Índice

ULACIT
UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGIA

LICENCIATURA EN INGENIERIA INFORMATICA
CON ÉNFASIS EN REDES Y SISTEMAS TELEMATICOS

"Desarrollo de un modelo de control interno que permita una adecuada administración del riesgo en el área de tecnologías de información para las entidades y órganos sujetos a la fiscalización de la Contraloría General de la República."

Sustentante: Marvin Moraga Calvo

PROYECTO DE GRADUACIÓN PARA OPTAR POR EL GRADO DE LICENCIADO EN INGENIERIA INFORMATICA

San José – Costa Rica
Junio 2004

Capítulo I : Introducción

I.1 Justificación

Debido al mundo económico integrado que existe hoy en día se ha creado la necesidad de integrar metodologías y conceptos en todos los niveles de las diversas áreas administrativas y operativas con el fin de ser competitivos y responder a las nuevas exigencias empresariales, surge así un nuevo concepto de control interno.

El control interno posee cinco componentes que pueden ser aplicados en todas las organizaciones de acuerdo con las características administrativas, operacionales y de tamaño. Los componentes son: el ambiente de control, la valoración de riesgos, las actividades de control (políticas y procedimientos), información y comunicación y, finalmente, el monitoreo o supervisión.

La aplicación del control interno implica que cada uno de sus componentes esté adaptado a cada categoría esencial de la organización convirtiéndose en un proceso integrado, dinámico y permanente. Como paso previo cada entidad debe establecer los objetivos, políticas y estrategias relacionadas entre sí con el fin de garantizar el desarrollo organizacional y el cumplimiento de las metas.

Aunque el sistema de control interno debe ser intrínseco a la administración de la entidad y busca que esta sea más flexible y competitiva en el mercado, se producen ciertas limitaciones inherentes que impiden que el sistema como tal sea confiable 100%, como hay un pequeño porcentaje de incertidumbre, por esta razón se hace necesario un estudio adecuado de los riesgos internos y externos para que el control provea una seguridad razonable para la categoría a la cual fue diseñado. Estos riesgos pueden ser atribuidos a fallas humanas, como la toma de decisiones erróneas, simples equivocaciones o confabulaciones de varias personas.

Es muy importante destacar que la responsabilidad principal de la aplicación del control interno en la organización debe, estar siempre de primero en la administración o alta gerencia con el fin de que exista un compromiso real en todos los niveles de la empresa. Debe ser función del departamento de auditoria interna, o quien haga sus veces, la adecuada evaluación o supervisión independiente del sistema, con el fin de garantizar la actualización, eficiencia y existencia a través del tiempo. Estas evaluaciones pueden ser continuas o puntuales, y carecer de una frecuencia predeterminada o fija. Así mismo se debe mantener una correcta documentación con el fin de analizar los alcances de la evaluación, los niveles de autorización, los indicadores de desempeño e impactos de las deficiencias encontradas. Estos análisis

deben detectar, en el momento oportuno, cómo los cambios internos o externos del contexto organizacional pueden afectar el desarrollo o aplicación de las políticas en función del logro de los objetivos.

La comprensión del control interno puede así ayudar a cualquier entidad pública o privada a obtener logros significativos en su desempeño, con eficiencia, eficacia y economía; indicadores indispensables para el análisis, toma de decisiones y cumplimiento de metas.

El establecimiento de la administración del riesgo como un método lógico y sistemático permitirá a las organizaciones enmarcar, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso, de una manera que las organizaciones puedan minimizar pérdidas y alcanzar los objetivos.

El desconocimiento en los niveles directivos de la situación informática de la institución, así como la falta de una planificación informática adecuada, falta de políticas, objetivos, normas, metodologías, asignación de tareas, administración del recurso informático y administración del riesgo que permita la consecución de los objetivos planteados, impiden el funcionamiento correctamente de las áreas de tecnologías de información. También es evidente que la falta de documentación o documentación incompleta de procesos, revela la dificultad de efectuar una oportuna administración del riesgo que trae consigo consecuencias en la organización de la materialización del riesgo.

I.2 Formulación del problema

¿Cómo desarrollar un modelo que permita una adecuada administración del riesgo en el área de tecnologías de información acorde con las nuevas Normas Generales de Control Interno implementadas por la Contraloría General de la República para las entidades y órganos sujetos a su fiscalización?

I.3 Objetivos

Objetivos generales y específicos

Determinar la existencia de políticas, mecanismos o acciones de control interno asociados con una actividad, función o proceso en el área de tecnologías de información que permitan a las organizaciones la correcta administración del riesgo minimizando pérdidas y que ayuden a alcanzar los objetivos.

- Identificar políticas internas existentes en actividades, funciones o procesos que permitan la correcta administración del riesgo.

- Identificar mecanismos o acciones de control interno ya existentes en actividades, funciones o procesos que permiten la correcta administración del riesgo.

- Evaluar la aplicación de políticas, procedimientos, mecanismos o acciones de control internos que existentes para la correcta administración del riesgo.

Desarrollar un modelo para aplicar políticas, mecanismos o acciones de control interno en actividades, funciones o procesos, en el área de tecnologías de información que permita a las organizaciones una adecuada administración del riesgo, asegurando la calidad de las actividades, administración adecuada de los recursos concernientes con las tecnologías de información, así como la consecución de los objetivos de la organización.

- Proponer políticas en actividades, funciones o procesos que permitan una adecuada administración del riesgo, de acuerdo con la normativa vigente en materia de control interno.

- Definir mecanismos o acciones de control internos en actividades, funciones o procesos para una adecuada administración del riesgo.

- Proponer la adopción de un estándar de administración de riesgos en actividades, funciones o procesos que permita una adecuad administración del riesgo en el área de Tecnologías de Información.

Capítulo II : Marco Teórico

II.1 Manual de Normas Generales de Control Interno para la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización

El crecimiento de los mercados, los cambios tecnológicos, la necesidad de seleccionar la información más útil de entre grandes cantidades, la promulgación de leyes y otros instrumentos jurídicos con mayores exigencias de control, la aparición de nuevas formas de

abuso de los bienes públicos y el creciente reclamo a los administradores públicos de rendir cuentas por su gestión, son condiciones que requieren la toma de acciones concretas por parte de la Administración Activa para mejorar sus sistemas de control interno, a fin de que éstos se conviertan en herramientas efectivas para conducir a las instituciones hacia el logro de su cometido, aprovechar al máximo los recursos disponibles y prevenir el desperdicio y el uso inadecuado o ilícito de esos recursos.

Como respuesta a esos cambios, se han desarrollado métodos que permiten tener una visión global y estratégica de las organizaciones y de su entorno, como punto de partida para el éxito en la gestión. Estos esfuerzos han dado como resultado diversos enfoques de control interno que actualmente configuran una concepción más novedosa e integral del papel que el control debe cumplir como parte de los sistemas administrativos y por ende, de un sistema de rendición de cuentas.

De conformidad con lo comentado, y a la luz de las potestades constitucionales y legales conferidas a la Contraloría General, con el afán de contribuir al mejoramiento de los sistemas de control interno institucionales y, por ende, al manejo legal, económico, eficiente y eficaz del patrimonio público, se emiten el presente “Manual de normas generales de control interno para la Contraloría General de la República y las instituciones y órganos sujetos a su fiscalización”, las cuales constituyen una normativa de carácter general, que proporciona un esquema básico para la transparencia en la gestión pública en el marco de la legalidad, la ética y la rendición de cuentas.

II.1.1 Definición del control interno

Según el Manual de normas generales de control interno para la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización, el control interno comprende la serie de acciones diseñadas y ejecutadas por la administración activa para proporcionar una seguridad razonable en torno a la consecución de los objetivos de la organización, fundamentalmente en las siguientes categorías: a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal; b) Confiabilidad y oportunidad de la información; c) Eficiencia y eficacia de las operaciones; d) Cumplir con el ordenamiento jurídico y técnico.

II.1.2 Objetivos del control interno

El control interno tiene como fin coadyuvar con la organización en el cumplimiento de sus objetivos, fundamentalmente en las siguientes categorías (Manual de normas generales de

control interno para la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización, 2002):

- Eficiencia y eficacia de las operaciones.
- Confiabilidad y oportunidad de la información.
- Cumplimiento de la normativa vigente.
- Protección y conservación del patrimonio contra pérdida, despilfarro, uso indebido, irregularidad o acto ilegal

II.1.3 Componentes

Según el Manual de normas generales de control interno para la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización, los componentes del control interno son funcionales y orgánicos. Los componentes funcionales son el ambiente de control, la evaluación del riesgo, la información y la comunicación, las actividades de control y el monitoreo. Los componentes orgánicos son la Administración Activa y la Auditoría Interna.

II.1.3.1 Ambiente de control

El ***ambiente de control***, relacionado con las actitudes y acciones de los jerarcas, los titulares subordinados y demás funcionarios de la institución, sus valores y el ambiente en el que desempeñan sus actividades dentro de la institución, que sirva como fundamento para la operación exitosa de los demás componentes y el sistema como un todo.

II.1.3.2 Evaluación de riesgos

La ***valoración de riesgos***, que conlleva la existencia de un sistema de detección y valoración de los riesgos derivados del ambiente entendidos como los factores o situaciones que podrían afectar el logro de los objetivos institucionales, que permita a la administración efectuar una gestión eficaz y eficiente por medio de la toma de acciones válidas y oportunas para prevenir y enfrentar las posibles consecuencias de la eventual materialización de esos riesgos, entendida como el hecho de que el perjuicio al logro de los objetivos institucionales por esos riesgos deje de ser probable y se convierta en una realidad.

II.1.3.3 Actividades de control (políticas, procedimientos)

Las ***actividades de control***, que comprenden todos los métodos, políticas, procedimientos y otras medidas establecidas y ejecutadas como parte de las operaciones para

asegurar que se están aplicando las acciones necesarias para manejar y minimizar los riesgos y realizar una gestión eficiente y eficaz.

II.1.3.4 Información y comunicación

La ***información*** y la ***comunicación***, que comprenden los sistemas de información y comunicación existentes en la institución, los cuales deben permitir la generación, la captura, el procesamiento y la transmisión de información relevante sobre las actividades institucionales y los eventos internos y externos que puedan afectar su desempeño positiva o negativamente.

II.1.3.5 Monitoreo

El ***monitoreo***, que consiste en un proceso de seguimiento continuo para valorar la calidad de la gestión institucional y del sistema de control interno.

II.2 Planificación estratégica

II.2.1 La planificación

La planificación es una herramienta presente en toda corriente de administración, y como tal se le identifica como una función de la administración que mejora las oportunidades de alcanzar resultados deseados. Los mayores beneficios de la planificación para una organización son: la anticipación de contingencias que pudieran impedir el logro de sus metas, la preparación de una estructura para que su organización crezca y progrese, y la disponibilidad de una estrategia para asignar recursos de manera que la organización pueda alcanzar sus metas.

La planificación es necesaria por que obliga a las organizaciones a vincular su proceso de toma de decisiones con sus valores y su finalidad, que están por encima de todo, así como a establecer metas y objetivos. La planificación transforma la intención en acción. Sin planificación solamente queda reaccionar antes los acontecimientos sin la posibilidad de vislumbrar los impactos y las consecuencias, ni menos influir en ellas.

Existen cuatro grandes razones para planificar; la primera, es el lapso de tiempo cada vez mayor que transcurre entre las actuales decisiones y los resultados futuros; la segunda, es la creciente complejidad de la organización; la tercera, son las crecientes necesidades; y la cuarta, es el impacto de la planificación sobre las demás funciones de gestión.

II.2.2 Los tipos de planificación

Las actividades de planificación difieren debido a su ámbito, a su marco temporal y a su nivel de especificidad. El ámbito es el área de actividades cubierta por el plan. El marco temporal es el período de tiempo que se tiene en cuenta en el plan, que oscila desde el plazo inmediato, pasa por el corto, sigue por el distante y llega al largo plazo. El nivel de especificidad es una medida de la adecuación del plan. En atención a estos tres factores es posible identificar tres niveles de planificación, la planificación estratégica, la planificación táctica y la planificación operacional.

II.2.2.1 La planificación estratégica

Es comprensiva a largo plazo y relativamente general. Se centra en temas amplios y duraderos que aseguran la efectividad de la organización y su desarrollo durante años. El plan estratégico establece la finalidad de la organización y puede describir un conjunto de metas y objetivos.

II.2.2.2 La planificación operativa

Se establece a corto plazo es especifica y orientada a la consecución del objetivo determinado. Convierte los conceptos generales del plan estratégico en cifras claras y en pasos concretos y en objetivos evaluables a corto plazo. La planificación operativa demanda una aplicación de recursos que sea eficiente y efectiva en costos, en la solución del problema y en la consecución de los objetivos establecidos.

II.2.2.3 La planificación táctica

Se ubica en el enlace que puede establecerse entre los procesos de la planificación estratégica y de la planificación operativa. Es más limitada, específica y de medio plazo, en comparación con la planificación estratégica. La táctica se refiere más a asuntos relativos a la eficiencia que a la eficacia a largo plazo.

II.2.3 El proceso de planificación

El proceso de planificación tiene muchas semejanzas con el proceso de toma de decisiones y consta de seis etapas que consideran las siguientes acciones (Ivancevich et al. 1996):

II.2.3.1 Evaluar las condiciones actuales

Proporciona a la planificación estratégica una visión panorámica de los ambientes internos y externos a la organización; a la planificación operativa, un conjunto de antecedentes ciertos respecto a la disponibilidad de recursos, personal, cantidad de beneficiarios, etc.; para la planificación estratégica, un conjunto de alternativas para emprender una acción observando y comparando los riesgos y beneficios.

II.2.3.2 Determinar objetivos y metas

Las metas se definen como estados o condiciones futuras que contribuyen al cumplimiento de la finalidad última de la organización. Siendo más concretas y específicas que las propias finalidades, las metas expresan criterios de eficacia intermedios. Pueden expresarse también en términos de producción, de eficacia y de satisfacción. Las metas hacen referencia a lo que es importante para la organización y dan al personal de la municipalidad un sentido de propósito. Los objetivos son fines específicos, medibles, planteados a corto plazo y su consecución previa es precisa para poder alcanzar las metas de la organización. Los objetivos permiten que los trabajadores y los ciudadanos sepan qué es importante. Los objetivos han de ser relevantes, desafiantes y bien enfocados, esto último significa que deben ser comprensibles, aceptables, específicos y medibles. La gestión da inicio a la planificación para determinar la prioridad y la oportunidad de los objetivos. Además, la gestión debe resolver también los conflictos entre los objetivos.

II.2.3.3 Establecer un plan de acción

Para el logro de los objetivos se requieren planes de acción. Las acciones son medios específicos prescritos para el logro de los objetivos. Los cursos de acción planificados reciben

el nombre de estrategias y tácticas, y suelen diferenciarse por los mismos factores que dan nacimiento a los tres niveles de planificación. Sea cual fuere el nombre que pueda dársele, toda acción planificada está dirigida a cambiar una condición futura, es decir, está dirigida a la consecución de un objetivo.

II.2.3.4 Asignar recursos

Todo plan requiere la asignación de recursos. Los recursos son los activos financieros, físicos, humanos, de tiempo, o de otra índole con los que cuenta una organización. El gasto de recursos suele controlarse mediante el presupuesto. Un presupuesto es una predeterminada cantidad de recursos relacionada con una actividad. La información es otro recurso que está sujeto a la presupuestación. La información es tal vez el recurso más importante para las organizaciones modernas, cuya gestión se basa en el conocimiento. Es difícil planificar si no se tiene acceso pleno a la información de la organización, y si no hay un conocimiento preciso del entorno en donde se ubica el plan.

II.2.3.5 Ejecución

Se relaciona con la delegación de tareas, con la acción impulsada por los objetivos y con la obtención de datos para la retroalimentación, sea ésta para el monitoreo o la toma de decisiones oportuna. Sin una ejecución eficaz, las cuatro etapas anteriores no tendrían sentido. Ejecutar significa consumir utilizar recursos para poner en práctica un plan.

II.2.3.6 Control

Es el conjunto de actividades de gestión que tienen por objeto asegurar que los resultados en curso se correspondan con los resultados planeados y que del proceso comparativo se pueda verificar el cumplimiento de los estándares establecidos. El control constituye una parte de la función de planificación, como también lo es del proceso de administración en general.

II.2.4 Los Planes

Los productos característicos del proceso de planificación son los planes. Estos pueden clasificarse en objetivos, políticas, procedimientos, reglas, presupuestos, programas y estrategias (Koontz et al. 1990).

II.2.4.1 Objetivos

Son los fines hacia donde se encaminan las actividades, representando el punto final de la planificación desagregada del plan maestro. Estos objetivos se encuentran en distintos niveles de la organización, en distintas áreas de gestión y satisfacen distintas necesidades de la organización.

II.2.4.2 Políticas

Las políticas son afirmaciones generales o declaraciones que guían o canalizan a los funcionarios en el proceso de toma de decisiones. Las políticas delimitan un área dentro de la cual una decisión va a ser tomada y aseguran que la decisión sea consistente con los objetivos y metas de la organización. Las políticas representan el aprendizaje de la organización expresado en recomendaciones generales, permitiendo la delegación de la toma de decisiones.

Tanto los objetivos como las políticas guían el pensamiento y la acción, pero con una diferencia. Los objetivos son los puntos finales de la planificación, mientras que las políticas son los canales de decisión a lo largo del camino hacia estos fines.

II.2.4.3 Procedimientos

Son guías para la acción, permitiendo un método habitual para el manejo de las actividades futuras, detallando de manera precisa como una actividad debe ser cumplida. Representan la normalización de aquellas acciones rutinarias no relevantes en el proceso de toma de decisiones.

II.2.4.4 Reglas

Son líneas generales establecidas para apoyar las acciones administrativas, como también algunos procedimientos, que están exentas de discreción en su aplicación.

II.2.4.5 Presupuestos

Es un estado de resultados expresado en términos numéricos, ya que intenta anticipar un comportamiento financiero, o un estado de situación en el tiempo.

II.2.4.6 Programas

Son un conjunto de políticas, procedimientos, reglas, presupuestos y otros elementos, necesarios para llevar a cabo una determinada línea de acción.

II.2.4.7 Estrategias

Es la identificación de las posibles rutas para alcanzar los objetivos más relevantes que soportan la misión de la organización, considerando el comportamiento de los distintos factores que pueden colaborar o perjudicar el logro de estos objetivos.

II.2.5 La planificación estratégica

El concepto de estrategia se ha tomado prestado de lo militar y se ha adaptado para el uso en las empresas. En las empresas como en lo militar, la estrategia vincula y articula las políticas (metas de alto nivel) y las tácticas (acciones concretas). Juntas, la estrategia y las tácticas, comunican y conectan los medios y los fines.

La estrategia, en general, se refiere a cómo un objetivo dado será alcanzado. Por consiguiente, la estrategia se preocupa por las relaciones entre los medios y fines, es decir, entre los resultados que se buscan y los recursos disponibles. Tanto la estrategia como las tácticas están relacionadas con la formulación y la ejecución de los cursos de acción deseados para alcanzar objetivos particulares. En su mayor parte, la estrategia se preocupa por desplegar los recursos disponibles, mientras que las tácticas se preocupan por emplearlos.

II.2.5.1 Beneficios de la planificación estratégica

La planificación estratégica sirve para una gran variedad de propósitos en las organizaciones, tales como (Wells et al. 1996, 1994):

- Definir claramente el propósito de la organización y establecer metas realistas y objetivos consistentes con esa misión, en un marco de tiempo definido, dentro de la capacidad de la organización para la aplicación.
- Proveer una estructura y un centro para los esfuerzos de mejoramiento.
- Optimizar el sistema organizacional.
- Asegurar que se hace el más efectivo uso de los recursos de la organización, enfocándolos en las prioridades claves.
- Proporcionar una base desde la cual pueda medirse el progreso y establecer un mecanismo para informar los logros.
- Suministrar una guía para las decisiones del día a día.
- Tender un puente entre todo el personal y compartir la información que genera pertenencia.

- Estimular la formación de equipos de trabajo en torno a las visiones y las tareas de la organización.

II.2.5.2 Oportunidades en las que debe realizarse un plan estratégico

La programación para el proceso de planificación estratégica depende de la naturaleza y necesidades de la organización y de su entorno inmediato. La planificación estratégica es aconsejable realizarla una vez por año y en la profundidad y extensión que la situación lo amerite.

En general la planificación estratégica debería realizarse:

- Cuando una nueva organización esté justamente arrancando.
- Cuando se emprenda una nueva aventura o se presente un nuevo desafío.
- Cuando termine un año fiscal.
- Cuando sea necesario revisar y/o actualizar el plan estratégico.
- Cuando se requiera mejorar el desempeño de la organización.

II.2.5.3 Formas de estrategia

No hay un modelo de planificación estratégica perfecto para cada organización. Cada organización termina desarrollando su propio modelo de acuerdo a su naturaleza, el que a menudo se modifica a lo largo del desarrollo de su propio proceso de planificación. Los siguientes modelos proporcionan un rango de alternativas de las que las organizaciones podrían seleccionar un enfoque y comenzar a desarrollar su propio proceso de planificación estratégica. Nótese que una organización podría escoger e integrar más de un modelo, por ejemplo, usando un modelo de escenarios para identificar creativamente los problemas y las metas estratégicas, y otro modelo basado en los problemas para jerarquizarlos cuidadosamente para alcanzar las metas (McNamara 2001).

Los modelos de planificación más utilizados son: planificación estratégica básica, planificación basada en los problemas (o en las metas), planificación de alineación, planificación de escenarios y planificación orgánica.

II.2.5.3.1 Modelo de planificación estratégica básica

Este es un proceso muy básico y es típicamente utilizado por organizaciones que son

extremadamente pequeñas, ocupadas y que no han hecho mucha planificación estratégica antes. El proceso puede ser implementado en el primer año de puesta en marcha, para obtener el sentido de cómo la planificación es conducida, y entonces enriquecerlo en los años posteriores con más fases y actividades, para asegurar una buena dirección y un buen cuerpo para organizaciones sin fines de lucro. La planificación generalmente es consumada por la administración del nivel superior. El proceso de planificación estratégica básica incluye:

- Identificación del Propósito (declaración de la misión). Esta es la declaración que describe por qué la organización existe, esto es, su propósito básico. La declaración debería describir las necesidades que son deseadas por el cliente, para ser satisfechas, y con qué servicios. El tipo de comunidad se menciona a veces. La administración del nivel superior debe desarrollar un acuerdo con la declaración de la misión. La declaración de la misión cambiará un poco con los años.

- Selección de las metas que la organización debe alcanzar para lograr su misión. Las metas son en general afirmaciones acerca de lo que se necesita para lograr reunir los propósitos, o misión, y solucionar los mayores problemas que enfrenta la organización.

- Identificación de estrategias o métodos específicos que puedan ser implementadas para alcanzar cada meta. A menudo son las estrategias lo que cambia a la mayoría de las organizaciones que conducen las planificaciones estratégicas más robustas, particularmente por el examen más cerrado de los entornos externos e internos de la organización.

- Identificación de planes de acción específicos para implementar cada estrategia. Estas son las actividades específicas que cada función principal (por ejemplo departamentos, etc.) deben emprender para asegurar la efectiva implementación de cada estrategia. Los objetivos deben ser claramente expresados en el alcance en que las personas puedan evaluar si los objetivos se han reunido o no. Idealmente la administración superior desarrolla comités específicos en los que cada uno tiene un plan de trabajo, o un conjunto de objetivos.

- Monitoreo y puesta al día del plan. Los planificadores regularmente reflexionan sobre el grado en el cual las metas están siendo cumplidas y si los planes de acción están siendo implementados. Quizás el más importante indicador de éxito de la organización, es la positiva retroalimentación de los clientes de la organización.

Note que las organizaciones que siguen este método de planificación pueden desear

conducirse más allá del paso 3 —citado anteriormente—, al grado en que las metas adicionales son identificadas para impulsar el desarrollo de las operaciones centrales o de la administración de la organización, ejemplo, fortalecer la administración financiera.

II.2.5.3.2 Modelo de planificación basada en los problemas (o en las metas)

Las organizaciones que comienzan con el método de planificación estratégica básica, identificado anteriormente, frecuentemente evolucionan para usar este tipo de planificación más comprensiva y efectiva. El siguiente cuadro bosqueja una visión directa preferente de este tipo de proceso de planificación.

Resumen de la planificación estratégica basada en los problemas (o en las metas)

(Una organización puede que no haga todas las siguientes actividades cada año).

- Evaluación interna y externa para hacer un análisis de fortalezas, oportunidades, debilidades y fortalezas (FODA).
- Análisis estratégico para identificar y priorizar los principales problemas y/o metas.
- Diseñar las principales estrategias (o programas) para orientar los problemas y/o las metas.
- Diseñar y actualizar la visión, la misión y la importancia (algunas organizaciones hacen esto primero en la planificación).
- Establecer planes de acción (objetivos, recursos necesarios, roles y responsabilidades para la implementación).
- Registrar los problemas, metas, estrategias y programas, y actualizar la misión, la visión y los planes de acción en el documento del Plan Estratégico, adjuntando el análisis FODA y otros anexos importantes.
- Desarrollar y documentar un plan de operaciones anuales (desde el primer año del plan estratégico multianual).
- Elaborar y autorizar el presupuesto para el primer año (localización de fondos necesarios para financiar el primer año).
- Conducir las operaciones del primer año de la organización.
- Monitorear, revisar, evaluar y actualizar el documento del Plan Estratégico.

II.2.5.3.3 Modelo de planificación de alineamiento

El propósito general de este modelo es asegurar un fuerte alineamiento entre la misión de la organización y sus recursos para una efectiva operación de la organización. Este modelo es útil para organizaciones que necesitan un ajuste fino de sus estrategias o encontrar por qué ellos no trabajan bien. Una organización puede también elegir este modelo sí está experimentando una gran cantidad de problemas en torno a su eficiencia interna. El conjunto de pasos incluye:

El grupo de planificación delinea la misión, los programas y los recursos de la organización, y el apoyo necesario.
Identifica qué está trabajando bien y que necesita ajustes.
Identifica cómo estos ajustes deberían ser hechos.
Incluye los ajustes como estrategias en el plan estratégico.

