultar en la falta de prevención o detección de irregularidades.

- **Tipos de auditorías informáticas.**

Dentro de la auditoría de sistemas se puede destacar los siguientes tipos de auditorías:

- Gestión, validación del cumplimiento de políticas y procedimientos del área de sistemas constatando la documentación soporte necesaria.

- Funcional, clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas y procesos.

- Bases de datos, controles de acceso, de actualización, de integridad y de calidad de datos.

- Seguridad referido a datos e información verificando disponibilidad, integridad, confidencialidad y autenticación y sus métodos de autentificación.

- Seguridad física, se refiere al nivel de protección que tienen los diferentes dispositivos de la infraestructura tecnológica de la empresa.

- Comunicaciones, se refiere a la auditoría de los procesos de comunicaciones y conexiones con otras plataformas tecnológicas.

- **Pruebas y herramientas utilizadas.**

Al realizar una auditoría de sistemas, el auditor puede hacer uso de tres tipos de prueba según sea necesario para el caso:

- Pruebas clásicas, consiste en probar las aplicaciones con datos de prueba, observando la entrada, el resultado esperado y el resultado obtenido.

- Pruebas sustantivas, permiten al auditor obtener la suficiente evidencia para que este se pueda formar un juicio, este tipo de pruebas se suelen obtener mediante observación, cálculos, muestreos, entrevistas, etc.

- Pruebas de cumplimiento, determina si un sistema de control interno funciona adecuadamente.

Las principales herramientas con las que cuenta un auditor son:

- Observación.
- Cuestionarios.
- Entrevistas.
- Muestreo estadístico.
- Flujogramas.
- Check Lists.
- Herramientas de análisis de datos.
- Marcos referenciales a nivel mundial (Ej. Cobit).

1.3 ENCUESTA EMPRESARIAL Y ANÁLISIS DE LOS RESULTADOS OBTENIDOS

Dentro del alcance se definió realizar una encuesta las empresas más grandes de Quito con el objetivo de determinar el grado de penetración del área de auditoría de sistemas en las empresas de Quito.

Alcance de la encuesta

El objetivo era encuestar a las 25 empresas más grandes de Quito, independientemente del sector en el que se desarrollan. Las empresas fueron seleccionadas en base a la información proporcionada por la Superintendencia de Compañías, Bancos y la revista Vistazo. Además las encuestas fueron enviadas a las áreas de Auditoría Interna de las empresas en caso que esta área no se encuentre dentro del organigrama de la Institución, se envía al Gerente de Financiero. Adjunto la lista de las empresas encuestadas:

- Produbanco.
- Banco Pichincha.
- Banco Internacional.
- Banco Rumiñahui.
- Corporación Favorita C.A.
- Andes Petroleum.
- Omnibus BB Transportes.
- Procesadora Nacional de Aves – Pronaca.

- Telefónica – Otecel.
- Repsol YPF.
- Nestlé Ecuador.
- Petróleos y Servicios.
- Acerías del Ecuador (Adelca).
- STIMM Soluciones.
- Oleoducto de Crudos Pesados del Ecuador – OCP.
- Industrial Danec.
- Empresa Eléctrica Quito.
- Ecuador Bottling Company – EBC.
- Farmacias y Comisariatos del Ecuador.
- Exxon Mobile Ecuador.
- General Motors del Ecuador.
- Maquinarias y Repuestos – Maresa.
- Schlumberger Surenco.
- Toyota del Ecuador.
- Industrias Ales.

De las siguientes empresas encuestadas no recibimos respuesta:

- Banco Internacional.
- Nestlé Ecuador.
- Petróleos y Servicios.
- STIMM Soluciones.
- Exxon Mobile Ecuador.

- General Motors del Ecuador.
- Schlumberger Surenco.

Estas son las preguntas enviadas en la encuesta:

Auditoría Informática

El objetivo de esta encuesta es exclusivamente educativa

a) Cuenta su empresa con un área de auditoría interna de sistemas?

Si……. No……

b) Cuantas veces al año realiza una revisión de sus sistemas?

c) Su empresa ha contratado servicios de auditoría de sistemas o revisión de seguridades en el último año?

Si……. No……

Favor seleccionar el alcance:

- Gobierno de IT ☐
- Seguridad de información ☐
- Auditoría de aplicaciones ☐

- Auditoría de infraestructura Ethical Hacking Interno ☐
- Seguridades en Internet Ethical Hacking Externo ☐

d) Cuán importante considera usted es la función de auditoría de sistemas para su organización?

Porqué?

e) Cree usted que la empresa puede beneficiarse al contar con una función de auditoría de sistemas?

Cómo?

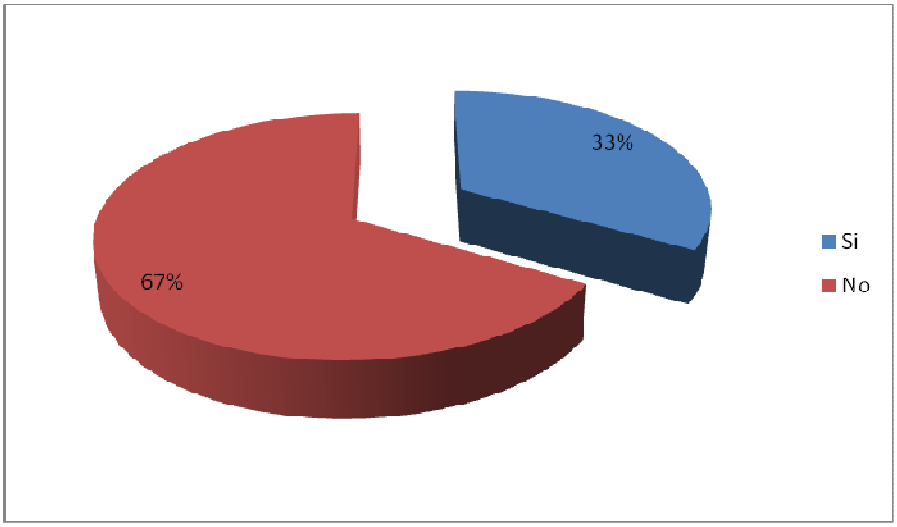
f) Conoce que marcos referenciales se utilizan en la ejecución de una auditoría de sistemas?

Considerando que las encuestas recibidas son la mayoría, se procesaron y se obtuvieron los siguientes resultados:

a) Cuenta su empresa con un área de auditoría interna de sistemas?

Si…… No……

GRÁFICO N° 1

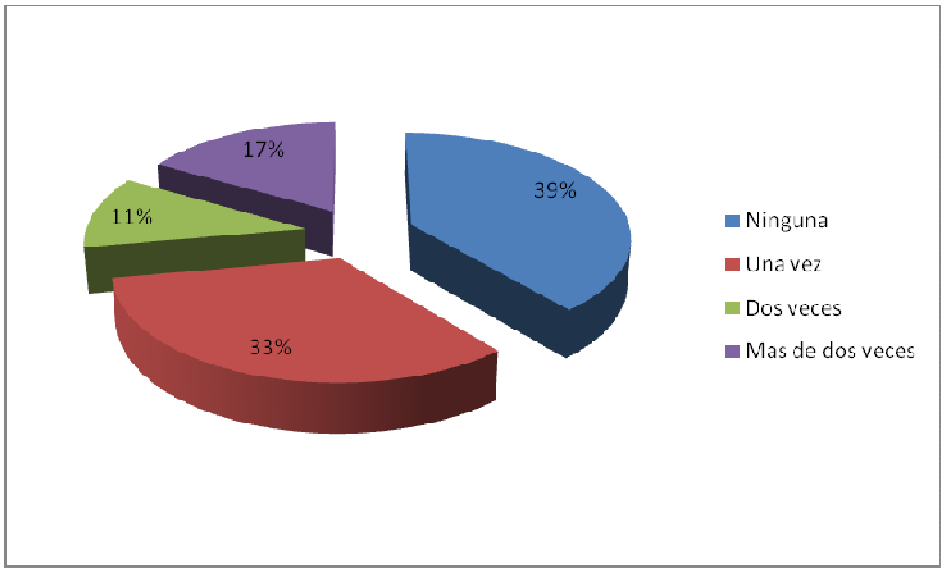


Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

Los resultados demuestran que la mayoría de las empresas en Quito no cuentan con un área de auditoría de sistemas dentro de su estructura organiacional, ya que el 67% contesto negativamente.

b) Cuantas veces al año realiza una revisión de sus sistemas?

GRÁFICO N° 2



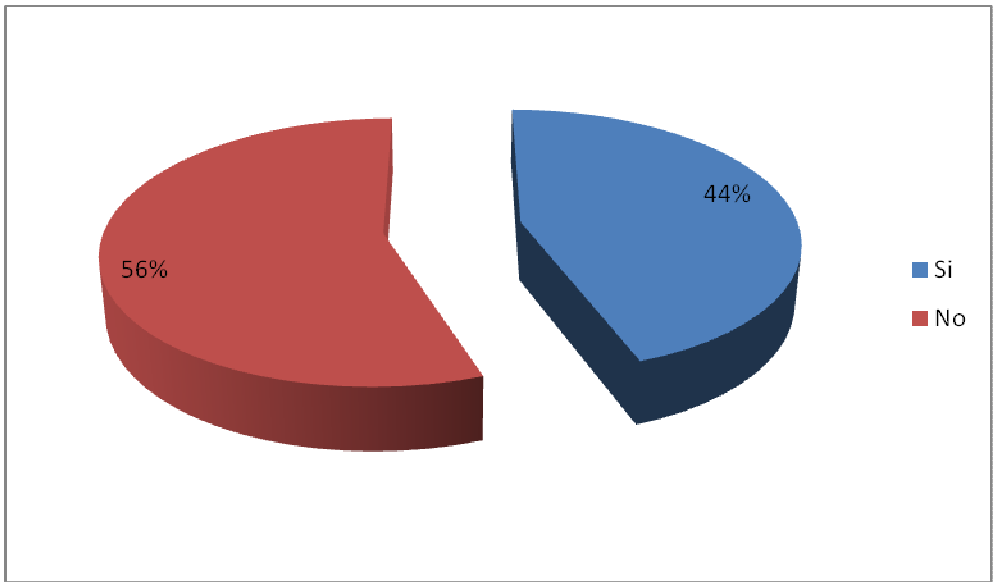
Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

El 39% de las empresas encuestadas no ha realizado una revisión de sus sistemas de información sea físicos o lógicos.

c) Su empresa ha contratado servicios de auditoría de sistemas o revisión de seguridades en el último año?

Si…… No……

GRÁFICO N° 3



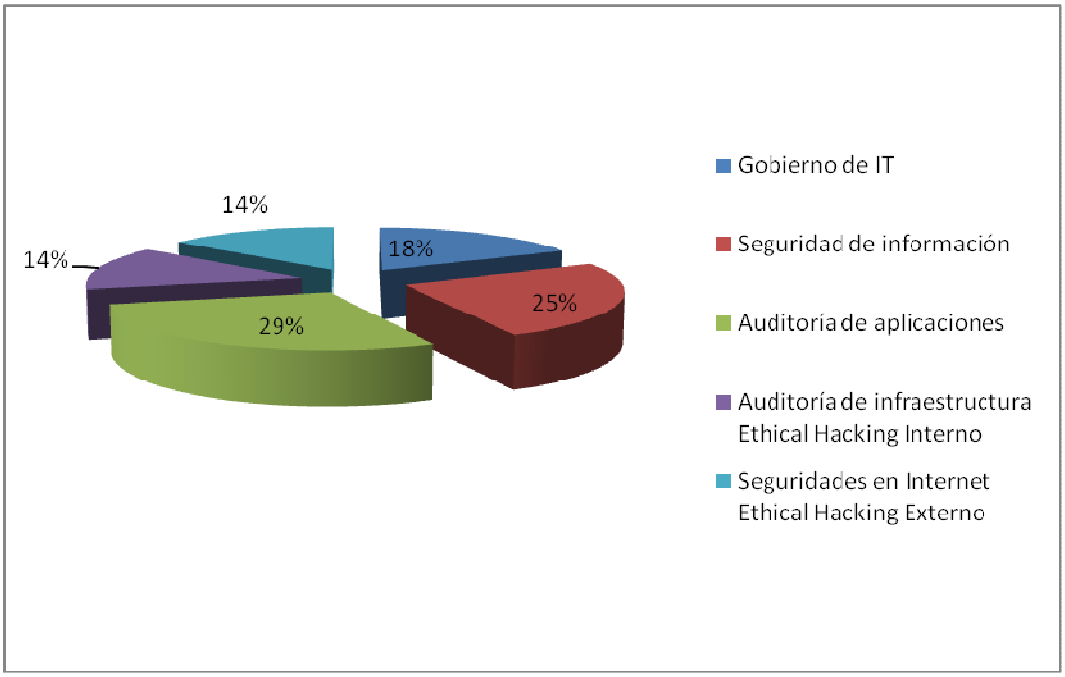
Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

El 56% de las empresas encuestadas contesto que no ha contratado servicios de auditoría o revisión de seguridades de sus sistemas en el último año.

Favor seleccionar el alcance

- Gobierno de IT
- Seguridad de información
- Auditoría de aplicaciones
- Auditoría de infraestructura Ethical Hacking Interno
- Seguridades en Internet Ethical Hacking Externo

GRÁFICO N° 4



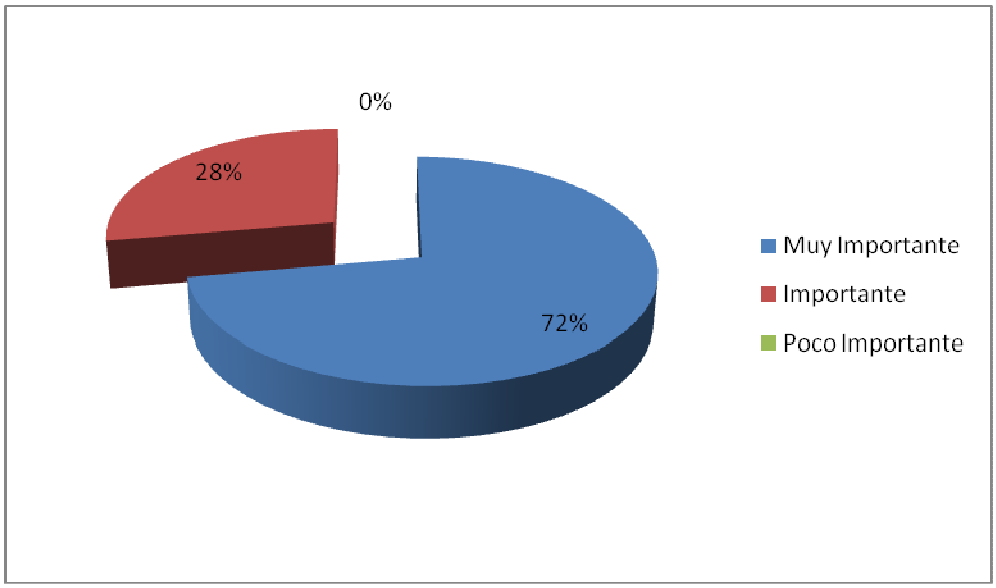
Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

Del 44% de las empresas encuestadas que que si han contratado servicios de seguridades el 29% focalizó la revisión en las sistemas aplicativos.

d) Cuán importante considera usted es la función de auditoría de sistemas para su organización?

Porqué?

GRÁFICO N° 5



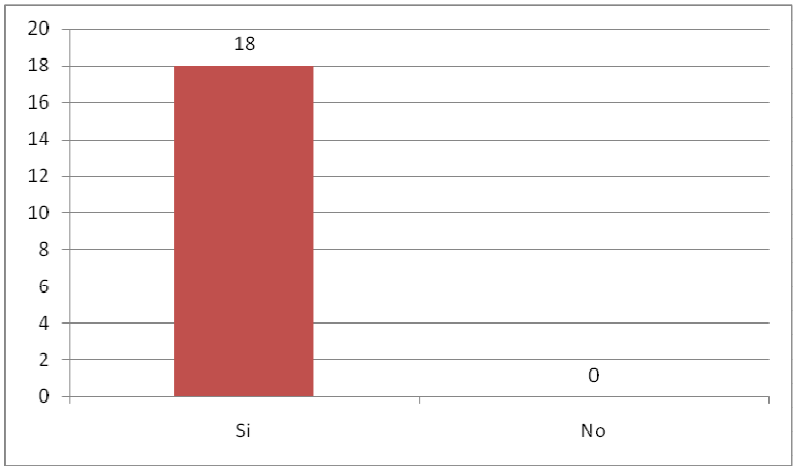
Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

El 72% de las empresas encuestadas consideran que la función de auditoría de Sistemas de es muy importante, principalemnte por el adelanto tecnologico y la automatización de las tareas que realizan las empresas dentro de sus procesos productivos o de servicios.

e) Cree usted que la empresa puede beneficiarse al contar con una función de auditoría de sistemas?

Cómo?

GRÁFICO N° 6

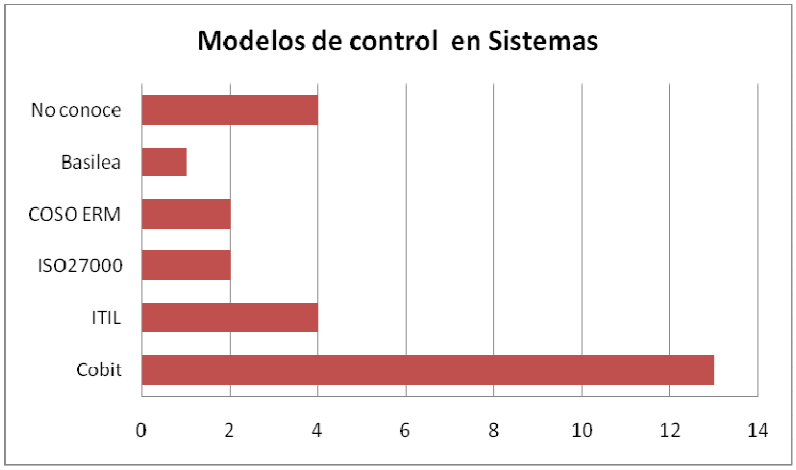


Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

El 100% de las empresas encuestadas considera que la auditoría de sistemas apoya positivamente a las empresas ya que ayuda a mantener segura la información, los resultados de los sistemas son correctos y permitiría implementar oportunidades de mejora que la apoyen a un mejor desarrollo de la empresa.

f) Conoce que marcos referenciales se utilizan en la ejecución de una auditoría de sistemas?