II.2.5.3.4 Modelo de planificación de escenarios

Este modelo puede ser usado en conjunto con otros modelos para asegurar a los planificadores una verdadera comprensión del pensamiento estratégico. El modelo puede ser útil, particularmente en la identificación de problemas y metas estratégicas:

- Seleccionar varias fuerzas externas e imaginar los cambios relacionados que podrían influir en la organización, por ejemplo, cambio en las regulaciones, cambios demográficos, etc. La exploración de los titulares claves en los periódicos frecuentemente sugieren potenciales cambios que pueden afectar a la organización.

- Para cada fuerza de cambio se discuten tres diferentes escenarios organizacionales futuros, (incluyendo el mejor caso, el peor y el razonable) que podrían surgir con la organización como resultado de cada cambio. La revisión del escenario para el peor caso, frecuentemente provoca una fuerte motivación para cambiar la organización.

- Pensar en lo que la organización podría hacer, o las estrategias potenciales, en cada uno de los tres escenarios para responder a cada cambio.

- Los planificadores detectan tempranamente consideraciones comunes o estrategias que pueden ser dirigidas para responder a los posibles cambios externos.

- Seleccionar el cambio externo más probable que puede afectar a la organización, por ejemplo, sobre los siguientes tres a cinco años, e identificar la estrategia más razonable que la organización puede emprender para responder al cambio.

II.2.5.3.5 Modelo de planificación “orgánica” (o de auto organización)

Los procesos de panificación estratégica tradicionales, a veces son considerados “mecánicos” o “lineales”, esto es, ellos son en naturaleza más bien “generales a específicos” o “causa y efecto”. Por ejemplo, los procesos comienzan frecuentemente por la conducción de una amplia evaluación de los entornos externos e internos de la organización, dirigiendo un análisis estratégico (análisis FODA) limitándolo para identificar y priorizar problemas, y entonces desarrollar estrategias específicas para orientar los problemas específicos.

Otra visión de la planificación es similar al desarrollo de un cuerpo, esto es, un proceso “orgánico” auto organizacional. Ciertas organizaciones, por ejemplo, los equipos deportivos de alto rendimiento, prefieren desplegar un proceso de planificación “orgánico” y naturalista, más que un proceso tradicional mecánico y lineal. La auto organización requiere referencias continuas a valores comunes, diálogos alrededor de estos valores y reflexiones permanentemente compartidas en torno de los actuales procesos del sistema. Este también es utilizado preferentemente por los círculos de calidad. Los pasos generales incluyen:

- Clarificar y articular los valores culturales de la organización. Se debe utilizar el diálogo y las técnicas de sondeo, apoyados en instrumentos de diagnóstico (encuestas).

- Articular la visión de la organización para el grupo. Se debe utilizar el diálogo y las técnicas de sondeo, apoyados en instrumentos de diagnóstico (encuestas).

- Sobre un progreso básico, por ejemplo, se debe conversar acerca de los procesos actuales y de las mejoras necesarias para llegar a la misión y lo que el grupo va a hacer ahora sobre esos procesos.

- Recordar continuamente que este tipo de planificación naturalista nunca está verdaderamente “acabada”, y que el grupo más bien necesita aprender a clarificar sus propios valores, diálogos, reflexiones y actualizaciones de los procesos.

- Proporcionar capacitación y apoyo de la dirección superior.

- Enfocarse más sobre el aprendizaje y menos sobre el método.

- Reflexionar sobre cómo la organización describirá sus planes estratégicos a los sostenedores (autoridades, contribuyentes o la comunidad toda), etc., quiénes frecuentemente esperan un plan de formato “mecánico” o “lineal”.

II.3 Estándar de control Interno Informe COSO

El denominado "INFORME COSO[1]" sobre control interno, publicado en EE.UU. en 1992, surgió como una respuesta a las inquietudes que planteaban la diversidad de conceptos, definiciones e interpretaciones existentes en torno a la temática referida.

Plasma los resultados de la tarea realizada durante más de cinco años por el grupo de trabajo que la TREADWAY COMMISSION, NATIONAL COMMISSION ON FRAUDULENT FINANCIAL REPORTING creó en Estados Unidos en 1985 bajo la sigla COSO (COMMITTEE OF SPONSORING ORGANIZATIONS). El grupo estaba constituido por representantes de las siguientes organizaciones:

- American Accounting Association (AAA)

- American Institute of Certified Public Accountants (AICPA)
- Financial Executive Institute (FEI)
- Institute of Internal Auditors (IIA)
- Institute of Management Accountants (IMA)

II.3.1 DEFINICION Y OBJETIVOS

El Control Interno es un proceso integrado a los procesos, y no un conjunto de pesados mecanismos burocráticos añadidos a los mismos, efectuado por el consejo de la administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar una garantía razonable para el logro de objetivos incluidos en las siguientes categorías (Control interno. Estructura Conceptual Integrada (COSO,2002):

- Efectividad y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes y regulaciones aplicables.

Completan la definición algunos conceptos fundamentales:

- El control interno es un proceso, es decir un medio para alcanzar un fin y no un fin en sí mismo.
- Lo llevan a cabo las personas que actúan en todos los niveles, no se trata solamente de manuales de organización y procedimientos.
- Sólo puede aportar un grado de seguridad razonable, no la seguridad total, a la conducción.
- Está pensado para facilitar la consecución de objetivos en una o más de las categorías señaladas las que, al mismo tiempo, suelen tener puntos en común.

Al hablarse del control interno como un proceso, se hace referencia a una cadena de acciones extendida a todas las actividades, inherentes a la gestión e integrados a los demás procesos básicos de la misma: planificación, ejecución y supervisión. Tales acciones se hallan incorporadas (no añadidas) a la infraestructura de la entidad, para influir en el cumplimiento de sus objetivos y apoyar sus iniciativas de calidad.

Según la Comisión de Normas de Control Interno de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), el control interno puede ser definido como el plan de organización, y el conjunto de planes, métodos, procedimientos y otras medidas de una institución, tendientes a ofrecer una garantía razonable de que se cumplan los siguientes objetivos principales:

- Promover operaciones metódicas, económicas, eficientes y eficaces, así como productos y servicios de la calidad esperada.
- Preservar al patrimonio de pérdidas por despilfarro, abuso, mala gestión, errores, fraudes o irregularidades.
- Respetar las leyes y reglamentaciones, como también las directivas y estimular al mismo tiempo la adhesión de los integrantes de la organización a las políticas y objetivos de la misma.
- Obtener datos financieros y de gestión completos y confiables y presentados a través de informes oportunos.

Para la alta dirección es primordial lograr los mejores resultados con economía de esfuerzos y recursos, es decir al menor costo posible. Para ello debe controlarse que sus decisiones se cumplan adecuadamente, en el sentido que las acciones ejecutadas se correspondan con aquéllas, dentro de un esquema básico que permita la iniciativa y contemple las circunstancias vigentes en cada momento.

Por consiguiente, siguiendo los lineamientos de INTOSAI, incumbe a la autoridad superior la responsabilidad en cuanto al establecimiento de una estructura de control interno idónea y eficiente, así como su revisión y actualización periódica.

Ambas definiciones (COSO e INTOSAI) se complementan y conforman una versión amplia del control interno: la primera enfatizando respecto a su carácter de proceso constituido por una cadena de acciones integradas a la gestión, y la segunda atendiendo fundamentalmente a sus objetivos.

II.3.2 COMPONENTES

El marco integrado de control que plantea el informe COSO consta de cinco componentes interrelacionados, derivados del estilo de la dirección, e integrados al proceso de gestión:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control
- Información y comunicación
- Supervisión

El ambiente de control refleja el espíritu ético vigente en una entidad respecto del

comportamiento de los agentes, la responsabilidad con que encaran sus actividades, y la importancia que le asignan al control interno.

El ambiente de control tiene una influencia profunda en la manera como se estructuran las actividades del negocio, se establecen los objetivos y se valoran los riesgos. Esto es cierto no solamente en su diseño, sino también en la manera como opera en la práctica (Control Interno. Estructura Conceptual Integrada (COSO, 2002)).

II.3.2.1 AMBIENTE DE CONTROL

El ambiente de control define al conjunto de circunstancias que enmarcan el accionar de una entidad desde la perspectiva del control interno y que son por lo tanto determinantes del grado en que los principios de este último imperan sobre las conductas y los procedimientos organizacionales.

Es, fundamentalmente, consecuencia de la actitud asumida por la alta dirección, la gerencia, y por carácter reflejo, los demás agentes con relación a la importancia del control interno y su incidencia sobre las actividades y resultados.

Fija el tono de la organización y, sobre todo, provee disciplina a través de la influencia que ejerce sobre el comportamiento del personal en su conjunto.

Constituye el andamiaje para el desarrollo de las acciones y de allí deviene su trascendencia, pues como conjunción de medios, operadores y reglas previamente definidas, traduce la influencia colectiva de varios factores en el establecimiento, fortalecimiento o debilitamiento de políticas y procedimientos efectivos en una organización.

Según Samuel, los principales factores del ambiente de control son:

- Integridad y valores éticos.
- Compromisos por la competencia.
- Consejo de directores o comité de auditoria.
- Filosofía y estilo de operación de la administración
- Estructura organizacional.
- Valoración de autoridad y responsabilidad.
- Políticas y prácticas sobre recursos humanos.

El ambiente de control reinante será tan bueno, regular o malo como lo sean los factores

que lo determinan. El mayor o menor grado de desarrollo y excelencia de éstos hará, en ese mismo orden, a la fortaleza o debilidad del ambiente que generan y consecuentemente al tono de la organización.

II.3.2.2 EVALUACION DE RIESGOS

El control interno ha sido pensado esencialmente para limitar los riesgos que afectan las actividades de las organizaciones. A través de la investigación y análisis de los riesgos relevantes y el punto hasta el cual el control vigente los neutraliza se evalúa la vulnerabilidad del sistema.

Según Samuel, la definición de objetivos es una condición previa para la valoración de riesgo. Primero que todo, deben definirse los objetivos a fin de que la administración pueda identificar los riesgos y tomas las decisiones necesarias para administrarlos. La definición de objetivos, entonces, es una parte clave del proceso administrativo. No es un componente de control interno, pero es un prerrequisito para hacer posible el control interno.

La definición de objetivos puede ser un proceso altamente estructurado o informal. Los objetivos pueden definirse explícitamente, o ser implícitos, tal como mantenerse en un nivel pasado de desempeño. Los objetivos a menudo están representados por la misión de la entidad y por la declaración de valores. El conocimiento de las fortalezas y debilidades de la entidad, y de las oportunidades y amenazas, conducen hacia un estrategia global (Control Interno. Estructura Conceptual Integrada (COSO, 2002)).

A este respecto cabe recordar que los objetivos de control deben ser específicos, así como adecuados, completos, razonables e integrados a los globales de la institución.

Luego que una entidad ha definido los riesgos globales de la entidad y los riesgos de actividad, necesita hacer un análisis de riesgos. La metodología para analizar riesgos puede variar ampliamente. Sin embargo, el proceso que puede ser más o menos formal usualmente incluye (Control Interno. Estructura Conceptual Integrada (COSO, 2002)):

- Estimación del significado de un riesgo.
- Valoración de la probabilidad (o frecuencia) de ocurrencia del riesgo.
- Consideración de cómo puede administrarse el riesgo, esto es, una valoración de qué acciones deben ser tomadas.

Dado que las condiciones en que las entidades se desenvuelven suelen sufrir

variaciones, se necesitan mecanismos para detectar y encarar el tratamiento de los riesgos asociados con el cambio. Aunque el proceso de evaluación es similar al de los otros riesgos, la gestión de los cambios merece efectuarse independientemente, dada su gran importancia y las posibilidades de que los mismos pasen inadvertidos para quienes están inmersos en las rutinas de los procesos.

Existen circunstancias que pueden merecer una atención especial en función del impacto potencial que plantean. Este centro de atención sobre el cambio administrativo está fundamentado en la premisa de que, dado su impacto potencial, ciertas condiciones deberán ser sujeto de consideración especial. La extensión de cuánta atención de la administración requiere tales condiciones, por supuesto, depende del efecto que puedan tener en las circunstancias particulares.

Tales condiciones son (Control Interno. Estructura Conceptual Integrada (COSO, 2002)):

- Cambió el ambiente de operación.
- Personal nuevo.
- Sistemas de información nuevos o reconstruidos.
- Crecimiento rápido.
- Tecnología nueva.
- Líneas, productos, actividades nuevas.
- Reestructuración corporativa.
- Operaciones en el extranjero.

Los mecanismos para prever, identificar y administrar los cambios deben estar orientados hacia el futuro, de manera de anticipar los más significativos a través de sistemas de alarma complementados con planes para un abordaje adecuado de las variaciones.

II.3.2.3 ACTIVIDADES DE CONTROL

Las actividades de control son políticas y procedimientos, son acciones de las personas para implementar las políticas, para ayudar a asegurar que se están llevando a cabo las directivas administrativas identificadas como necesarias para manejar los riesgos. Las actividades de control se pueden dividir en tres categorías, basadas en la naturaleza de los objetivos de la entidad con los cuales se relaciona (Control Interno. Estructura Conceptual Integrada (COSO, 2002)):

- Operaciones.

- Información financiera.
- Cumplimiento de leyes y reglamentos

En muchos casos, las actividades de control pensadas para un objetivo suelen ayudar también a otros: los operacionales pueden contribuir a los relacionados con la confiabilidad de la información financiera, éstas al cumplimiento normativo, y así sucesivamente.

A su vez en cada categoría existen diversos tipos de control:

- Preventivo / Correctivos
- Manuales / Automatizados o informáticos
- Gerenciales o directivos

La gama que se expone a continuación muestra la amplitud abarcativa de las actividades de control, pero no constituye la totalidad de las mismas:

- Análisis efectuados por la dirección.
- Seguimiento y revisión por parte de los responsables de las diversas funciones o actividades.
- Comprobación de las transacciones en cuanto a su exactitud, totalidad, y autorización pertinente: aprobaciones, revisiones, cotejos, recálculos, análisis de consistencia, prenumeraciones.
- Controles físicos patrimoniales: arqueos, conciliaciones, recuentos.
- Dispositivos de seguridad para restringir el acceso a los activos y registros.
- Segregación de funciones.
- Aplicación de indicadores de rendimiento.

Es necesario remarcar la importancia de contar con buenos controles de las tecnologías de información, pues éstas desempeñan un papel fundamental en la gestión, destacándose al respecto el centro de procesamiento de datos, la adquisición, implantación y mantenimiento del software, la seguridad en el acceso a los sistemas, los proyectos de desarrollo y mantenimiento de las aplicaciones.

A su vez los avances tecnológicos requieren una respuesta profesional calificada y anticipativa desde el control.

II.3.2.4 INFORMACION Y COMUNICACIÓN

Cada empresa debe capturar información pertinente, financiera y no financiera, relacionada con actividades y eventos tanto externos como internos. La información debe ser identificada por la administración como relevante para el manejo del negocio. Debe entregársela a la gente que la necesita, en una forma y oportunidad que le permita llevar a cabo su control y sus otras responsabilidades (Control Interno. Estructura Conceptual Integrada (COSO, 2002)).

Así como es necesario que todos los agentes conozcan el papel que les corresponde desempeñar en la organización (funciones, responsabilidades), es imprescindible que cuenten con la información periódica y oportuna que deben manejar para orientar sus acciones en consonancia con los demás, hacia el mejor logro de los objetivos.

La información relevante debe ser captada, procesada y transmitida de tal modo que llegue oportunamente a todos los sectores permitiendo asumir las responsabilidades individuales.

La información operacional, financiera y de cumplimiento conforma un sistema para posibilitar la dirección, ejecución y control de las operaciones.

Está conformada no sólo por datos generados internamente sino por aquellos provenientes de actividades y condiciones externas, necesarios para la toma de decisiones.

Los sistemas de información permiten identificar, recoger, procesar y divulgar datos relativos a los hechos o actividades internas y externas, y funcionan muchas veces como herramientas de supervisión a través de rutinas previstas a tal efecto. No obstante resulta importante mantener un esquema de información acorde con las necesidades institucionales que, en un contexto de cambios constantes, evolucionan rápidamente. Por lo tanto deben adaptarse, distinguiendo entre indicadores de alerta y reportes cotidianos en apoyo de las iniciativas y actividades estratégicas, a través de la evolución desde sistemas exclusivamente financieros a otros integrados con las operaciones para un mejor seguimiento y control de las mismas.

Ya que el sistema de información influye sobre la capacidad de la dirección para tomar decisiones de gestión y control, la calidad de aquél resulta de gran trascendencia y se refiere entre otros a los aspectos de contenido, oportunidad, actualidad, exactitud y accesibilidad.

La comunicación es inherente a los sistemas de información. Las personas deben conocer a tiempo las cuestiones relativas a sus responsabilidades de gestión y control. Cada

función ha de especificarse con claridad, entendiendo en ello los aspectos relativos a la responsabilidad de los individuos dentro del sistema de control interno.

Asimismo el personal tiene que saber cómo están relacionadas sus actividades con el trabajo de los demás, cuáles son los comportamientos esperados, de que manera deben comunicar la información relevante que generen.

Los informes deben transferirse adecuadamente a través de una comunicación eficaz. Esto es, en el más amplio sentido, incluyendo una circulación multidireccional de la información: ascendente, descendente y transversal.

La existencia de líneas abiertas de comunicación y una clara voluntad de escuchar por parte de los directivos resultan vitales.

Además de una buena comunicación interna, es importante una eficaz comunicación externa que favorezca el flujo de toda la información necesaria, y en ambos casos importa contar con medios eficaces, dentro de los cuales tan importantes como los manuales de políticas, memorias, difusión institucional, canales formales e informales, resulta la actitud que asume la dirección en el trato con sus subordinados. Una entidad con una historia basada en la integridad y una sólida cultura de control no tendrá dificultades de comunicación. Una acción vale más que mil palabras.

II.3.2.5 Monitoreo

El monitoreo asegura que el control interno continuará operando efectivamente. Este proceso implica la valoración, por parte del personal apropiado, del diseño y de la operación de los controles en una adecuada base de tiempo, y realizando las acciones necesarias. Se aplica para todas las actividades en una organización, lo mismo que algunas veces para contratistas externos (Control Interno. Estructura Conceptual Integrada (COSO, 2002)).

Incumbe a la dirección la existencia de una estructura de control interno idónea y eficiente, así como su revisión y actualización periódica para mantenerla en un nivel adecuado. Procede la evaluación de las actividades de control de los sistemas a través del tiempo, pues toda organización tiene áreas donde los mismos están en desarrollo, necesitan ser reforzados o se impone directamente su reemplazo debido a que perdieron su eficacia o resultaron inaplicables. Las causas pueden encontrarse en los cambios internos y externos a la gestión que, al variar las circunstancias, generan nuevos riesgos a afrontar.

El objetivo es asegurar que el control interno funciona adecuadamente, a través de dos modalidades de supervisión: actividades continuas o evaluaciones puntuales.

Las primeras son aquellas incorporadas a las actividades normales y recurrentes que, ejecutándose en tiempo real y arraigadas a la gestión, generan respuestas dinámicas a las circunstancias sobrevinientes.

En cuanto a las evaluaciones puntuales, corresponden las siguientes consideraciones:

a. Su alcance y frecuencia están determinados por la naturaleza e importancia de los cambios y riesgos que éstos conllevan, la competencia y experiencia de quienes aplican los controles, y los resultados de la supervisión continuada.
b. Son ejecutados por los propios responsables de las áreas de gestión (auto evaluación), la auditoria interna (incluidas en el planeamiento o solicitadas especialmente por la dirección), y los auditores externos.
c. Constituyen en sí todo un proceso dentro del cual, aunque los enfoques y técnicas varíen, priman una disciplina apropiada y principios insoslayables.

La tarea del evaluador es averiguar el funcionamiento real del sistema: que los controles existan y estén formalizados, que se apliquen cotidianamente como una rutina incorporada a los hábitos, y que resulten aptos para los fines perseguidos.

d. Responden a una determinada metodología, con técnicas y herramientas para medir la eficacia directamente o a través de la comparación con otros sistemas de control probadamente buenos.
e. El nivel de documentación de los controles varía según la dimensión y complejidad de la entidad.

Existen controles informales que, aunque no estén documentados, se aplican correctamente y son eficaces, si bien un nivel adecuado de documentación suele aumentar la eficiencia de la evaluación, y resulta más útil al favorecer la comprensión del sistema por parte de los empleados. La naturaleza y el nivel de la documentación requieren mayor rigor cuando se necesite demostrar la fortaleza del sistema ante terceros.

f. Debe confeccionarse un plan de acción que contemple:

- El alcance de la evaluación
- Las actividades de supervisión continuadas existentes.

- La tarea de los auditores internos y externos.
- Áreas o asuntos de mayor riesgo.
- Programa de evaluaciones.
- Evaluadores, metodología y herramientas de control.
- Presentación de conclusiones y documentación de soporte
- Seguimiento para que se adopten las correcciones pertinentes.

Las deficiencias o debilidades del sistema de control interno detectadas a través de los diferentes procedimientos de supervisión deben ser comunicadas a efectos de que se adopten las medidas de ajuste correspondientes.

Según el impacto de las deficiencias, los destinatarios de la información pueden ser tanto las personas responsables de la función o actividad implicada como las autoridades superiores.

II.4 Estándar Objetivos de Control para la Información y Tecnologías Relacionadas COBIT

II.4.1 ANTECEDENTES

Desarrollo del producto COBIT

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (TI). COBIT es la herramienta innovadora para el gobierno de TI.

COBIT se fundamenta en los Objetivos de Control existentes de la *Information Systems Audit and Control Foundation* (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento. Los Objetivos de Control resultantes han sido desarrollados para su aplicación en sistemas de información en toda la empresa.

Este estándar es relativamente pequeño en tamaño, con el fin de ser práctico y responder, en la medida de lo posible, a las necesidades de negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de TI adoptadas en una organización. El proporcionar indicadores de desempeño (normas, reglas, etc.), ha sido identificado como prioridad para las mejoras futuras que se realizarán al marco referencial.

El desarrollo de COBIT ha resultado en la publicación de:

- Un resumen ejecutivo, que consiste en una síntesis ejecutiva que proporciona a la alta gerencia un entendimiento y conciencia sobre los conceptos clave y principios de COBIT;

- El marco referencial que describe en detalle los 34 objetivos de control de alto nivel e identifica los requerimientos del negocio para la información y los recursos de TI que son impactados en forma primaria por cada objetivo de control;

- Objetivos de control, los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 302 objetivos de control detallados y específicos a través de los 34 procesos de TI;

- Directrices de auditoría, las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionara asistencia a los auditores de sistemas en la revisión de los procesos de TI con

respecto a los 302 objetivos detallados de control recomendados para proporcionar a la gerencia certeza o una recomendación de mejoramiento;

- Un conjunto de herramientas de implementación, el cual proporciona lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo.

II.4.2 El Marco Referencial de COBIT

En años recientes, ha sido cada vez más evidente para los legisladores, usuarios y proveedores de servicios la necesidad de un Marco Referencial para la seguridad y el control de tecnología de información (TI). Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) relacionada. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) esta criticalidad emerge de:

- la creciente dependencia en información y en los sistemas que proporcionan dicha información la creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información

- la escala y el costo de las inversiones actuales y futuras en información y en tecnología de información; y

- el potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa. Las organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar sin embargo, también comprenden y administran los riesgos asociados con la implementación de la nueva tecnología. Por lo tanto, la administración debe tener una apreciación por, y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados

La administración debe decidir la inversión razonable en seguridad y control en TI y cómo lograr un balance entre riesgos e inversiones en control en un ambiente de TI frecuentemente impredecible. La administración necesita un Marco Referencial de prácticas de

seguridad y control de TI generalmente aceptadas para medir comparativamente su ambiente de TI, tanto el existente como el planeado.

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

COBIT está diseñado para ser utilizado por tres audiencias distintas:

1. Administración

   Para ayudarlos a lograr un balance entre los riesgos y las inversiones en control en un ambiente de tecnología de información frecuentemente impredecible.

2. Usuarios

   Para obtener una garantía en cuanto a la seguridad y controles de los servicios de tecnología de información proporcionados internamente o por terceras partes.

3. Auditores de sistemas de información

   Para dar soporte a las opiniones mostradas a la administración sobre los controles internos.

Además de responder a las necesidades de la audiencia inmediata de la Alta Gerencia, a los auditores y a los profesionales dedicados al control y seguridad, *COBIT* puede ser utilizado dentro de las empresas por el propietario de procesos de negocio en su responsabilidad de control sobre los aspectos de información del proceso, y por todos aquellos responsables de TI en la empresa.

Los Objetivos de Control muestran una relación clara y distintiva con los objetivos de negocio con el fin de apoyar su uso en forma significativa fuera de las fronteras de la comunidad de auditoría. Los Objetivos de Control están definidos con una orientación a los procesos, siguiendo el principio de reingeniería de negocios. En dominios y procesos identificados, se identifica también un objetivo de control de alto nivel para documentar el enlace con los objetivos del negocio. Se proporcionan consideraciones y guías para definir e implementar el Objetivo de Control de TI.

La clasificación de los dominios a los que se aplican los objetivos de control de alto nivel (dominios y procesos); una indicación de los requerimientos de negocio para la información en ese dominio, así como los recursos de TI que reciben un impacto primario por parte del objetivo del control, forman conjuntamente el marco Referencial COBIT. El marco referencial toma como base las actividades de investigación que han identificado 34 objetivos de alto nivel y 302 objetivos detallados de control. El Marco Referencial fue mostrado a la industria de TI y a los profesionales dedicados a la auditoría para abrir la posibilidad a revisiones, dudas y comentarios. Las ideas obtenidas fueron incorporadas en forma apropiada.

El concepto fundamental del marco referencial COBIT se refiere a que el enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información que deben ser administrados por procesos de TI.

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como requerimientos de negocio para la información. Al establecer la lista de requerimientos, COBIT combina los principios contenidos en los modelos referenciales existentes y conocidos:

Requerimientos de calidad:

- Calidad
- Costo
- Entrega (de servicio)

Requerimientos fiduciarios COSO

- Efectividad & eficiencia de operaciones
- Confiabilidad de la información
- Cumplimiento de las leyes & regulaciones

Requerimientos de seguridad

- Confidencialidad
- Integridad
- Disponibilidad

Comenzando el análisis a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad más amplios, se extrajeron siete categorías distintas, ciertamente superpuestas. A continuación se muestran las definiciones de trabajo de COBIT:

Efectividad: Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

Eficiencia: Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

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

Integridad: Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

Disponibilidad: Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

Cumplimiento: Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.

Confiabilidad de la Información: Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Los recursos de TI identificados en COBIT pueden explicarse/definirse como se muestra a continuación (COBIT, 1998):

Datos: Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

Aplicaciones: Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.

Tecnología: La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.

Instalaciones: Recursos para alojar y dar soporte a los sistemas de información. Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

Personal: Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

El marco referencial consta de Objetivos de Control de TI de alto nivel y de una estructura general para su clasificación y presentación. La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TI al considerar la administración de sus recursos. Comenzando por la base, encontramos las actividades y tareas necesarias para alcanzar un resultado medible. Las actividades cuentan con un concepto de ciclo de vida, mientras que las tareas son consideradas más discretas. El concepto de ciclo de vida cuenta típicamente con requerimientos de control diferentes a los de actividades discretas. Algunos ejemplos de esta categoría son las actividades de desarrollo de sistemas, administración de la configuración y manejo de cambios. La segunda categoría incluye tareas llevadas a cabo como soporte para la planeación estratégica de TI, evaluación de riesgos, planeación de la calidad, administración de la capacidad y el desempeño.

Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas con “cortes” naturales (de control). Al nivel más alto, los procesos son agrupados de manera natural en dominios. Su agrupamiento natural es confirmado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI.

Por lo tanto, el marco referencial conceptual puede ser enfocado desde tres puntos estratégicos: (1) recursos de TI, (2) requerimientos de negocio para la información y (3) procesos de TI. Estos puntos de vista diferentes permiten al marco referencial ser accedido eficientemente.

Con lo anterior como marco de referencia, los dominios son identificados utilizando las palabras que la gerencia utilizaría en las actividades cotidianas de la organización. Por lo tanto, cuatro grandes dominios son identificados: planeación y organización, adquisición e implementación; entrega y soporte y monitoreo (COBIT, 1998).

Las definiciones para los dominios mencionados son las siguientes:

Planeación y organización

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Adquisición e implementación

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Entrega y soporte

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrena-miento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. *Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.*

Monitoreo

Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

En resumen, los Recursos de TI necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos.

II.4.3 Relaciones de Objetivos de Control, Dominios, Procesos y Objetivos de Control

En las páginas siguientes se individualizan los objetivos de control detallado para cada uno de los 34 procesos dentro de una función de Tecnologías de Información (COBIT, 1998).

II.4.3.1 PLANEACION Y ORGANIZACIÓN

1. Definición de un plan estratégico de tecnologías de información

1.1 Tecnología de Información como parte del Plan de la Organización a corto y largo plazo.

OBJETIVO DE CONTROL

La alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas de la organización. A este respecto, la alta gerencia deberá asegurar que los problemas de tecnología de información, así como las oportunidades, sean evaluados adecuadamente y reflejados en los planes a largo y corto plazo de la organización.

1.2 Plan a largo plazo de Tecnología de Información

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información será responsable de desarrollar regularmente planes a largo plazo de tecnología de información que apoyen el logro de la misión y las metas generales de la organización.

De la misma manera, la Gerencia deberá implementar un proceso de planeación a largo plazo, adoptar un enfoque estructurado y determinar la estructura para el plan.

1.3 Plan a largo plazo de Tecnología de Información - Enfoque y Estructura

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá establecer y aplicar un enfoque estructurado al proceso de planeación a largo plazo. Esto deberá traer como resultado un plan de alta calidad que cubra las preguntas básicas de qué, quién y cuándo. Los aspectos que necesitan ser tomados en cuenta y ser cubiertos adecuadamente durante el proceso de planeación son el modelo de organización y sus cambios, la distribución geográfica, la evolución tecnológica, los costos, los

requerimientos legales y regulatorios, requerimientos de terceras partes o del mercado, el horizonte de planeación, reingeniería de procesos del negocio, la asignación de personal, la designación de fuentes internas o externas, etc. El plan mismo deberá hacer referencia a otros planes tales como el plan de calidad de la organización y el plan de manejo de riesgos de información.

1.4 Cambios al Plan a largo plazo de Tecnología de Información

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la tecnología de información.

1.5 Planeación a corto plazo para la Función de Servicios de Información

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que el plan a largo plazo de tecnología de información sea traducido regularmente en planes a corto plazo de tecnología de información. Estos planes a corto plazo deberán asegurar que se asignen los recursos apropiados de la función de servicios de tecnología de información con una base consistente con el plan a largo plazo de tecnología de información. Los planes a corto plazo deberán ser reevaluados y modificados periódicamente según se considere necesario respondiendo a las condiciones de cambios en el negocio y en la tecnología de información. La realización oportuna de estudios de factibilidad deberá asegurar que la ejecución de los planes a corto plazo sea iniciada adecuadamente.

1.6 Evaluación de Sistemas Existentes

OBJETIVO DE CONTROL

En forma previa al desarrollo o modificación del Plan Estratégico de TI, la Gerencia de servicios de información debe evaluar los sistemas existentes en términos de:

nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.

2 Definición de la arquitectura de la información

2.1 Modelo de la Arquitectura de Información

OBJETIVO DE CONTROL

La información deberá conservar consistencia con las necesidades y deberá ser identificada, capturada y comunicada en una forma y dentro de períodos de tiempo que permitan a los responsables llevar a cabo sus tareas eficiente y oportunamente. Asimismo, la función de sistemas de información deberá crear y actualizar regularmente un modelo de arquitectura de información, abarcando el modelo de datos corporativo y los sistemas de información asociados. El modelo de arquitectura de información deberá conservar consistencia con el plan a largo plazo de tecnología de información.

2.2 Diccionario de Datos y Reglas de Sintaxis de Datos de la Corporación

OBJETIVO DE CONTROL

La función de servicios de información deberá asegurar la creación y la continua actualización de un diccionario de datos corporativo que incorpore las reglas de sintaxis de datos de la organización.

2.3 Esquema de Clasificación de Datos

OBJETIVO DE CONTROL

Deberá establecerse un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información (por ejemplo, categorías de seguridad), así como a la asignación de propiedad. Las reglas de acceso para las clases deberán definirse apropiadamente.

2.4 Niveles de Seguridad

OBJETIVO DE CONTROL

La Gerencia deberá definir, implementar y mantener niveles de seguridad para cada una de las clasificaciones de datos identificadas con un nivel superior al de "no requiere protección". Estos niveles de seguridad deberán representar el conjunto de medidas de seguridad y de control apropiado (mínimo) para cada una de las clasificaciones.

3 Determinación de la dirección tecnológica

3.1 Planeación de la Infraestructura Tecnológica

OBJETIVO DE CONTROL

La función de servicios de información deberá crear y actualizar regularmente un plan de infraestructura tecnológica que concuerde con los planes a largo y corto plazo de tecnología de información. Dicho plan deberá abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.

3.2 Monitoreo de Tendencias y Regulaciones Futuras

OBJETIVO DE CONTROL

La función de servicios de información deberá asegurar el continuo monitoreo de tendencias futuras y condiciones regulatorias, de tal manera que estos factores puedan ser tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.

3.3 Contingencias en la Infraestructura Tecnológica

OBJETIVO DE CONTROL

El plan de infraestructura tecnológica deberá ser evaluado sistemáticamente en cuanto a aspectos de contingencia (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura).

3.4 Planes de Adquisición de Hardware y Software

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que los planes de adquisición de hardware y software sean establecidos y que reflejen las necesidades identificadas en el plan de infraestructura tecnológica.

3.5 Estándares de Tecnología

OBJETIVO DE CONTROL

Tomando como base el plan de infraestructura tecnológica, la Gerencia deberá definir normas de tecnología con la finalidad de fomentar la estandarización.

4 Definición de la organización y de las relaciones de TI

4.1 Comité de planeación o dirección de la función de servicios de información

OBJETIVO DE CONTROL

La alta gerencia de la organización deberá designar un comité de planeación o dirección para vigilar la función de servicios de información y sus actividades. Entre los miembros del comité deberán encontrarse representantes de la alta gerencia, de la gerencia usuaria y de la función de servicios de información. El comité deberá reunirse regularmente y reportar a la alta gerencia.

4.2 Ubicación de los servicios de información en la organización

OBJETIVO DE CONTROL

Al ubicar la función de servicios de información en la estructura organizacional general, la alta gerencia deberá asegurar la existencia de autoridad, actitud crítica e independencia por parte del departamento usuario con un grado tal que sea posible garantizar soluciones de tecnología de información efectivas y progreso suficiente al implementarlas, así como establecer una relación de sociedad con la alta Gerencia para incrementar la capacidad de previsión, la comprensión y las habilidades para identificar y resolver problemas de tecnología de información.

4.3 Revisión de Logros Organizacionales

OBJETIVO DE CONTROL

Deberá establecerse un marco de referencia con el propósito de revisar que la estructura organizacional cumpla continuamente con los objetivos y se adapte a las cambiantes circunstancias.

4.4 Funciones y Responsabilidades

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que todo el personal en la organización conozca sus funciones y responsabilidades en relación con los sistemas de información. Todo el personal deberá contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas. Todos deberán estar conscientes de que tienen una cierta responsabilidad con respecto a la seguridad y al control interno. Consecuentemente, deberán organizarse y emprenderse campañas regulares para aumentar la conciencia y la disciplina.

4.5 Responsabilidad del aseguramiento de la calidad

OBJETIVO DE CONTROL

La Gerencia deberá asignar la responsabilidad de la ejecución de la función de aseguramiento de calidad a miembros del personal de la función de servicios de información y asegurar que existan sistemas de aseguramiento de calidad apropiados, controles y experiencia en comunicación dentro del grupo de aseguramiento de calidad de la función de servicios de información. La ubicación de la función dentro del área de servicios de información, las responsabilidades y el tamaño del grupo de aseguramiento de calidad deberán satisfacer los requerimientos de la empresa.

4.6 Responsabilidad de la Seguridad Lógica y Física

OBJETIVO DE CONTROL

La Gerencia deberá asignar formalmente la responsabilidad de la seguridad lógica y física de los activos de información de la organización a un Gerente de seguridad de la información, quien reportará a la alta gerencia. Como mínimo, la responsabilidad de la Gerencia de seguridad deberá establecerse a todos los niveles de la organización para manejar los problemas generales de seguridad en la organización. En caso necesario, deberán asignarse responsabilidades gerenciales de seguridad adicionales a niveles específicos con el fin de resolver los problemas de seguridad relacionados con ellos.

4.7 Propiedad y Custodia

OBJETIVO DE CONTROL

La Gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.

4.8 Propiedad de Datos y Sistemas

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que todos los activos de información (sistemas y datos) cuenten con un propietario asignado que tome decisiones sobre la clasificación y los derechos de acceso. Los propietarios del sistema normalmente delegarán la custodia diaria al grupo de liberación/ operación de sistemas y las responsabilidades de seguridad a un administrador de la seguridad. Los Propietarios, sin embargo, permanecerán como responsables del mantenimiento de medidas de seguridad apropiadas.

4.9 Supervisión

OBJETIVO DE CONTROL

La alta gerencia deberá implementar prácticas de supervisión adecuadas en la organización de servicios de información para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente, para evaluar si todo el personal cuenta con suficiente autoridad y recursos para llevar a cabo sus tareas y responsabilidades, y para revisar de manera general los indicadores clave de desempeño.

4.10 Segregación de Funciones

OBJETIVO DE CONTROL

La alta gerencia deberá implementar una división de funciones y responsabilidades que excluya la posibilidad de que un solo individuo resuelva un proceso crítico. La Gerencia deberá asegurar también que el personal lleve a cabo únicamente aquellas tareas estipuladas para sus respectivos puestos. En particular, deberá mantenerse una segregación de funciones entre las siguientes funciones:

- uso de sistemas de información;
- entrada de datos;
- operación de cómputo;
- administración de redes;
- administración de sistemas;
- desarrollo y mantenimiento de sistemas
- administración de cambios
- administración de seguridad; y
- auditoría de seguridad

4.11 Asignación de Personal para Tecnología de Información

OBJETIVO DE CONTROL

Las evaluaciones de los requerimientos de asignación de personal deberán llevarse a cabo regularmente para asegurar que la función de servicios de información cuente con un número suficiente de personal competente de tecnología de información. Los requerimientos de asignación de personal deberán ser evaluados por lo menos anualmente o al presentarse cambios mayores en el negocio, en el ambiente operacional o de tecnología de información. Deberá actuarse oportunamente tomando como base los resultados de las evaluaciones para asegurar una asignación de personal adecuada en el presente y en el futuro.

4.12 Descripción de Puestos para el Personal de la Función de Servicios de Información

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que las descripciones de los puestos para el personal de la función de servicios de información sean establecidos y actualizados regularmente. Estas descripciones de puestos deberán delinear claramente tanto la responsabilidad como la autoridad, incluir las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.

4.13 Personal Clave de TI

OBJETIVO DE CONTROL

La Gerencia deberá definir e identificar al personal clave de tecnología de información.

4.14 Procedimientos para personal por contrato

OBJETIVO DE CONTROL

La Gerencia deberá definir e implementar procedimientos relevantes para controlar las actividades de consultores y demás personal externo contratado por la función de servicios de información para asegurar la protección de los activos de información de la organización.

4.15 Relaciones

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá llevar a cabo las acciones necesarias para establecer y mantener una coordinación, una comunicación y un enlace óptimos entre la función de servicios de información y demás elementos interesados dentro y fuera de la función de servicios de información (usuarios, proveedores, oficiales de seguridad, Gerentes).

5 Manejo de la inversión en tecnologías de información

5.1 Presupuesto Operativo Anual para la Función de Servicios de Información

OBJETIVO DE CONTROL

La alta gerencia deberá implementar un proceso de definición de presupuestos para asegurar que un presupuesto operativo anual para la función de Servicios de Información sea establecido y aprobado en línea con los planes a largo y corto plazo de la organización, así como con los planes a largo y corto plazo de tecnología de información. Deberán investigarse alternativas de financiamiento.

5.2 Monitoreo de Costo – Beneficios

OBJETIVO DE CONTROL

La Gerencia deberá establecer un proceso de monitoreo de costos que compare los costos reales contra los presupuestados. Aun más, los posibles beneficios derivados de la actividad de tecnología de información deberán ser identificados y reportados.

En cuanto al monitoreo de costos, la fuente de las cifras reales deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información. Por lo que toca a monitoreo de beneficios, se deberán definir indicadores de medición de desempeño de alto nivel y ser reportados y revisados regularmente para asegurar su adecuación.

5.3 Justificación de Costo – Beneficio

OBJETIVO DE CONTROL

Deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos y se encuentre en línea con la industria. Los beneficios derivados de las actividades de tecnología de información deberán ser analizados en forma similar.

6 Comunicación de la dirección y aspiraciones de la gerencia

6.1 Ambiente Positivo de Control de la Información

OBJETIVO DE CONTROL

La Gerencia deberá crear un marco de referencia y un programa de previsión que fomente un ambiente de control positivo a través de toda la organización al aplicar elementos tales como: integridad, valores éticos, competencias del empleado, filosofía y estilo operativo de la Gerencia, responsabilidad, atención y dirección proporcionadas por el Consejo Directivo. Deberá ponerse especial atención a los aspectos relacionados con tecnología de información.

6.2 Responsabilidad de la Gerencia en cuanto a Políticas

OBJETIVO DE CONTROL

La Gerencia deberá asumir la responsabilidad completa de la formulación, el desarrollo, la documentación, la promulgación y el control de políticas que cubran metas y directrices generales. Deberán llevarse a cabo revisiones regulares de las

políticas para asegurar su conveniencia. La complejidad de las políticas y los procedimientos escritos deberán estar siempre en proporción con el tamaño de la organización y el estilo gerencial.

6.3 Comunicación de las Políticas de la Organización

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que las políticas organizacionales sean comunicadas y comprendidas por todos los niveles de la organización.

6.4 Recursos para la implementación de Políticas

OBJETIVO DE CONTROL

Posterior a la comunicación, la Gerencia deberá destinar recursos para la implementación de sus políticas. La Gerencia deberá también monitorear la duración de la implementación de sus políticas.

6.5 Mantenimiento de Políticas

OBJETIVO DE CONTROL

Las políticas deberán ser ajustadas regularmente para adecuarse a las condiciones cambiantes. Las políticas deberán ser reevaluadas, por lo menos anualmente o al momento de presentarse cambios significativos en el ambiente operacional o del negocio, para evaluar que sean convenientes y apropiadas y deberán ser modificadas en caso necesario. La Gerencia deberá proporcionar un marco de referencia y un proceso para las revisiones periódicas y la aprobación de estándares, políticas, directrices y procedimientos.

6.6 Cumplimiento de Políticas, Procedimientos y Estándares

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que se establezcan procedimientos apropiados para determinar si el personal comprende los procedimientos y políticas implementados, y que éste cumple con dichas políticas y procedimientos. El cumplimiento de las reglas de ética, seguridad y estándares de control interno deberá ser establecido por la Alta Gerencia y promoverse a través del ejemplo.

6.7 Compromiso con la Calidad

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, así como políticas y objetivos que sean consistentes con la filosofía y las políticas de la corporación a este respecto. La filosofía de calidad, las políticas y los objetivos deberán ser comprendidos, implementados y mantenidos a todos los niveles de la función de servicios de información.

6.8 Política sobre el Marco de Referencia para la Seguridad y el Control Interno

OBJETIVO DE CONTROL

La Gerencia deberá asumir la responsabilidad total del desarrollo y mantenimiento de una política sobre el marco de referencia, que establezca el enfoque general de la organización en cuanto a seguridad y control interno. La política deberá cumplir con los objetivos generales del negocio y estar dirigida a la minimización de riesgos a través de medidas preventivas, identificación oportuna de irregularidades, limitación de pérdidas y recuperación oportuna. Estas medidas deberán basarse en análisis costo-beneficio y deberá priorizarse. Además, la alta gerencia deberá asegurar que esta política de seguridad de alto nivel y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento con las políticas de seguridad y control interno.

6.9 Derechos de propiedad intelectual

OBJETIVO DE CONTROL

La gerencia deberá proveer e implementar una política por escrito sobre derechos de propiedad intelectual, que cubra el desarrollo de software, tanto interno como contratado a externos.

6.10 Políticas para Situaciones Específicas

OBJETIVO DE CONTROL

Deberán ponerse en práctica medidas que aseguren el establecimiento de políticas para situaciones específicas con el fin de documentar las decisiones gerenciales con respecto al tratamiento de actividades, aplicaciones, sistemas o tecnologías particulares.

7 Administración de recursos humanos

7.1 Reclutamiento y Promoción de Personal

OBJETIVO DE CONTROL

La Gerencia deberá implementar y evaluar regularmente los procesos necesarios para asegurar que las prácticas de reclutamiento y promoción de personal tengan como base criterios objetivos y consideren factores como la educación, la experiencia y la responsabilidad. Estos procesos deberán estar en línea con las políticas y procedimientos generales de la organización a este respecto.

7.2 Personal Calificado

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá verificar regularmente que el personal que lleva a cabo tareas específicas esté calificado tomando como base una educación, entrenamiento y/ o experiencia apropiados, según se requiera. La Gerencia deberá alentar al personal para que participe como miembro, en organizaciones profesionales.

7.3 Entrenamiento de Personal

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que los empleados reciban orientación al ser contratados, así como entrenamiento y capacitación constantes con la finalidad de conservar los conocimientos, habilidades, destrezas y conciencia de seguridad al nivel requerido, para la ejecución efectiva de sus tareas. Los programas de educación y entrenamiento dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal deberán ser revisados regularmente.

7.4 Entrenamiento Cruzado o Respaldo de personal

OBJETIVO DE CONTROL

La Gerencia deberá proporcionar un entrenamiento “cruzado” o contar con suficiente personal de respaldo con la finalidad de solucionar posibles ausencias. El personal

encargado de puestos delicados deberá tomar vacaciones ininterrumpidas con una duración suficiente como para probar la habilidad de la organización para manejar casos de ausencia y detectar actividades fraudulentas.

7.5 Procedimientos de Acreditación de Personal

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que su personal se sujete a una revisión o acreditación de seguridad antes de ser contratado, transferido o promovido, dependiendo de lo delicado o sensible del puesto. Un empleado que no haya pasado por este procedimiento de revisión o acreditación al ser contratado por primera vez, no deberá ser colocado en un puesto delicado hasta que éste haya obtenido la acreditación de seguridad.

7.6 Evaluación de Desempeño de los Empleados

OBJETIVO DE CONTROL

La Gerencia deberá implementar un proceso de evaluación de desempeño de los empleados y asegurar que dicha evaluación sea llevada a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

7.7 Cambios de Puesto y Despidos

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que se tomen acciones oportunas y apropiadas con respecto a cambios de puesto y despidos, de tal manera que los controles internos y la seguridad no se vea perjudicados por estos eventos.

8 Aseguramiento de cumplimiento de requerimientos externos

8.1 Revisión de Requerimientos Externos

OBJETIVO DE CONTROL

La organización deberá establecer y mantener procedimientos para la revisión de requerimientos externos y para la coordinación de estas actividades. La investigación continua deberá determinar los requerimientos externos aplicables en la

organización. Deberán revisarse los requerimientos legales, gubernamentales o cualquier otro requerimiento externo relacionado con las prácticas y controles de tecnología de información. La Gerencia deberá también evaluar el impacto de cualquier relación externa en las necesidades generales de información de la organización, incluyendo la determinación del grado al cual las estrategias de la función de servicios de información deben soportar o cumplir con los requerimientos de terceros.

8.2 Prácticas y Procedimientos para el Cumplimiento de Requerimientos Externos

OBJETIVO DE CONTROL

Las prácticas organizacionales deberán asegurar que se lleven a cabo oportunamente las acciones correctivas apropiadas para garantizar el cumplimiento de los requerimientos externos. Además, deberán establecerse y mantenerse procedimientos adecuados que aseguren el cumplimiento continuo. A este respecto la Gerencia deberá solicitar apoyo legal en caso necesario.

8.3 Cumplimiento de Seguridad y Ergonomía

OBJETIVO DE CONTROL

La Gerencia deberá asegurar el cumplimiento de los estándares ergonómicos y de seguridad en el ambiente de trabajo de los usuarios y el personal de la función de servicios de información.

8.4 Privacidad, propiedad intelectual y flujos de datos y Flujo de Datos

OBJETIVO DE CONTROL

La Gerencia deberá asegurar el cumplimiento de las regulaciones sobre privacidad o confidencialidad, propiedad intelectual, flujo de datos externos y criptografía aplicables a las prácticas de tecnología de información de la organización.

8.5 Comercio Electrónico

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que se establezcan contratos formales para determinar acuerdos entre socios comerciales sobre procesos de comunicación, así como sobre estándares de mensajes de transacción, seguridad y almacenamiento de datos. Cuando se realicen operaciones de intercambio en *Interne*t, la gerencia deberá

imponer adecuados controles para asegurar el cumplimiento de leyes locales y costumbres en un ámbito mundial.

8.6 Cumplimiento con los Contratos de Seguros

OBJETIVO DE CONTROL
La Gerencia deberá asegurar la identificación y el continuo cumplimiento de los requerimientos de los contratos de seguros.

9 Evaluación de riesgos

9.1 Evaluación de Riesgos del Negocio

OBJETIVO DE CONTROL
La Gerencia deberá establecer un marco de referencia de evaluación sistemática de riesgos. Este marco de referencia deberá incorporar una evaluación regular de los riesgos de información relevantes para el logro de los objetivos del negocio, formando una base para determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable. El proceso deberá proporcionar evaluaciones de riesgos tanto a un nivel global como a niveles específicos del sistema (para nuevos proyectos y para casos recurrentes) y deberá asegurar actualizaciones regulares a la información sobre evaluación de riesgos utilizando los resultados de auditorias, inspecciones e incidentes identificados.

9.2 Enfoque de Evaluación de Riesgos

OBJETIVO DE CONTROL
La Gerencia deberá establecer un enfoque general para la evaluación de riesgos que defina el alcance y los límites, la metodología a ser adoptada para las evaluaciones de riesgos, las responsabilidades y las habilidades requeridas. La calidad de las evaluaciones de riesgos deberá estar asegurada por un método estructurado y por asesores expertos en riesgos.

9.3 Identificación de Riesgos

OBJETIVO DE CONTROL
La evaluación de riesgos deberá enfocarse al examen de los elementos esenciales de riesgo, tales como activos, amenazas, elementos vulnerables, protecciones,

consecuencias y probabilidad de amenaza.

9.4 Medición de Riesgos

OBJETIVO DE CONTROL

El enfoque de la evaluación de riesgos deberá asegurar que el análisis de la información de identificación de riesgos genere como resultado una medida cuantitativa y/o cualitativa del riesgo al cual está expuesta el área examinada. Asimismo, deberá evaluarse la capacidad de aceptación de riesgos de la organización.

9.5 Plan de Acción contra Riesgos

OBJETIVO DE CONTROL

El enfoque de evaluación de riesgos deberá proporcionar la definición de un plan de acción contra riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continua.