GRÁFICO N° 7



Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

El modelo referencial más conocido para realizar revisión de sistemas es Cobit, el cual es en realizadad un modelo de Gobierno de TI, con un capitulo que permite que este sea auditado una vez sea implementado en la organización.

1.4 REQUERIMIENTOS DE ENTES DE CONTROL REFERENTE A AUDITORÍA DE SISTEMAS (SUPER DE CIAS, SUPER DE BANCOS, SRI U OTROS)

Existen leyes y normas que tiene muy en cuenta los riesgos que existen con la información almacenada en las bases de datos y equipos de las empresas, así encontramos que se realizaron reformas al Código Tributario en los siguientes artículos:

Art. 91.- Forma directa.- La determinación directa se hará sobre la base de la declaración del propio sujeto pasivo, de su contabilidad o registros y más

documentos que posea, así como de la información y otros datos que posea la administración tributaria en sus **bases de datos, o los que arrojen sus sistemas informáticos** por efecto del cruce de información con los diferentes contribuyentes o responsables de tributos, con entidades del sector público u otras; así como de otros documentos que existan en poder de terceros, que tengan relación con la actividad gravada o con el hecho generador.

Art. 344.- Casos de defraudación.- A más de los establecidos en otras leyes tributarias, son casos de defraudación:

7.- La alteración dolosa, en perjuicio del acreedor tributario, de libros o **registros informáticos de contabilidad**, anotaciones, asientos u operaciones relativas a la actividad económica, así como el registro contable de cuentas, nombres, cantidades o datos falsos;

8.- Llevar doble contabilidad deliberadamente, con distintos asientos en libros o **registros informáticos**, para el mismo negocio o actividad económica;

9.- **La destrucción dolosa total o parcial, de los libros o registros informáticos de contabilidad** u otros exigidos por las normas tributarias, o de los documentos que los respalden, para evadir el pago o disminuir el valor de obligaciones tributarias;

También encontramos en el reglamento para la aplicación de la ley orgánica de régimen tributario interno lo siguiente:

Art. 243.- Diligencia de inspección.- El funcionario responsable del proceso de determinación podrá efectuar la inspección y verificación de los registros contables, procesos y sistemas relacionados con temas tributarios, así como de sus respectivos soportes y archivos, **tanto físicos como magnéticos**, en el domicilio fiscal del sujeto pasivo o en el lugar donde mantenga tal información. **También podrá realizar inspecciones y revisiones a los sistemas informáticos que manejen información relacionada con aspectos contables y/o tributarios,** utilizados por el contribuyente, y obtener, en medio magnético o impreso, los respaldos que considere pertinentes para fines de control tributario. Para ejecutar las diligencias de inspección, el funcionario responsable del proceso de determinación podrá acudir a las mismas acompañado de un equipo de trabajo multidisciplinario, de acuerdo a la finalidad de cada proceso. Una vez que se haya revisado y analizado la información, procesos, sistemas y demás documentos pertinentes se elaborará un acta en la que sentará razón de la culminación de dicha inspección y de la información analizada; esta acta será firmada, en dos ejemplares, tanto por el funcionario responsable del proceso de determinación como por el sujeto pasivo o por su representante debidamente autorizado, y por el contador general, de ser el caso; uno de los ejemplares del acta se entregará al sujeto pasivo y otro se agregará al expediente del proceso de determinación.

El artículo innumerado siguiente al Art. 202 del Código Penal Ecuatoriano, contempla la pena de 6 meses a 1 año de prisión y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica a quien, **"empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información;**

para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad".

El segundo Inciso del mismo Cuerpo Legal, considera una figura agravada, imponiendo una pena de 1 a 3 años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica, si la información obtenida se refiere a la "seguridad nacional o secretos comerciales o industriales".

Es oportuno señalar, que la informática, no es sólo un fenómeno científico de carácter subjetivo, por el contrario, los ordenadores, al permitir un manejo rápido y eficiente de grandes volúmenes de información, facilitan la concentración automática de los datos referidos a las personas, convirtiéndose en un verdadero factor de poder, ante el cual, los particulares deben tener las respectivas protecciones.

Es evidente, que la persona que violenta claves, sistemas de seguridad para obtener información, lesiona la intimidad y por consiguiente la confidencialidad de la persona jurídica en muchos casos.

1.5 PERFIL DEL AUDITOR DE SISTEMAS

En el pasado el papel que desempeñaba el auditor de sistemas se basaba en dar apoyo a los equipos de auditoría financiera, pues su función básica era obtener información financiera contenida en los sistemas de información utilizados por el ente auditado.

El auditor de sistemas se encargaba de validar la información y la manejaba con herramientas especializadas para el análisis de datos.

En la actualidad dicha labor continúa siendo una función importante del auditor de sistemas, sin embargo, a medida que la tecnología avanza y las empresas manejan cada vez más información, surge la duda de que si los datos que están manejando son íntegros y confiables, con esa preocupación, poco a poco, en esa labor de apoyo al auditor financiero, el auditor informático pasa, de meramente tratar los datos contables, a cuestionarse la fiabilidad de los mismos. Aplicando los conceptos de escepticismo profesional hasta quedar satisfecho con la información soporte necesaria.

Comienza entonces a plantearse nuevos objetivos de control, como son: el control de acceso sobre la información, la gestión de autorizaciones y los mecanismos de registro de actividad sobre dicha información.

En el momento en el que el auditor de sistemas comienza a plantearse objetivos de control sobre ¿quién debe acceder a qué información?, ¿qué puede hacer con ella?, o a cuestionarse la integridad de la misma, comienza a necesitar y a obtener un conocimiento profundo sobre los procesos de negocio de la compañía. Por otra parte, la integración de dichos procesos en aplicaciones informáticas, provoca que gran parte de los controles que se aplican sobre los mismos se definan en dichas aplicaciones.

A partir de este instante, la labor del auditor de sistemas comienza a confluir con la del auditor financiero, adquiriendo una doble versión de especialista en la definición de procesos de control interno en los procesos de negocio y en su aplicación o análisis sobre los sistemas de información que los soportan.

Finalmente, en paralelo a la función de apoyo de la auditoría financiera, comenzaron a plantearse nuevas funciones relacionadas con la auditoría de sistemas.

El auditor de sistemas como encargado de la verificación y certificación de la informática dentro de las organizaciones, deberá contar con un perfil que le permita poder desempeñar su trabajo con la calidad y la efectividad esperada. Para ello a continuación se establecen algunos elementos con que deberá contar:

CONOCIMIENTOS GENERALES

- Conocimientos tecnológicos, de forma actualizada y especializada respecto a las plataformas existentes en la organización.

- Normas estándares para la auditoría interna; (COSO).

- Políticas organizacionales sobre la información y las tecnologías de la información.

- Conocimiento de las características de la organización respecto a la ética, estructura organizacional, tipo de supervisión existente, compensaciones monetarias a los empleados, extensión de la presión laboral sobre los empleados, historia de la organización, cambios en la administración, operaciones o sistemas, la industria o ambiente competitivo en la cual se desempeña la organización, etc.

- Aspectos legales.

- Herramientas.

- Control y verificación de la seguridad.

- Monitoreo de actividades, etc.

TÉCNICAS

- Evaluación de riesgos.
- Muestreo.
- Cálculo pos operación.
- Monitoreo de actividades.
- Recopilación de grandes cantidades de información.
- Verificación de desviaciones en el comportamiento de datos.
- Análisis e interpretación de la evidencia, etc.

La responsabilidad del auditor para detectar irregularidades o fraude se establece en el prefacio de las normas y estándares de auditoría. En este prefacio se indica que aunque el cometido de los auditores externos no exige normalmente la búsqueda específica de fraudes, la auditoría deberá planificarse de forma que existan unas expectativas razonables de detectar irregularidades materiales o fraude.

Si el auditor externo detecta algún tipo de delito deberá presentar un informe detallado sobre la situación y aportar elementos de juicio adicionales durante las

investigaciones criminales posteriores. El auditor externo solamente puede emitir opiniones basado en la información recabada y normalmente no estará involucrado directamente en la búsqueda de pruebas; a menos que su contrato sea extendido a otro tipo de actividades normalmente fuera de su alcance.

El cometido y responsabilidad de los auditores internos vienen definidos por la dirección de la empresa a la que pertenecen. En la mayoría de ellas, se considera que la detección de delitos informáticos forma parte del cometido de los auditores internos.

De acuerdo al ISACA (Information Systems Audit and Control Association), un auditor de sistemas debe cumplir con los siguientes estándares:

TÍTULO DE AUDITORÍA

Responsabilidad, autoridad y rendimiento de cuentas

La responsabilidad, la autoridad y el rendimiento de cuentas abarcados por la función de auditoría de los sistemas de información se documentarán de la manera apropiada en un título de auditoría o carta de contratación.

INDEPENDENCIA

Independencia profesional

En todas las cuestiones relacionadas con la auditoría, el auditor de sistemas de información deberá ser independiente de la organización auditada tanto en actitud como en apariencia.

Relación organizativa

La función de auditoría de los sistemas de información deberá ser lo suficientemente independiente del área que se está auditando para permitir completar de manera objetiva la auditoría.

ÉTICA Y NORMAS PROFESIONALES

Código de Ética Profesional

El auditor de sistemas de información deberá acatar el Código de Ética Profesional de la Asociación de Auditoría y Control de Sistemas de Información.

Atención profesional correspondiente

En todos los aspectos del trabajo del auditor de sistemas de información, se deberá ejercer la atención profesional correspondiente y el cumplimiento de las normas aplicables de auditoría profesional.

IDONEIDAD

Habilidades y conocimientos

El auditor de sistemas de información debe ser técnicamente idóneo, y tener las habilidades y los conocimientos necesarios para realizar el trabajo como auditor.

Educación profesional continua

El auditor de sistemas de información deberá mantener la idoneidad técnica por medio de la educación profesional continua correspondiente.

PLANIFICACIÓN

Planificación de la auditoría

El auditor de sistemas de información deberá planificar el trabajo de auditoría de los sistemas de información para satisfacer los objetivos de la auditoría y para cumplir con las normas aplicables de auditoría profesional.

EJECUCIÓN DEL TRABAJO DE AUDITORÍA

Supervisión

El personal de auditoría de los sistemas de información debe recibir la supervisión apropiada para proporcionar la garantía de que se cumpla con los objetivos de la auditoría y que se satisfagan las normas aplicables de auditoría profesional.

Evidencia

Durante el transcurso de una auditoría, el auditor de sistemas de información deberá obtener evidencia suficiente, confiable, relevante y útil para lograr de manera eficaz los objetivos de la auditoría. Los hallazgos y conclusiones de la auditoría se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia.

INFORMES

Contenido y formato de los informes

En el momento de completar el trabajo de auditoría, el auditor de sistemas de información deberá proporcionar un informe, de formato apropiado, a los destinatarios en cuestión. El informe de auditoría deberá enunciar el alcance, los objetivos, el período de cobertura y la naturaleza y amplitud del trabajo de auditoría realizado. El informe deberá identificar la organización, los destinatarios en cuestión y cualquier restricción con respecto a su circulación. El informe deberá enunciar los

hallazgos, las conclusiones y las recomendaciones, y cualquier reserva o consideración que tuviera el auditor con respecto a la auditoría.

ACTIVIDADES DE SEGUIMIENTO

Seguimiento

El auditor de sistemas de información deberá solicitar y evaluar la información apropiada con respecto a hallazgos, conclusiones y recomendaciones relevantes anteriores para determinar si se han implementado las acciones apropiadas de manera oportuna.

Al necesitar un profundo nivel de conocimiento de los procesos de negocio, controles, tecnología, regulaciones legales, finanzas, contabilidad y conceptos de seguridad, entre otros aspectos generales el perfil del auditor de sistemas, estaría orientado a personas con formación en sistemas de información con un sólido conocimiento de procesos, contabilidad, y control interno o a una persona con formación en contabilidad y finanzas con un sólido conocimiento de sistemas de información, cualquiera de los dos sería un perfil deseado, considerando que cada día los procesos de negocio se automatizan permanentemente lo que exige que los auditores financieros deban conocer como auditarlos.

El Instituto de Auditores Internos ha entendido completamente este cambio y ahora para otorgar el CIA (Certificado de Auditor Interno por sus siglas en inglés) exige la aprobación de un nivel importante de sistemas de información previo a otorgar dicho certificado.

2 TECNOLOGÍA DE INFORMACIÓN – CONTROL INTERNO

2.1 ASPECTOS GENERALES

La tecnología de información surgió con la utilización de la tecnología para el procesamiento de la información, esto involucra desde la entrada de datos, transformación, almacenamiento y recuperación de la misma.

En la actualidad la tecnología de la información ha tenido un avance vertiginoso convirtiéndose en una herramienta poderosa en todas las áreas de los negocios debido a que las empresas implantan sistemas computarizados para el manejo eficiente de sus operaciones y de esta manera obtener ventajas competitivas siempre y cuando se realicen las modificaciones y actualizaciones pertinentes.

Es importante mencionar que la tecnología de la información va de la mano con la seguridad informática por lo tanto son imprescindibles las políticas y procedimientos con respecto a este tema y la difusión de las mismas en todos los niveles de la entidad.

El objetivo de las políticas de seguridad es definir qué están haciendo los usuarios con la información de la empresa y de qué manera están haciendo uso de los recursos tanto de hardware como de software con costos eficientes.

Los atributos para mantener protegida la información en cada una de las entidades son los siguientes:

GRÁFICO N° 8

Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

Es así que la tecnología nos brinda facilidades para el procesamiento de la información pero esto también conlleva a riesgos que pueden en ocasiones ser críticos para la entidad, es por esto que se dice que el activo más importante de cualquier compañía es la información y por lo tanto se debe invertir en la seguridad de la misma, ya que se vuelve una pieza clave en la obtención de los objetivos.

En los últimos años se ha observado la importancia del buen manejo del control interno en todas las entidades por la facilidad que representa el poder medir la eficiencia en cada una de las àreas claves del negocio determinando así la situación real y la verificación de que los controles implantados se están cumpliendo.

Por consiguiente, el control interno comprende el plan de organización en todos los procedimientos coordinados de manera coherente a las necesidades del negocio, para proteger y resguardar sus activos, verificar su exactitud y confiabilidad de los datos contables, así como también llevar la eficiencia, productividad y custodia en las operaciones para estimular la adhesión a las exigencias ordenadas por la gerencia.

De lo anterior se desprende, que todos los departamentos que conforman una empresa son importantes, pero, existen dependencias que siempre van a estar en constantes cambios, con la finalidad de afinar su funcionabilidad dentro de la organización.

El Control Interno lo podemos definir como una serie de acciones que ocurren de manera constante a través del funcionamiento y operación de una entidad, reconociéndose como parte integral de la estructura administrativa y la parte operativa de toda organización con el objeto de que se alcancen las metas definidas.

Basándonos en los modelos referenciales más usados, el control interno debe estar estructurado en los siguientes elementos: ambiente de control, en donde combinará los factores que afectan las políticas y procedimientos de la entidad, de tal manera que evaluará los riesgos, identificando, analizando y administrándolos para que sea posible alcanzar los objetivos de la entidad, mediante sistemas de información y comunicación que provoquen una cuantificación de la información, estableciendo procedimientos de control con el fin de proporcionar una seguridad razonable de que los objetivos específicos de la entidad se van a lograr de forma eficaz y eficiente, teniendo una responsabilidad y papel importante el consejo de administración que se encargará de establecer y mantener los controles internos establecidos.

2.2 OBJETIVOS DEL CONTROL INTERNO

Se han definido objetivos específicos para lograr el control interno en las entidades los cuales están orientados a cumplir con las intenciones de la administración, estos son:

- Proteger los activos de la organización evitando pérdidas por fraudes o negligencias.

- Asegurar la exactitud y veracidad de los datos contables y extracontables, los cuales son utilizados por la dirección para la toma de decisiones.

- Promover la eficiencia.

- Estimular el seguimiento de las prácticas ordenadas por la gerencia.

- Promover y evaluar la seguridad, la calidad y la mejora continua.

En definitiva podemos observar que es de gran importancia el control interno en las organizaciones para la optimización de sus operaciones y el crecimiento de las mismas mostrando así un alto grado de confianza con la generación de mayor rentabilidad.

2.3 LA TECNOLOGÍA Y EL CONTROL INTERNO, HERRAMIENTAS PARA PREVENIR EL FRAUDE

Debido a que las organizaciones deben cumplir con estándares de seguridad, confiabilidad en sus procesos e información se han tomado medidas para evitar el fraude el cual se lo define como un acto intencional en la presentación o elaboración de los estados financieros.

Precisamente se ha establecido que existen dos tipos de fraudes: alteración de activos de la empresa y presentación intencional de información financiera errónea.

Es importante mencionar que la manera de evitar un fraude es el establecer el control en toda la organización en donde se preverán todas las medidas administrativas para el alcance de los objetivos, implementando políticas y procedimientos dentro de las cuales se establezca el verificar la exactitud y veracidad de la información. De aquí que la efectividad del control interno dependa de gran medida de la integridad y de los valores éticos del personal que diseña, administra y vigila el control interno de la entidad.

La Norma Internacional de Auditoría No. 315, que se refiere al entendimiento de la entidad y su entorno y evaluación de los riesgos de representación errónea de importancia relativa, define las características de elementos manuales y automatizados del control interno relevantes para la evaluación del riesgo por el auditor. En cuanto a los controles automatizados destaca el hecho que los mismos proporcionan beneficios potenciales de efectividad y eficiencia para el control interno al hacer posible que la entidad aplique de manera consistente reglas de negocios predefinidas al procesar grandes volúmenes de transacciones de una misma manera, así como mejorar la oportunidad, disponibilidad y exactitud de la información, al igual que facilita el análisis adicional de información.

Se han identificado riesgos específicos para el área de Tecnología de Información involucrados con el control interno:

- Procesamiento erróneo de los datos ocasionando resultados erróneos y la multiplicación de los mismos en otros.

- Acceso no autorizado a datos o cambios no autorizados a sistemas o programas.

- Potencial pérdida de datos o incapacidad de acceder a los datos según se requiere.

Conociendo todos estos posibles riesgos es importante monitorear la efectividad de los controles automatizados teniendo muy presente como ha respondido la entidad ante estas situaciones.

En años anteriores no se mencionaba el riesgo como punto importante sobre la base de una auditoría en las entidades pero a partir de años recientes las normas mantienen un énfasis especial en controles generales del computador y controles que se encuentren implementados en la aplicación sobre la cual desarrollan sus operaciones.

2.4 LA LEY SARBANES OXLEY: IMPLICACIONES CON LA GERENCIA DE TECNOLOGÍA

La Ley Sarbanes - Oxley, (SOX) fue publicada en julio del 2002, durante la presidencia de George W. Bush, esta ley despertó un interés especial en la dependencia de las organizaciones a la tecnología de información preocupando a todos los niveles de la empresa. El Instituto de Auditores Internos de los Estados

Unidos (THEIIA), promulgó en el mes de noviembre de 2006 la Guía para la Evaluación de los Controles Generales de la Tecnología de la Información sobre la Base del Riesgo (GAIT, con la finalidad de facilitar tanto a auditores internos como externos el cumplimiento de los requerimientos de la ley SOX.

SOX está diseñado para revisar los requisitos de una auditoría, la responsabilidad empresarial, la independencia del auditor y la presentación de la información financiera, con la aplicación de esta ley se requiere información adicional así como también existen sanciones penales y civiles para los que incurran voluntariamente en la presentación errónea de los estados financieros, es por esto que se define como un proceso rutinario el diseño, evaluación y mejoramiento del control interno. En este sentido, la Tecnología de Información (TI) juega un papel imprescindible en mantener, de manera adecuada y en el tiempo, un esquema de control interno estable y preventivo, más que detectivo y correctivo.

La mayoría de los CEOs, CFOs y CIOs comprenden el rol que el área de TI posee dentro de una Compañía, más aun, cuando es difícil imaginar una Compañía exitosa en el siglo XXI que no posea cierto nivel de dependencia de la tecnología como apoyo a los procesos de negocio. En los ambientes corporativos hoy en día, el procesamiento y emisión de los reportes financieros son realizados utilizando sistemas de información, bien sean integrados o no, por lo que el control interno de TI debe ser diseñado, evaluado y mantenido como cualquier otro proceso de negocio de la corporación, a fin de cumplir con las exigencias de la Ley SOX.

La TI provee el control para hacer efectivas las operaciones, tales como:

- Información gerencial (Data Warehouse).

- Gestión de usuarios (autenticación, autorización a transacciones sensitivas, segregación de funciones).

- Emisión de reportes financieros, operativos y administrativos en tiempo real.

- Procesamiento de grandes volúmenes de información.

Los profesionales de TI responsables de llevar a cabo la identificación, diseño y/o evaluación del control interno en la Compañía, en el marco de un proyecto destinado a dar cumplimiento de lo exigido por la Ley SOX, deben contar con una metodología apropiada, para llevar a cabo dicho proceso. Los pasos a seguir para llevar a cabo el diseño y evaluación de controles en conformidad con lo exigido por la Ley SOX son los siguientes:

1. **Planificar y definir el alcance:** Inicialmente, las organizaciones deben entender cómo funciona el proceso de divulgación financiera e identificar dónde la tecnología es más crítica en el apoyo de este proceso. Esto permitirá identificar los sistemas de información claves que necesitan ser incluidos en el alcance del proyecto. Comúnmente, los sistemas de información deberán ser considerados para el alcance, si éstos participan en la generación, registro, procesamiento y emisión de la información financiera.

2. **Determinación de riesgo:** La determinación del riesgo permite a organizaciones entender cómo los acontecimientos pueden inhibir el logro de los objetivos de

negocio. La misma requiere dos (2) perspectivas: probabilidad e impacto. También debe considerarse la significación financiera y operacional de las unidades de negocio. Para determinar cuáles deben incluirse en el alcance del programa, las organizaciones deben considerar el grado de la dependencia de TI de las unidades de negocio y el grado de consistencia de los procesos y procedimientos con otras unidades de negocio.

3. **Identificar cuentas/controles significativos:** la Ley SOX, sustentada en el modelo COSO, identifica dos grupos para las actividades de control de los sistemas de información, a saber:

   - Los controles de aplicación, para los cuales las organizaciones deben primero identificar las cuentas significativas que podrían tener un impacto material en el proceso financiero de reporte y divulgación.

   - Los controles generales de cómputo, los cuales aplican a todos los sistemas de información y apoyan la operación segura y continua del negocio, y para los cuales las organizaciones deben determinar los controles que apoyen la calidad y la integridad de la información, y que se diseñan para atenuar los riesgos identificados.

4. **Documentación del diseño de control:** No existe una forma particular de documentación aprobada o requerida; el grado de la documentación puede variar, dependiendo del tamaño y de la complejidad de la organización; sin embargo, es importante contar con un sistema de información que permita clasificar la documentación según su confidencialidad y criticidad.

5. **Evaluar el diseño de control:** Las organizaciones deben evaluar la capacidad de su control interno para reducir el riesgo de TI a un nivel aceptable y de asegurarse que es entendido por los usuarios. El modelo diseñado por Espiñeira, Sheldon y Asociados de las "Etapas de Evolución en el Nivel de Seguridad en las Organizaciones". Algunas organizaciones pueden estar dispuestas a aceptar un nivel de control ubicado en la etapa 1 ó la etapa 2; sin embargo, dado los requisitos de la Ley SOX para la certificación del control interno por parte de los auditores externos, los controles implantados requerirán de las cualidades y las características que sólo pueden lograrse al llegar a la etapa 3 ó la etapa 4.

6. **Evaluar la eficacia operacional:** Luego de haber realizado el diseño del control interno, debe confirmarse la eficiencia y eficacia del mismo, por lo que es necesario realizar pruebas, conducidas por responsables de los controles y del equipo de la gerencia interna del programa de control con el objetivo de corroborar que los controles operaron consistentemente a lo largo del periodo revisado.

7. **Determinar las debilidades materiales:** Una debilidad material se entiende como las deficiencias significativas que imposibilitan el control interno de la organización para proporcionar un aseguramiento razonable de las cifras expuestas en los estados financieros. En este sentido, para la evaluación de las deficiencias del control de TI, los auditores externos considerarán varios factores, tales como el tamaño de operaciones, la complejidad y diversidad de actividades, la estructura de organización y la probabilidad que la deficiencia del control diera lugar a errores en la declaración de los registros financieros de la organización.

8. **Documentar los resultados:** Los resultados de las pruebas realizadas deben ser registrados, pues formarán la base para la aserción de la Gerencia y la opinión del auditor tanto interno como externo. Es importante mencionar, que no hay un formato prescrito para llevar a cabo esta actividad: el objetivo es proporcionar un resumen comprensivo, fácilmente entendible de la eficacia del control interno y de las pruebas realizadas para probar el mismo.

9. **Construir la sustentación:** La determinación de los controles debe formar parte de la organización y de la cultura de la Gerencia de TI. La organización debe asegurar que los controles internos diseñados e implementados sean sustentables y sostenidos en el tiempo.

GRÁFICO N° 9

Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

Esta situación coloca a las Gerencias de TI en una posición comprometedora, ya que deberán velar porque la información generada por los sistemas de información,

utilizada para la emisión de los reportes financieros de la Compañía, sea íntegra, veraz y oportuna.

Actualmente aún existen compañías que no cuentan con una gestión de riesgos del área de TI, por estas razones, muchas organizaciones se verán en la necesidad de buscar apoyo externo de especialistas en TI y riesgos, a fin de lograr la asesoría en las áreas claves para TI, tomando en cuenta que el control es un proceso que requiere la ayuda y la evaluación continua para permanecer en el tiempo.

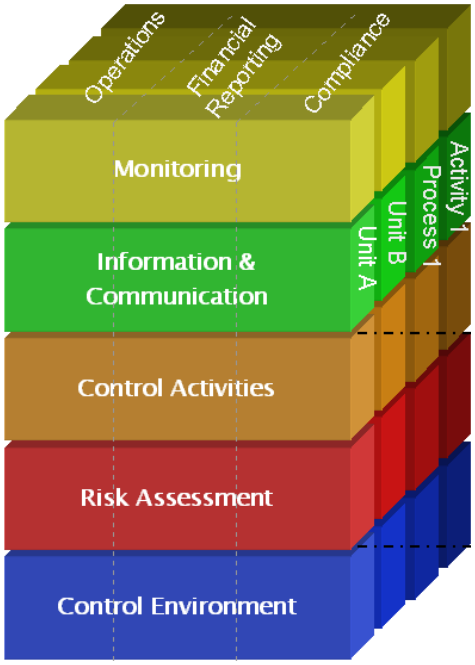
Esta ley originada en Estados Unidos ha sido regida para todas las empresas que estén registradas en la New York Stock Exchange (NYSE) y la National Association of Securities Dealers by Automatic Quotation, conocida como NASDAQ, y bajo la supervisión de la Securities and Exchange Commission (SEC), esto implica por supuesto que también se acogen a esta ley todas las empresas extranjeras que cotizan en dichas bolsas de valores, incluyendo a la casa matriz, las subsidiarias y afiliadas.

En conclusión, esta ley impone el implementar mecanismos que aseguren un correcto estudio de los posibles riesgos a su vez identificar los controles que ayudarían a la mitigación de los mismos evitando así errores en la presentación de los estados financieros. Las empresas han manifestado que la aplicación de SOX ha sido un poco costosa debido a que han tenido que incurrir costos en actualizaciones de los sistemas de información entre otros más.

2.5 NUEVAS CORRIENTES DE CONTROL INTERNO

GRÁFICO N° 10

CONTROL INTERNO BASADO EN COSO I



Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

COSO (Committee of Sponsoring Organizations of the Treadway Commission) es una metodología para la evaluación de los controles internos dentro de una entidad, se hace específicamente referencia a una serie de actividades, inherentes a la gestión e integrados a los demás procesos de la misma como lo son la planificación, ejecución y supervisión.

Uno de los principales puntos por los cuales las empresas se basan en el modelo COSO es porque ayuda a las organizaciones a mejorar la eficacia y la eficiencia de su sistema interno de control además de proporcionar una guía práctica que muestre cómo el control puede ser incorporado a los procesos de control interno de una organización.

La finalidad del marco COSO es:

1. Establecer una definición común del control interno que responda a las necesidades de todas las empresas y otras entidades.

2. Definir un modelo o marco de referencia sobre la base del cual las empresas y otras entidades, sin importar su tamaño y naturaleza, puedan evaluar su sistema de control interno.

Priorizar los riesgos es una parte natural del componente del control interno consistente en la evaluación del riesgo. Su inclusión aquí no implica la necesidad de una función de evaluación de riesgos dedicada exclusivamente al apoyo de la función de vigilancia.

El informe COSO define el control interno como un proceso efectuado por el Consejo de Administración, la alta dirección y en "cascada" por, el resto del personal de una organización, diseñado para proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes y normas que sean aplicables.

Los 20 principios básicos que COSO recalca con la finalidad de obtener un efectivo control interno son los mencionados a continuación:

- **Ambiente de Control**

1. Integridad y Valores Éticos. La sana integridad y los valores éticos, particularmente en la alta gerencia, han sido desarrollados, comprendidos y adoptados, fijando el estándar de conducta para la divulgación financiera.

2. Comité de Dirección. La Junta de Directores entiende y ejercita la responsabilidad por los errores relacionados con el reporte financiero y el control interno.

3. Filosofía de Dirección y Estilo de Gestión. La filosofía del management y el estilo de apoya el alcance de un control interno efectivo sobre el reporte financiero.

4. Estructura Organizativa. La estructura organizativa de la empresa soporta el alcance de un eficaz control interno sobre la información financiera.

5. Competencias para el Adecuado Reporte Financiero. La compañía retiene a los individuos competentes en el reporte financiero y la detección de errores relacionados con dichos reportes.

6. Autoridad y Responsabilidad. El Management y los empleados son asignados de acuerdo a niveles adecuados de autoridad y responsabilidad para facilitar un control interno efectivo sobre el reporte financiero.

7. Recursos Humanos. Las Políticas y prácticas de RRHH son diseñadas e implementadas para facilitar un control interno efectivo sobre el reporte financiero.

- **Evaluación de Riesgos**

8. Objetivos del Reporte Financiero. El Management especifica los objetivos sobre el reporte financiero con suficiente claridad y criterio para permitir la identificación de riesgos sobre la divulgación del reporte financiero.

9. Riesgos del Reporte Financiero. La compañía identifica y analiza los riesgos relacionados con el alcance de los objetivos de divulgación del reporte financiero como base para determinar cómo los riesgos deberían ser manejados.

10. Riesgos de Fraude. El riesgo potencial para la declaración errónea material relacionada con la producción del fraude se considera explícitamente en la identificación de riesgos relacionados con los objetivos de divulgación financiera.

- **Actividades de Control**

11. Integración con la Evaluación de Riesgos. Son tomadas acciones para direccionarlas a los riesgos de alcanzar los objetivos del reporte financiero.

12. Selección y Desarrollo de las Actividades de Control. Las actividades de control son seleccionadas y desarrolladas considerando sus costos y su potencial de efectividad para mitigar riesgos de alcanzar los objetivos del adecuado reporte financiero.

13. Políticas y Procedimientos. Las políticas relacionadas con la divulgación de información confiable sobre el reporte financiero son establecidas y comunicadas a través de la compañía, con sus correspondientes procedimientos.

14. Tecnología de la Información. Los controles de TI, donde son aplicables, son diseñados e implementados para dar soporte al alcance de los objetivos del reporte financiero.

- **Información y Comunicación**

15. Reporte de Información Financiera. La información pertinente es identificada, capturada, utilizada en todos los niveles de la compañía, y distribuida en tiempo y forma tal que contribuya al alcance de los objetivos sobre el reporte financiero.

16. Información sobre el Control Interno. La información utilizada para ejecutar otro componente del control interno es identificada, capturada, y distribuida en tiempo y forma tal que permita que el personal lleve a cabo sus responsabilidades frente al control interno.

17. Comunicación Interna. Las comunicaciones permiten y facilitan la comprensión y ejecución de los objetivos del control interno, de los procesos y de las responsabilidades individuales, en todos los niveles de la organización.

18. Comunicación Externa. Los temas que podrían afectar el alcance de los objetivos de la información financiera son comunicados a las terceras partes interesadas.

- **Monitoreo**

19. Evaluaciones Continuas y Puntuales. Las evaluaciones permanentes y separadas permiten al management determinar si el control interno está presente y funciona en forma adecuada en el tiempo.

20. Reporte de Deficiencias. Las deficiencias de control interno son identificadas y comunicadas de manera oportuna a las partes responsables de tomar acciones correctivas, a la gerencia y al Directorio.

GRÁFICO N° 11

COSO II - EL ENFOQUE INTEGRADO PARA LA ADMINISTRACIÓN CORPORATIVA DE RIESGOS

Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

COSO realizó un estudio con el cual pudo detectar que ha existido un incremento en la preocupación por la administración de los riesgos en las compañías por lo que se determinó la necesidad de la creación de un reconocido marco de administración integral de riesgos, por lo cual se dio paso a la creación de COSO ERM.

La administración de riesgos corporativos es una tarea llevada a cabo por el directorio, la administración y las personas de la organización, es aplicado desde la definición estratégica hasta las actividades del día a día, diseñado para identificar eventos potenciales que pueden afectar a la organización y administrar los riesgos dentro de su gusto, con el fin de proveer una seguridad razonable respecto del logro de los objetivos de la organización.

Beneficios de ERM:

- Alinear el riesgo con la estrategia.
- Relacionar crecimiento, riesgo y retorno.
- Mejorar las decisiones de respuesta al riesgo.
- Reducir sorpresas y pérdidas operacionales.
- Identificar y gestionar la diversidad de riesgos por compañía y grupo agregado.
- Aprovechar las oportunidades.
- Mejorar la asignación de capital.

ERM, es un proceso formal diseñado para identificar, evaluar, responder, comunicar y monitorear los riesgos a lo largo de toda la organización, adicionalmente, dado que COSO Enterprise Risk Management - Integrated Framework se encuentra completamente alineado con el Internal Control - Integrated Framework, las mejoras en la gestión de riesgo permitirán mejorar, aún más, sobre la inversión ya realizada en control interno bajo las disposiciones de la Ley Sarbanes-Oxley.

Es importante mencionar que esta nueva metodología otorga la estructura conceptual para lograr manejar las incertidumbres y así evitar posibles riesgos contribuyendo en la mejora de su organización.