9.6 Aceptación de Riesgos

OBJETIVO DE CONTROL

El enfoque de la evaluación de riesgos deberá asegurar la aceptación formal del riesgo residual, dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de qué tan económico resulte implementar protecciones y controles. El riesgo residual deberá compensarse con una cobertura de seguro adecuada.

10 Administración de proyectos

10.1 Marco de Referencia para la Administración de Proyectos

OBJETIVO DE CONTROL

La Gerencia deberá establecer un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de

responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.

10.2 Participación del Departamento Usuario en la Iniciación de Proyectos

OBJETIVO DE CONTROL

El marco de referencia de la administración de proyectos de la organización deberá fomentar la participación del departamento usuario afectado en la definición y autorización de cualquier proyecto de desarrollo, implementación o modificación.

10.3 Miembros y Responsabilidades del Equipo del Proyecto

OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá especificar las bases para asignar a los miembros del personal al proyecto y definir las responsabilidades y autoridades de los miembros del equipo del proyecto.

10.4 Definición del Proyecto

OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá generar la creación de un estatuto claro por escrito que defina la naturaleza y el alcance de cada proyecto de implementación antes de que los trabajos del mismo sean iniciados.

10.5 Aprobación del Proyecto

OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá asegurar que, para cada proyecto propuesto, la alta gerencia de la organización revise los reportes de los estudios de factibilidad relevantes como una base para fundamentar la decisión de proceder con el proyecto.

10.6 Aprobación de las Fases del Proyecto

OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá

disponer que los Gerentes designados para las funciones del usuario y de los servicios de información aprueben el trabajo realizado en cada fase del ciclo antes de iniciar los trabajos de la siguiente fase.

10.7 Plan Maestro del Proyecto

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que, para cada proyecto aprobado, se cree un plan maestro adecuado que mantenga el control del proyecto a través de todo su desarrollo e incluya un método de monitoreo del tiempo y los costos incurridos durante su vida.

10.8 Plan de Aseguramiento de la Calidad de Sistemas

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que la implementación de un sistema nuevo o modificado incluya la preparación de un plan de calidad que sea integrado posteriormente al plan maestro del proyecto y que sea formalmente revisado y acordado por todas las partes interesadas.

10.9 Planeación de Métodos de Aseguramiento

OBJETIVO DE CONTROL

Las tareas de aseguramiento deberán ser definidas durante la fase de planeación del marco de referencia de administración de proyectos. Las tareas de aseguramiento deberán apoyar la acreditación de sistemas nuevos o modificados y garantizar que los controles internos y los dispositivos de seguridad cumplan con los requerimientos necesarios.

10.10 Administración Formal de Riesgos de Proyectos

OBJETIVO DE CONTROL

La Gerencia deberá implementar un programa de administración formal de riesgos de proyectos para eliminar o minimizar los riesgos asociados con proyectos individuales (por ejemplo, identificación y control de áreas o eventos que tengan el potencial de causar cambios no deseados).

10.11 Plan de Prueba

OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá requerir la creación de un plan de pruebas para cada proyecto de desarrollo, implementación y modificación.

10.12 Plan de Entrenamiento

OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá requerir la creación de un plan de entrenamiento para cada proyecto de desarrollo, implementación y modificación.

10.13 Plan de Revisión Post – Implementación

OBJETIVO DE CONTROL

El marco de referencia de administración de proyectos de la organización deberá disponer que, como parte integral de las actividades del equipo del proyecto, se desarrolle un plan de revisión post - implementación para cada sistema de información nuevo o modificado, con la finalidad de determinar si el proyecto ha generado los beneficios planeados.

11 Administración de la calidad

11.1 Plan General de Calidad

OBJETIVO DE CONTROL

La alta gerencia deberá desarrollar y mantener regularmente un plan general de calidad basado en los planes organizacionales y de tecnología de información a largo plazo. El plan deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.

11.2 Enfoque de Aseguramiento de Calidad

OBJETIVO DE CONTROL

La Gerencia deberá establecer un enfoque estándar con respecto al aseguramiento

de calidad, que cubra tanto las actividades de aseguramiento de calidad generales como las específicas de un proyecto. El enfoque deberá determinar el (los) tipo(s) de actividades de aseguramiento de calidad (tales como revisiones, auditorias, inspecciones, etc.) que deben realizarse para alcanzar los objetivos del plan general de calidad. Asimismo deberá requerir una revisión específica de aseguramiento de calidad.

11.3 Planeación del Aseguramiento de Calidad

OBJETIVO DE CONTROL

La Gerencia deberá implementar un proceso de planeación de aseguramiento de calidad para determinar el alcance y la duración de las actividades de aseguramiento de calidad.

11.4 Revisión del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares y Procedimientos de la Función de Servicios de Información

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que las responsabilidades asignadas al personal de aseguramiento de calidad incluyan una revisión del cumplimiento general de los estándares y procedimientos de la función de servicios de información.

11.5 Metodología del Ciclo de Vida de Desarrollo de Sistemas

OBJETIVO DE CONTROL

La alta gerencia de la organización deberá definir e implementar estándares de sistemas de información y adoptar una metodología del ciclo de vida de desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información computarizados y tecnología afín. La metodología del ciclo de vida de desarrollo de sistemas elegida deberá ser la apropiada para los sistemas a ser desarrollados, adquiridos, implementados y mantenidos.

11.6 Metodología del Ciclo de Vida de Desarrollo de Sistemas para Cambios Mayores a la Tecnología Actual

OBJETIVO DE CONTROL

En el caso de requerirse cambios mayores a la tecnología actual, la Gerencia deberá asegurar el cumplimiento de la metodología del ciclo de vida de desarrollo de sistemas, como en el caso de adquisición de nueva tecnología.

11.7 Actualización de la Metodología del Ciclo de Vida de Desarrollo de Sistemas

OBJETIVO DE CONTROL

La alta gerencia deberá implementar una revisión periódica de su metodología del ciclo de vida de desarrollo de sistemas para asegurar que incluya técnicas y procedimientos actuales generalmente aceptados.

11.8 Coordinación y Comunicación

OBJETIVO DE CONTROL

La Gerencia deberá establecer un proceso para asegurar la coordinación y comunicación estrecha entre los clientes de la función de servicios de información y los implementadores de sistemas. Este proceso deberá ocasionar que los métodos estructurados que utilicen la metodología del ciclo de vida de desarrollo de sistemas aseguren la provisión de soluciones de tecnología de información de calidad que satisfagan las demandas de negocio. La Gerencia deberá promover una organización que se caracterice por la estrecha cooperación y comunicación a lo largo del ciclo de vida de desarrollo de sistemas.

11.9 Marco de Referencia de Adquisición y Mantenimiento para la Infraestructura de Tecnología

OBJETIVO DE CONTROL

Deberá establecerse un marco de referencia general referente a la adquisición y mantenimiento de la infraestructura de tecnología. Los diferentes pasos que deben ser seguidos con respecto a la infraestructura de tecnología (tales como adquisición; programación, documentación y pruebas; establecimiento de parámetros; mantenimiento y aplicación de correcciones) deberán estar regidos por y mantenerse en línea con el marco de referencia para la adquisición y mantenimiento de la infraestructura de tecnología.

11.10 Relaciones con Terceras Partes como Implementadores

OBJETIVO DE CONTROL

La Gerencia deberá implementar un proceso para asegurar las buenas relaciones de trabajo con terceras partes como implementadores externos. Dicho proceso deberá disponer que el usuario y el implementador estén de acuerdo sobre los criterios de aceptación, el manejo de cambios, los problemas durante el desarrollo, las funciones de los usuarios, las instalaciones, las herramientas, el software, los estándares y los procedimientos.

11.11 Estándares para la Documentación de Programas

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas deberá incorporar estándares para la documentación de programas que hayan sido impuestos y comunicados al personal interesado. La metodología deberá asegurar que la documentación creada durante el desarrollo del sistema de información o de los proyectos de modificación coincida con estos estándares.

11.12 Estándares para Pruebas de Programas

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proporcionar estándares que cubran los requerimientos de pruebas, verificación, documentación y retención para probar las unidades de software y los programas agregados, creados como parte de cada proyecto de desarrollo o modificación de sistemas de información.

11.13 Estándares para Pruebas de Sistemas

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proporcionar estándares que cubran los requerimientos de pruebas, verificación, documentación y retención para probar el sistema total, como parte de cada proyecto de desarrollo o modificación de sistemas de información.

11.14 Pruebas Piloto/En Paralelo

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe definir las condiciones bajo las cuales deberán conducirse las pruebas piloto o en

paralelo de sistemas nuevos y/o actuales.

11.15 Documentación de las Pruebas del Sistema

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe disponer, como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información, que se conserve la documentación de los resultados de las pruebas del sistema.

11.16 Evaluación del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares de Desarrollo

OBJETIVO DE CONTROL

El enfoque de aseguramiento de calidad de la organización deberá requerir que una revisión post - implementación de un sistema de información operacional evalúe si el equipo encargado del proyecto, cumplió con las estipulaciones de la metodología del ciclo de vida de desarrollo de sistemas.

11.17 Revisión del Aseguramiento de Calidad sobre el Logro de los Objetivos de la Función de Servicios de Información

OBJETIVO DE CONTROL

El enfoque de aseguramiento de calidad deberá incluir una revisión de hasta qué punto los sistemas particulares y las actividades de desarrollo de aplicaciones han alcanzado los objetivos de la función de servicios de información.

11.18 Métricas de calidad

OBJETIVO DE CONTROL

La gerencia deberá definir y utilizar métricas para medir los resultados de actividades, evaluando si las metas de calidad han sido alcanza-das.

11.19 Reportes de Revisiones de Aseguramiento de Calidad

OBJETIVO DE CONTROL

Los reportes de revisiones de aseguramiento de calidad deberán ser preparados y enviados a la Gerencia de los departamentos usuarios y de la función de servicios de

información.

II.4.3.2 DOMINIO ADQUISICION E IMPLEMENTACION

1. Identificación de soluciones

1.1 Definición de Requerimientos de Información

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que los requerimientos del negocio ya satisfechos por el sistema actual y a ser satisfechos por el sistema nuevo propuesto o modificado (software, datos e infraestructura), estén claramente definidos antes de aprobar cualquier proyecto de desarrollo, implementación o modificación. La metodología del ciclo de vida de desarrollo de sistemas deberá exigir que los requerimientos de las soluciones funcionales y operacionales sean especificados, incluyendo desempeño, protección, confiabilidad, compatibilidad, seguridad y legislación.

1.2 Formulación de Acciones Alternativas

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proveer el análisis de las acciones alternativas que deberán satisfacer los requerimientos del negocio, establecidos para un sistema nuevo o modificado.

1.3 Formulación de Estrategias de Adquisición

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular un plan de estrategia de adquisición, definiendo si el software será “adquirido del mostrador”, desarrollados internamente, a través de contratación o mediante una combinación de estos.

1.4 Requerimientos de Servicios de Terceros

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe

estipular la evaluación de requerimientos y las especificaciones para una Solicitud de Propuesta cuando se negocie con un proveedor de servicios externo.

1.5 Estudio de Factibilidad Tecnológica

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular un examen de factibilidad tecnológica de cada alternativa con la finalidad de satisfacer los requerimientos de negocio establecidos para el desarrollo de un proyecto propuesto de cualquier sistema nuevo o modificado.

1.6 Estudio de Factibilidad Económica

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe generar, en cada proyecto de desarrollo, implementación y modificación de sistemas de información propuesto, el análisis de los costos y beneficios asociados con cada alternativa considerada para satisfacer los requerimientos del negocio establecidos.

1.7 Arquitectura de Información

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que se tome en consideración el modelo de datos de la empresa al definir las soluciones y analizar la factibilidad de las mismas.

1.8 Reporte de Análisis de Riesgos

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar, en cada proyecto de desarrollo, implementación y modificación de sistemas de información propuesto, el análisis y la documentación de las amenazas a la seguridad, puntos de impacto y debilidad y protecciones factibles de seguridad y control interno, con la finalidad de reducir o eliminar el riesgo identificado. Esto deberá llevarse a cabo en línea con el marco de referencia general de evaluación de riesgos.

1.9 Controles de Seguridad Económicos

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que los costos y beneficios de seguridad sean examinados cuidadosamente en términos monetarios y no monetarios, para garantizar que los costos de los controles no excedan a los beneficios. La decisión requerirá la firma de aprobación formal de la Gerencia.

1.10 Diseño de Pistas de Auditoría

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que existan mecanismos adecuados para pistas de auditoría o que dichos mecanismos puedan ser desarrollados para la solución identificada y seleccionada. Los mecanismos deberán proporcionar la capacidad de proteger datos sensitivos (ej. identificación de usuarios contra divulgación o mal uso)

1.11 Ergonomía

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que los proyectos de desarrollo, implementación y cambios emprendidos por la función de servicios de información, tomen en consideración los aspectos ergonómicos asociados con la introducción de soluciones automatizadas.

1.12 Selección del Software del Sistema

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que la función de servicios de información cumpla con un procedimiento estándar para identificar todos los programas de software potenciales que deberán satisfacer sus requerimientos operacionales.

1.13 Control de Abastecimiento

OBJETIVO DE CONTROL

La Gerencia deberá desarrollar e implementar un enfoque central de abastecimientos que describa un conjunto común de procedimientos y estándares a ser seguidos en la adquisición de hardware, software y servicios relacionados con la tecnología de información. Los productos deberán ser revisados y probados antes de su utilización y pago.

1.14 Adquisición de Productos de Software

OBJETIVO DE CONTROL

La adquisición de productos de software deberá seguir las políticas de adquisición de la organización.

1.15 Mantenimiento de Software de Terceras Partes

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que, para el software con licencia adquirido a terceras partes, los proveedores cuenten con los procedimientos apropiados para validar, proteger y mantener los derechos de integridad de los productos de software. Deberá tomarse en consideración el soporte del producto en cualquier acuerdo de mantenimiento relacionado con el producto entregado.

1.16 Contratos de Programación de Aplicaciones

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que los servicios de programación contratados estén justificados con una solicitud de servicios por escrito por parte de un miembro designado de la función de servicios de información. El contrato deberá estipular que el software, la documentación y otros elementos entregables estén sujetos a pruebas y revisiones antes de ser aceptados. Además, deberá asegurar que los productos finales terminados por los servicios de programación contratados sean revisados y probados de acuerdo con los estándares definidos por el grupo de aseguramiento de calidad de la función de servicios de información y otras partes interesadas (como usuarios, administradores de proyecto, etc.) antes de pagar por el trabajo y aprobar el producto final. Las pruebas que deberán ser incluidas en las especificaciones del contrato deberán consistir en pruebas del sistema, pruebas de integración, pruebas de hardware y componentes, pruebas de procedimientos, pruebas de carga y estrés,

pruebas de afinación y desempeño, pruebas de regresión, pruebas de aceptación del usuario y, finalmente, pruebas piloto del sistema total, con la finalidad de evitar fallas no esperadas del mismo.

1.17 Aceptación de Instalaciones

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que, dentro del contrato con el proveedor, se acuerde un plan de aceptación para las instalaciones a ser proporcionadas, el cual defina los procedimientos y criterios de aceptación. Además, deberán llevarse a cabo pruebas de aceptación para garantizar que el acomodo y el medio cumplan con los requerimientos especificados en el contrato.

1.18 Aceptación de Tecnología

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que, dentro del contrato con el proveedor, se acuerde un plan de aceptación para la tecnología específica a ser proporcionada, el cual defina los procedimientos y criterios de aceptación. Además, las pruebas de aceptación establecidas en el plan, deberán incluir inspección, pruebas de funcionalidad y seguimiento de cargas de trabajo.

2 Adquisición y mantenimiento de software de aplicaciones

2.1 Métodos de Diseño

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular que sean aplicados a técnicas y procedimientos apropiados, incluyendo una estrecha relación con los usuarios del sistema, en la creación de las especificaciones de diseño para cada nuevo proyecto de desarrollo de sistemas de información, y verificar las especificaciones del diseño contra los requerimientos del usuario.

2.2 Cambios Significativos a Sistemas Actuales

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que, en caso de presentarse la necesidad de realizar modificaciones significativas a los sistemas actuales, se siga un proceso de

desarrollo similar al utilizado en el desarrollo de sistemas nuevos.

2.3 Aprobación del Diseño

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización requerirá que las especificaciones de diseño para todos los proyectos de desarrollo y modificación de sistemas de in-formación, sean revisados y aprobados por la Gerencia, por los departamentos usuarios afectados y por la alta gerencia de la organización, cuando esto sea pertinente.

2.4 Definición y Documentación de Requerimientos de Archivos

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar la aplicación de un procedimiento apropiado para la definición y documentación del formato de los archivos para cada proyecto de desarrollo y modificación de sistemas de información. Este procedimiento deberá garantizar el respeto a las reglas de diccionario de datos.

2.5 Especificaciones de Programas

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir la preparación de especificaciones detalladas por escrito, de los programas para cada proyecto de desarrollo o modificación de sistemas de información. Además, la metodología deberá garantizar que las especificaciones de los programas correspondan a las especificaciones del diseño del sistema.

2.6 Diseño para la Recopilación de Datos Fuente

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir la especificación de mecanismos adecuados, para la recopilación y entrada de datos para cada proyecto de desarrollo y modificación de sistemas de información.

2.7 Definición y Documentación de Requerimientos de Entrada de Datos

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que existan mecanismos adecuados para definir y documentar los requerimientos de entrada de datos para cada proyecto de desarrollo o modificación de sistemas de información.

2.8 Definición de Interfases

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular que se especifiquen, diseñen y documenten apropiadamente todas las interfases internas y externas.

2.9 Interfase Usuario-Máquina

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar el desarrollo de una interfase entre el usuario y la máquina fácil de utilizar y que sea capaz de auto documentarse (por medio de funciones de ayuda en línea).

2.10 Definición y Documentación de Requerimientos de Procesamiento

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que existan mecanismos adecuados para definir y documentar los requerimientos de procesamiento para cada proyecto de desarrollo o modificación de sistemas de información.

2.11 Definición y Documentación de Requerimientos de Salida de Datos

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que existan mecanismos adecuados para definir y documentar los requerimientos de salida de datos para cada proyecto de desarrollo o modificación de sistemas de información

2.12 Controlabilidad

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que se especifiquen mecanismos adecuados, para garantizar que se identifiquen los requerimientos de seguridad y control internos para cada proyecto de desarrollo o modificación de sistemas de información. La metodología deberá asegurar además que los sistemas de información estén diseñados para incluir controles de aplicación que garanticen que los datos de entrada y salida estén completos, así como su precisión, oportunidad y autorización. Deberá llevarse a cabo una evaluación de sensibilidad durante el inicio del desarrollo o modificación del sistema. Los aspectos básicos de seguridad y control interno de un sistema a ser desarrollado o modificado deberán ser evaluados junto con el diseño conceptual del mismo, con el fin de integrar los conceptos de seguridad en el diseño tan pronto como sea posible.

2.13 Disponibilidad como Factor Clave de Diseño

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que la disponibilidad sea considerada en el proceso de diseño de nuevos o modificados sistemas de información en la fase más temprana posible. La disponibilidad debe ser analizada y, en caso necesario, incrementada a través de mejoras de mantenimiento y confiabilidad.

2.14 Consideraciones de Integridad de Tecnología para Software de Programas de Aplicación

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para asegurar, cuando esto aplique, que los programas de aplicación contengan estipulaciones que verifiquen rutinariamente las tareas realizadas por el software, para apoyar el asegura-miento de la integridad de los datos y el cual haga posible la restauración de la integridad a través de procedimientos de recuperación en reversa u otros medios.

2.15 Pruebas de Software de Aplicación

OBJETIVO DE CONTROL

Deberán aplicarse pruebas unitarias, pruebas de aplicación, pruebas de integración y pruebas de carga y estrés, de acuerdo con el plan de prueba del proyecto y con los estándares de pruebas establecidos antes de ser aprobado por el usuario. Se deberán aplicar adecuadas medidas de seguridad para prevenir divulgación de información sensitiva durante las pruebas.

2.16 Materiales de Consulta y Soporte para Usuarios

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se preparen manuales de referencia y soporte para usuarios adecuados (preferiblemente en formato electrónico) como parte de cada proyecto de desarrollo o modificación de sistemas de información.

2.17 Reevaluación del Diseño del Sistema

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que el diseño del sistema sea reevaluado siempre que ocurran discrepancias técnicas y/o lógicas durante el desarrollo o mantenimiento del sistema.

3 Adquisición y mantenimiento de arquitectura tecnológica

3.1 Evaluación de Nuevo Hardware y Software

OBJETIVO DE CONTROL

Deberán establecerse procedimientos para evaluar el impacto de nuevo hardware y software sobre el rendimiento del sistema en general.

3.2 Mantenimiento Preventivo para Hardware

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá calendarizar el mantenimiento rutinario y periódico del hardware con el fin de reducir la frecuencia y el impacto de fallas de rendimiento.

3.3 Seguridad del Software del Sistema

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que la instalación del software del sistema no arriesgue la seguridad de los datos y programas ya almacenados en el mismo. Deberá ponerse gran atención a la instalación y mantenimiento de los parámetros del software del sistema.

3.4 Instalación del Software del Sistema

OBJETIVO DE CONTROL

Deberán implementarse procedimientos para asegurar que el software del sistema sea instalado de acuerdo al marco de referencia de adquisición y mantenimiento de infraestructura de tecnología. Las pruebas deberán ser llevadas a cabo antes de autorizarse su utilización en ambiente de producción.

3.5 Mantenimiento del Software del Sistema

OBJETIVO DE CONTROL

Deberán implementarse procedimientos para asegurar que el software del sistema sea mantenido de acuerdo al marco de referencia de adquisición y mantenimiento para infraestructura de tecnología.

3.6 Controles para Cambios del Software del Sistema

OBJETIVO DE CONTROL

Deberán implementarse procedimientos para asegurar que las modificaciones realizadas al software del sistema sean controladas de acuerdo con los procedimientos de administración de cambios de la organización.

4 Desarrollo y mantenimiento de procedimientos relacionados con tecnologías de información

4.1 Requerimientos Operacionales y Niveles de Servicios Futuros

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar la definición oportuna de requerimientos operacionales y niveles de servicios futuros.

4.2 Manual de Procedimientos para Usuario

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se preparen y actualicen manuales adecuados de procedimientos para los usuarios como parte de cada proyecto de desarrollo o modificación de sistemas de información.

4.3 Manual de Operaciones

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se prepare y se mantenga actualizado un manual de operaciones adecuado como parte de cada proyecto de desarrollo o modificación de sistemas de información.

4.4 Material de Entrenamiento

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se desarrollen materiales de entrenamiento adecuados como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información. Estos materiales deberán enfocarse al uso del sistema en la práctica diaria.

5 Instalación y acreditación de sistemas

5.1 Entrenamiento

OBJETIVO DE CONTROL

El personal de los departamentos usuarios afectados y el grupo de operaciones de la función de servicios de información deberán estar entrenados de acuerdo al plan de entrenamiento definido y los materiales relacionados, como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información.

5.2 Adecuación del Desempeño del Software de Aplicación

OBJETIVO DE CONTROL

La medición (optimización) del desempeño del software de aplicación deberá establecerse como una parte integral de la metodología del ciclo de vida de desarrollo de sistemas de la organización para predecir los recursos requeridos para operar software nuevo o significativamente modificado.

5.3 Conversión

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar, como parte de cada proyecto de desarrollo, implementación o modificación de sistemas de información, que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo de acuerdo con el plan preestablecido.

5.4 Pruebas de Cambios

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que los cambios sean probados por un grupo de prueba independiente (distinto al de los desarrolladores) de acuerdo con la evaluación de impacto y recursos en un ambiente de prueba separado antes de comenzar su uso en el ambiente de operación regular. También deberán desarrollarse planes de respaldo externo. Las pruebas de aceptación deberán llevarse a cabo en un ambiente representativo del ambiente operacional futuro (por ejemplo, condiciones similares de seguridad, controles internos, cargas de trabajo, etc.)

5.5 Criterios y Desempeño de Pruebas en Paralelo/Piloto

OBJETIVO DE CONTROL

Deben establecerse procedimientos para asegurar que las pruebas piloto o en paralelo sean llevadas a cabo de acuerdo con un plan preestablecido y que los criterios para la terminación del proceso de pruebas sean especificados con anterioridad.

5.6 Prueba de Aceptación Final

OBJETIVO DE CONTROL

Los procedimientos deberán asegurar, como partes de las pruebas de aceptación final o de aseguramiento de calidad de sistemas de información nuevos o modificados, una evaluación y aprobación formal de los resultados de las pruebas por parte de la Gerencia de los departamentos usuarios afectados y de la función de servicios de información. Las pruebas deben cubrir todos los componentes del sistema de información (software de aplicación, instalaciones, tecnología, procedimientos de usuarios).

5.7 Pruebas y Acreditación de Seguridad

OBJETIVO DE CONTROL

La Gerencia deberá definir e implementar procedimientos para asegurar que la Gerencia de operaciones y la Gerencia usuaria aceptan formalmente los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.

5.8 Prueba Operacional

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que, antes de poner el sistema en operación, el usuario o custodio designado (la parte designada para correr el sistema en nombre del usuario), valide su operación como un producto completo, bajo condiciones similares a las del ambiente de aplicación y en la manera en la que el sistema será operado en un ambiente de producción.

5.9 Paso a Producción

OBJETIVO DE CONTROL

La Gerencia deberá definir e implementar procedimientos formales para controlar la entrega del sistema de desarrollo a pruebas y a operación. Los ambientes respectivos deberán separarse y protegerse apropiadamente.

5.10 Evaluación de la Satisfacción de los Requerimientos del Usuario

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que se realice una revisión post - implementación de los requerimientos operacionales del sistema de información (por ejemplo, capacidad, desempeño de procesamiento a través del sistema etc.) con el fin de evaluar si las necesidades del usuario están siendo satisfechas por el mismo.

5.11 Revisión Gerencial Post – Implementación

OBJETIVO DE CONTROL

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que una revisión post - implementación del sistema de información operacional evalúe y reporte si el sistema proporcionó los beneficios esperados de la manera más económica.