Podemos concluir entonces que, el antecedente principal de la gestión integral de riesgo es que cada entidad con o sin fines de lucro, se enfrenta a incertidumbres y el desafío para la administración es determinar qué cantidad de incertidumbre puede la entidad aceptar en su búsqueda de aumentar su rentabilidad. Cabe mencionar que

esta incertidumbre se manifiesta tanto como riesgo y oportunidad, con el potencial de erosionar o generar valor.

3 DISEÑO DE MODELO DE REVISIÓN DE AMBIENTES DE PROCESAMIENTO DE DATOS

El objetivo de realizar la revisión del ambiente de procesamiento de datos es analizar y evaluar los controles establecidos por la compañía para salvaguardar los activos de información, para esto se realiza revisiones: a nivel de seguridad lógica y física; a los procedimientos para realizar desarrollos y/o modificaciones en las aplicaciones; a los procedimientos para resolución de problemas (help desk), seguridad de la información y ejecución de respaldos de información; y al plan de continuidad del negocio que la compañía posea.

El esquema de revisión propuesto está soportado en COSO por lo que la revisión de controles se divide en revisión del Diseño e Implementación, en adelante D&I; y revisión de la Eficacia Operativa, en adelante EO. A continuación una breve explicación de lo que comprende cada una de las revisiones:

En D&I se corrobora que el control identificado se encuentre diseñado e implementado correctamente en el momento de la revisión, se solicitará políticas o procedimientos que validen que efectivamente la compañía ha diseñado dicho control, y con un ejemplo, verificar su correcto funcionamiento.

En EO se valida que el control diseñado e implementado haya funcionado correctamente durante el periodo de la auditoría, es decir, en base a la selección de una muestra

representativa se corrobora que los controles se cumplan a lo largo de todo el período sujeto a revisión.

El tipo de control se lo puede clasificar en:

- Manual: Control ejecutado por el usuario.
- Automático: Control ejecutado parte por el usuario y parte automática.
- Combinado: Para la ejecución del control no existe intervención humana.

3.1 SEGURIDAD LÓGICA Y FÍSICA DE LA PLATAFORMA TECNOLÓGICA

Es importante para la organización salvaguardar los activos de información, por esta razón es necesaria la implementación de controles lógicos y físicos en las instalaciones donde se realiza el procesamiento de información y que estos se encuentren ubicados en áreas protegidas garantizando que los controles implementados sean apropiados. Se debe proteger contra accesos no autorizados, daños e intromisiones de terceros.

Es necesario implementar políticas y procedimientos que garanticen la seguridad lógica de la información: políticas de escritorios y pantallas limpias; cambios periódicos de contraseñas; pistas de auditoría; políticas para asignación de accesos a los aplicativos y sistema operativo; asignación de superusuarios en las aplicaciones; entre otros.

En cuanto a la seguridad física se deben implementar controles para proteger los equipos, así como el edificio e instalaciones que los albergan; contemplando

situaciones de sabotaje, incendios, robos, catástrofe naturales, problemas de suministro de energía eléctrica, entre otros.

A continuación detallamos los objetivos de control y las actividades que permitan validar que éstos se cumplan de acuerdo con las intenciones de la gerencia.

Objetivo:

En la compañía se han configurado técnicas para restringir el acceso a los datos, aplicativos y recursos de información.

Requerimientos de Información

- Solicitar al Gerente de Sistemas que nos explique las políticas y procedimientos relacionados con seguridad de la información, así como las herramientas de seguridad utilizadas para restringir el acceso a los recursos de información y los aplicativos involucrados.

- Solicitar las políticas y procedimientos de seguridad aplicables.

Procedimiento para probar D&I

Pedir a un usuario al azar que acceda a los sistemas que utiliza y verificar que la contraseña cumpla con los parámetros definidos en la política, e indagar cada qué tiempo cambia de contraseña y qué complejidad tiene ésta.

Procedimiento para probar EO

1. Revisar con ayuda del personal responsable del Sistema, los parámetros de seguridad establecidos en el servidor principal.

2. Solicitar la lista de usuarios privilegiados (superusuarios) y validar con el Gerente de Sistemas que sea personal autorizado.

3. Validar que las políticas de seguridad de contraseñas (longitud máxima, longitud mínima, complejidad, historial, tiempo máximo de vigencia, número de intentos antes de bloqueo, entre otros) se encuentren conforme lo indican las políticas de la compañía.

4. Verificar los parámetros de seguridad establecidos en cada uno de los aplicativos a través de la revisión de los módulos de seguridad propios de cada aplicación. Se puede revisar si se han implementado perfiles de usuarios, contraseñas, las cuales cumplan los parámetros de seguridad definidos por la compañía.

5. Adicionalmente, verificar la existencia de pistas de auditoría y que se realice el monitoreo sobre las mismas.

Objetivo:

En la compañía se han implementado políticas y procedimientos para asegurar el acceso autorizado a los aplicativos, datos y otros recursos de información.

Requerimiento de Información

Solicitar la siguiente información al área de Sistemas o TI:

- Políticas y procedimiento para administración del acceso a los sistemas de aplicación. (D&I).

- Formulario o solicitud para asignación de accesos a los sistemas de aplicación (creación, modificación y eliminación de accesos). (D&I).

- Lista de usuarios de los principales sistemas de aplicación. *Recuerde que debe validar a qué niveles existe seguridad (aplicación, base de datos y/o sistema operativo) para según eso solicitar los usuarios.* (EO).

- Lista de usuarios de red o sistema operativo. (EO).

- Carpetas de formularios de "solicitud de asignación de accesos" a sistemas de aplicación, base de datos y/o sistema operativo de todo el periodo de revisión. (EO).

- Listado de empleados activos con corte a la fecha de revisión y empleados que salieron de la compañía hasta la misma fecha. *Esto debe ser solicitado a RRHH.* (D&I – EO).

Procedimiento para probar D&I

1. Entreviste al Gerente de Sistemas con respecto al procedimiento para asignación de accesos a los sistemas de aplicación y seguridad lógica en sistemas de aplicación, bases de datos y/o sistemas operativos. Corrobore mediante revisión de documentos el diseño del control con ayuda de las políticas y procedimientos relacionados.

2. Solicite el último formulario de asignación de acceso, y valide que todos los requerimientos definidos en el procedimiento para procesarlo se hayan cumplido. Aspectos a considerar en la revisión: aprobaciones tales como firmas del Jefe/Gerente, del usuario funcionario requisitor y dueño de la información respectivamente, opciones solicitadas.

   Revise si los perfiles asignados en el sistema concuerdan con los solicitados en el formulario. Recuerde que el usuario puede ya haber existido y el formulario que solicitó es una extensión de sus permisos, valide esto antes de concluir sobre la implementación del control.

3. Solicite la documentación de la última revisión de accesos por cada uno de los responsables de los sistemas de aplicación (dueños de la información o data owners).

4. En cuanto a la consistencia del funcionamiento de las políticas de seguridad, debemos validar que las herramientas de seguridad configuradas tales como las

políticas de contraseñas en cuanto al tiempo máximo de vigencia se cumplan. Esto aplica para los usuarios de red, por lo tanto revise el campo de último cambio de contraseña y valide que se encuentren dentro de los rangos establecidos por las políticas y procedimientos. Esto basta para probar EO por ser controles automatizados, sin embargo usar su juicio profesional para considerar otros criterios.

Procedimiento para probar EO

1. Para el caso de las asignaciones de acceso, primero debemos determinar el tamaño de la muestra a revisar en base a la población total, es decir, del total de solicitudes atendidas durante el período de revisión, seleccionar una muestra representativa para verificar que todas las solicitudes de la muestra cumplan con todos los requerimientos tal como en el D&I.

2. Cruzar el reporte de usuarios de sistemas con el listado de RRHH, con el objetivo de verificar que a los usuarios que se les está otorgando acceso consten como funcionarios activos.

3. Verificar que todos los usuarios de sistemas de aplicación, base de datos y/o sistema operativo son válidos, para esto debemos cruzar dichos listados con la lista de personal activo de RRHH y validar que todos sean empleados activos. De encontrar excepciones, verificar que estos no se encuentren en la lista de personal retirado o ex empleados.

4. Con la lista de empleados cesantes (durante el periodo examinado) proporcionada por RRHH validar que ninguno de estos se encuentre activo en los aplicativos o sistema operativo.

5. Si existen excepciones, validarlas con el área involucrada. Si persisten, incluir un comentario en el informe final.

Objetivo:

El acceso físico al centro de cómputo se encuentra restringido para garantizar que solamente personal autorizado pueda tener acceso.

Requerimiento de Información

Solicitar la siguiente información al área de Sistemas o TI:

- Políticas y procedimiento para administración de acceso físico al centro de cómputo y mantenimiento del centro de cómputo (D&I).

- Formulario o solicitud para asignación de acceso físico (creación, modificación y eliminación). (D&I).

- Usuarios de mecanismos de restricción de acceso físico, estos pueden ser lectores biométricos, lectores de tarjetas magnéticas, cerraduras electrónicas. (EO).

- Bitácora de accesos físicos al centro de cómputo. (EO).

- Listado de empleados activos con corte a la fecha de revisión y empleados que salieron de la compañía hasta la misma fecha. *Esto debe ser solicitado a RRHH.*(D&I y EO).

Procedimiento para probar D&I

1. Entreviste al Gerente de Sistemas o responsables sobre la administración de accesos físicos al centro de cómputo. Corrobore mediante revisión de documentos el diseño del control de acceso al centro de cómputo con ayuda de las políticas y procedimientos relacionados.

2. Solicite la bitácora de registro de accesos al centro de cómputo y determine que todos los requerimientos se cumplan en cuanto a personal autorizado, firmas, entre otros.

3. Realice una visita al centro de cómputo y corrobore mediante observación la implementación del control tomando en cuenta el mecanismo de restricción física instalado (puede ir desde cerraduras tradicionales hasta lectores biométricos). Adicionalmente verifique que existan implementados otros mecanismos de control ambiental tales como medidores de temperatura y humedad, y de seguridad tales como extintores (revise fechas de caducidad), sensores de movimientos y UPS.

Procedimiento para probar EO

1. Si existen solicitudes de acceso físico, obtener una muestra de tamaño apropiado (obtener el tamaño en base a la frecuencia de solicitudes) y validar que se cumplan todos los requisitos.

2. Seleccionar una muestra de fechas en base a la frecuencia de accesos y verificar que se hayan registrado los accesos en la bitácora en las fechas seleccionadas. Además verificar que la información se haya registrado íntegramente.

3. Revisar en la bitácora que todos los campos del registro de visitantes al centro de cómputo estén llenos.

3.2 DESARROLLO Y MANTENIMIENTO DE APLICACIONES

El desarrollo y mantenimiento de las aplicaciones debe contar con un procedimiento formal y claro, donde se detalle todos los pasos a seguir. Dicho procedimiento debe establecer el tipo de cambio solicitado, niveles de aprobación, prioridad del cambio, responsables, entre otros aspectos que considere la Gerencia como primordiales.

Todo cambio debe ser identificado y aprobado previo el desarrollo. Se deben de realizar pruebas con los usuarios y al final debe aprobar y aceptar el cambio solicitado para realizar el pase a producción correspondiente.

La revisión del desarrollo y mantenimiento de las aplicaciones incluye las bases de datos sobre la cual se almacena la información. La compañía debe contar con un

procedimiento que permita conocer como se realizan los cambios en los datos, este procedimiento debe contar un "dueño de la información" que acepte el cambio a realizar previo su ejecución en producción.

Objetivo:

Los cambios solicitados a las aplicaciones de la compañía quedan implantados oportunamente, además de quedar documentados y autorizados conforme las políticas y procedimientos establecidos lo indican.

Requerimiento

Solicitar la siguiente información al área de Sistemas o TI:

- Políticas y procedimiento para mantenimiento y desarrollo de aplicaciones.
- Políticas y procedimientos para adquisición de aplicaciones.
- Listado de desarrolladores y/o consultores.
- Inventario de aplicaciones indicando dueños de la información o responsables de datos.
- Formulario de solicitud de cambios en las aplicaciones (desarrollo interno y software adquirido si aplica).

- Carpetas con todas las solicitudes de cambios en las aplicaciones.

Procedimiento para probar D&I

1. Entrevistar al Gerente de Sistemas o Jefe de Desarrollo sobre el procedimiento de cambios en las aplicaciones desde la solicitud hasta el pase a producción. Corroborar mediante revisión de documentos el diseño de este control con ayuda de las políticas y procedimientos aplicables. Si no existen políticas formales, relevar el procedimiento usado normalmente.

2. Pedir la última solicitud de cambio en aplicaciones finalizada y verificar que cuente con todas las aprobaciones del proceso relevado, usuario autorizado, Jefe Funcional de Sistemas previo al paso a producción.

3. Solicitar la documentación que debe acompañar al requerimiento de cambio; esto debe hacerlo en base al conocimiento recabado en la comprensión del proceso de cambio, dependiendo del requerimiento puede incluir el análisis de riesgos, plan de regresión, plan de pruebas, pase a producción, entre otros.

4. Para aplicaciones adquiridas, solicitar los documentos necesarios utilizados para dar seguimiento al trabajo de implementación del proveedor.

5. Segregación de funciones: verificar la segregación de funciones en cuanto a la aprobación de solicitudes y el pase a producción.

Procedimiento para probar EO

1. En base a la frecuencia identificada, seleccionar una muestra de tamaño apropiado de las solicitudes de cambios en las aplicaciones y verificar que todos los requisitos necesarios para su atención estén registrados (incluyendo los documentos adicionales: planes de pruebas, pases a producción, entre otros).

2. Utilizando los pases a producción seleccionados anteriormente, verificar que el personal apropiado haya trasladado los programas modificados al ambiente de producción. Verifique que existan las autorizaciones respectivas para el pase a producción.

3. Para el caso de aplicaciones adquiridas, solicitar la documentación soporte de seguimiento de solicitudes de cambios, pruebas de las actualizaciones enviadas (debidamente aprobadas) y pases a producción.

Objetivo:

Los cambios realizados a las aplicaciones quedan implantados de acuerdo con las intenciones del usuario que solicitó dicho cambio además de realizar las pruebas correspondientes.

Requerimiento de Información

Solicitar la siguiente información al área de Sistemas o TI:

- Políticas y procedimiento para realizar pruebas a las aplicaciones.
- Carpetas con todas las solicitudes de cambios en las aplicaciones.

Procedimiento para probar D&I

1. Entrevistar al Gerente de Sistemas o Jefe de Desarrollo sobre el procedimiento de pruebas a realizar para la modificación realizada en el aplicativo previo su pase a producción. Corroborar mediante revisión de documentos el diseño de este control con ayuda de las políticas y procedimientos aplicables a este punto. Si no existen políticas, relevar el procedimiento utilizado.

2. Solicitar el último documento de cambio realizado en las aplicaciones y que se encuentre finalizado, validar que todas las pruebas indicadas hayan sido realizadas y se encuentren documentadas, esto incluye: revisiones, aprobaciones, entre otros.

Procedimiento para probar EO

1. Obtenga una muestra de solicitudes de cambio en aplicaciones en base a la frecuencia identificada y verifique que todas las pruebas se hayan realizado en base a los procedimientos y políticas. Algunos tipos de pruebas pueden ser los siguientes:

   a. Pruebas de integración.
   b. Pruebas de aceptación del usuario.

Objetivo:

Las modificaciones a la estructura de información de la base de datos o cualquier cambio efectuado directamente a los datos quedan implantadas oportunamente de acuerdo a las políticas y procedimientos establecidos.

Requerimiento de Información

Solicitar la siguiente información al área de Sistemas o TI:

- Procedimientos para cambios a datos (directo a través de programación SQL) en la base de datos.

- Procedimientos para realizar cambios a la estructura de la base de datos; agregar tablas, campos, entre otros.

- Registro de todos los cambios realizados a los datos y/o estructura de la base de datos.

- Pruebas efectuadas antes del pase a producción de las nuevas tablas o campos en la estructura de la base de datos de producción.

- Usuarios de la base de datos con privilegios especiales (súper usuarios).

Procedimiento para probar D&I

1. Solicitar los procedimientos aplicados cuando ocurren situaciones que ameriten correcciones de datos a través de sentencias SQL (Directo a la base de Datos de Producción), en caso de no tener políticas y procedimientos sobre este tema, entrevistar al Jefe/Gerente de Sistemas e indagar cuales son los procedimientos aplicables en estas situaciones. Se debe corroborar que el procedimiento establecido (Escrito/No Escrito), prevea las revisiones de cambios por parte de un ente independiente (Auditoría Interna, Contraloría, Seguridades, Riesgos, etc), con el fin de asegurar que los cambios efectuados cumplen con las intenciones de la gerencia. Adicionalmente se debe corroborar que la autorización para efectuar este tipo de procedimientos sea otorgada por los dueños de la información o dueños del proceso afectado.

2. Solicitar un ejemplo de cambio a datos con la documentación soporte (Mails aprobatorios, pruebas, revisiones, etc.), con el fin de corroborar que los procedimientos indicados en el punto anterior se cumplen.

3. Para los cambios en la estructura de la base de datos solicitar los procedimientos aplicados, en caso de no tener políticas y procedimientos sobre este tema, entrevistar al Jefe/Gerente de Sistemas e indagar cuales son los procedimientos aplicables en estas situaciones. Se debe corroborar que el procedimiento establecido (Escrito/No Escrito), prevean las pruebas previo el pase a producción de las nuevas tablas, con el fin de asegurar que la nueva tabla generada cumpla con las intenciones de la gerencia. Adicionalmente se debe corroborar el flujo de aprobaciones correspondiente previo el cambio y el pase a producción.

4. Solicitar un ejemplo de cambio que afecte la estructura de la base de datos con la documentación soporte (Mails aprobatorios, pruebas, revisiones, etc.), con el fin de corroborar que los procedimientos indicados en el punto anterior se cumplen.

5. Solicitar los usuarios con privilegios especiales que pueden acceder a la base de datos (Administradores), así como indagar el custodio de los usuarios administradores definidos por default como el sa, corroborar que se encuentran asignados a personal autorizado.

Procedimiento para probar EO

Solicitar el registro de todos los cambios a datos efectuados durante nuestro periodo de revisión, seleccionar una muestra de acuerdo al número de cambios de estructura y solicitar la documentación soporte definida en los procedimientos establecidos para toda la muestra seleccionada.

Objetivo:

Los cambios o modificaciones en la topología de red o comunicaciones son implementados de manera oportuna y siguiendo las políticas y procedimientos establecidos.

Requerimiento de Información

Solicitar la siguiente información al área de Sistemas o TI:

- Políticas y procedimientos aplicables cuando existen ampliaciones al segmento de red.

- Solicitar los cambios a la estructura de red y ampliaciones en segmentos de red efectuados.

- Informe de Pruebas de Operatividad de nuevos Enlaces.

- Software de Monitoreo de Redes.

- Contrato de Comunicaciones

Procedimiento para probar D&I

1. Revisar las políticas y procedimientos aplicables cuando se efectúan ampliaciones a la red, en caso de no existir, indagar a través de entrevista con el Jefe/Gerente de Sistemas o Administrador de Red los procedimientos implementados.

2. Solicitar un ejemplo de una ampliación efectuada en nuestro período de revisión, corroborar que las solicitudes de las ampliaciones o cambios a la red son autorizados por la gerencia y verificar el informe de pruebas de nuevos enlaces, validar que dicha ampliación cuente con las autorizaciones correspondientes.

3. Indagar el software implementado para el monitoreo de enlaces activos en la red, identificar el personal responsable del monitoreo y medidas a tomar en caso de excepciones.

4. Relevar la existencia de Acuerdos de Niveles de Servicio, documentación de cumplimiento y sanciones. En caso de que la compañía cuente con Acuerdos de Niveles de Servicio, corroborar que se cumplen con los niveles contratados.

Procedimiento para probar EO

Solicitar un registro de todas las ampliaciones y nuevos enlaces implementados en nuestro período de revisión, de acuerdo a la información obtenida seleccionar una muestra representativa de la población para corroborar que el control ha operado correctamente e lo largo de todo el período bajo revisión.

Objetivo:

Las actualizaciones o modificaciones al sistema operativo quedan implantadas de manera oportuna.

Requerimiento de Información

Solicitar la siguiente información al área de Sistemas o TI:

- Procedimientos para actualizar nuevas versiones o parches de los sistemas operativos, ya sean estos automáticos o manuales. En caso de no existir procedimientos por escrito indagar los procedimientos aplicados con el Jefe/Gerente de Sistemas.

- Lista de cambios de versiones y parches instalados en nuestro período de revisión.

Procedimiento para probar D&I

1. Corroborar que los procedimientos de actualización garantizan la implantación oportuna de las nuevas versiones o parches al sistema operativo.

2. Solicitar un ejemplo de informes de pruebas para un cambio de versión efectuado al sistema operativo, corroborar las pruebas que se realizaron antes de los pases a producción.

3. En caso de que la compañía cuente con contratos para brindar soporte al sistema operativo, solicitar los contratos y corroborar el proceso para actualización de nuevas versiones.

Procedimiento para probar EO

Solicitar un listado con todos los cambios de versiones de sistemas operativos efectuados en el período de revisión, de acuerdo a la frecuencia seleccionar una muestra representativa para las pruebas de eficacia operativa.

3.3 OPERACIONES

Las actividades que realiza el Centro de Cómputo, es decir, el área donde se encuentran los servidores y los operadores que realizan sus actividades de monitoreo,

ejecución de tareas por lote y dan soporte a los usuarios son claves dentro de las organizaciones.

Una de sus principales actividades está relacionada con realizar periódicamente copias de respaldo de información y copias de las parametrizaciones de los principales aplicativos con el fin que la compañía se pueda recuperar en caso de una catástrofe. Además dichas copias deben contar con las adecuadas medidas de seguridad para garantizar su funcionamiento y disponibilidad, es recomendable que los respaldos sean almacenados en un sitio externo. Las disposiciones para el resguardo de cada uno de los sistemas deben ser probadas periódicamente para garantizar que cumplen con los requerimientos de los planes de continuidad de los negocios.

Además se debe de contar con un área de Mesa de Ayuda que brinde soporte y solución a los requerimientos que se presenten. Esta área debe tener procedimientos definidos y todos los requerimientos deben ser seguidos hasta su culminación correcta. Las estrategias de IT deben ser un soporte a las estrategias de negocio con el objetivo de que éstas se cumplan.

Objetivo:

Todas las tareas automáticas programadas a ejecutar por lote o por línea son procesadas oportunamente y se dan seguimiento registrando las incidencias encontradas hasta su terminación.

Requerimiento de Información

Solicitar la siguiente información al Centro de Cómputo:

- Políticas de Operaciones del Centro de Cómputo
- Bitácoras de ejecución de tareas programadas
- Responsables de ejecutarlas

Procedimiento para probar D&I

1. Solicitar al Gerente de Sistemas y al Administrador de Bases de Datos (si hubiere) que nos explique el proceso de administración de tareas automáticas configuradas, los niveles de autorización requeridos para crear y modificar dichas tareas y la documentación utilizada para registrar el procesamiento diario y las excepciones.

2. Solicitar un ejemplo de una bitácora de operaciones utilizada y validar que se cumplen los controles.

3. Requerir el listado de las tareas automáticas configuradas en el sistema.

Procedimiento para probar EO

1. Configuración Tareas Automáticas

   Por ser un control automático, verificar la configuración de tareas automáticas en el sistema, así como administradores de las mismas.

2. Bitácora de Operaciones

   De acuerdo a la frecuencia del control, generalmente, las bitácoras de operaciones son administradas diariamente, solicitar muestras de bitácoras de operaciones realizadas durante todo el periodo esperado de confianza.

   Para revisiones a fecha intermedia, realizar el alcance a la fecha final ejecutando pruebas de conexión.

Objetivo:

Los respaldos de información son manejados conforme las leyes, reglamentos y políticas de la compañía para permitir su recuperación cuando sea necesario.

Requerimiento de Información

Solicitar al Gerente de TI las políticas y procedimientos relacionados con la administración de respaldos diarios y externos, bitácoras de control utilizadas, así como programación de pruebas para medios de respaldos (si hubiere) y los responsables respectivos.

Procedimiento para probar D&I

1. Requerir un ejemplo de una bitácora de control de respaldos diarios utilizada, respaldos externos y restauraciones (si aplica).

2. Revisar el etiquetado de una cinta existente en el centro de cómputo y cotejarlo con los procedimientos establecidos.

Procedimiento para probar EO

1. Respaldos Locales:

   - De acuerdo a la frecuencia del control, generalmente, las bitácoras de respaldos son administradas diariamente, solicitar muestras de bitácoras de control de respaldos locales realizadas durante todo el periodo esperado de confianza.

   - Así mismo, probar el etiquetado de las cintas que reposan en la caja fuerte del centro de cómputo con el fin de verificar que cumplan con el procedimiento establecido.

2. Respaldos Externos:

   - De acuerdo a la frecuencia del control, solicitar muestras de bitácoras de control y respaldos externos realizados durante todo el periodo esperado de confianza.

   - Visitar con el responsable de Operaciones el lugar donde se almacenan los respaldos externos, el día que corresponda de acuerdo a su procedimiento normal de entrega de respaldos externos.

   - Verificar que la compañía cumpla con el procedimiento.

- Solicitar al sitio la bitácora de visitas realizadas y corroborar que se haya realizado las visitas de acuerdo a su procedimiento establecido.

3. Restauraciones (Si aplica):

- De acuerdo a la frecuencia del control, generalmente, las pruebas de restauraciones son realizadas mensualmente, solicitar muestras de bitácoras de restauraciones realizadas durante todo el periodo esperado de confianza.

  Así mismo, realizar una restauración respectiva.

- Para revisiones a fecha intermedia, realizar el alcance a la fecha final ejecutando pruebas de conexión.

Objetivo:

Se ha definido un plan estratégico de Tecnologías de Información.

Procedimiento para probar D&I

La compañía realiza un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo. Los planes a largo plazo deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo. Se debe entrevistar al siguiente grupo de personas, dependerá de la estructura organizacional de la compañía para que aplique o no algún cargo:

- Director General.
- Director de Operaciones.
- Director de Finanzas.
- Director de TI.

Se deberá solicitar la siguiente información:

- Políticas y procedimientos inherentes al proceso de planeación.
- Roles y responsabilidades del equipo de Dirección.
- Objetivos de la Organización a largo y corto plazo.
- Objetivos de TI a largo y corto plazo.
- Reportes y minutas de seguimiento de las reuniones del comité de Planeación/Dirección.

Procedimiento para probar EO

Se debe validar que se tenga evidencia de las reuniones en donde el comité de Planeación/Dirección tome decisiones y se documente respecto a los planes operacionales que afecten a la Compañía.

Objetivo:

Se tiene definida una arquitectura de información.

Procedimiento para probar D&I

1. Indagar con el Gerente de Sistemas si la compañía cuenta con personas que participan como "dueños de información" en los aplicativos, los mismos que podrían realizar autorizaciones para pases a producción, cambios en los datos, asignación de permisos, entre otros. Solicitar políticas o procedimientos donde se asigna a una persona como "dueño de información" y se indique las responsabilidades que adquiere.

2. Solicitar al Gerente de Sistemas la lista de dueños de información y validar que el personal se encuentren al tanto de sus funciones y sea personal autorizado.

Procedimiento para probar EO

Seleccionar una muestra para validar las actas donde se indica que una persona adquiere y conoce la responsabilidad de ser "dueño de información" de un módulo específico.

Objetivo:

Se ha establecido una compresión común del nivel de servicio requerido.

Procedimiento para probar D&I

1. Indagar con el Gerente de Sistemas si la compañía dispone de acuerdos de servicios con los usuarios, solicitar la última actualización de dichos acuerdos y el procedimiento a seguir para realizar algún cambio a los mismos. En caso que no se encuentren documentados, indagar la forma en la que se realiza y valida que los servicios se estén cumpliendo.

2. Validar que en alguna política o procedimiento se identifique lo siguiente:

   - Un proceso de acuerdo de nivel de servicio.

   - Se requiera participación en el proceso por parte del usuario para la creación y modificación de acuerdos.

   - Se encuentren definidas las responsabilidades de usuarios y proveedores.

   - La administración monitorea y emite reportes sobre el logro de los criterios de desempeño de servicio especificados y sobre todos los problemas encontrados.

3. Corroborar que exista un proceso de revisión regular por parte de la administración a los acuerdos de servicios establecidos.

4. Validar que el acuerdo cuente con algunos de los siguientes puntos:

   - Definición de servicio.

- Costo del servicio.

- Nivel de servicio mínimo cuantificable.

- Nivel de soporte por parte de la función de servicios de información.

- Disponibilidad, confiabilidad y capacidad de crecimiento.

- Plan de continuidad.

- Requerimientos de seguridad.

- Procedimientos de cambio para cualquier parte del acuerdo.

- Acuerdo por escrito y formalmente aprobado entre el proveedor y el usuario del servicio.

- Revisión/renovación/no renovación del período efectivo y del nuevo período.

- Contenido y frecuencia del reporte de desempeño y pago de servicios.

- Cargos son realistas comparados contra la historia, la industria y las buenas prácticas.

- Cálculo de cargos.

- Compromiso de mejoras al servicio.

Procedimiento para probar EO

Si se están realizando pruebas y actualizaciones a los acuerdos, solicitar al Gerente de Sistemas evidencia de que este procedimiento se esté realizando, se puede receptar actas de reuniones con las firmas y las observaciones que se han encontrado.

Indagar con el personal si los acuerdos de servicio se están cumpliendo conforme se indica en el documento.

Objetivo:

Se asegura que los problemas son resueltos y que las causas sean investigadas para prevenir cualquier recurrencia.

Procedimiento para probar D&I

1. Solicitar los procedimientos a seguir para dar solución a problemas reportados al área de Mesa de Ayuda.

2. Indagar con el Gerente de Sistemas si la compañía cuenta con un sistema de administración de problemas que registre y dé seguimiento a todos los incidentes.

3. Dicho sistema debe considerar:

- Suficientes pistas de auditoría de problemas y soluciones.
- Resolución oportuna de problemas reportados.
- Procedimientos de escalamiento.
- Reportes de incidentes.
- Acceso a la información de la configuración.
- Responsabilidades de los proveedores.
- Coordinación con administración de cambios.

4. Solicitar el último problema reportado al área de Mesa de Ayuda con el fin de corroborar que los procedimientos proporcionados se cumplan

Procedimiento para probar EO

Solicitar una cantidad de muestras en base a la frecuencia con la que se presentan los requerimientos y con cada una indagar que los procedimientos establecidos se cumplan.

Objetivo:

Se asegura que los roles y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos.

Procedimiento para probar D&I

Solicitar al Gerente de Sistemas las funciones y responsabilidad del personal del departamento. Corroborar que el documento con las funciones se encuentre actualizado, solicitar el procedimiento a seguir para cambios o asignaciones de nuevas funciones al personal. En caso de no tener políticas y procedimientos sobre este tema, entrevistar al jefe/gerente de sistemas e indagar cuales son los procedimientos aplicables en estas situaciones. Se debe corroborar que el procedimiento establecido (Escrito/No Escrito), prevean las autorizaciones correspondientes previa la asignación de nuevas funciones.

Procedimiento para probar EO

Según la frecuencia solicitar la cantidad de muestras de actas de reuniones donde se hayan efectuado cambios en las funciones a los empleados, validar que se cumpla con el procedimiento explicado previamente.

3.4 PLAN DE CONTINUIDAD DEL NEGOCIO

Es conveniente que la compañía implemente un plan de continuidad de los negocios con el fin de poder responder a interrupciones ocasionadas por desastres naturales y/o fallas en la seguridad. El plan de continuidad debe abarcar la Planeación para Recuperación de Desastres y la Planeación para el Restablecimiento del Negocio. El plan de recuperación de desastres es la capacitad de poder responder a la interrupción de los servicios identificando los procesos críticos y responder en el menor tiempo posible, para así poder iniciar las principales actividades del negocio.

La norma recomienda que dichos planes se deban mantener en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión. La administración de la continuidad de los negocios debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

Objetivo:

Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos de los negocios de los efectos de fallas significativas o desastres.

Procedimiento para probar D&I

Solicitar al Gerente de Sistemas el plan de continuidad del negocio en caso de no tenerlo solicitar un plan de contingencia o plan de recuperación de desastres.

La norma ISO 27001 recomienda que el plan de continuidad deba contemplar cómo mínimo los siguientes aspectos:

a) Comprensión de los riesgos que enfrenta la organización en términos de probabilidad de ocurrencia e impacto, incluyendo la identificación y priorización de los procesos críticos de los negocios;

b) Comprensión del impacto que una interrupción puede tener en los negocios (es importante que se tenga soluciones para los incidentes menos significativos, así como para los incidentes graves que podrían amenazar la viabilidad de la

organización) y definición de los objetivos comerciales de las herramientas de procesamiento de información;

c) Es conveniente que considere la contratación de seguros que podrían formar parte del proceso de continuidad del negocio;

d) Elaboración y documentación de una estrategia de continuidad de los negocios consecuente con los objetivos y prioridades de los negocios acordados;

e) Elaboración y documentación de planes de continuidad del negocio de conformidad con la estrategia de continuidad acordada;

f) Pruebas y actualización periódicas de los planes y procesos implementados.

Para el plan de continuidad, contingencia o recuperación de desastres se debe tener la aprobación de la Administración, además de tener evidencia que se estén actualizando y realizando simulacros periódicos. Se deben utilizar diversas técnicas para garantizar que los planes funcionarán en la vida real. Entre las pruebas que la Norma ISO 27001 recomienda incluir se encuentran:

a) Pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación del negocio utilizando ejemplo de interrupciones);

b) Simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis);

c) Pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia);

d) Pruebas de recuperación en un sitio alternativo (ejecutando procesos de negocio en paralelo, con operaciones de recuperación fuera del sitio principal);

e) Pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con el compromiso contraído);

f) Ensayos completos (probando que la organización, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones).

Procedimiento para probar EO

Solicitar al Gerente de Sistemas la documentación de la última prueba o simulacro ejecutado para verificar que los procedimientos de contingencia funciones y permitan identificar posibles variaciones en los escenarios que no permitan recuperar en su totalidad las aplicaciones más críticas de la compañía.

4 REVISIÓN DE SISTEMAS DE APLICACIÓN

4.1 RELEVAMIENTO DE LOS PROCESOS DE NEGOCIO Y APLICATIVOS RESPECTIVOS

Una parte integral de la revisión de los sistemas de aplicación es comprender el ámbito de los Sistemas de Información de la organización lo suficiente como para que el auditor pueda determinar la envergadura y complejidad de los sistemas, y el grado en que la organización depende de los Sistemas de Información. El auditor debe comprender la misión de la organización y los objetivos del negocio, el nivel y la manera en que se utiliza la tecnología de información y los sistemas de información para respaldar a la empresa, y los riesgos asociados con los objetivos de la organización y sus Sistemas de Información.

Asimismo, debe haber un entendimiento de la estructura organizacional que incluyen los roles y responsabilidades del personal clave de Sistemas de Información, procesos de negocio (secuencia de actividades desarrolladas por una organización para procesar o tramitar transacciones que permiten la ejecución de una función propia del negocio) y propietarios de los procesos de negocios cubiertos en el sistema de aplicación.