6 Administración de cambios

6.1 Inicio y Control de Requisiciones de Cambio

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que todas las requisiciones de cambios tanto internos como por parte de proveedores estén estandarizados y sujetos a procedimientos formales de administración de cambios. Las solicitudes deberán categorizarse, priorizarse y establecerse procedimientos específicos para manejar asuntos urgentes. Los solicitantes de cambios deben permanecer informados acerca del estatus de su solicitud.

6.2 Evaluación del Impacto

OBJETIVO DE CONTROL

Deberá establecerse un procedimiento para asegurar que todas las requisiciones de cambio sean evaluadas en una forma estructurada en cuanto a todos los posibles impactos sobre el sistema operacional y su funcionalidad.

6.3 Control de Cambios

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que la administración de cambios, así como el control y la distribución de software sean integrados apropiadamente en un sistema completo de administración de configuración.

6.4 Documentación y Procedimientos

OBJETIVO DE CONTROL

El procedimiento de cambios deberá asegurar que, siempre que se implementen modificaciones a un sistema, la documentación y procedimientos relacionados sean actualizados de manera correspondiente.

6.5 Mantenimiento Autorizado

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que el personal de mantenimiento tenga asignaciones específicas y que su trabajo sea monitoreado apropiadamente. Además, sus derechos de acceso al sistema deberán ser controlados para evitar riesgos de accesos no autorizados a los sistemas automatizados.

6.6 Política de Liberación de Software

OBJETIVO DE CONTROL

La Gerencia deberá garantizar que la liberación de software esté regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.

6.7 Distribución de Software

OBJETIVO DE CONTROL

Deberán establecerse medidas de control específicas para asegurar la distribución del elemento de software correcto al lugar correcto, con integridad y de manera oportuna con pistas de auditoría adecuadas.

II.4.3.3 DOMINIO ENTREGA DE SERVICIOS Y SOPORTE

1. Definición de niveles de servicio

1.1 Marco de Referencia para el Convenio de Nivel de Servicio

OBJETIVO DE CONTROL

La alta gerencia deberá establecer un marco de referencia en donde presente la definición de los convenios sobre niveles formales de servicio y determine el contenido mínimo: disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia/Recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio. Los usuarios y la función de servicios de información deberán contar con un convenio escrito que describa el nivel de servicio en términos cualitativos y cuantitativos. El convenio definirá las responsabilidades de ambas partes. La función de servicios de información deberá prestar la calidad y la cantidad de servicios ofrecida y los usuarios deberán ajustar los servicios solicitados a los límites acordados.

1.2 Aspectos sobre los Convenios de Nivel de Servicio

OBJETIVO DE CONTROL

Deberá lograrse un acuerdo explícito sobre los aspectos que el convenio de nivel de servicios deberá tener. El convenio de nivel de servicio deberá cubrir por lo menos los siguientes aspectos: disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados a los usuarios, plan de contingencia/ Recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambios

1.3 Procedimientos de Desempeño

OBJETIVO DE CONTROL

Deberán definirse procedimientos que aseguren que la manera y responsabilidades sobre las relaciones que rigen el desempeño (por ejemplo, convenios de

confidencialidad) entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.

1.4 Monitoreo y Reporte

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá designar a un Gerente de nivel de servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento. Las estadísticas de monitoreo deberán ser analizadas oportunamente. Deberán tomarse acciones correctivas apropiadas e investigarse las fallas.

1.5 Revisión de Convenios y Contratos de Nivel de Servicio

OBJETIVO DE CONTROL

La Gerencia deberá implementar un proceso de revisión regular de los convenios de nivel de servicio y de los contratos de proveedores de servicios como terceras partes.

1.6 Elementos sujetos a Cargo

OBJETIVO DE CONTROL

Deberán incluirse provisiones para elementos sujetos a cargo en los acuerdos de niveles de servicio para hacer posible comparaciones y decisiones de niveles de servicio contra su costo.

1.7 Programa de Mejoramiento del Servicio

OBJETIVO DE CONTROL

La Gerencia deberá implementar un proceso para asegurar que los usuarios y los Gerentes de nivel de servicio concuerden regularmente en un programa de mejoramiento del servicio con el fin de dar seguimiento a mejoras al nivel de servicio cuyo costo esté justificado.

2 Administración de servicios prestados por terceros

2.1 Interfases con Proveedores

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que todos los servicios prestados por terceros sean propiamente identificados y que las interfaces técnicas y organizacionales con los proveedores sean documentadas.

2.2 Relaciones de Dueños

Objetivos de Control

La Gerencia de la organización del cliente deberá designar un dueño que sea responsable de asegurar la calidad de las relaciones con terceros.

2.3 Contratos con Terceros

OBJETIVO DE CONTROL

La gerencia debe definir procedimientos específicos para asegurar que un contrato formal sea definido y acordado para cada relación de servicio con un proveedor.

2.4 Calificación de Terceros

OBJETIVO DE CONTROL

La gerencia debe asegurar en forma previa a su selección, que los terceros potenciales cuentan con las calificaciones adecuadas a través de una evaluación de su capacidad para proporcionar los servicios requeridos.

2.5 Contratos con Fuentes Externas

OBJETIVO DE CONTROL

Deberán definirse procedimientos organizacionales específicos para asegurar que el contrato entre la organización y el proveedor de la administración de instalaciones esté basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.

2.6 Continuidad de Servicios

OBJETIVO DE CONTROL

Con respecto al aseguramiento de la continuidad de los servicios, la gerencia deberá considerar el riesgo de negocios relacionado con la participación de terceros en términos de incertidumbre legal y con el concepto de interés sobre la continuidad y negociar contratos en depósito.

2.7 Relaciones de Seguridad

OBJETIVO DE CONTROL

Con respecto a las relaciones con los proveedores de servicios como terceras partes, la Gerencia deberá asegurar que los acuerdos de seguridad (por ejemplo, los acuerdos de no - revelación) sean identificados, declarados explícitamente y acordados, que éstos concuerden con los estándares de negocios universales y estén en línea con los requerimientos legales y regulatorios, incluyendo obligaciones.

2.8 Monitoreo

OBJETIVO DE CONTROL

La Gerencia deberá establecer un proceso continuo de monitoreo sobre la prestación de servicio de terceros, con el fin de asegurar el cumplimiento de los acuerdos del contrato.

3 Administración de desempeño y capacidad

3.1 Requerimientos de Disponibilidad y Desempeño

OBJETIVO DE CONTROL

El proceso de administración deberá asegurar que las necesidades de negocio con respecto a disponibilidad y desempeño de los servicios de información sean identificados y convertidas en requerimientos y términos de disponibilidad.

3.2 Plan de Disponibilidad

OBJETIVO DE CONTROL

La Gerencia deberá asegurar el establecimiento de un plan de disponibilidad para alcanzar, monitorear y controlar la disponibilidad de los servicios de información.

3.3 Monitoreo y Reporte

OBJETIVO DE CONTROL

La Gerencia deberá implementar un proceso que asegure que el desempeño de los recursos de tecnología de información sea continuamente monitoreado y que las excepciones sean reportadas de manera oportuna y completa.

3.4 Herramientas de Modelado

OBJETIVO DE CONTROL

La gerencia deberá asegurar que se utilicen las herramientas de modelado apropiadas para producir un modelo del sistema actual, calibrado y ajustado según la carga de trabajo real y que sea preciso dentro de los niveles de carga recomendados. Las herramientas de modelado deberán utilizarse para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de la configuración, desempeño y disponibilidad. Deberán llevarse a cabo investigaciones técnicas profundas sobre el hardware de los sistemas y deberán incluirse pronósticos acerca de futuras tecnologías.

3.5 Manejo Proactivo del Desempeño

OBJETIVO DE CONTROL

El proceso de administración del desempeño deberá incluir la capacidad de pronóstico para permitir que los problemas sean solucionados antes de que éstos afecten el desempeño del sistema. Deberán llevarse a cabo análisis de las fallas e irregularidades del sistema en cuanto a frecuencia, grado del impacto y magnitud del daño.

3.6 Pronóstico de Carga de Trabajo

OBJETIVO DE CONTROL

Deberán establecerse controles para asegurar que se preparen pronósticos de carga de trabajo con el fin de identificar tendencias y proporcionar la información necesaria para el plan de capacidad.

3.7 Administración de Capacidad de Recursos

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá establecer un proceso de planeación para la revisión del desempeño y capacidad del hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar las cargas de trabajo acordadas y para proporcionar la cantidad y calidad de desempeño requeridas, prescritas en los acuerdos de nivel de servicio. El plan de capacidad deberá cubrir escenarios múltiples.

3.8 Disponibilidad de Recursos

OBJETIVO DE CONTROL

La gerencia deberá prevenir que se pierda la disponibilidad de los recursos, mediante la implementación de mecanismos de tolerancia de fallas, mecanismos de asignación equitativa de recursos y la definición de prioridades de tareas.

3.9 Calendarización de Recursos

OBJETIVO DE CONTROL

La Gerencia deberá asegurar la adquisición oportuna de la capacidad requerida, tomando en cuenta aspectos como resistencia, contingencia, cargas de trabajo y planes de almacenamiento.

4 Asegurar la continuidad del servicio

4.1 Marco de Referencia de Continuidad de Tecnología de información

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá crear un marco de referencia de continuidad que defina los roles, responsabilidades, el enfoque basado en riesgo /la metodología a seguir y las reglas y la estructura para documentar el plan, así como los procedimientos de aprobación.

4.2 Estrategia y Filosofía de Continuidad de Tecnología de Información

OBJETIVO DE CONTROL

La Gerencia deberá garantizar que el Plan de continuidad de tecnología de información se encuentra en línea con el plan general de continuidad de la empresa para asegurar consistencia. Aún más, el plan de continuidad de TI debe tomar en consideración el plan a mediano y largo plazo de tecnología de información, con el fin de asegurar consistencia.

4.3 Contenido del Plan de Continuidad de Tecnología de Información

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que se desarrolle un plan escrito conteniendo lo siguiente:

Guías sobre la utilización del Plan de Continuidad;

- Procedimientos de emergencia para asegurar la integridad de todo el personal afectado;
- Procedimientos de respuesta definidos para regresar al negocio al estado en que se encontraba antes del incidente o desastre;
- Procedimientos para salvaguardar y reconstruir las instalaciones;
- Procedimientos de coordinación con las autoridades públicas;
- Procedimientos de comunicación con los interesados: empleados, clientes clave, proveedores críticos, accionistas y gerencia; y
- Información crítica sobre grupos de continuidad, personal afectado, clientes, proveedores, autoridades públicas y medios de comunicación.

4.4 Minimización de requerimientos de Continuidad de Tecnología de Información

OBJETIVO DE CONTROL

La Gerencia de servicios de información deberá establecer procedimientos y guías para minimizar los requerimientos de continuidad con respecto a personal, instalaciones, hardware, software, equipo, formatos, consumibles y mobiliario.

4.5 Mantenimiento Plan de Continuidad de Tecnología de Información

OBJETIVO DE CONTROL

La Gerencia de servicios de información deberá proveer procedimientos de control

de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja requerimientos de negocio actuales. Esto requiere de procedimientos de mantenimiento del plan de continuidad alineados con el cambio, la administración y los procedimientos de recursos humanos.

4.6 Pruebas del Plan de Continuidad de Tecnología de Información

OBJETIVO DE CONTROL

Para contar con un Plan efectivo de Continuidad, la gerencia necesita evaluar su adecuación de manera regular; esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas e implementar un plan de acción de acuerdo con los resultados.

4.7 Capacitación sobre el Plan de Continuidad de Tecnología de Información

OBJETIVO DE CONTROL

La metodología de Continuidad para desastres deberá asegurar que todas las partes interesadas reciban sesiones de entrenamiento regulares con respecto a los procedimientos a ser seguidos en caso de un incidente o un desastre.

4.8 Distribución del Plan de Continuidad de Tecnología de Información

OBJETIVO DE CONTROL

Debido a la naturaleza sensitiva de la información del plan de continuidad, dicha información deberá ser distribuida solo a personal autorizado y mantenerse bajo adecuadas medidas de seguridad para evitar su divulgación. Consecuentemente, algunas secciones del plan deberán ser distribuidas solo a las personas cuyas actividades hagan necesario conocer dicha información.

4.9 Procedimientos de respaldo de procesamiento para Departamentos usuarios

OBJETIVO DE CONTROL

La metodología de continuidad deberá asegurar que los departamentos usuarios establezcan procedimientos alternativos de procesamiento, que puedan ser utilizados hasta que la función de servicios de información sea capaz de restaurar completamente sus servicios después de un evento o un desastre.

4.10 Recursos Críticos de Tecnología de Información

OBJETIVO DE CONTROL

El plan de continuidad deberá identificar los programas de aplicación, servicios de terceros, sistemas operativos, personal, insumos, archivos de datos que resultan críticos así como los tiempos necesarios para la recuperación después de que se presenta un desastre.

4.11 Centro de cómputo y Hardware de Respaldo

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que la metodología de continuidad incorpora la identificación de alternativas relativas al centro de cómputo y al hardware de respaldo, así como una selección alternativa final. En caso de aplicar, deberá establecerse un contrato formal para este tipo de servicios.

4.12 Procedimiento de refinamiento del Plan de Continuidad

OBJETIVO DE CONTROL

Dada una exitosa reanudación de la función de servicios de información después de un desastre, la gerencia de servicios de información deberá establecer procedimientos para evaluar lo adecuado del plan y actualizarlo de acuerdo con los resultados de dicha evaluación.

5 Garantizar la seguridad de sistemas

5.1 Administrar Medidas de Seguridad

OBJETIVO DE CONTROL

La seguridad en Tecnología de Información deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye:

- traducir información sobre evaluación de riesgos a los planes de seguridad de tecnología;
- implementar el plan de seguridad de tecnología de información;

- actualizar el plan de seguridad de tecnología de información para reflejar cambios en la configuración de tecnología;
- evaluar el impacto de solicitudes de cambio en la seguridad de tecnología de información;
- monitorear la implementación del plan de seguridad de tecnología de información; y
- alinear los procedimientos de seguridad de tecnología de información a otras políticas y procedimientos

5.2 Identificación, Autenticación y Acceso

OBJETIVO DE CONTROL

El acceso lógico y el uso de los recursos de TI deberán restringirse a través de la instrumentación de un mecanismo adecuado de autenticación de usuarios identificados y recursos asociados con las reglas de acceso. Dicho mecanismo deberá evitar que personal no autorizado, conexiones telefónicas de marcado y otros puertos de entrada del sistema (redes) tengan acceso a los recursos de cómputo, de igual forma deberá mini-mizar la necesidad de firmas de entrada múltiples a ser utilizadas por usuarios autorizados. Asimismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso (por ejemplo, cambios periódicos de contraseñas o passwords).

5.3 Seguridad de Acceso a Datos en Línea

OBJETIVO DE CONTROL

En un ambiente de tecnología de información en línea, la Gerencia de la función de servicios de información deberá implementar procedimientos acordes con la política de seguridad que garantiza el control de la seguridad de acceso, tomando como base las necesidades individuales demostradas de visualizar, agregar, modificar o eliminar datos.

5.4 Administración de Cuentas de Usuario

OBJETIVO DE CONTROL

La Gerencia deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario. Deberá incluirse un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.

5.5 Revisión Gerencial de Cuentas de Usuario

OBJETIVO DE CONTROL

La Gerencia deberá contar con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso.

5.6 Control de Usuarios sobre Cuentas de Usuario

OBJETIVO DE CONTROL

Los usuarios deberán controlar en forma sistemática la actividad de su(s) propia(s) cuenta(s). También se deberán establecer mecanismos de información para permitirles supervisar la actividad normal, así como alertarlos oportunamente sobre actividades inusuales.

5.7 Vigilancia de Seguridad

OBJETIVO DE CONTROL

La administración de seguridad de la función de servicios de información debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente al administrador y que las acciones consecuentes sean tomadas en forma automática.

5.8 Clasificación de Datos

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que todos los datos son clasificados en términos de sensitividad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación. Aún los datos que requieran “no protección” deberán contar con una decisión formal que les asigne dicha clasificación.

5.9 Clasificación de Datos

OBJETIVO DE CONTROL

Deben existir controles para asegurar que la identificación y los derechos de acceso

de los usuarios, así como la identidad del sistema y la propiedad de los datos, son establecidos y administrados de forma única y centralizada, para obtener consistencia y eficiencia de un control global de acceso.

5.10 Reportes de Violación y de Actividades de Seguridad

OBJETIVO DE CONTROL

La administración de la función de servicios de información deberá asegurar que las violaciones y la actividad de seguridad sean registradas, reportadas, revisadas y escaladas apropiadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas. El acceso lógico a la información sobre el registro de recursos de cómputo (seguridad y otros registros) deberá otorgarse tomando como base el principio de menor privilegio (necesidad de saber).

5.11 Manejo de Incidentes

OBJETIVO DE CONTROL

La Gerencia deberá implementar la capacidad de manejar incidentes de seguridad computacional, dar atención a dichos incidentes mediante el establecimiento de una plataforma centralizada con suficiente experiencia y equipada con instalaciones de comunicación rápidas y seguras. Deberán establecerse las responsabilidades y los procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna a los incidentes de seguridad.

5.12 Re-acreditación

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que se lleve a cabo periódicamente una reacreditación de seguridad por ejemplo, a través de equipos de personal técnico *"tigre"* con el fin de conservar al día el nivel de seguridad aprobado formalmente y la aceptación del riesgo residual.

5.13 Confianza en Contrapartes

OBJETIVO DE CONTROL

Las políticas organizacionales deberán asegurar que se instrumenten prácticas de control para verificar la autenticidad de las contrapartes que proporcionan instrucciones o transacciones electrónicas. Esto puede lograrse mediante el

intercambio confiable de passwords, dispositivos de seguridad o llaves criptográficas.

5.14 Autorización de transacciones

OBJETIVO DE CONTROL

Las políticas organizacionales deberán asegurar que, en donde sea apropiado, sean instrumentados controles para proporcionar autenticidad de transacciones. Esto requiere el empleo de técnicas criptográficas para “firmar” y verificar transacciones.

5.15 No negación

OBJETIVO DE CONTROL

Las políticas organizacionales deberán asegurar que, en donde sea apropiado, las transacciones no puedan ser negadas por ninguna de las partes y que se instrumenten controles para proporcionar no negación *(non repudiatio*n) de origen o destino, prueba de envío *(proof of submissio*n), y recibo de transacciones. Esto puede ser implementado a través de firmas digitales, registro de tiempos y terceros confiables.

5.16 Sendero Seguro

OBJETIVO DE CONTROL

Las políticas organizacionales deberán asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales o senderos seguros *(trusted path*s). La información sensitiva incluye: información sobre administración de seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas. Para lograr esto, se pueden establecer canales confiables mediante el encriptamiento entre usuarios, entre usuarios y sistemas y entre sistemas.

5.17 Protección de funciones de seguridad

OBJETIVO DE CONTROL

Todo el hardware y software relacionado con seguridad debe encontrarse permanentemente protegido contra intromisiones para proteger su integridad y contra divulgación de sus claves secretas. Adicionalmente, la organización deberá mantener discreción sobre el diseño de su seguridad, pero no basar la seguridad en

mantener el diseño como secreto.

5.18 Administración de Llaves Criptográficas

OBJETIVO DE CONTROL

La Gerencia deberá definir e implementar procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas contra modificaciones y divulgación no autorizada. Si una llave se encuentra comprometida (en riesgo), la gerencia deberá asegurarse de que esta información se hace llegar a todas las partes interesadas a través de un listado de revocación de certificados o mecanismos similares.

5.19 Prevención, Detección y Corrección de Software “Malicioso”

OBJETIVO DE CONTROL

Con respecto al software malicioso, tal como los virus computacionales o *Caballos de Troya*, la Gerencia deberá establecer un marco de referencia de adecuadas medidas de control preventivas, detectivas y correctivas.

5.20 Arquitectura de *Fire Walls* y conexión a redes públicas

OBJETIVO DE CONTROL

Si existe conexión con Internet u otras redes públicas en la organización. Se deberá contar con sistemas *Fire Wall* adecuados para proteger en contra de negación de servicios y cualquier acceso no autorizado a los recursos internos; deberá controlar en ambos sentidos cualquier flujo de administración de infraestructura y de aplicaciones y deberá proteger en contra de negación o ataques de servicio.

5.21 Protección de Valores Electrónicos

OBJETIVO DE CONTROL

La Gerencia debe proteger consistentemente la integridad de todas las tarjetas o dispositivos físicos similares, que son utilizados para autenticación o almacenamiento de información financiera u otra información sensitiva, tomando en consideración las instalaciones relacionadas, dispositivos, empleados y métodos de validación utiliza-dos.

6 Identificación y asignación de costos

6.1 Elementos Sujetos a Cargo

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que los elementos sujetos a cargo sean identificables, medibles y predecibles para los usuarios. Los usuarios deberán ser capaces de controlar el uso de los servicios de información y de los niveles de facturación asociados.

6.2 Procedimientos de Costeo

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá definir e implementar procedimientos de costeo para proporcionar información gerencial acerca del costo de prestar servicios de información, asegurando al mismo tiempo la economía. Las variaciones entre los costos pronosticados y los reales deberán ser analizadas adecuadamente y reportados, con el fin de facilitar el monitoreo de los mismos. Además, la alta gerencia deberá evaluar periódicamente los resultados de los procedimientos de contabilidad de costos de la función de servicios de información, a la luz de los otros sistemas de medición financiera de la organización.

6.3 Procedimientos de Cargo y Facturación a Usuarios

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá definir y utilizar procedimientos de cargo y facturación. Esta deberá mantener procedimientos de cargo y facturación que fomenten el uso apropiado de los recursos de cómputo y aseguren el trato justo de los departamentos usuarios y sus necesidades. El monto cargado deberá reflejar los costos asociados con la prestación de servicios.

7 Educación y entrenamiento de usuarios

7.1 Identificación de Necesidades de Entrena-miento

OBJETIVO DE CONTROL

En línea con el plan a largo plazo, la Gerencia deberá establecer y mantener procedimientos para identificar y documentar las necesidades de entrenamiento de

todo el personal que haga uso de los servicios de información. Deberá establecerse un currículo de entrenamiento para cada grupo de empleados.

7.2 Organización del Entrenamiento

OBJETIVO DE CONTROL

Tomando como base las necesidades identificadas, la Gerencia deberá definir los grupos objetivo, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento. Asimismo, deberán investigarse las alternativas de entrenamiento (Localidad interna o externa, entrenadores internos o externos, etc.).

7.3 Entrenamiento sobre Principios y Conciencia de Seguridad

OBJETIVO DE CONTROL

Todo el personal deberá estar capacitado y entrenado en los principios de seguridad de sistemas. La alta gerencia deberá proporcionar un programa de educación y entrenamiento que incluya: conducta ética de la función de servicios de información, prácticas de seguridad para proteger de una manera segura contra daños que afecten la disponibilidad, la confidencialidad la integridad y el desempeño de las tareas.

8 Apoyo y asistencia a los clientes de tecnologías e información

8.1 Buró de Ayuda

OBJETIVO DE CONTROL

Deberá establecerse un soporte para usuarios dentro de una función de buró de ayuda. Las personas responsables de llevar a cabo esta función deberán interactuar estrechamente con el personal de manejo de problemas.

8.2 Registro de Preguntas del Usuario

OBJETIVO DE CONTROL

Deberán establecerse procedimientos para asegurar que todas las preguntas de los clientes sean registradas adecuadamente por el buró de ayuda.

8.3 Escalamiento de Preguntas del Cliente

OBJETIVO DE CONTROL

Los procedimientos del buró de ayuda deberán asegurar que las preguntas de los clientes que no puedan ser resueltas inmediatamente sean reasignadas apropiadamente dentro de la función de servicios de información hasta el nivel adecuado para atenderlas.

8.4 Monitoreo de Atención a Clientes

OBJETIVO DE CONTROL

La Gerencia deberá establecer procedimientos para monitorear oportunamente la atención a las preguntas de los clientes. Las preguntas que permanezcan pendientes por largo tiempo deberán ser investigadas y atendidas.

8.5 Análisis y Reporte de Tendencias

OBJETIVO DE CONTROL

Deberán establecerse procedimientos que aseguren el reporte adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias. Los reportes deberán ser analizados y sus resultados deberán ser atendidos adecuadamente.

9 Administración de la configuración

9.1 Registro de la Configuración

OBJETIVO DE CONTROL

Deberán establecerse procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de la adquisición. Por otra parte, deberán establecerse procedimientos para dar seguimiento a los cambios en la configuración (nuevo elemento, cambio de estatus de desarrollo a prototipo). El registro en bitácoras y el control deberán ser una parte integrada del sistema de registro de configuración, incluyendo revisiones de registros modificados.

9.2 Configuración Base

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurarse de que exista una configuración base de elementos como punto de verificación al cual regresar después de las modificaciones.

9.3 Registro de Estatus

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que los registros de configuración reflejen el estatus real de todos los elementos de la configuración incluyendo la historia de los cambios.

9.4 Control de la Configuración

OBJETIVO DE CONTROL

Los procedimientos deberán asegurar que la existencia y consistencia del registro de la configuración de la función de servicios de información sean revisadas periódicamente.

9.5 Software no Autorizado

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá revisar periódicamente la existencia de software no autorizado en las computadoras personales de la organización.

9.6 Almacenamiento de Software

OBJETIVO DE CONTROL

Deberá definirse un área de almacenamiento de archivos (biblioteca) para todos los elementos de software válidos en las fases apropiadas del ciclo de vida de desarrollo de sistemas. Estas áreas deberán estar separadas unas de otras y de las áreas de almacenamiento de archivos de desarrollo, pruebas y producción.