Proceso Contable

Debemos obtener una comprensión del proceso contable, incluyendo evaluar el diseño de los controles y determinar si se han implementado para permitirnos identificar y evaluar los riesgos de error material en los estados financieros y para desarrollar un plan de auditoría apropiado.

Nuestra comprensión del proceso contable debe incluir los procesos de negocios en los cuales se procesan las clases de transacciones que son significativas para los estados financieros, incluyendo la identificación de lo siguiente para cada proceso:

- Flujo de las transacciones involucradas desde el inicio de una transacción hasta su inclusión en los estados financieros.

- Actividades principales de negocios.

- Clases de transacciones significativas que se procesan sistemáticamente y las que no.

- La manera en que los sistemas de información capturan los hechos y condiciones, distintos a las clases de transacciones, que son significativos para los estados financieros.

- Políticas y procedimientos establecidos para mantener una segregación de funciones.

- Las actividades de control dentro de los procesos de negocios, en los cuales se procesan las clases de transacciones que son significativas para los estados financieros, suficientes para identificar y evaluar los riesgos de error material y para diseñar procedimientos de auditoría adicionales que sirvan como respuesta al riesgo evaluado.

- Los controles generales de la computadora dentro de los ambientes de procesamiento de la computadora suficientes para identificar y evaluar los riesgos de error material en los estados financieros y para diseñar y realizar procedimientos de auditoría adicionales que sirvan como respuesta al riesgo evaluado.

- Nuestra comprensión de la manera en que la entidad ha respondido a los riesgos procedentes de la tecnología de información, incluyendo la consideración de si la entidad ha respondido adecuadamente a los riesgos que surgen de la tecnología de información al establecer los controles generales de la computadora y los controles de aplicación eficaces.

- Las actividades de control dentro del proceso de informes financieros suficientes para identificar y evaluar los riesgos de error material en los estados financieros y para diseñar y realizar procedimientos de auditoría adicionales que sirvan como respuesta al riesgo evaluado.

- Nuestra comprensión de la manera en que la entidad comunica las funciones y las responsabilidades de información financiera, así como los asuntos significativos relacionados con la información financiera.

- El proceso, incluyendo las actividades de control clave, sobre el registro y procesamiento de asientos de diario.

- Nuestra compresión del proceso de la entidad para determinar mediciones y revelaciones a valor razonable y de las actividades de control suficientes y relevantes para identificar y evaluar los riesgos de error material para diseñar y realizar procedimientos de auditoría adicionales.

Procesos de Negocio

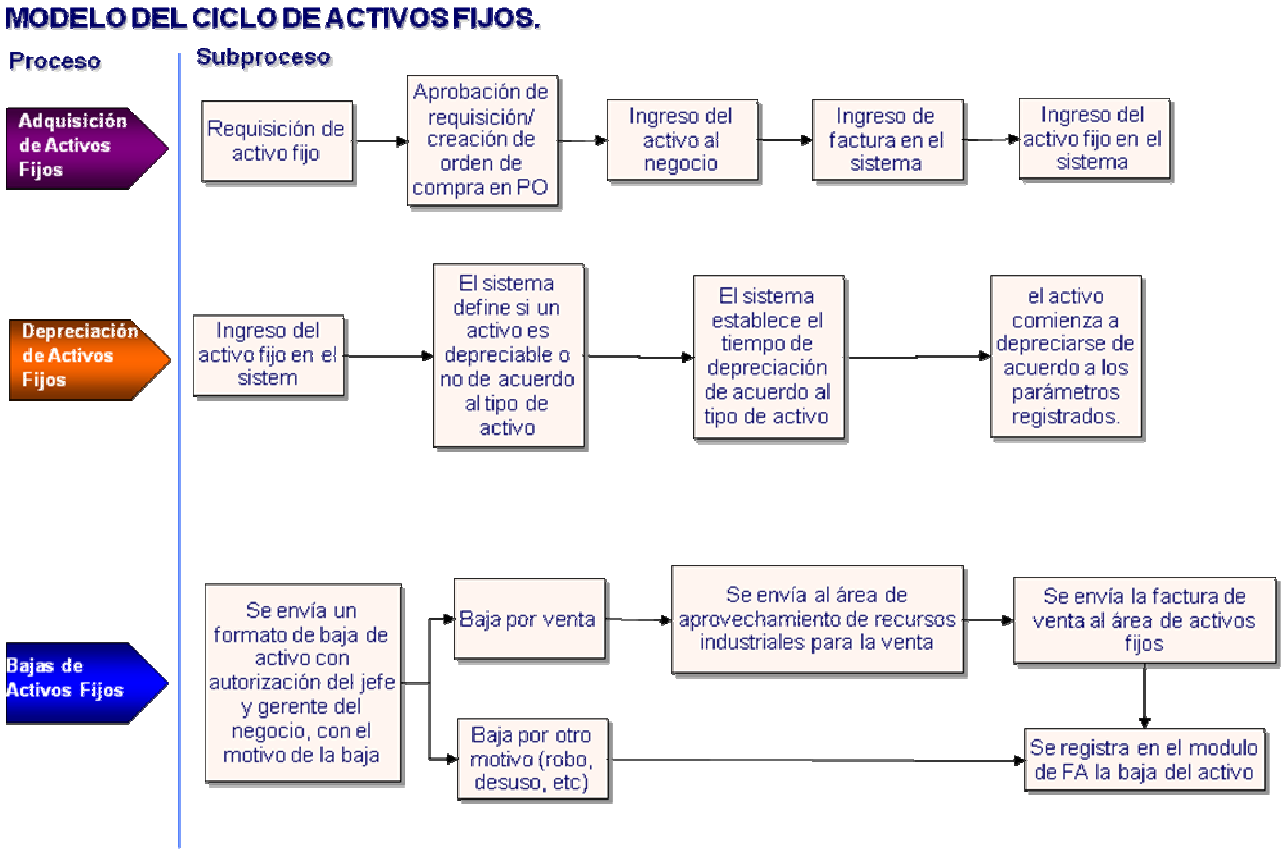
- Debemos comprender el flujo de las transacciones (proceso) involucrado desde el inicio de la transacción hasta su incorporación en los estados financieros.

- De igual forma, debemos tener un conocimiento global de los Procesos de negocio:

  - Financiero contable.
  - Gastos.
  - Activos fijos.
  - Nómina.
  - Ingresos.
  - Tesorería.

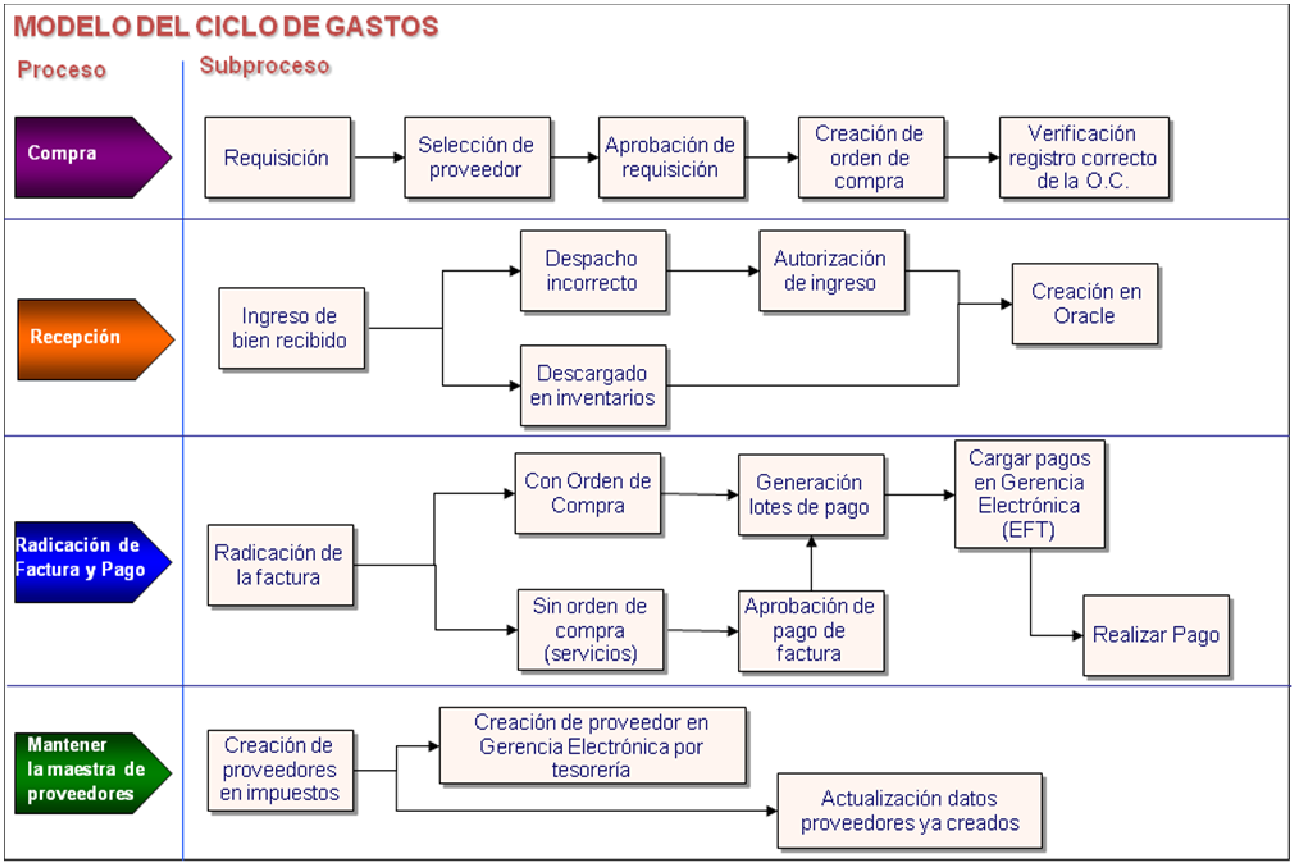
Se detallan dos Procesos de Negocios modelo:

GRÁFICO N° 12



Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

GRÁFICO N° 13



Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

Revisión de Aplicaciones

Las fases a revisar dentro de la revisión de una aplicación las dividiremos en:

- Usuarios y perfiles de aplicaciones
- Controles de entrada, procesamiento y salida de información
- Licencias y derechos de uso
- Modificación de Aplicaciones y Base de Datos
- Funcionalidad de la Aplicación

A continuación detallamos las actividades a realizar en cada fase.

4.2 USUARIOS Y PERFILES EN LA APLICACIÓN

Los usuarios de las aplicaciones deben cumplir con las siguientes características:

- Deben conocer las normas de uso de los aplicativos.

- Los usuarios deben tener un mecanismo de autentificación para el ingreso a los aplicativos; Así mismo, deben tener un perfil o rol asignado el cual le permitirá el ingreso a las opciones del aplicativo acorde a la función desempeñada dentro de la compañía.

- Los nombres y ubicación de todos los usuarios deben ser identificables.

- Los equipos y aplicativos utilizados por los usuarios deben ser claramente identificados.

- Se deben verificar las violaciones a las normas de uso.

- Las aplicaciones no-laborales o no-útiles (Chat, Messenger, Radio, Adultos, mp3, etc.) deben ser de uso restringido de acuerdo a las políticas y procedimientos de las empresas.

Objetivo de la revisión

Asegurar que los usuarios y perfiles de los aplicativos estén acorde a las funciones desempeñadas de los empleados propietarios.

Alcance de la revisión

- Políticas y Procedimientos de relacionados con Control de Accesos.
- Configuración usuarios y perfiles.
- Listado de usuarios y perfiles por cada sistema de aplicación.

Objetivos y Actividades de Control Asociados

CUADRO N° 1

Objetivo de Control	Actividad de Control	Revisión
Aplican todos los objetivos de control de cada ciclo de negocio relacionados con controles de accesos.	Sólo personal autorizado posee acceso en el aplicativo a la opción especificada.	Solicitar la lista del personal activo al área de Recursos Humanos y compararla con la lista de usuarios de la aplicación. Solicitar la lista de personal activo de la compañía y cruzarlo versus los usuarios de l. Solicitar al área de Sistemas, el listado del personal que posea el acceso en el aplicativo para la función seleccionada. Verificar que los perfiles de dicho personal son apropiados en relación a la función desempeñada dentro de la compañía.

Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

4.3 CONTROLES DE ENTRADA, PROCESAMIENTO Y SALIDA DE INFORMACIÓN

El objetivo de la revisión es analizar y evaluar la eficacia de los controles de los sistemas o aplicaciones ya existentes, estos controles deben asegurar que sólo se ingresan y actualizan datos completos, exactos y válidos en un sistema, que el procesamiento de estos datos es correcto, que los resultados del procesamiento cumplen las expectativas; y que los datos se mantienen seguros. Quienes diseñan los

sistemas ubican controles en el ingreso de datos o input, en el procesamiento y en el output del sistema.

1. Procedimientos de control de input. controles de acceso: Con esto se asegura que los datos ingresados al sistema son los autorizados y las responsabilidades sobre el cambio de datos se encuentra definida.

   - Control de secuencia: Los registros de las transacciones llevan un número que los identifica y son consecutivos, por lo que no pueden haber duplicidades ni intervalos vacíos de secuencia.

   - Control de límite: Se verifican los límites de valores que puede asumir una variable de entrada y que se rechazará o advertirá en caso no cumpla con los límites establecidos.

   - Control de Rango: Es similar al anterior, pero se trata de un par de límites.

   - Control de paridad: Se utiliza para verificar una transmisión de datos (que puede ser la fuente para el ingreso de datos a otro sistema).

   - Control de validez: Consiste en considerar como válidos aquellos campos codificados con valores predeterminados.

   - Control de razonabilidad: Los datos ingresados se comparan con límites de razonabilidad o de ocurrencia de datos.

- Búsquedas en tablas: Se valida un campo con el contenido de una tabla de datos, por ejemplo una tabla de códigos de países y los nombres de países se utiliza para validar el campo país de una pantalla de ingreso de datos.

- Control de existencia: Es un control que sirve para validar un dato que ingresa al sistema y además asegura que el proceso sea según un orden establecido, por ejemplo: la autorización electrónica de una orden de trabajo, exige primero que esta haya sido ingresada y luego sea marcada por otra persona como autorizada.

- Verificación de ingreso por teclado: Consiste en redigitar el ingreso de datos por otra persona sobre el archivo digitado primero por otra persona.

- Dígito de control: Consiste en agregar al dato ingresado un dígito, el que se calcula matemáticamente por un algoritmo sobre los dígitos del dato ingresado, los más comunes son el módulo 10 o módulo 11.

- Control de integridad: consiste en que un campo siempre debe contener datos, no puede estar vacío, etc.

2. Procedimientos de control de procesos

- Recálculos manuales: Consiste en recalcular manualmente una muestra de las transacciones a fin de asegurar que el procesamiento está realizando la tarea esperada.

- Edición: Consiste en comprobar que el input de datos es correcto, aquí se interpreta el paso de input como parte del proceso.

- Verificación de razonabilidad de cifras calculadas: Consiste en probar la razonabilidad de los resultados de las transacciones para asegurarse de la adecuación a criterios predeterminados.

- Verificación de la cantidad de registros procesados.

- Manejo de archivo de errores para su posterior investigación.

- Verificación por rangos de fechas o períodos.

- Aprobación electrónica: Para que un determinado registro pase de un estado a otro por la autorización de un usuario diferente al que generó el registro.

- Archivos de seguimiento: que permiten identificar el status de una determinada operación en un momento determinado.

3. Procedimientos de Output o salida

- Resguardo de formularios negociables, sensibles o críticos: deben ser adecuadamente controlados en un listado de formularios recibidos, utilizados y dando razón de las excepciones, rechazos y mutilaciones para protegerlos de robo o daño.

- Autorización de distribución: Las opciones de reporte del sistema deben estar de acuerdo con las funciones que tiene el usuario en el sistema y ser controlado por los accesos definidos en el sistema.

- Estructura estándar de los formatos de los reportes: como son el número de páginas, la hora, fecha, nombre del programa que lo produce, cabeceras, etc.

4.4 LICENCIAS Y DERECHOS DE USO

Una licencia de software es una especie de contrato, en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado programa, principalmente se estipulan los alcances de uso, instalación, reproducción y copia de estos productos.

El tema de las licencias de software puede ser muy complejo. El negocio del software se basa en licencias binarias. La propiedad intelectual de los distribuidores de software comercial nace del código fuente. Las licencias de software se crean con diversos fines empresariales y para afrontar diversos tipos de relaciones (como distribuidor/cliente y partner/partner). Los desarrolladores de software tanto comercial como no comercial utilizan decenas de licencias que abarcan una gran variedad de términos y condiciones.

Los costos en las empresas representan un tema crítico. Con la irrupción de las computadoras han surgido costos y beneficios no existentes hasta hace algunas décadas atrás, convirtiéndose el manejo eficiente de la información en un factor clave para la obtención del éxito y para el desarrollo de ventajas comparativas sobre los competidores.

Dado este panorama, es común que las grandes empresas dispongan de sistemas que poseen altos costos de mantenimiento, actualización, capacitación, soporte, etc. que muchas veces superan el costo de obtención de la licencia. Por otra parte, han surgido cada vez con mayor fuerza programas de código libre amigables para el "usuario del hogar" que le permiten abaratar costos.

Conocer las ventajas, desventajas, derechos y deberes de las empresas y de los usuarios finales, además de todas las otras personas que se relacionan con el software, de las licencias de software más utilizadas, tanto el software libre como el software comercial. Es imprescindible para que las empresas y los usuarios finales puedan tomar las mejores decisiones acerca de los sistemas que utilizarán.

Es importante también conocer cómo afectan estas licencias al trabajo de otras personas, como por ejemplo a los desarrolladores, vendedores, distribuidores, etc., y conocer también sus derechos y deberes para las licencias que se expondrán en este trabajo.

Las licencias de uso de software generalmente se clasifican en:

- Licencia propietaria. Uso en una computadora por el pago de un precio.

- Shareware. Uso limitado en tiempo o capacidades, después pagar un precio.

- Freeware. Usar y copiar ilimitadamente, precio es cero.

- Software libre. Usar, copiar, estudiar, modificar, redistribuir. Código fuente incluido.

Es posible dividir las licencias de software libre en dos grandes familias. Una de ellas está compuesta por las licencias que no imponen condiciones especiales, sólo especifican que el software se puede redistribuir o modificar. Estas son las llamadas licencias permisivas.

La otra familia, denominadas licencias robustas o licencias copyleft, imponen condiciones en caso de que se quiera redistribuir el software, condiciones que van en la línea de forzar a que se sigan cumpliendo las condiciones de la licencia después de la primera redistribución.

Objetivo de la revisión

Asegurar que la empresa cuente con software licenciado en sus aplicativos respectivos

Alcance de la revisión

- Políticas y Procedimientos de relacionados con Licenciamiento de Software.
- Tipos de Licencias de Software.
- Derechos de Uso.
- Inventario de Software de la empresa.

Objetivos y Actividades de Control Asociados.

CUADRO N° 2

Objetivo de Control	Actividad de Control	Revisión
El software solamente se carga en los sistemas de cómputo de la entidad y/o se utiliza de conformidad con los contratos de licencia y la autorización de la gerencia.	El software que se carga en las computadoras de la entidad se compara periódicamente con un inventario del software otorgado en licencia. Si se encuentra algún software que no esté autorizado o que no se haya otorgado en licencia, se obtendrán las licencias o se retirará el software.	Procedimientos relacionados con Licenciamiento de Software. Revisión del Inventario de Software de la Empresa, con el fin de corroborar que todo el Software sea autorizado y legal.

Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

4.5 MODIFICACIÓN DE LA APLICACIÓN

La creación o modificación de un sistema es un proceso que consiste en dos etapas principales, de análisis y diseño de sistema; comienza cuando la gerencia, usuario o en algunas ocasiones el personal técnico, se da cuenta que un sistema necesita mejorar o surge la necesidad de un nuevo sistema. En esta fase se revisa la solicitud del servicio de sistemas. Esta solicitud provee la información indispensable para la revisión inicial del proyecto, su evaluación y la clasificación realizada por el personal técnico durante esta fase. Al revisar la solicitud, se debe verificar lo siguiente:

- Debe ser iniciada por un usuario o gerente.

- Debe enviarse una copia de la solicitud de sistema al comité técnico.

- Debe contener la firma de la comisión técnica evaluadora a nivel de recomendación.

- Debe contener la firma de aprobación del comité de sistema.

Estudio de Factibilidad

Esta fase brinda los antecedentes, el fundamento para identificar el esfuerzo necesario en el proyecto al definir la diferencia entre la situación actual y los objetivos del sistema propuesto. Aquí se hace un análisis económico preliminar y se brinda una recomendación. Los productos tangibles que se deben producirse en esta fase son:

- Estudio del proyecto.
- Recomendaciones.
- Proceder.
- Transferir (mantenimiento).
- Cancelar.
- Presentación Formal.

Al revisar estos productos, se deben evaluar que se estén cumpliendo con las siguientes políticas:

- El usuario debe asignar un representante.

- Al inicio de esta fase, el comité técnico designa un gerente líder del proyecto.

- Se debe clasificar el proyecto como mayor, mediano o menor, de acuerdo a su costo estimado de desarrollo.

- El gerente del proyecto debe preparar las recomendaciones y asegurarse que éstas son aprobadas por el usuario, en caso de proceder a transferir.

- Cuando la recomendación es transferir el proyecto, el gerente del mismo es responsable de enviar una copia del estudio del proyecto al jefe de TI y de obtener su aceptación por escrito.

- En caso de proceder, las recomendaciones deben ser firmadas el gerente del proyecto y usuario.

- Se debe enviar una copia de las recomendaciones al área de Proyectos como parte de un esfuerzo de coordinación centralizada.

- Solo para proyectos mayores, el gerente del proyecto envía una copia del estudio del proyecto para recibir su acuerdo.

Análisis Funcional

El análisis funcional identifica todas las funciones tanto manuales como automatizadas que el nuevo sistema debe realizar, no describe el sistema actual. La

participación activa día a día del usuario es esencial para asegurar el éxito. Al final de esta fase debe estar, tanto el usuario como el personal técnico, satisfecho de que las especificaciones funcionales provean toda la información necesaria para el análisis definitivo de costo / beneficio y para el diseño del sistema. A continuación se presenta los productos tangibles que debe proveer esta fase:

- Las especificaciones funcionales.
- El plan para la siguiente fase.
- La presentación a la gerencia (opcional).

Se debe cumplir las siguientes políticas:

- Cuando todas las especificaciones funcionales hayan sido completadas debe entonces seguirse el ciclo de aprobación que se especifica.

- Las especificaciones funcionales completas y el plan para la siguiente fase, deben ser enviadas en forma simultánea para su aprobación.

- Cuando estos hayan sido aprobados, los resultados de esta fase pueden ser revisados con el comité de sistemas mediante una presentación formal, la cual es una realidad funcional.

- La aprobación de las especificaciones funcionales y del plan para la siguiente fase constituyen la evidencia de que esta fase ha sido completada en forma satisfactoria.

Análisis y Selección del Diseño

El propósito de esta fase es el de recomendar una estrategia que debe ser factible desde el punto técnico y efectivo, desde el punto de vista de costo. La selección del diseño empieza con el enunciado detallado de los objetivos del proyecto, desarrollados bajo el análisis funcional. Esta fase provee los siguientes productos tangibles:

- Propuesta del diseño.
- Revisión del diseño.
- Requerimiento de recursos técnicos.
- Plan para la siguiente fase.
- Presentación a la gerencia.
- Propuesta de gastos mayores.

A continuación presentamos las siguientes políticas que se deben tomar en cuenta en esta fase:

- Para proyectos mayores, el acuerdo de Proyectos es requerido sobre los tres primeros productos tangibles y además, la propuesta de gastos mayores.

- Al final de esta fase es un requisito realizar una presentación a la gerencia y al comité de sistemas; esto es válido para todos los proyectos mayores y opcional para los medianos y menores.

- Si al culminar esta fase la gerencia aprueba el proyecto, se procede a la adquisición del hardware/software de acuerdo a las normas establecidas por el estado.

Diseño del Sistema

Esta fase se inicia con la alternativa recomendada en la selección del diseño y el desarrollo que termina siendo un diseño final del sistema. Esta se logra mediante la descripción del sistema propuesto con diagramas de flujo y narrativas, además de la producción de las especificaciones técnicas detalladas para cada uno de los programas, procedimientos, manuales, pruebas, conversión e instalación. En esta fase podemos mencionar cinco productos tangibles:

- El diseño del sistema.
- El plan piloto o plan de prueba del sistema.
- Presentación a la gerencia.
- Plan del proyecto.

Políticas que se deben tomar en cuenta:

- El diseño de un sistema usualmente es desarrollado por parte o secciones en lugar de hacerse como un todo. Cuando el sistema completo es diseñado, entonces el ciclo normal de aprobación debe cumplirse.

- El plan piloto, las estrategias de conversión y el plan del proyecto se entregan o envían simultáneamente, pero pudiesen ser entregados después que el diseño del sistema.

- Una presentación a la gerencia y/o comité de sistema es requerido para todos los proyectos al final de la fase.

- El diseño del sistema, plan piloto, estrategias de conversión y plan de proyecto aprobado constituyen la evidencia de que dicha fase ha sido completada satisfactoriamente.

Programación y Prueba

La planificación, análisis y diseño de las cinco fases previas se hacen efectivas, cobran vida, durante la fase de Programación y Prueba. En las pruebas del sistema como un todo y la aceptación por parte del usuario permiten al sistema ser calificado como apto para entrar en la etapa de paralelo.

Las metas de esta fase son calificar un sistema nuevo para entrar un paralelo, mediante su documentación con una prueba de aceptación y producir la documentación necesaria para el usuario y para el área de producción, de modo que ellos puedan asumir el control del nuevo sistema al momento del corte final o entrada a la operación en vivo.

Productos tangibles que deben contemplarse:

- Documentación de los programas.
- Manual de usuario.
- Manual de operación - producción.
- Documentación de la prueba de aceptación.
- Plan del paralelo.
- Presentación a la Gerencia.

Se debe cumplir las siguientes políticas:

- La documentación de los programas, el manual del usuario y el manual de operación y producción deben integrarse simultáneamente, antes de ejecutar una prueba de aceptación.

- Los estándares para el rendimiento de las pruebas definen tres niveles.

- Prueba individual de programas.

- Prueba del sistema global.

- Prueba de aceptación.

- Una presentación a la gerencia, al final de esta fase, es opcional.

- La aprobación de los productos tangibles que deben producirse durante esta fase representa la evidencia de que dicha fase ha sido completada satisfactoriamente.

Paralelo:

La instalación es la última fase de desarrollo del ciclo de vida de un proyecto mientras el sistema se encuentra en operación en paralelo, se realiza la conversión de los datos que serán utilizados por el nuevo sistema. Finalmente el nuevo sistema se traspasa de manera oficial al usuario y al centro de cómputo. Esta fase está estructurada de manera tal que permite la salida "en vivo" del nuevo sistema con el mínimo riesgo posible dentro del área o la organización, y ocasionando el menor contratiempo posible a la operación y producción que es responsabilidad del área de producción. Los productos tangibles que deben darse como resultado de esta fase son la documentación en paralelo y la aprobación del sistema.

Al revisar los siguientes productos se deben tomar en cuenta las siguientes políticas:

- La operación en paralelo no puede ser finalizada sin la aprobación por escrito del usuario y del director técnico.

- El usuario es responsable por la preparación de la documentación del paralelo y de la aprobación del sistema.

- El usuario envía una copia de la aprobación del sistema al comité técnico como parte del esfuerzo centralizado de coordinación del proyecto.

- Los productos tangibles de esta fase constituyen la evidencia de que la misma ha sido completada satisfactoriamente.

Implementación:

Esta fase cubre la vida útil del sistema. Esta etapa se inicia con un sistema completamente probado. El producto tangible son los indicadores de resultados que fueron identificados en la fase III, análisis funcional, serán utilizados para medir el rendimiento del sistema en su vida útil.

Las políticas son las siguientes:

- El jefe de TI es responsable de que se realice el mantenimiento y actualización de la documentación del sistema.

- El usuario es el responsable de la iniciativa de solicitud de modificaciones al sistema.

Evaluación

Esta fase se desarrolla periódicamente y durante la vida útil del sistema. Se debe evaluar periódicamente el nivel de cambios de emergencia, mantenimientos y modificaciones que se han realizado durante la operación del sistema. Los productos tangibles son los resultados y conclusiones de cada evaluación del sistema debe presentarse en el producto tangible, denominado "Evaluación Periódica del Sistema".

Las políticas que se deben observar son las siguientes:

- Es responsabilidad del Jefe de TI conjuntamente con auditoría y controles gerenciales, realizar estas evaluaciones

Nota:

Las fases indicadas, son implementadas en las organizaciones dependiendo del tamaño y complejidad de los aplicativos instaurados que soportan los ciclos de negocios respectivos.

Personal Involucrado en el desarrollo y mantenimiento de Aplicaciones

Gerente de desarrollo de aplicaciones

- Supervisa la programación, prueba, entrenamiento del usuario y documentación de los sistemas.

- Traduce propuestas de aplicación aprobadas a un diseño de sistemas, creando cronogramas de desarrollo detallados y estimando fechas de terminación y presupuestos.

- Establece cronogramas e informes de progreso para actividad de análisis y programación.

Líder de proyecto/Analista de sistemas

- Supervisa el diseño detallado de los programas de aplicación, proporciona asistencia técnica a los programadores.

- Crea cronogramas para los módulos de programación y monitorea su terminación, ayuda a los programadores en la prueba y depuración de los programas.

- Verifica y supervisa la corrección de los programas de producción según las solicitudes aprobadas de cambios de sistemas.

Programador de aplicaciones

- Efectúa la codificación de los programas y realiza la prueba primaria o inicial.

- Realiza descripciones formales de programas, funciones e interfases, incluyendo diagramas de flujo, descripciones de datos y procedimientos de recuperación.

- Mantiene un conocimiento actualizado de los lenguajes de programación.

Quality Assurance (QA)

La función de quality assurance (QA) es responsable de verificar el cumplimiento de las políticas y la metodología utilizada en los desarrollos y mantenimientos de aplicaciones. Esto implica:

- Verificar el cumplimiento de las diferentes pruebas (analista, programador, usuario).

- Verificar la aprobación del sector usuario.

- Asegurar el cumplimiento de los estándares de programación.

- Realizar el pase a producción de los desarrollos o verificar su puesta en producción.

Administrador de Bases de Datos

El administrador de la base de datos es responsable de los controles de integridad y seguridad de los datos. Son sus responsabilidades:

- Definir el contenido y estructura de la base de datos e informar a los programadores de software de base y de aplicaciones acerca de las técnicas eficientes de programación.

- Asegurarse que cada pieza de información (dato) resida en un único lugar y sea actualizado por todas las aplicaciones / usuarios necesarios.

- Mantener la documentación del sistema de base de datos actualizada y exacta.

- Evaluar con el gerente de programación de aplicaciones el impacto de las nuevas aplicaciones sobre la base de datos.

Segregación de Funciones para el Desarrollo de Aplicaciones

A continuación se detallan los accesos autorizados de acuerdo a la función desempeñada.

CUADRO N° 3

Usuarios Principales	Ambientes			
	Desarrollo	Prueba	QA	Producción
Analista Programador	✔	✔		
Quality Assurance			✔	✔
Operaciones		✔ (Optativo)	✔	✔
Usuarios Finales		✔	✔	✔

Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

Tipos de Acceso por Ambiente

X → Ejecución W → Escritura R → Lectura

CUADRO N° 4

Usuario	Editor	Compilador	Datos	Programas	Ambiente
Analista / Programador	X	X	W	W	Desarrollo
Usuario	---	---	---	---	
Analista / Programador	---	---	W	X	Prueba
Implementador	R	X	W	W	
Usuario	---	---	W	X	
Analista / Programador	---	---	R	R	Producción
Usuario	---	---	W	X	

Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

Revisión de Sistemas de Aplicación

La revisión de los sistemas de aplicación tiene como objetivo asegurar la disponibilidad, integridad performance y capacidad de las aplicaciones críticas.

La evaluación del desarrollo de un sistema no implica juzgar las técnicas de codificación utilizadas en el mismo. El objetivo central es asegurar que los resultados alcanzados hayan sido obtenidos de manera eficiente, eficaz de forma tal que estén acordes a las expectativas generadas y que la documentación creada a través del proceso represente el trabajo desarrollado y sea confiable. Los procesos y los procedimientos utilizados en el desarrollo son de vital importancia debido a que son la base de los controles y estructura que conduce a los resultados íntegros.

El desarrollo es una opción que proporciona el software necesario para resolver los requisitos funcionales y para diseñar criterios. Los sistemas comprados podrían ser utilizados para satisfacer parte o toda la necesidad. Se debe comparar la necesidad del usuario versus las ventajas que brinda el desarrollo y/o la compra del aplicativo como parte de consideraciones básicas del análisis.

En situaciones en donde se encuentren disponibles paquetes comerciales de software que requieren adaptaciones considerables para alcanzar el objetivo de la administración, la gerencia debe considerar el desarrollo interno como una alternativa para ahorrar costos y recursos.

Una vez que se decida acerca del desarrollo o compra del software, el próximo paso consistirá en decidir acerca del hardware y sistemas operativos requeridos para la implementación de la solución, no sólo para el soporte del producto final, sino adicionalmente para apoyar la ejecución de los ambientes del desarrollo y pruebas respectivamente. Los riesgos asociados al hardware y los sistemas operativos adquiridos, así como su compatibilidad con la infraestructura de la organización, deberán ser evaluados como parte de la revisión realizada.

Alcance de la revisión

- Organización y Conocimiento sobre Aplicaciones y Procesos.
- Administración de Recursos y Eventos.
- Caídas de Servicio.
- Metodología / Normas de prueba, conversión y Puesta en Producción.

- Quality Assurance.
- Planificación de crecimiento (escalabilidad).

Requerimientos de documentación

Metodología

- Selección.
- Implementación.
- Desarrollo/mantenimiento.
- Estándares de programación.

Requerimientos usuarios

Documentación aplicaciones

- Manual del Usuario.
- Documentación Técnica.

Pruebas de usuarios

Pases a producción

Quality assurance (QA)

Problemas potenciales

- Puesta en producción de desarrollos/ modificaciones de sistemas.
- Metodología de desarrollo/ mantenimiento de sistemas.
- Requerimientos de los sectores usuarios.
- Prueba de desarrollos/ modificaciones de sistemas.
- Documentación de los sistemas de aplicación.
- Dependencia de programadores externos.

Evaluación

Software documentador (funcional y de programas).

- Supervisión personal.
- Interno.
- Externo.

Participación usuarios.

Sistema control de proyectos.

Asignación costo.

Puesta en producción.

Sistema control de bibliotecas.

Software comparador de versiones.

Back-up versiones anteriores.

Ambiente separado.

Participación usuarios.

Satisfacción usuarios.

Objetivos y Actividades de Control Asociados

En el caso de implementaciones de nuevos aplicativos.