10 Administración de problemas e incidentes

10.1 Sistema de Administración de Problemas

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá definir e implementar un sistema de administración de problemas para asegurar que todos los eventos operacionales que no formen parte de la operación estándar (incidentes, problemas y errores) sean registrados, analizados y resueltos oportunamente. Deberán emitirse reportes de incidentes en el caso de problemas significativos.

10.2 Escalamiento de Problemas

OBJETIVO DE CONTROL

La Gerencia deberá definir e implementar procedimientos de escalamiento de problemas para asegurar que los problemas identificados sean resueltos oportunamente de la manera más eficiente. Estos procedimientos deberán asegurar que las prioridades sean establecidas apropiadamente. Los procedimientos también deberán documentar el procedimiento de escalamiento para la activación del plan de continuidad de tecnología de información.

10.3 Seguimiento de Problemas y Pistas de Auditoría

OBJETIVO DE CONTROL

El sistema de administración de problemas deberá proporcionar elementos adecuados para pistas de auditoría que permitan el seguimiento de las causas a partir de un incidente (por ejemplo, liberación de paquetes o implementación de cambios urgentes) y viceversa. Deberá trabajar estrechamente con la administración de cambios, la administración de disponibilidad y la administración de configuración.

11 Administración de datos

11.1 Procedimientos de Preparación de Datos

OBJETIVO DE CONTROL

La Gerencia deberá establecer procedimientos de preparación de datos a ser seguidos por los departamentos usuarios. En este contexto, el diseño de formas de entrada de datos deberá ayudar a minimizar los errores y las omisiones. Durante la

creación de los datos, los procedimientos de manejo de errores deberán asegurar razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.

11.2 Procedimientos de Autorización de Documentos Fuente

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que los documentos fuente sean preparados apropiadamente por personal autorizado que actúa dentro de su autoridad, y que se establezca una separación de funciones adecuada con respecto al origen y aprobación de documentos fuente.

11.3 Recopilación de Datos de Documentos Fuente

OBJETIVO DE CONTROL

Los procedimientos de la organización deberán asegurar que todos los documentos fuente autorizados estén completos, sean precisos, registrados apropiadamente y transmitidos oportunamente para la entrada de datos.

11.4 Manejo de errores de documentos fuente

OBJETIVO DE CONTROL

Los procedimientos de manejo de errores durante la creación de datos deberán asegurar razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.

11.5 Retención de Documentos Fuente

OBJETIVO DE CONTROL

Deberán establecerse procedimientos para asegurar que la organización pueda retener o reproducir los documentos fuente originales durante un período de tiempo razonable para facilitar la recuperación o reconstrucción de datos, así como para satisfacer requerimientos legales.

11.6 Procedimientos de Autorización de Entrada de Datos

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos apropiados para asegurar que la

entrada de datos sea llevada a cabo únicamente por personal autorizado.

11.7 Chequeos de Exactitud, Suficiencia y Autorización

OBJETIVO DE CONTROL

Los datos sobre transacciones, capturados para su procesamiento (generados por personas, por sistemas o entradas de interfase) deberán estar sujetos a una variedad de controles para verificar su exactitud, suficiencia y validez. Asimismo, deberán establecerse procedimientos para asegurar que los datos de entrada sean validados y editados tan cerca del punto de origen como sea posible.

11.8 Manejo de Errores en la Entrada de Datos

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para la corrección y reenvío de datos que hayan sido capturados erróneamente.

11.9 Integridad de Procesamiento de Datos

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para el procesamiento de datos que aseguren que la segregación de funciones sea mantenida y que el trabajo realizado sea verificado rutinariamente. Los procedimientos deberán asegurar que se establezcan controles de actualización adecuados como totales de control "corrida a corrida" y controles de actualización de archivos maestros.

11.10 Validación y Edición de Procesamiento de Datos

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para asegurar que la validación, autenticación y edición del procesamiento sean llevadas a cabo tan cerca del punto de origen como sea posible. Cuando se utilicen sistemas de Inteligencia Artificial, dichos sistemas serán ubicados en una infraestructura de control interactiva con operadores humanos para asegurar que las decisiones vitales son aprobadas.

11.11 Manejo de Errores en el Procesamiento de Datos

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos de manejo de errores en el procesamiento de datos que permitan la identificación de transacciones erróneas sin que éstas sean procesadas y sin interrumpir el procesamiento de otras transacciones válidas.

11.12 Manejo y Retención de Datos de Salida

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para el manejo y la retención de datos de salida de sus programas de aplicación de tecnología de información. En caso de que instrumentos negociables (ej. tarjetas de valor) sean los receptores de la salida, se deberá poner cuidado especial en prevenir usos inadecuados.

11.13 Distribución de Datos de Salida

OBJETIVO DE CONTROL

La organización deberá establecer y comunicar procedimientos escritos para la distribución de datos de salida de tecnología de información.

11.14 Balanceo y Conciliación de Datos de Salida

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para asegurar que los datos de salida sean balanceados rutinariamente con los totales de control relevantes. Deberán existir pistas de auditoría para facilitar el seguimiento del procesamiento de transacciones y la conciliación de los datos con problema.

11.15 Revisión de Datos de Salida y Manejo de Errores

OBJETIVO DE CONTROL

La Gerencia de la organización deberá establecer procedimientos para asegurar que la precisión de los reportes de los datos de salida sea revisada por el proveedor y por los usuarios relevantes. Asimismo, deberán establecerse procedimientos para controlar los errores contenidos en los datos de salida.

11.16 Provisiones de Seguridad para Reportes de Salida

OBJETIVO DE CONTROL

La organización deberá establecer procedimientos para garantizar que la seguridad de los reportes de datos de salida sea mantenida para todos aquellos reportes que estén por distribuirse, así como para todos aquéllos que ya hayan sido distribuidos a los usuarios.

11.17 Protección de Información Sensible durante transmisión y transporte

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que durante la transmisión y transporte de información sensible, se proporcione una adecuada protección contra acceso o modificación no autorizada, así como contra envíos a direcciones erróneas.

11.18 Protección de Información Crítica a Ser Des-echada

OBJETIVO DE CONTROL

La Gerencia deberá definir e implementar procedimientos para impedir la divulgación indebida o el desecho de información delicada de la organización. Tales procedimientos deberán garantizar que ninguna información marcada como “borrada” o “desechada”, pueda ser accedida por personas internas o externas a la organización.

11.19 Administración de Almacenamiento

OBJETIVO DE CONTROL

Deberán desarrollarse procedimientos para el almacenamiento de datos que consideren requerimientos de recuperación, de economía y las políticas de seguridad.

11.20 Períodos de Retención y Términos de Almacenamiento

OBJETIVO DE CONTROL

Deberán definirse los períodos de retención y los términos de almacenamiento para documentos, datos, programas, reportes y mensajes (de entrada y de salida), así como los datos (claves, certificados) utilizados para su encriptamiento y autenticación.

11.21 Sistema de Administración de la Librería de Medios

OBJETIVO DE CONTROL

La función de servicios de información deberá establecer procedimientos para asegurar que el contenido de su librería de medios sea inventariado sistemáticamente, que cualquier discrepancia revelada por un inventario físico sea solucionada oportunamente y que se lleven a cabo las medidas necesarias para mantener la integridad de los medios magnéticos almacenados en la librería.

11.22 Responsabilidades de la Administración de la Librería de Medios

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá establecer procedimientos de administración para proteger el contenido de la librería de medios. Deberán definirse estándares para la identificación externa de medios magnéticos y el control de su movimiento y almacenamiento físico para soportar su seguimiento y registro. Las responsabilidades sobre el manejo de la librerías de medios (cintas magnéticas, cartuchos, discos y disquetes) deberán ser asignadas a miembros específicos del personal de servicios de información.

11.23 Respaldo y Restauración

OBJETIVO DE CONTROL

La Gerencia deberá implementar una estrategia apropiada de respaldo y restauración para asegurar que ésta incluya una revisión de los requerimientos del negocio, así como el desarrollo, implementación, prueba y documentación del plan de recuperación. Se deberán establecer procedimientos para asegurar que los respaldos satisfagan los requerimientos mencionados anteriormente.

11.24 Funciones de Respaldo

OBJETIVO DE CONTROL

Deberán establecerse procedimientos para asegurar que los respaldos sean realizados de acuerdo con la estrategia de respaldo definida, y que su utilidad sea verificada regularmente.

11.25 Almacenamiento de Respaldos

OBJETIVO DE CONTROL

Los procedimientos de respaldo para los medios relacionados con tecnología de información deberán incluir el almacenamiento apropiado de los archivos de datos, del software y de la documentación relacionada, tanto dentro como fuera de las instalaciones. Los respaldos deberán ser almacenados con seguridad y las instalaciones de almacenamiento deberán ser revisadas periódicamente con respecto a la seguridad de acceso físico y la seguridad de los archivos de datos y otros elementos.

11.26 Archivo

OBJETIVO DE CONTROL

La Gerencia deberá implementar una política y procedimientos para asegurar que el archivo cumple con requerimientos legales y de negocio y que se encuentra debidamente protegido y registrado adecuadamente.

11.27 Protección de Mensajes Sensitivos

OBJETIVO DE CONTROL

Con respecto a la transmisión de datos a través de Internet u otra red pública, la Gerencia deberá definir e implementar procedimientos y protocolos para ser utilizados para el aseguramiento de la integridad, confidencialidad y “no negación” de mensajes sensitivos.

11.28 Autenticación e Integridad

OBJETIVO DE CONTROL

Previamente a que alguna acción crítica sea tomada sobre información originada fuera de la Organización que se reciba vía teléfono, correo de voz, documentos (en papel), fax o correo electrónico, se deberá verificar adecuadamente la autenticidad e integridad de dicha información.

11.29 Integridad de Transacciones Electrónicas

OBJETIVO DE CONTROL

Tomando en consideración que las fronteras tradicionales de tiempo y de geografía son me-nos precisas y confiables, la Gerencia deberá definir e implementar apropiados procedimientos y prácticas para transacciones electrónicas que sean sensitivas y críticas para la Organización, asegurando la integridad y autenticidad de:

- *atomicidad* (unidad de trabajo indivisible, todas sus acciones tienen éxito o todas ellas fallan)
- *consistencia* (si la transacción no logra alcanzar un estado final estable, deberá regresar al sistema a su estado inicial);
- *aislamiento* (el comportamiento de una transacción no es afectado por otras transacciones que se ejecutan concurrentemente); y
- *durabilidad* (los efectos de una transacción son permanentes después que concluye su proceso, los cambios que origina deben sobrevivir fallas de sistema)

11.30 Integridad Continua de Datos Almacenados

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que la integridad y lo adecuado de los datos mantenidos en archivos y otros medios (ej. tarjetas electrónicas) se verifique periódicamente. Atención específica deberá darse a dispositivos de valor, archivos de referencia y archivos que contengan información privada.

12 Administración de instalaciones

12.1 Seguridad Física

OBJETIVO DE CONTROL

Deberán establecerse apropiadas medidas de seguridad física y control de acceso para las instalaciones de tecnología de información de acuerdo con la política de seguridad general, incluyendo el uso de dispositivos de información fuera de las instalaciones. El acceso deberá restringirse a las personas que hayan sido autorizadas a contar con dicho acceso.

12.2 Discreción de las Instalaciones de Tecnología de Información

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que se lleve un bajo perfil ó discreción y que la identificación física de las instalaciones relacionadas con sus operaciones de tecnología de información sea limitada.

12.3 Escolta de Visitantes

OBJETIVO DE CONTROL
Deberán establecerse procedimientos apropiados que aseguren que las personas que no formen parte del grupo de operaciones de la función de servicios de información sean escoltadas por algún miembro de ese grupo cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes.

12.4 Salud y Seguridad del Personal

OBJETIVO DE CONTROL
Deberán establecerse y mantenerse prácticas de salud y seguridad en línea con las leyes y regulaciones internacionales, nacionales, regionales, estatales y locales.

12.5 Protección contra Factores Ambientales

OBJETIVO DE CONTROL
La Gerencia de la función de servicios de información deberá asegurar que se establezcan y mantengan las suficientes medidas para la protección contra los factores ambientales (por ejemplo, fuego, polvo, electricidad, calor o humedad excesivos). Deberán instalarse equipo y dispositivos especializados para monitorear y controlar el ambiente.

12.6 Suministro Ininterrumpido de Energía

OBJETIVO DE CONTROL
La Gerencia deberá evaluar regularmente la necesidad de generadores y baterías de suministro ininterrumpido de energía para las aplicaciones críticas de tecnología de información, con el fin de asegurarse contra fallas y fluctuaciones de energía. Cuando sea justificable, deberá instalarse el equipo más apropiado.

13 Administración de operaciones

13.1 Manual de procedimientos de Operación e Instrucciones

OBJETIVO DE CONTROL

La función de servicios de información deberá establecer y documentar procedimientos estándar para las operaciones de tecnología de información (incluyendo operaciones de red). Todas las soluciones y plataformas de tecnología de información establecidas deberán ser operadas utilizando estos procedimientos, los cuales deberán ser revisados periódicamente para asegurar su efectividad y cumplimiento.

13.2 Documentación del Proceso de Inicio y de Otras Operaciones

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que el personal de operaciones esté adecuadamente familiarizado y se sienta seguro con las tareas del proceso de inicio y con otras operaciones al tenerlas documentadas y al ser éstas probadas y ajustadas periódicamente según se requiera.

13.3 Calendarización de Trabajos

OBJETIVO DE CONTROL

La Gerencia de la función de servicios de información deberá asegurar que la calendarización continua de trabajos, procesos y tareas sea organizada en la secuencia más eficiente, maximizando el proceso y la utilización, con el fin de alcanzar los objetivos establecidos en los convenios de nivel de servicio. Las caledarizaciones iniciales así como los cambios a estas caledarizaciones deberán ser autorizados apropiadamente.

13.4 Salidas de la Calendarización de Trabajos Estándar

OBJETIVO DE CONTROL

Deberán establecerse procedimientos para identificar, investigar y aprobar las salidas de calendarización de trabajos estándar.

13.5 Continuidad de Procesamiento

OBJETIVO DE CONTROL

Los procedimientos deberán requerir continuidad de procesamiento durante los cambios de turno de operadores mediante la existencia de un paso o entrega formal de actividades, actualizaciones y reportes de estatus sobre las responsabilidades actuales.

13.6 Bitácoras de Operación

OBJETIVO DE CONTROL

Los controles de la Gerencia deberán garantizar que se esté almacenando suficiente información cronológica en bitácoras de operaciones para permitir la reconstrucción, la revisión y el examen oportunos de las secuencias de tiempo de procesamiento y otras actividades que lo rodean y soportan.

13.7 Operaciones Remotas

OBJETIVO DE CONTROL

Para las operaciones remotas, deberán existir procedimientos específicos que aseguren que la conexión y desconexión de los enlaces con la(s) instalación(es) remota(s) sean identificadas e implementadas.

II.4.3.4 DOMINIO MONITOREO

1. Monitoreo del proceso

1.1 Recolección de Datos de Monitoreo

OBJETIVO DE CONTROL

Para los procesos de tecnología de información y de control interno, la Gerencia deberá asegurar que se definan indicadores de desempeño relevantes (ej. comparaciones externas) tanto para actividades internas como las proporcionadas por terceros y que se recolecten datos para la creación de reportes relevantes de desempeño y reportes de excepción relacionados con estos indicadores.

1.2 Evaluación de Desempeño

OBJETIVO DE CONTROL

Los servicios a ser proporcionados por la función de servicios de información deberán ser medidos (indicadores clave de desempeño y/o factores críticos de éxito) y comparados con los niveles objetivo. Las evaluaciones a la función de servicios de información deberán ser desarrolladas en forma continua.

1.3 Evaluación de la satisfacción de Clientes

OBJETIVO DE CONTROL

A intervalos regulares, la Gerencia deberá efectuar mediciones de la satisfacción de los clientes con respecto a los servicios proporcionados por la función de servicios de información, con la intención de identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento.

1.4 Reportes Gerenciales

OBJETIVO DE CONTROL

Deberán proporcionarse reportes gerenciales para ser revisados por la alta gerencia en cuanto al avance de la organización hacia las metas identificadas. Con base en la revisión, la Gerencia deberá iniciar y controlar las acciones pertinentes.

2 Evaluar lo adecuado del control interno

2.1 Monitoreo de Control Interno

OBJETIVO DE CONTROL

La Gerencia deberá monitorear la efectividad de los controles internos en el curso normal de las operaciones a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias. Las desviaciones deberán evocar análisis y acciones correctivas.

2.2 Operación Oportuna de Controles Internos

OBJETIVO DE CONTROL

La confiabilidad en los controles internos requiere que los controles operen rápidamente para resaltar errores e inconsistencias y que éstos sean corregidos antes de que impacten a la producción y a la prestación de servicios. La información relacionada con los errores, inconsistencias y excepciones deberá ser conservada y reportada sistemáticamente a la Gerencia.

2.3 Reporte sobre el Nivel de Control Interno

OBJETIVO DE CONTROL

La Gerencia deberá reportar información sobre niveles de control interno y excepciones a las partes afectadas para asegurar la efectividad continua de su sistema de control interno. Deberán llevarse a cabo acciones para identificar qué información es requerida a un nivel particular de toma de decisiones.

2.4 Seguridad de Operación y Aseguramiento de Control Interno

OBJETIVO DE CONTROL

La garantía de seguridad operacional y el aseguramiento de control interno deberán ser establecidos a través de una “auto auditoria” o de una auditoría independiente para examinar si la seguridad y los controles internos se encuentran operando de acuerdo con los requerimientos de seguridad y control interno establecidos o implícitos. Las actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

3 Obtención de aseguramiento independiente

3.1 Certificación / Acreditación Independiente de Control y Seguridad de los servicios de TI

OBJETIVO DE CONTROL

La Gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos y obtener re-certificaciones o reacreditaciones de estas actividades en forma una cíclica rutinaria después de haber hecho la implementación.

3.2 Certificación / Acreditación Independiente de Control y Seguridad de proveedores externos de servicios

OBJETIVO DE CONTROL

La Gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de utilizar proveedores de servicios de tecnología de información y obtener re-certificaciones o re-acreditaciones de estas actividades en forma cíclica rutinaria.

3.3 Evaluación Independiente de la Efectividad de los Servicios de TI

OBJETIVO DE CONTROL

La Gerencia deberá obtener una evaluación independiente sobre la efectividad de los servicios de tecnología de información en forma cíclica rutinaria.

3.4 Evaluación Independiente de la Efectividad de proveedores externos de servicios

OBJETIVO DE CONTROL

La Gerencia deberá obtener una evaluación independiente sobre la efectividad de los proveedores de servicios de tecnología de información en forma cíclica rutinaria.

3.5 Aseguramiento Independiente del Cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales

OBJETIVO DE CONTROL

La Gerencia deberá obtener un aseguramiento independiente sobre el cumplimiento de la función de servicios de tecnología de información con respecto a requerimientos regulatorios y compromisos contractuales en forma cíclica rutinaria.

3.6 Aseguramiento Independiente del Cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales de proveedores externos de servicios

OBJETIVO DE CONTROL

La Gerencia deberá obtener un aseguramiento independiente sobre el cumplimiento de proveedores externos de servicios de tecnología de información con respecto a requerimientos regulatorios y compromisos contractuales en forma cíclica rutinaria.

3.7 Competencia de la Función de Aseguramiento Independiente

OBJETIVO DE CONTROL

La Gerencia deberá asegurarse de que la función de aseguramiento independiente posee competencia técnica, habilidades y conocimiento necesario para desempeñar dicha función en una forma efectiva, eficiente y económica.

3.8 Participación Proactiva de Auditoría

OBJETIVO DE CONTROL

La Gerencia de Tecnología de Información deberá buscar la participación de auditoría en una forma proactiva, antes de finalizar soluciones de servicio de tecnología de información.

4 Proveer auditoria independiente

4.1 Estatutos de Auditoría

OBJETIVO DE CONTROL

La alta gerencia de la organización deberá establecer los estatutos para la función de auditoría. Este documento deberá establecer la responsabilidad, autoridad y obligaciones de la función de auditoría. Asimismo este documento deberá ser revisado periódicamente para asegurar que se mantengan la independencia, autoridad y responsabilidad de la función de auditoría.

4.2 Independencia

OBJETIVO DE CONTROL

El auditor deberá ser independiente del auditado tanto en actitud como en apariencia (real y percibida). Los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado, y en la medida de lo posible, deberá también ser independiente de la propia empresa. De esta manera, la función de auditoría deberá ser suficientemente independiente del área auditada para concluir una auditoría en forma objetiva.

4.3 Ética y Estándares Profesionales

OBJETIVO DE CONTROL

La función de auditoría deberá asegurar el cumplimiento de los códigos aplicables de ética profesional (ej. Código de Ética de la *Information Systems Audit and Control Associatio*n) y estándares de auditoría (ej. Estándares de la *Information Systems Audit and Control Associatio*n) en todo lo que lleve a cabo. El debido cuidado profesional deberá observarse en todos los aspectos del trabajo de auditoría, incluyendo el respeto de estándares aplicables sobre auditoría y tecnología de información.

4.4 Competencia

OBJETIVO DE CONTROL

La Gerencia deberá asegurar que los auditores responsables de las revisiones de las actividades de la función de servicios de información de la organización, sean técnicamente competentes y cuentan en forma general con las habilidades y conocimientos (ej. dominios de CISA) necesarios para desempeñar dichas revisiones en forma efectiva, eficiente y económica. La Gerencia deberá asegurar que el personal asignado a tareas de auditoría de sistemas de información, mantiene su nivel de competencia técnica mediante un programa adecuado de educación profesional continua.

4.5 Planeación

OBJETIVO DE CONTROL

La alta gerencia deberá establecer un plan de auditoría para garantizar que se obtenga un aseguramiento regular e independiente con respecto a la efectividad, eficiencia y economía de la seguridad y de los procedimientos de control interno, así como de la habilidad de la Gerencia para controlar las actividades de la función de servicios de información. Dentro de este plan la Gerencia deberá determinar las prioridades relacionadas con la obtención de aseguramiento independiente. Los auditores deberán planear el trabajo de auditoría para alcanzar los objetivos de auditoría y cumplir con los estándares profesionales correspondientes.

4.6 Ejecución del Trabajo de Auditoría

OBJETIVO DE CONTROL

Las auditorias deberán ser supervisadas apropiadamente para proporcionar certeza de que los objetivos de auditoría están siendo alcanzados y que los estándares profesionales de auditoría que sean aplicables están siendo observados. Los auditores deberán asegurarse de obtener evidencia suficiente, confiable, relevante y útil para alcanzar los objetivos de auditoría de forma efectiva. Los hallazgos y conclusiones de auditoría deben estar soportadas por un análisis apropiado y una correcta interpretación de esta evidencia.

4.7 Reporte

OBJETIVO DE CONTROL

La función de auditoría de la organización deberá proporcionar un reporte en un formato adecuado, para todo el personal interesado una vez concluida su revisión. El reporte de auditoría deberá mostrar los objetivos de la auditoría, el período de cobertura y la naturaleza y extensión de trabajo de auditoría realizado. El reporte deberá identificar a la Organización, los destinatarios del informe y cualquier restricción en su circulación. El reporte de auditoría deberá también mostrar los hallazgos, conclusiones y recomendaciones relacionadas con el trabajo de auditoría llevado a cabo, así como cualquier salvedad o comentario que el auditor tenga con respecto a la auditoría.

4.8 Actividades de Seguimiento

OBJETIVO DE CONTROL

La resolución acerca de los comentarios sobre la auditoría depende de la Gerencia. Los auditores deberán solicitar y evaluar información pertinente sobre hallazgos, conclusiones y recomendaciones previos para determinar si las acciones apropiadas han sido implementadas de manera oportuna.

Capítulo III : Marco Metodológico

III.1 Tipo de Investigación

En la presente investigación se aplicó el método de investigación descriptivo, con el fin de describir situaciones, eventos y hechos relacionados con la administración del riesgo en el área de tecnologías de información; esto se logro a través de la recopilación de información y la aplicación de entrevistas y cuestionarios.

Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis (Danhke, 1989). Miden, evalúan o recolectan datos sobre diversos aspectos, dimensiones o componentes del fenómeno a investigar. Desde el punto de vista científico, describir es recolectar datos (para los investigadores cuantitativos, medir; y para los cualitativos, recolectar información). Esto es, en un estudio descriptivo se selecciona una serie de cuestiones y se mide o recolecta información sobre cada una de ellas, para así describir lo que se investiga (Hernández, S. y otros, 1998).

Además se aplicó el método de investigación exploratorio, el cuál permitió ir más allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre conceptos relacionados con la administración del riesgo en el área de tecnologías de información.

III.2 Sujetos

Se aplica la investigación a una muestra de ocho municipalidades, tres ministerios, tres instituciones autónomas, cuatro entidades financieras, la Contraloría General de la República, el Tribunal Supremo de Elecciones.

III.3 Descripción del lugar y organizaciones donde se realiza la labor

Este trabajo de investigación se lleva a cabo en las instituciones del sector público costarricense, ubicadas dentro del área metropolitana, y propiamente en las áreas de tecnologías de información de cada organización.

III.4 Selección de la muestra

La muestra seleccionada para la investigación, corresponde a encargados, directores o jefes de las áreas de tecnologías de información de organizaciones del sector público costarricense, de las cuales se seleccionó en forma aleatoria aproximadamente un 15%.

A continuación se listan las Instituciones del Sector Público Costarricense seleccionadas para aplicar entrevistas, y cuestionarios con el fin de medir el grado de aplicación del control interno y administración del riesgo en actividades, funciones y procesos de tecnologías de información.

Instituciones del Sector Público Costarricense	Cantidad
Municipalidades	8
Instituciones Autónomas	2
Ministerios	5
Banca Nacional	4
Otros	3
Total	22

Municipalidades

- Municipalidad de Cartago
- Municipalidad de San José
- Municipalidad de Heredia
- Municipalidad de Limón
- Municipalidad de Puntarenas
- Municipalidad de Guanacaste
- Municipalidad de Alajuela
- Municipalidad de Montes de Oca

Instituciones Autónomas

- Consejo Nacional de Rehabilitación y Educación Especial
- Instituto Sobre Alcoholismo y Fármaco dependencia

Ministerios

- Ministerio de Educación Pública
- Ministerio de Salud
- Ministerio de Agricultura y Ganadería
- Ministerio de Hacienda
- Ministerio de Industria Economía y Comercio

Banca Nacional

- Banco Nacional de Costa Rica
- Banco Popular y de Desarrollo Comunal
- Banco Crédito Agrícola
- Banco Central de Costa Rica

Otros

- Contraloría General de la República
- Tribunal Supremo de Elecciones
- Corte

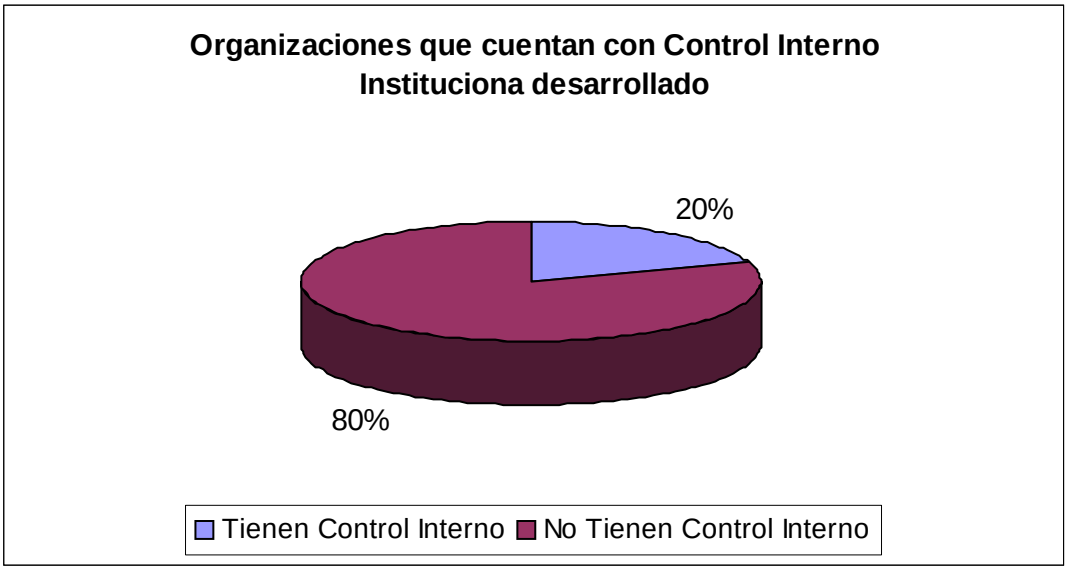
III.5 Instrumentos para el análisis de la información

La información se obtuvo a través de la aplicación de entrevistas, cuestionarios, a los encargados, directores o jefes de las áreas de tecnologías de información de las organizaciones del sector público costarricense, con el fin de medir el grado de aplicación del control interno y administración del riesgo en actividades, funciones y procesos de tecnologías de información.

Capítulo IV : Análisis e interpretación de resultados

A pesar de la publicación de la Ley 8292 Ley General de Control Interno, publicada el 4 de setiembre del 2002, donde se establecen los criterios que deben seguir la Contraloría General de la República y los entes u órganos sujetos a su fiscalización, en el establecimiento, funcionamiento, mantenimiento, perfeccionamiento y evaluación de sus sistemas de control interno; actualmente solo el 20% de las organizaciones consultadas cuentan con un sistema de control interno institucional acorde con las nuevas normas generales de control interno implementadas por la Contraloría General de la República para las entidades y órganos sujetos a su fiscalización.

Gráfico N°1



Fuente: Organizaciones del sector público costarricense consultadas

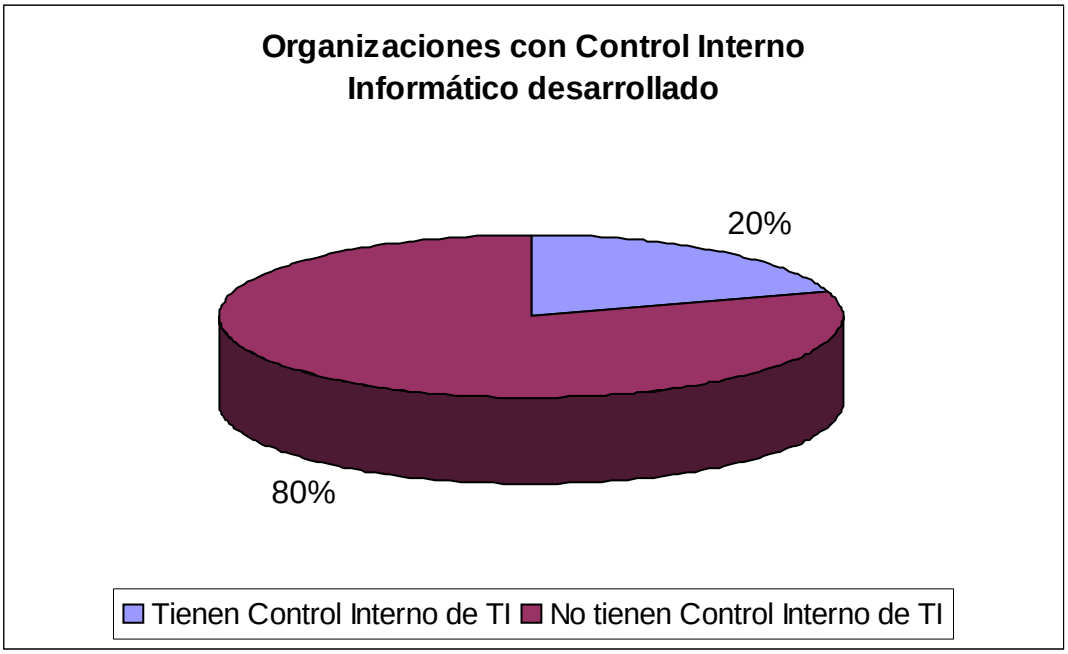
El control interno debe ser aplicado en todas las áreas de la organización con el fin de proporcionar una seguridad razonable en torno a la consecución de los objetivos de la organización, fundamentalmente para proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal; confiabilidad y oportunidad de la información; eficiencia y eficacia de las operaciones y cumplir con el ordenamiento jurídico y técnico.

El control interno informático deberá ser una función del departamento de informática de una organización cuyo; objetivo es el de controlar que todas las actividades relacionadas a los sistemas de información automatizados se realicen cumpliendo las normas, políticas, estándares, procedimientos y disposiciones legales establecidas.

En relación a la consulta si la organización cuenta con un sistema de control interno informático, se desprende que actualmente el 80% de las organizaciones del sector público

costarricense no cuentan con un sistema de control interno informático.

Gráfico Nº2

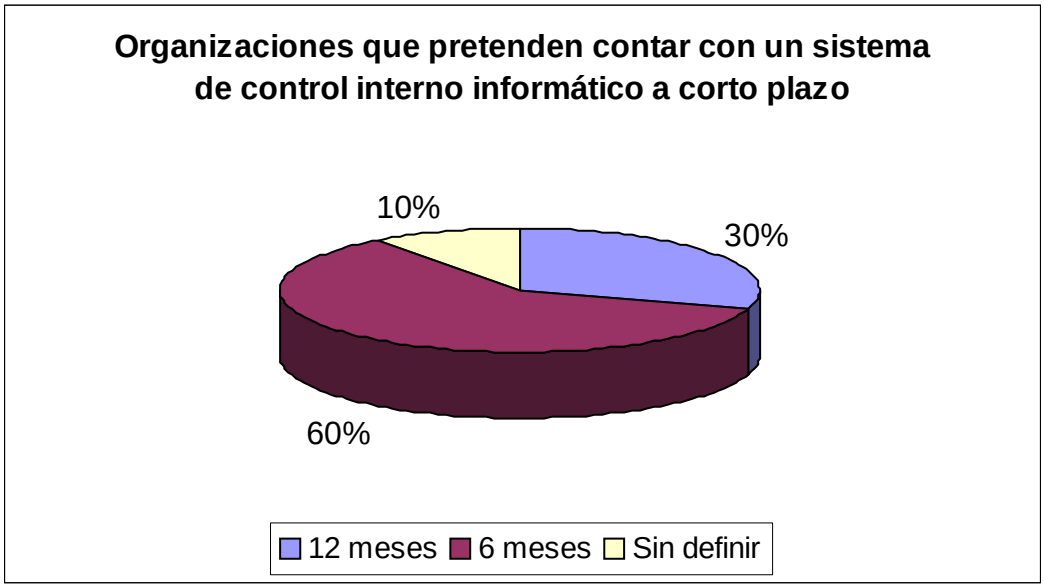


Fuente: Organizaciones del sector público costarricense consultadas

Las organizaciones del sector público costarricense deben desarrollar un control interno informático como sistema integrado al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados.

Del 80% de las organizaciones que actualmente no cuentan con un sistema de control interno informático, se les consultó en relación a cuanto tiempo les llevará contar con el sistema de control interno informático desarrollado, desprendiéndose que el 60% de las organizaciones pretenden contar el sistema de control interno informático en los próximos 12 meses, un 30% respondió que pretenden contar con el sistema de control interno informático dentro de 6 meses, y solo el 10% de las organizaciones consultadas respondió que aún no han planificado el desarrollo del control interno informático.

Gráfico Nº3

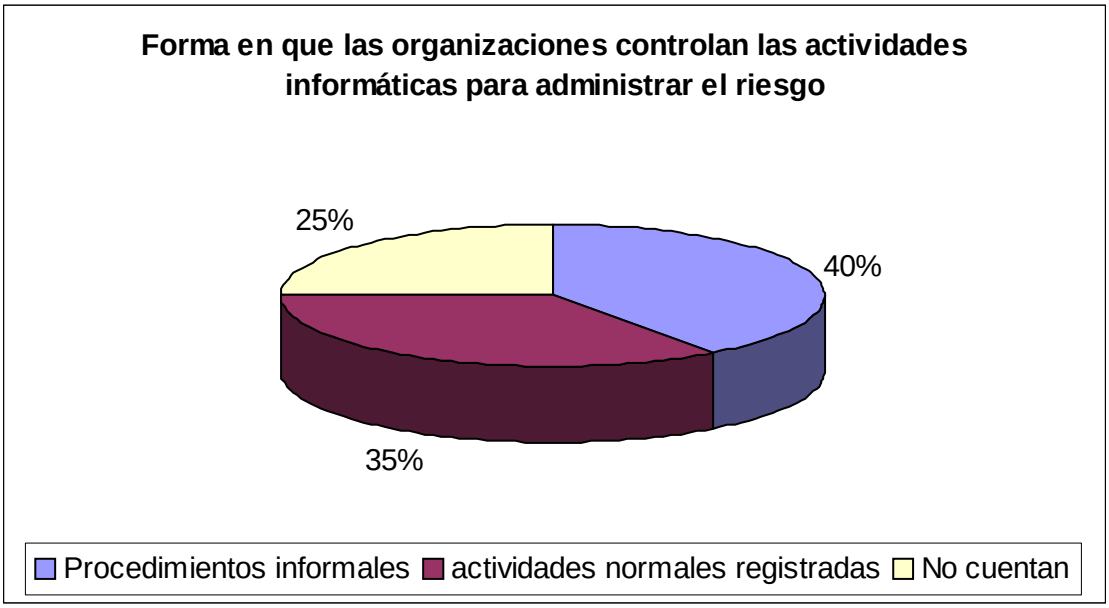


Fuente: Organizaciones del sector público costarricense consultadas

El control interno informático permite prevenir, corregir errores o irregularidades que puedan afectar el funcionamiento del sistema teniéndose así una adecuada administración del riesgo en actividades, funciones o procesos de tecnologías de información. Además, el sistema de control interno informático permite asegurar la integridad, disponibilidad y eficacia de los sistemas informáticos a través de normas, políticas, procedimientos, y mecanismos o actividades de control. Estos controles deben ser sencillos, completos, confiables, revisables y económicos.

Del mismo 80% de las organizaciones que actualmente no cuentan con un sistema de control interno informático completo, se les consulto sobre la forma que estas controlan los riesgos sobre las actividades informáticas y así poder tener una mejor administración del riesgo, desprendiéndose que el 40% controla las actividades mediante procedimientos informales, el 35% lo hacen por actividades normales registradas, y el 25% restante no cuenta con ningún tipo de control.

Gráfico N°4



Fuente: Organizaciones del sector público costarricense consultadas

Dentro de otros hallazgos importantes de resaltar están que el 80% de las organizaciones actualmente no cuentan con un sistema de control interno completo, acorde con la Ley de Control Interno Ley 8292, tampoco cuentan con sistema de control interno informático, no tienen desarrollado políticas formales para el área de tecnologías de información, no cuentan con mecanismos o acciones de control desarrolladas formalmente, no cuentan con administración de riesgos. Lo cual les impide actualmente tener un buen control de las operaciones, protección de recursos y mejoras de eficiencia y efectividad de los procesos, tampoco le permite prevenir, corregir errores o irregularidades que puedan afectarlos.

Gráfico N°5

Fuente: Organizaciones del sector público costarricense consultadas

Capítulo V : Conclusiones y recomendaciones

V.1 Conclusiones

El control interno es un proceso que lleva a cabo el seno de la Administración, la dirección y los demás miembros de una entidad, con el objeto de proporcionar un grado razonable de confianza en la consecución de objetivos en los ámbitos de eficacia y eficiencia de las operaciones, fiabilidad de la información, cumplimiento de las leyes y normas aplicables.

El sistema de control interno aporta una seguridad razonable, pero no completa, al seno de la administración, ya que existen limitaciones que son inherentes a todos los sistemas de control interno. Estas limitaciones se deben a que: las opiniones en que se basan las decisiones pueden ser erróneas, los empleados encargados del establecimiento de controles tienen que analizar la relación entre costos/beneficios de los mismos, y pueden producirse problemas en el funcionamiento del sistema como consecuencia de fallos humanos, aunque se trate de un simple error o equivocación.

Con la implantación de un sistema de control interno informático las organizaciones del sector público costarricense podrán controlar que todas las actividades se realicen cumpliendo

los procedimientos y normas fijadas, evaluando su bondad y asegurando el cumplimiento de las normas legales, definir, implantar y ejecutar mecanismos y controles para comprobar el grado de cumplimiento de los servicios informáticos, además realizar en los diferentes sistemas y entornos informáticos el control de las diferentes actividades que se realicen.

El control interno da cabida a los subgrupos de control interno. Así, uno puede centrarse en, por ejemplo, los controles sobre tecnologías de información o los relacionados con el cumplimiento de la legislación aplicable en el área operativa. Asimismo permite centrarse en los controles sobre unas unidades o actividades determinadas de una entidad.

El control interno informático controla diariamente que todas las actividades de sistema de información sean realizadas cumpliendo los procedimientos, estándares, políticas y normas fijados por la dirección de la organización y/o la dirección informática, así como los requerimientos legales.

Toda organización tiene que hacer frente a riesgos del más diverso estilo que pueden afectar a los más diversos aspectos de la actividad de la organización. Cualquier organización debe determinar cuáles son los niveles de riesgo aceptables y tratar de evitar que los riesgos sobrepasen esos límites. Previamente a determinar los riesgos hay que determinar los objetivos. Cada organización debe determinar sus objetivos, sus puntos fuertes y débiles y las oportunidades y amenazas del entorno. De esta manera obtendrá un plan estratégico que identificará los factores de éxito o condiciones previas para que la entidad consiga sus objetivos.

La informática crea unos riesgos informáticos de los que hay que proteger y preservar a la entidad con un entramado de controles. Por lo tanto las organizaciones del sector público costarricense debe profundizar más en ese entramado de controles para ver que exista una adecuada administración del riesgo que les permita prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema de control interno informático.

Las organizaciones necesitan desarrollar un plan de administración de riesgos y se necesitan medidas de sustento para contar con una estructura para la adopción de un proceso de administración de riesgos. El plan deberá encarar las estrategias para la adopción e incorporación del proceso de administración de riesgos en los sistemas, procesos y prácticas de la organización para que resulte totalmente eficaz y sustentable

Las actividades de control junto con ciertas actividades de gestión nos ayudarán a evitar

que los riesgos a los que está sujeta la entidad se lleguen a materializar y producir efectos negativos en ésta.

Las actividades de control se traducen en políticas (lo que debe de hacerse) y procedimientos (mecanismos concretos de control). Las actividades de control constituyen un elemento importante del proceso mediante el que una entidad consigue sus objetivos.

V.2 Recomendaciones

Como se puede apreciar en las conclusiones, con la implantación de un sistema de control interno informático las organizaciones del sector público costarricense podrán controlar que todas las actividades se realicen cumpliendo los procedimientos y normas fijadas, asegurando el cumplimiento de las normas legales; además podrán definir, implantar y ejecutar mecanismos y controles para comprobar el grado de cumplimiento de los servicios informáticos, realizando en los diferentes sistemas y entornos informáticos el control de las diferentes actividades que se realicen.

Para lograr este control interno informático es importante tener políticas bien concebidas y efectivas que puedan proteger la inversión y los recursos de información de la organización.

Se recomienda a las organizaciones del sector público costarricense realizar la adopción de las políticas descritas en el capítulo VI de propuesta, las cuales les permitirá dotar a la organización con mecanismos que refuercen la seguridad, privacidad e integridad de sus datos y software, así como proveer un uso apropiado y racional del equipo de cómputo con que se cuenta.

La adopción de estas políticas redundará en beneficios para la organización, y para todos los funcionarios en el ejercicio cotidiano de sus funciones.

Estas políticas se basan en la experiencia y mejores prácticas en materia de normativas de seguridad, aceptadas, probadas y aplicadas internacionalmente, tanto por empresas como por organismos de seguridad en tecnologías de información.

Las políticas podrán variarse eventualmente, para cubrir un ámbito mayor de situaciones potencialmente peligrosas, para ajustarse a las nuevas necesidades de la institución, sean estas últimas de carácter político, administrativo, legal o tecnológico; siempre con el objetivo de mantener el mejor balance posible entre seguridad y eficiencia.

Como se citó en las conclusiones, la informática crea unos riesgos informáticos de los que hay que proteger y preservar a la entidad con un entramado de controles. Por lo tanto las organizaciones del sector público costarricense debe profundizar más en ese entramado de controles para ver que exista una adecuada administración del riesgo que les permita prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema de control interno informático.

Las organizaciones del sector público costarricense podrán adoptar los mecanismos o acciones de control descritas en el capítulo VI de propuesta, las cuales permitirán establecer las condiciones necesarias que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones, mediante la aplicación de controles preventivos; también podrán identificar causas de riesgo, actuando como alarmas que permiten registrar el problema y sus causas, mediante la aplicación de controles detectivos; o bien podrán rectificar los errores y sus causas a través de controles correctivos.

Además se cita en las conclusiones que un sistema de control interno informático debe asegurar la integridad, disponibilidad y eficacia de los sistemas informáticos a través de mecanismos o actividades de control. Estos mecanismos o actividades de control descritas en el capítulo VI de propuesta permiten a las organizaciones cumplir con estos requerimientos a través de la aplicación de los controles que se describen a continuación:

- Gestión Administrativa de recursos informáticos:
- acciones de control sobre la planificación y administración de los proyectos para adquisiciones, sustituciones, implementación o mantenimiento de plataformas tecnológicas y servicios conexos.

- Desarrollo y mantenimiento de sistemas de información: acciones de control que consiste en una revisión de procedimientos de control en los sistemas, que posteriormente son puestos en operación, considerando amplias pruebas y corridas paralelas para reducir lo más posible, las fallas en los sistemas cuando se está usando en producción.

- Controles de las aplicaciones los cuales se diseñaron con el fin de cumplir con los objetivos específicos de controles sobre captura de datos: altas de movimientos, modificaciones de movimientos, mantenimiento de los ficheros; controles sobre el proceso de datos: estos se incluyen en los programas y se diseñan para detectar o prevenir errores (entrada de datos repetidos, procesamiento y actualización de ficheros equivocados, entrada de datos ilógicos, perdida o distorsión de datos durante el

proceso);, controles de salida y distribución: diseñados para asegurarse de que el resultado del proceso es exacto y que los informes y demás salidas los reciben solo las personas que estén autorizadas.

- Controles de la tecnología de información, que deben existir en todo centro de procesamiento de datos para asegurar la confidencialidad, integridad y disponibilidad de los datos informatizados. Estos controles aseguran que los procedimientos programados dentro de un sistema informático se diseñen, implanten, mantengan y operen de forma adecuada y que solo se introduzcan cambios autorizados en los programas y en los datos. Dentro de estos controles definidos citamos los siguientes:

    - Controles de desarrollo e implantación de aplicaciones.

    - Controles de mantenimiento: destinados a asegurar que las modificaciones de los procedimientos programados están adecuadamente diseñadas, probadas, aprobadas e implantadas.

    - Controles de explotación.

    - Controles de seguridad de ficheros de datos: destinados a garantizar que no se puedan efectuar cambios no autorizados en los procedimientos programados.
    - Controles de seguridad de ficheros de datos: destinados a asegurar que no se puedan efectuar modificaciones no autorizadas en los archivos de datos.

- Controles de los usuarios que se deben ejecutar sobre los documentos y transacciones antes y después de su proceso en el ordenador para comprobar el adecuado y continuo funcionamiento de los controles de las aplicaciones.

- Bases de datos: acciones de control para la revisión de procedimientos para una adecuada administración de las base de datos, que contemple controles sobre el acceso a la información y sobre el uso de utilitarios. Asimismo, se pueda identificar una clara definición del rol de administrador de bases de datos y de la propiedad sobre la información

- Redes y telecomunicaciones: acciones de control para la revisión de controles para la transmisión de datos por medio de computadores, con el propósito de garantizar la privacidad y confidencialidad de la información ante posibles accesos, sobre todo externos, así como frente a virus por diferentes vías de infección, incluyendo correo

electrónico.

Las actividades de control junto con ciertas actividades de gestión nos ayudarán a evitar que los riesgos a los que está sujeta la entidad se lleguen a materializar y producir efectos negativos en ésta.

Una de las conclusiones se refiere a que las organizaciones necesitan desarrollar un plan de administración de riesgos y se necesitan medidas de sustento para contar con una estructura para la adopción de un proceso de administración de riesgos. El plan deberá encarar las estrategias para la adopción e incorporación del proceso de administración de riesgos en los sistemas, procesos y prácticas de la organización para que resulte totalmente eficaz y sustentable

En el capítulo VI de propuesta se sugiere un estándar de administración de riesgos que puede ser adoptada por las organizaciones del sector público costarricense y que les permitirá establecer una infraestructura y cultura apropiada y aplicar un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con cualquier actividad, función o proceso de forma tal que permita a las organizaciones minimizar pérdida y maximizar beneficios.

Capítulo VI : Propuesta

VI.1 Definición de políticas para el área de Tecnologías e Información

VI.1.1 Políticas de control de acceso

Introducción

Los controles de acceso lógico permitirán únicamente el ingreso a los usuarios autorizados por la dependencia correspondiente, y en el nivel asignado, sobre los datos o sistemas necesarios para desempeñar sus tareas habituales.

1. Se deberá documentar un procedimiento, difundido en toda la Organización, para solicitar y dar efectivamente el alta, la baja, la modificación y la rehabilitación de usuarios en cualquier sistema.

   En el caso de que una persona se desvincule del sector donde desempeñaba sus funciones, el Superior de la misma solicitará en forma perentoria la baja del usuario y el Administrador lo inhabilitará inmediatamente en el sistema que corresponda.

   Cuando se produzca la ausencia prolongada de un agente en sus funciones, su Superior inmediato solicitará, conforme los procedimientos previstos para cada sistema, la inhabilitación temporaria de los accesos del usuario.

   Todo Usuario inhabilitado solicitará la rehabilitación a su Superior inmediato y éste al Administrador por los medios instrumentados en el procedimiento mencionado anteriormente. El Administrador del Sistema es el único autorizado a rehabilitar un usuario.

2. Cada persona autorizada a ingresar a los Sistemas tendrá en principio una única identificación personal (login) para el acceso a cualquier plataforma de hardware o software donde esté autorizado.

3. Por lo anterior, no deberán existir usuarios genéricos (usuarios agrupados bajo un password común para todos ellos) para la aplicación. Si por razones técnicas o propias de la administración es necesaria la existencia de usuarios genéricos, estos deberán ser aprobados por el área tecnologías de Información.

4. Se deshabilitarán todas las cuentas del proveedor que vengan instaladas por defecto en el producto adquirido (sistema operativo, software de base, herramienta, aplicación, etc.). Si no fuera técnicamente posible, se restringirán sus permisos de tal manera que reduzcan al mínimo sus posibilidades de acceso a todos los recursos. Asimismo se inhabilitarán

cuentas de invitado “guest”.

5. Reglas para las claves de ingreso

La longitud de la contraseña será automáticamente chequeada en el momento en que el usuario la construya. Todas las contraseñas deberán tener un mínimo de ocho (8) caracteres de longitud, contener al menos una letra, al menos un número y al menos un caracter especial, donde un caracter especial puede ser: *, +, -, %, #, $, /, @, &, etc. No está permitido utilizar en su conformación palabras propias del idioma, nombres propios de personas o cosas, sobrenombres, fechas de cumpleaños, aniversarios, secuencias predecibles de números o letras o cualquier combinación que sea obvia o que se pueda deducir fácilmente.

Se deberá cambiar la clave inicial asignada. Es decir, cuando el usuario ingrese por primera vez con su nueva clave, el sistema lo obligará al cambio de la misma.

Deberá tener una vigencia máxima de TREINTA (30) días corridos. El sistema deberá obligar al usuario a cambiar la clave vencido ese plazo

Deberá advertir sobre el vencimiento del período de validez durante los últimos CINCO (5) días anteriores al cumplimiento de la vigencia máxima. Durante ese período el sistema avisará al usuario quien deberá cambiar su clave.