CUADRO N° 5

Objetivo de Control	Actividad de Control	Revisión
Los nuevos sistemas de aplicación se implantan de manera apropiada y funcionan de acuerdo con las intenciones de la gerencia.	Los nuevos sistemas de aplicación y las modificaciones a los sistemas de aplicación se prueban de conformidad con los planes de prueba que incluyen, según sea el caso, prueba de la unidad y sistema, prueba de la interface, prueba paralela, prueba de capacidad y prueba de aceptación de usuarios.	Este objetivo aplica *solo si* dentro de la comprensión del ambiente(s) identificamos que se han producido nuevos desarrollos dentro del periodo de revisión y se debe tomar en consideración los siguientes puntos: • Cumplimiento de metodología de desarrollo o adquisición • Completitud de entregables y documentación • Para el caso de software adquirido, tomar en cuenta cotizaciones, informes técnicos, contratos y SLAs. (Niveles de Servicio)
Cuando se implantan nuevos sistemas de aplicación, la información existente que se convierte al sistema nuevo es completa, exacta y válida.	La gerencia aprueba los resultados de la conversión de información (por ejemplo, actividades de conciliación y balance) de la estructura de información o sistema de aplicación obsoleto a la nueva estructura de información o sistema de aplicación y monitorea que la conversión se realice de conformidad con los procedimientos y políticas de conversión establecidos.	Considerar para la revisión las pruebas de los nuevos sistemas, documentación y aceptación por parte de los usuarios finales responsables.

Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

Para revisión de modificaciones a los aplicativos actuales:

CUADRO N° 6

Objetivo de Control	Actividad de Control	Revisión
Todas las modificaciones necesarias a los sistemas de aplicación existentes son implantadas oportunamente.	La gerencia aprueba e implanta las solicitudes del usuario y de otro tipo de modificaciones a los sistemas de aplicación, software y estructura de información incluyendo actualizaciones y ajustes puestos a la venta por los proveedores si son consecuentes con los planes de los sistemas de información y la gerencia.	Puntos de revisión: Procedimiento para el mantenimiento a las aplicación (solicitudes de cambios), autorizaciones, pruebas y pases a producción. Para el caso de software adquirido, determinar el procedimiento para dar seguimiento e implantación de cambios por parte del proveedor
Las modificaciones a los sistemas de aplicación existentes quedan implantadas de manera adecuada y los sistemas de aplicación modificados funcionan de acuerdo con las intenciones de la gerencia.		Este objetivo abarca la ejecución de pruebas de interfase, unidad, capacidad y de usuario para software desarrollado internamente y adquirido. Para algunas empresas se debe tomar en cuenta la inclusión de un plan de regresión.

Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

Nivel de Madurez

Basado en el esquema de Cobit se resume el nivel de madurez:

- Inicial
    - No se han definido procedimientos y políticas para la administración de aplicaciones críticas.
    - Las aplicaciones no son escalables y/o no cumplen con los SLAs.
    - No se han implementado herramientas de monitoreo.
    - No se han definido formalmente procedimientos de control de cambio.
- Definido
    - Se han creado y acordado los SLAs, y las medidas han sido establecidas.
    - Todas las caídas son planificadas.
    - Los responsables tienen los skills adecuados, y existen políticas y medidas establecidas.
- Optimizado
    - SLAs fueron implementadas en forma detallada.
    - Nuevas tecnologías son consideradas, para mejorar la administración de las aplicaciones.

- Se mejoran continuamente los procedimientos, políticas y se incorporan nuevas tecnologías para la administración de aplicaciones.

Soporte a la Base de Datos

Objetivo

- Diseñar, Implementar, monitorear y mantener los procedimientos necesarios para asegurar la integridad, performance y disponibilidad de los datos de la Organización.

Alcance

- Definición de modelos de datos que aseguren que los datos sean precisos, íntegros y unívocos.

- Actualización y modificación de los estándares.

- Configuración de la base de datos para asegurar adecuados tiempos de respuesta de procesos de actualización, almacenamiento y depuración.

- Roles de Operadores y Administradores de bases de datos (DBA).

Objetivos y Actividades de Control Asociados

CUADRO N° 7

Objetivo de Control	Actividad de Control	Revisión
IR07020 Todas las modificaciones necesarias a la estructura de información y los datos existentes quedan implantados oportunamente.	IR171 La gerencia aprueba las solicitudes del usuario y de otras personas de modificaciones a las estructuras de información incluyendo actualizaciones y ajustes emitidos por los proveedores y las implanta si son consecuentes con los planes de los sistemas de información y las intenciones de la gerencia.	Procedimientos de cambio en base de datos (datos y no estructura). Autorizaciones para dichos cambios. Pruebas (si es aplicable). Adicionalmente revisión de usuarios de base de datos con privilegios especiales.

Fuente: Investigación realizada
Elaborado por: Oswaldo Bravo Arellano

Nivel de madurez

Basado en el esquema de Cobit se resume el nivel de madurez:

- Inicial

    - No existe un plan integral de Data Management. Existen dudas sobre la integridad y/o consistencia de los datos de las diversas aplicaciones (“silos” de aplicaciones).

- No se encuentra asignada la función de Administración de Datos ni existe capacitación al respecto. Falta coordinación en las actividades de administración de bases de datos.

- No existen estándares ni herramientas de administración de datos que permitan, modelar los datos, diseñar repositorios, manejar la performance de las bases de datos.

- Definido

  - Existe documentación de datos que no está 100% integrada y/o actualizada.

  - Se han definido responsabilidades específicas (aunque son cumplidas por personal que no está suficientemente capacitado o certificado).

  - Existen estándares de datos y procesos operativos para Administración de Datos, pero no están totalmente automatizados.

- Optimizado

  - Existe un Diccionario de datos formalizado y actualizado.

  - Se han desarrollado estándares de datos, permitiendo optimizar la consistencia de la información, y definir correctamente los derechos de acceso.

- Se han definido los roles y son cubiertos por personal capacitado y con las habilidades necesarias.

- La performance es monitoreada en forma centralizada por una herramienta de administración, la cual permite solucionar errores en forma automatizada.

4.6 FUNCIONALIDAD DE LA APLICACIÓN

Al realizar un proyecto de software, el encargado del mismo debe especificar los elementos del sistema detalladamente, preparando planes de trabajo detallados que tratarán todo el desarrollo necesario para resolver los requisitos y necesidades funcionales de los usuarios. Estas especificaciones de sistema detallan el comportamiento previsto del sistema e incluyen cosas tales como:

- Plantillas de Documentación.

- Casos de Uso Finales contra versiones piloto probadas.

- Flujo de Datos para transacciones.

- Puntos de Interfases de usuarios (Definiciones de dispositivos de navegación).

- Definiciones de Pantallas.

- Definiciones de Tablas.

- Definiciones de Interfases de Datos.

- Algoritmos Estándares.

- Flujos de Proceso.

- Descripciones de puntos donde las decisiones serán tomadas.

- Descripciones de puntos donde los datos serán almacenados como parte del proceso.

- Todos los casos de uso necesarios para satisfacer los requerimientos funcionales del negocio.

Las especificaciones de sistema necesitarán ser documentadas claramente y a fondo, y las definiciones del alcance del proyecto deben ser utilizadas como base para cambios futuros. Esta tarea requerirá que los controles aseguren el éxito del proyecto según lo aprobado. Los cambios significativos al diseño del sistema y la funcionalidad necesitarán ser aprobados formalmente por una autoridad predeterminada que represente al comité de dirección de la gerencia. La documentación de control de cambios debe incluir evaluaciones del impacto en términos de coste y los marcos de tiempo así como interfases y usuarios afectados (si es significativo).

Parte del desarrollo de especificaciones de sistemas implica un detalle de los casos del uso y el aseguramiento de que las experiencias previstas del usuario estén

alineadas con las necesidades del proceso del negocio y las expectativas. Esta tarea se puede lograr con una serie de entrevistas con los usuarios representativos quienes describirán sus necesidades y visiones de cómo las cosas necesitan ser realizadas para efectuar sus requerimientos de trabajo.

Es muy importante asegurar que dichas tareas se encuentren bien documentadas para verificar que las necesidades de los usuarios y sus ideas estén capturadas e incluidas en el diseño del sistema. Las necesidades del usuario deben ser tabuladas como parte del proceso de la revisión, asegurándose que la documentación satisfaga los procesos del negocio.

Los esfuerzos se deben documentar para asegurar que toda información relevante de cada tipo de usuario previsto está recolectada, que las pantallas y los flujos de trabajo (workflows) estén documentados para casos de uso particulares, y que las especificaciones del diseño estén acordes a las funciones de trabajo respectivas.

Una vez terminadas las especificaciones de sistemas, la documentación asociada debe ser revisada para asegurar que dichas especificaciones reflejen exactamente las características del diseño funcional y los requerimientos de usuarios. Cualquier desviación debe ser analizada para determinar la materialidad y la notificación posible de la variación a la gerencia para la conciliación correspondiente.

Una revisión de las especificaciones de sistema con el fin de determinar su capacidad de proveer controles internos adecuados, seguridad de la información, privacidad y cumplimiento con entidades reguladoras debe ser realizada por el auditor quien

evalúa el desarrollo del proyecto. Herramientas de auditoria, archivos logs y evidencia de errores, seguimientos, así como una inadecuada identificación de usuarios y reportes deben ser incluidos como puntos de evaluación requeridos.

Es así, como las especificaciones de los sistemas se constituyen en una base del desarrollo del aplicativo y de desarrollos de software futuros. Todas las pruebas realizadas así como los criterios de aceptación de usuario deben ser documentados. De igual forma, se deben documentar datos de carácter sensible, planes de protección de datos y accesos permitidos.

Finalmente, una parte relevante del proceso de desarrollo de un aplicativo constituye el control de calidad.

Se debe realizar una evaluación con el fin de asegurar que todos los puntos de control han sido revisados, direccionados y documentados adecuadamente. Adicionalmente, se debe verificar que todos los procesos estén siendo monitoreados.

El control de calidad, marca la diferencia tanto en las primeras etapas del proyecto como en las etapas de pruebas más cruciales.

5 CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Las principales conclusiones que destaco de este trabajo son que, si dividimos por sectores podemos afirmar que las empresas industriales y comerciales, si bien tienen clara la necesidad de que sus procesos soportados por herramientas tecnológicas sean probados y revisados, no han incluido dentro de su estructura la función de auditoría de sistemas, el 100% de las empresas entrevistadas de esos sectores no cuenta con un auditor de sistemas.

En el caso de las instituciones financieras y empresas de telecomunicaciones sobre todo las internacionales, tienen en su área de auditoría un responsable para la parte de sistemas y esto es comprensible; ya que en el primer caso es una exigencia de su ente de control la Superintendencia de Bancos y Seguros y la segunda es por exigencia de su casa matriz y de la velocidad de desarrollo de la tecnología en este sector.

También queda claro que la mayoría de las empresas prefieren tercerizar el servicio de auditoría de sistemas realizando revisiones periódicas, en el mejor de los casos una vez al año y solo en ciertos temas puntuales.

Este trabajo demuestra la importancia que tiene la auditoría de sistemas en las empresas actuales a mayor o menor grado dependiendo de su nivel de

automatización, sin embargo la mayoría de las compañías han emprendido una carrera dirigida hacia el mejoramiento de sus procesos con el apoyo de la tecnología, lo que les obligaría a buscar personal especializado en seguridad y control de sistemas de información, que les permita tener la certeza de que los procesos se están implementando adecuadamente.

Esta situación genera un reto en los auditores financieros ya que el conocimiento de temas relacionados a la tecnología de información se hace cada vez más latente. Si quieren auditar procesos, probar controles y recomendar oportunidades de mejora, en compañías con una importante nivel de automatización deben tener claros todos los conceptos de tecnología de información, es más, hoy para obtener el Certificado de Auditor Interno (CIA), emitido por el Instituto de Auditores Interno de Estados Unidos (IIA), es necesario aprobar una serie de exámenes, entre ellos un capitulo completo que trata sobre Sistemas de Información.

En esta investigación se identificó que las empresas o sus responsables de control interno están consientes de la importancia que tiene en la actualidad la revisión de los sistemas y todos concuerdan en que el realizar este tipo de revisiones apoyaría a la organización aportándole beneficios inclusive económicos, sin embargo también nos hace ver que esa preocupación no se plasma aún, en acciones que les permita corregir esta debilidad y que demuestren la importancia que tiene la auditoría de sistemas con el objetivo de ser consecuentes con sus comentarios.

El objetivo final de este modelo de revisión es que sirva de guía para que los auditores financieros con un nivel bajo de conocimientos de sistemas de información

realicen una revisión de sistemas, identifiquen riesgos y les permita entregar recomendaciones que agreguen valor a la organización y todas las personas interesadas dentro de la organización.

5.2 RECOMENDACIONES

Las áreas de auditoría de las empresas deberían, en base a la complejidad de sus procesos contar con la función formal de un auditor de sistemas, sea que se contrate una persona o un equipo de personas para realizar esta actividad, dependiendo de la complejidad y el tamaño de la organización o que se contrate a una consultora para realizar el trabajo periódicamente, incluido el respectivo seguimiento de cumplimiento de la implementación de las oportunidades de mejora identificadas.

Las Universidades dentro de la currícula de estudios de las áreas de Auditoría Financiera deberían fortalecer el nivel de conocimiento que imparten a los estudiantes en temas relacionados a sistemas de información y controles automatizados, tratando que este acorde al nivel de tecnificación de nuestro medio.

Hoy por hoy los riesgos que se generan debido al adelanto tecnológico es muy alto, no contar con conocimientos de sistemas, controles en tecnología, marcos referenciales que apoyan esta función, dan una ventaja importante a personas que deseen de una u otra forma evadir los controles implementados y realicen un fraude dentro de la empresa.

Los profesionales que están dedicados a la auditoría financiera, tienen la obligación de actualizarse en temas de tecnología, controles automáticos, modelos referenciales

de control de sistemas de información de tal forma que estén preparados para realizar un trabajo efectivo dentro de las organizaciones en la cuales trabajan o asesoran, recuerden que los Normas Internacionales de Auditoría (NIA) contienen algunas normas que incluyen la revisión de los sistemas por lo que se vuelve un requisito para el ejercicio de la practica.

Finalmente, pongo a disposición de la Universidad o de cualquiera de sus alumnos este trabajo que espero les ayude a entender la importancia de los sistemas de información, sus procesos y como pueden estos ser controlados con el objetivo de contar con una visión integral del control interno de cualquier empresa.

BIBLIOGRAFÍA

1. ACAICR. [http://www.acaicr.org/archivos/est%C3%A1ndares%20de%20auditor%C3%ADa%20sistemas%20de%20informaci%C3%B3n%20definidos%20por%20la%20isaca.pdf].

2. ARGENTINA. JEL 22. [http://www.jel22.com.ar/sabor1/sarbanes.pdf]

3. ARGENTINA. SARBANES - OXLEY. [http://www.sarbanes-oxley.com.ar/foro/viewtopic.php?p=496&sid=f4851647ab3496867ea45dedc9adee25].

4. AUDITORIA DE SISTEMAS. [http://auditoriasistemas.com/].

5. CHILE. IICAU. [http://www.iicau.cl/SAC/Descargas/COSO.pdf].

6. COLOMBIA. CONTROL INTERNO. [http://controlinterno.udea.edu.co/ciup/nuevo_sci.htm].

7. DATASEC-SOFT. [http://www.datasec-soft.com/archivos/sp/PPTS/meycor_coso.ppt].

8. DE GERENCIA. [http://www.degerencia.com/area.php?areaid=2001].

9. DE GERENCIA. [http://www.degerencia.com/articulo/el_control_interno_dentro_de_la_organizacion].

10. DELOITTE RESOURCES. [https://www.deloitteresources.com/pgContent.aspx?sid=16270&cid=117782].

11. DELOITTE RESOURCES. [www.deloitteresources.com].

12. DERECHO ECUADOR. [http://www.derechoecuador.com/].

13. DIRECTRICES DE AUDITORÍA. ***COBIT 4.1.***

14. ECUADOR. DIARIO LA HORA. [http://www.dlh.lahora.com.ec/paginas/judicial/PAGINAS/D.Informatico.29.htm].

15. ESPAÑA. SOCIEDAD DE LA INFORMACIÓN TELÉFONICA. [http://sociedaddelainformacion.telefonica.es/jsp/articulos/detalle.jsp?elem=6293].

16. GESTIOPOLIS. [http://www.gestiopolis.com/operaciones/reingenieria-de-procesos-de-negocios.htm].

17. HERNÁNDEZ CH., Sergio Alberto. ***Apoyo de las TIC al negocio.***

18. IASPLUS. [http://www.iasplus.com/dttpubs/0503undercontrol.pdf].

19. INTERAMERICAN USA. [http://www.interamericanusa.com/articulos/Leyes/Ley-Sar-Oxley.htm].

20. ISACA. [www.isaca.org].

21. MAIL X MAIL. [http://www.mailxmail.com/].

22. MÉXICO. TU OBRA. [http://www.tuobra.unam.mx/publicadas/040702105342-__191_Qu.html].

23. NORMA ISO 17799. ***Tecnología de la Información.***

24. NORMA ISO 27001:2005. ***Information Security Management System (ISMS).***

25. PONS ORTEGA, Fernando. ***Auditoría informática, una aproximación a la mejora del Control Interno.***

26. ROJAS, José Luis. ***Presentación de Deloitte.*** Socio Director de Servicios de Auditoría Interna para Latinoamérica CLAIN 2005.

27. WIKIPEDIA. [http://es.wikipedia.org/wiki/Acta_Sarbanes-Oxley#Novedades_y_puntos_m.C3.A1s_importantes_que_introduce_la_Ley_Sarbanes-Oxley].

28. WIKIPEDIA. [http://es.wikipedia.org/wiki/Ley_Sarbanes-Oxley].