6. Sobre contraseñas escritas y dejadas donde otros las puedan ver o encontrar

Las contraseñas no deberán ser escritas y dejadas en lugares donde los funcionarios no autorizados “no propietarios” las puedan descubrir. Inclusive, no deben ser vistas por los compañeros de trabajo.

7. Prohibición de compartir contraseñas

Las contraseñas no deben ser compartidas ni reveladas a nadie, de lo contrario, el propietario asumirá la responsabilidad por las acciones que otro funcionario realice usando su contraseña, ya que para efectos prácticos estará actuando en su nombre. Si los usuarios requieren compartir datos, deben utilizar el correo electrónico, directorios públicos compartidos en la red, carpetas públicas y otros mecanismos similares. En casos de ausencias justificadas, el sustituto, a través de la dirección correspondiente, deberá solicitar al área de tecnologías de Información un perfil equivalente al funcionario

sustituido.

8. Responsabilidad de los usuarios por toda actividad que involucre su cuenta de usuario

Los usuarios son responsables por toda actividad que se lleve a cabo con su cuenta de usuario personal. Las cuentas de usuario no deben ser utilizadas por nadie excepto el funcionario al cual fue asignada. Los usuarios no deben permitir que otras personas ejecuten cualquier actividad utilizando su cuenta de usuario personal. De igual forma, no está permitido a los funcionarios de la Institución realizar cualquier actividad con las cuentas pertenecientes a otros usuarios.

9. Obteniendo acceso no autorizado

No está permitido obtener o realizar accesos no autorizados a cualquier sistema de información, así como dañar, alterar o interrumpir las operaciones de estos sistemas. Adicionalmente, los funcionarios no tienen permitido capturar u obtener contraseñas, llaves de encriptación o cualquier otro mecanismo de control de acceso que pudiese permitir accesos no autorizados.

10. Conducta inapropiada y revocación de privilegios de acceso

No serán permitidas aquellas conductas que interfieran con la operación propia y normal de los sistemas de información o que afecten adversamente la facilidad de otros usuarios para acceder estos sistemas, o que sea dañina, ofensiva, proselitista, racista o despectiva para los demás usuarios. En caso de presentarse alguna de las conductas anteriores el área de tecnología de información de la institución, en conjunto o a solicitud de la administración, se reserva el derecho de revocar los privilegios de acceso de cualquier usuario en cualquier momento.

11. Reportar los cambios en los deberes de usuarios a los administradores de los sistemas de información

El área de tecnologías de información otorgará aquellos permisos y privilegios requeridos para utilizar los sistemas de información de acuerdo con la información que la Administración provea oportunamente. Cualquier cambio en las responsabilidades de los usuarios finales deberá ser comunicado por la Administración o por el Usuario Administrador del Sistema según corresponda, mediante el envío de un correo dirigido a la cuenta "Administración de usuarios", para que los cambios correspondientes a los

privilegios de la misma sean actualizados de acuerdo con las nuevas responsabilidades del funcionario. Cuando se trate de cambios en el estatus de un empleado, éste deberá ser comunicado por la Administración siguiendo el procedimiento descrito anteriormente, con el objetivo de realizar las modificaciones correspondientes en la cuenta de usuario.

12. Eliminación de cuenta de usuario y borrado de archivos luego de que un trabajador deja de laborar para la institución

A menos que se reciban instrucciones señalando lo contrario todos los archivos que tenían dichos usuarios serán eliminados de los servidores. Se debe eliminar también cualquier cuenta de usuario, privilegio y permiso que haya tenido el ex-funcionario. Todo lo anterior aplica siempre y cuando se haya recibido la notificación de cese de funciones del Departamento de Recursos Humanos que deberá ser realizada por el director de departamento o de la división correspondiente a la ubicación del usuario. Adicionalmente, apenas sea recibida la notificación respectiva se debe proceder a bloquear la cuenta del usuario.

13. Cuenta de usuario

Cualquier usuario nuevo de la red institucional, funcionario de la institución, empleado temporal, practicante, miembro de compañías que hacen outsourcing y cualesquiera otro que requiera utilizar la red institucional, tendrá que utilizar una cuenta de usuario. En el caso de funcionarios nuevos, la solicitud deberá ser realizada por el Departamento de Recursos Humanos ó deberá ser realizada por el director de departamento o de la división correspondiente a la ubicación del nuevo usuario. En ambos casos, se deberá utilizar el procedimiento normal de reporte de problemas definido por el área de tecnologías de información. Si no se trata de un funcionario de la institución, se debe indicar además por cuanto tiempo se requerirá la cuenta solicitada, de tal forma que, automáticamente, los sistemas de seguridad desactiven luego de transcurrido el tiempo estipulado.

14. Desactivación de cuenta por desuso

Toda cuenta de usuario que no presente actividad por un mes será desactivada. Para su reactivación el usuario afectado deberá hacer un reporte utilizando el método normal de reporte de problemas establecido por el área de tecnologías de información.

VI.1.2 Política de privacidad de los datos

1. Utilización de herramientas automatizadas para prevenir daños, robo, alteración o mal uso de la información

   La institución en aras de velar por la seguridad de los datos e información contenida y enviada mediante los sistemas, herramientas y equipo de cómputo de la institución, así como para velar por el buen uso de sus recursos y asegurar el cumplimiento de las leyes y normativas vigentes, instalará y configurará herramientas automatizadas que permitan detectar y eliminar entre otros: virus informáticos en todas sus variaciones, acceso a sitios de Internet cuyo contenido no es propio de las funciones asignadas, tipos de archivos cuyas características de formato o extensión no pertenecen a la operativa normal (por ejemplo, archivos con extensiones musicales, archivos con extensiones de juegos). Estas herramientas serán configuradas para tomar acciones tales como limpiar o eliminar los archivos o mensajes infectados con virus.

2. El copiado de información sensitiva o confidencial no está permitido sin el correspondiente permiso

   La información o datos de carácter sensitivo o confidencial no puede ser “bajada” o copiada a ningún medio electrónico o impreso, a menos que exista una necesidad real de trabajo o, en su defecto, se cuente con el permiso escrito del propietario de la información, que normalmente será la jefatura superior o dirección correspondiente.

3. Confidencialidad de la información

   Los usuarios, a los que se haya instruido de que la información que manejan es confidencial aún cuando no esté almacenada en medios electrónicos, están obligados a guardar la discrecionalidad respectiva. En particular, los usuarios de hojas electrónicas, deberán usar passwords y asegurar tanto la confidencialidad como la integridad y permanencia de respaldos de la información que manejan.

Debe tenerse presente, que en general, todo funcionario tiene prohibido divulgar o dar mal uso a la información que maneja o a la que tiene acceso, independientemente del medio en que ésta sea tratada o almacenada.

VI.1.3 Política de uso del equipo computacional

1. Liberación de responsabilidad por daños a datos de índole personal

Las instituciones usarán controles de acceso y otras medidas de seguridad para proteger la confidencialidad de los datos, su integridad y la disponibilidad de la información utilizada por las computadoras y los equipos de comunicación. Con el propósito de mantener estos objetivos, la administración se reserva el derecho de: (1) restringir o revocar cualquier privilegio o permiso de usuario, (2) remover cualquier dato, programa u otro recurso que pueda socavar los objetivos señalados. Esta autoridad puede ser ejercida con o sin notificación para los usuarios involucrados. La institución no asume responsabilidad alguna por pérdidas o daños a los archivos de índole personal, ajenos al quehacer de la institución, que resulten de sus esfuerzos para cumplir con los objetivos de seguridad citados anteriormente.

2. Prohibición contra la explotación de vulnerabilidades en la seguridad de los sistemas

Los usuarios no deben explotar vulnerabilidades o deficiencias en la seguridad de los sistemas de información, ya sea para dañar los sistemas o la información misma, obtener recursos más allá de aquellos a los cuales se les ha dado acceso, tomar recursos de otros usuarios u obtener acceso a otros sistemas para los cuales no se les ha dado autorización. Toda posible vulnerabilidad o deficiencia que se detectare en los sistemas de información deberá ser reportada inmediatamente, con carácter de obligatoriedad, al área de tecnologías de información.

3. Modificación de configuraciones e instalación de software

No está permitida la modificación de la configuración de las estaciones de trabajo o de los servidores de la red (por ejemplo: cambiar iconos, fondos de pantalla, permisos del disco, derechos de usuarios, entre otros), ya sea utilizando las herramientas de software provistas por el Sistema Operativo o cualquier herramienta adicional. Tampoco está permitida la instalación de hardware o software en tales equipos. Solamente el área de tecnologías de información está autorizada para realizar configuraciones e instalaciones de cualquier índole en los mismos.

VI.1.4 Política de uso de antivirus de computadoras

- Los usuarios no deben intentar remover virus de sus computadoras.

Los usuarios no deben intentar erradicar virus de sus máquinas sin la asistencia experta del personal del área de tecnologías de Información. Si los usuarios sospechan de infección debida a un virus, deben inmediatamente apagar sus máquinas y solicitar la asistencia respectiva. Posteriormente, utilizar el procedimiento normal de reporte de problemas desde una máquina sin infección.

- Revisión contra virus en el software antes de usarlo.

Para prevenir la infección por virus en las computadoras, el personal no debe usar software provisto por entes externos, sin que el mismo haya sido examinado y probado en el área de tecnologías de información.

- Revisión contra virus en cualquier medio de almacenamiento de datos de origen externo.

Cualquier dispositivo de almacenamiento de datos cuyo origen sea externo, deberá ser revisado contra virus de computadoras. Califican entre estos dispositivos externos: disquetes, unidades de ZIP, etc. El usuario deberá contactar al área de tecnologías de información para la asistencia respectiva, utilizando para ello el procedimiento normal de

reporte de problemas.

- Involucramiento de los usuarios con los virus de computadoras.

Los usuarios no tienen permitido: escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier código de programa diseñado para auto replicarse, dañar o reducir el desempeño o impedir el acceso a cualquier computador, a la red o a la información digitalizada. Tal software es conocido como un virus, bacteria, gusano, caballo de Troya o nombres similares. El comportamiento intencional anterior será considerado malicioso y calificado como falta grave.

VI.1.5 Política de uso de Internet

1. Bajado de archivos desde Internet (“downloads”)

   No está permitido el “bajado” de algún archivo desde Internet sin la previa autorización del área de tecnologías de información. Califican dentro de esta prohibición: programas gratuitos (shareware, freeware, trial, public domain), protectores de pantalla, software de evaluación y cualesquiera que no haya sido instalado bajo la configuración estándar previamente aprobados por el Departamento de Ingeniería en Tecnologías. Los archivos o programas señalados en la prohibición pueden comprometer la eficacia de las configuraciones de las máquinas, así como la seguridad de la red. Se excluyen de la prohibición, aquellos datos o archivos con información necesaria o requerida para el cumplimiento de las labores asignadas a cada funcionario o dependencia.

2. Conexiones a Internet y a otras redes

   No está permitida la realización de conexiones a Internet o a otras redes de computadoras utilizando medios ajenos a los proporcionados y habilitados por el área de tecnologías, a menos que exista una justificación de peso que cuente con la aprobación respectiva del área de tecnologías de información. Por ejemplo, está prohibido utilizar módems para conectarse a Internet.

VI.1.6 Política de Custodia de software, de licencias, y prohibición de realizar copias no autorizadas del software

1. El área de tecnologías de información es el custodio del almacenamiento físico de los medios magnéticos, de las licencias, y del control y registro que ambos conllevan, para todo el software con que cuente la institución. No está permitida la utilización fuera de la institución de las licencias y del software adquirido. Únicamente el área de tecnologías de información podrá realizar copias de seguridad del software original, siempre y cuando se cumpla que se cuenta con sólo un original del mismo. El área de tecnologías de Información será el encargado de velar porque aquellas copias de seguridad que se realicen, cumplan también con los lineamientos señalados anteriormente.

VI.1.7 Política de Revisiones de seguridad en la red

1. Revisiones de la seguridad en los equipos computacionales

   El área de tecnologías de información cumpliendo con su obligación de mantener la seguridad de los equipos y de los datos de la red institucional, se reserva el derecho de realizar revisiones periódicas de seguridad (o cuando las circunstancias así lo exijan), sobre cualquier equipo computacional que se encuentre conectado a la red, labor a cargo del área tecnologías de información. El objetivo de estas revisiones de seguridad será detectar y corregir posibles vulnerabilidades que tales equipos puedan presentar y que atenten contra la seguridad de los mismos, de la información que almacenan, o de la infraestructura tecnológica. Se incluyen todos los equipos bajo la administración directa del área de tecnologías de información y cualesquiera otro que no esté bajo la tutela directa de la misma, pero que esté conectado a la red institucional.

2. Revisiones del software instalado en las máquinas

   El área de tecnologías de información realizará revisiones periódicas del software instalado en los equipos computacionales. Las revisiones podrán ser manuales o automáticas y se realizarán con o sin previo aviso.

3. No se permite la cancelación de procesos de revisión automática

   No está permitido a los usuarios cancelar los procesos automáticos utilizados para diagnosticar, revisar, e inventariar el hardware y software instalado en los equipos. Tampoco está permitida la cancelación de procesos automáticos utilizados para diagnosticar el nivel de seguridad de los equipos y datos de la red institucional.

VI.1.8 Política de Utilización de directorios de red, respaldo y recuperación de datos

1. Directorio de trabajo en la red, personal o de una dependencia en particular

El área de tecnologías de información proveerá a cada usuario de la red institucional con un directorio personal ubicado en alguno de los servidores de la red, al cual sólo tendrá acceso el usuario mismo y el administrador de la red con el objetivo de realizar labores de mantenimiento y administración. El usuario será responsable de la información que allí almacene, en concordancia con las normas, pautas y reglamentos vigentes. Este directorio será respaldado periódicamente de acuerdo a las normas de respaldo empleadas por la División de Tecnologías de Información garantizando así la recuperación del mismo si así se requiriese. No se realizarán respaldos sobre directorios o archivos localizados en las estaciones de trabajo, por lo tanto, si el usuario requiere respaldos automáticos de sus archivos, deberá almacenarlos en su directorio personal de la red. El área de tecnologías de información no hará respaldos de los archivos almacenados en las estaciones de trabajo. Para el caso de una dependencia que requiera un directorio compartido en la red se seguirán las mismas restricciones señaladas anteriormente.

VI.1.9 Política de resguardo y recuperación de sistemas (Backup/Recovery)

La recuperación de sistemas resulta necesaria posterior a la interrupción del servicio. Estas no siempre se deben a factores extraordinarios, sino que, pueden surgir de un mal funcionamiento del sistema, errores humanos u otras fallas, que producen un tiempo de caída del sistema comparativamente menor al que produciría un desastre.

En tales circunstancias se exige una acción rápida para recuperar el estado operativo anterior a la ocurrencia del siniestro. Esta acción rápida puede desarrollarse si se cuenta con el respaldo adecuado de la información. Esto es, la información que reside en el sistema resguardada en algún otro dispositivo como cintas, Cd´s, cartridge, etc. Los procedimientos de resguardo (backups) y recuperación (recovery) de la información tienen el propósito de preparar a la Organización para dichas situaciones.

1. Todo sistema deberá contar con la documentación de los procedimientos de resguardo y recuperación antes de entrar en producción. La misma será controlada por el área responsable del tecnologías de información para verificar que es clara, completa y contempla como mínimo la recuperación de los siguientes elementos:

    a. El reemplazo de los servidores críticos.
    b. El sistema operativo y su configuración (parámetros, file systems, particiones, usuarios y grupos, etc.).
    c. Los utilitarios y paquetes de software de base necesarios para que la aplicación se ejecute.
    d. Los programas que componen la aplicación.
    e. Los archivos y/o bases de datos del sistema.
    f. Horario de ejecución de la copia de resguardo.

No se pondrá en producción ningún sistema que no cumpla este requerimiento.

2. Todas las copias de resguardo deberán estar claramente identificadas, con etiquetas que indiquen como mínimo

    a. Equipo al que pertenecen.
    b. Fecha y hora de ejecución.
    c. Frecuencia: anual, mensual, semanal, diario.
    d. número de secuencia o lote.

e. Tipo de backup.
f. Nombre del sistema o aplicativo y otros datos necesarios para su fácil reconocimiento.

3. Se llevará un registro diario de las cintas en uso indicando al menos:

a. Fecha de ejecución del resguardo.
b. Qué cintas integran el backup de los equipos.
c. Cantidad de veces que se usó la cinta.
d. Lugares asignados para su guarda.

El área responsable de tecnologías de información revisará periódicamente que se cumpla con este registro en tiempo y forma.

4. Todos los procedimientos de respaldo deberán generar un log en el equipo que permita la revisión del resultado de la ejecución, y dentro de lo posible, se realizarán con la opción de verificación de integridad (lectura posterior a la escritura.)

5. Los sitios donde se almacenen las copias de resguardo deberán ser físicamente seguros, con los controles físicos y ambientales según normas estándares; las cintas deben guardarse dentro de armario ignífugo.

6. Se crearán en lo posible 2 copias de resguardo, guardándose una de ellas en un edificio diferente al del ámbito de procesamiento en un lugar que cumpla con los requerimientos mencionados en el punto 5) y a distancia tal que la ocurrencia de cualquier contingencia en uno no afecte al otro. En caso de tener solo una copia esta debe ser llevada fuera del ámbito de procesamiento de la forma anteriormente mencionada.

7. Se realizarán copias de resguardo del sistema completo de acuerdo a lo indicado en la frecuencia asignada a cada aplicación o sistema, previendo la conservación de estos backups por el período de tiempo también estipulado previamente conforme a la criticidad de la información.

8. En el caso de utilizar backups incrementales se deberá tener en cuenta lo siguiente:
a. Se documentará la identificación de secuencia de los backups incrementales.
b. Deberán existir controles para prevenir la carga de cintas en una secuencia equivocada.
c. Se realizará un backup del sistema completo cada 7 días.

9. Se efectuarán pruebas de recuperación de las copias de resguardo al menos una vez cada 30 días. Estas pruebas servirán para constatar que se puedan obtener correctamente los datos grabados en la cinta al momento de ser necesarios, de forma de garantizar su propósito.

10. Los servidores críticos deberán contar con RAIDs de, a los efectos de que la información sensible no se vea afectada por potenciales desperfectos en los discos.

11. Para el caso de aplicaciones críticas se implementarán técnicas de replicación automática, por hardware o software, de forma tal que si el equipo/base de datos principal deje de funcionar el equipo/base de datos espejo tome el control inmediatamente.

12. Los períodos de retención de la información histórica son los siguientes:

    a. Fuentes y base de datos: perpetuo
    b. Lotes de transaf: perpetuo.
    c. Actividades de los usuarios y pistas de auditoría: 3 años.

13. El resguardo de la información histórica se realizará utilizando soportes magnéticos de preferencia no reutilizables (CDs, discos ópticos, etc).

14. Los procedimientos de generación y grabación de estos archivos serán automáticos, a fin de evitar su modificación.

VI.1.10 Política de seguridad física y ambiental

Introducción

Las normas para Seguridad física y ambiental brindan el marco para evitar accesos no autorizados, daños e interferencias en la información de la organización

Estas normas deberán permitir solamente el ingreso a las zonas restringidas a las personas

autorizadas. Una persona podría retirar sin autorización discos, cintas, o inclusive un servidor de archivos con datos cruciales y/o dañarlos de forma tal para sacarlos de servicio.

Asimismo, los controles ambientales evitan o disminuyen los riesgos de pérdidas de información o interrupción de las actividades por problemas del medio ambiente.

Dentro de este apartado se denominará “visitante” a toda persona que no cumple tareas en forma habitual en el lugar protegido.

Acceso a zonas restringidas

1. El edificio donde se encuentre el Ámbito de Procesamiento deberá tener todas sus entradas controladas por medio de una recepción, guardia de seguridad o cualquier otro método que asegure que el acceso al edificio lo realizan solo personas debidamente autorizadas.

2. Todos los visitantes se registrarán en Seguridad o Recepción firmando la entrada y la salida. Los datos mínimos a requerir son: apellido y nombres, tipo y Nº de documento presentado, empresa a la que pertenece, empleado de referencia y motivo de la visita. El empleado organizador de la visita debe recibir al visitante en su oficina y desde allí lo acompañará al área restringida.

3. La entrada del visitante al Centro de Procesamiento de datos se hará acompañado de una persona debidamente autorizada. Además se registrará el ingreso en una planilla completando como mínimo los siguientes datos: apellido y nombres, empresa, motivo de la visita, hora de entrada y de salida.

4. La entrada de cualquier persona al Centro de Procesamiento de datos fuera del horario habitual de trabajo, deberá estar autorizada formalmente y registrada en la bitácora o planilla de ingresos.

5. El responsable del Ámbito de Procesamiento es el encargado primario del control y seguimiento de los registros de accesos, y deberá actuar en consecuencia ante sospechas de violaciones de la misma. Entre otros, deberá controlar:

5.1 Que exista un registro por cada acceso al área de informática de personas autorizadas en horarios no usuales.

5.2 Que exista un registro por cada acceso al área de informática de los visitantes en la planilla de acceso o bitácora.

6. Todos los servidores o equipos centrales, y las consolas de operación, que integran el ámbito de procesamiento deberán residir dentro del Centro de Procesamiento de Datos o Centro de Cómputos.

7. En el Centro de Cómputos o Centro de Procesamiento de Datos preferiblemente deberá existir un único punto de ingreso. Esta entrada debe estar protegida apropiadamente contra accesos no autorizados (por ej: cerraduras, mecanismos de control, alarmas, etc.) y su señalización debe ser la mínima indispensable, a fin de evitar la identificación de actividades de procesamiento de datos en esa área.

   En el caso que existieran más puertas externas, estas deben contar con los mismos requerimientos de seguridad explicados en el párrafo anterior.

8. Las tareas de limpieza en el Centro de Cómputos serán supervisadas por una persona responsable de la sala que pueda advertir y evitar incidentes accidentales o intencionales sobre los equipos.

Seguridad Ambiental dentro del Centro de Cómputo

1. Todos los servidores o equipos centrales del ambiente de procesamiento deberán contar con estabilizadores de tensión y/o UPS (Uninterruptible Power Supply), estar instalados de acuerdo a las instrucciones del proveedor y montados en un Rack donde los cables estén asegurados de manera tal de evitar accidentes no intencionales. Todos los dispositivos se probarán periódicamente en los días y horarios que determine el responsable del ambiente de procesamiento.

2. Preferentemente deberán existir dos llaves de desconexión eléctrica de emergencia, una dentro de la sala y la otra cerca, pero fuera de la misma. Deberán estar claramente identificadas, ser de fácil acceso y estar protegidas de personas no autorizadas a fin de evitar que se las active en forma accidental.

   Estos dispositivos se probarán junto con los de suministro eléctrico

3. Preferentemente la instalación deberá estar alimentada por dos líneas de suministro de electricidad, de forma tal que la interrupción por accidentes ambientales de una (agua,

incendio, rayos, corte, etc.) no afecte a la otra.

4. El ambiente de procesamiento deberá estar limpio y ordenado, adecuadamente ambientado con aire acondicionado, con control de temperatura y humedad, regulado desde el mismo ambiente, a fin de mantener estable la temperatura de los equipos.

5. La sala de servidores o procesador central no deberá estar en los subsuelos o sótanos del edificio, ni tampoco en el último piso.

6. El ambiente de procesamiento deberá contar con un sistema de detección de incendios. Dicho sistema deberá producir una señal audible cuando sea activado tanto manual como automáticamente y deberá estar conectado a la sala de guardia y/o al departamento de bomberos, a fin de que sean monitoreados en forma periódica.

7. Deberán existir extinguidores portátiles de fuego ubicados en posiciones estratégicas en todo el ambiente de procesamiento. Los mismos tendrán una etiqueta de inspección con la indicación de la clase de incendios a los que extinguen y serán revisados de acuerdo a los estándares establecidos para cada tipo.

8. No se almacenará material combustible innecesario dentro o cerca de la sala de servidores o procesador central, tales como papeles, cajas, etc.

9. Está prohibido comer, beber y/o fumar dentro de la sala de servidores o procesador central.

Controles Generales

1. No deberán quedar papeles u otros materiales sobre los escritorios fuera del horario habitual de trabajo (política de “escritorios limpios”.)

2. Los reportes o impresiones que tengan información confidencial serán destruidos antes de tirarlos en depósitos de residuos.

3. Al momento de entrar en vigencia la norma deberá practicarse un inventario del hardware completo, el cual debe ser revisado periódicamente y validado por el responsable del sector.

4. El inventario de hardware debe contener la información relevante del equipamiento, incluyendo tipo de procesador, tamaño y tipo de memoria, tamaño y velocidad de los discos rígidos y CD-ROM’s, velocidad de módems, etc.

5. El área técnica registrará obligatoriamente la entrada y salida de computadoras y equipos, indicando como mínimo fecha, hora, responsable, identificación del elemento y causal que provoca el movimiento del Centro de Procesamiento de Datos.

6. Además deberá existir un diagrama topológico de las redes y un plano detallado del Centro de Cómputos

7. Todos los movimientos de recambio de equipos deberán estar aprobados por el área Técnica.

VI.1.11 Políticas en el uso de los servicios de correo y acceso a Internet

OBJETIVO

El objetivo de la política es la de regular el uso de los servicios de correo y el acceso a Internet, para lo cual se emiten los siguientes lineamientos que son de cumplimiento obligatorio para todo el personal que utilice los recursos de la red.

ALCANCE

La institución considera necesario regular el uso de los servicios de correo y el acceso a Internet, para lo cual emite los siguientes lineamientos, de cumplimiento obligatorio para todo el personal que utilice los recursos de la red. Es necesario que todos los usuarios estén enterados y conscientes de los compromisos, normas y reglamentos que han adquirido para el uso del correo y el acceso a Internet; y tomar todas las medidas que correspondan para que estas normas se respeten y se cumplan.

La red de la Institución está disponible para agilizar el flujo de información interna, la investigación administrativa, educativa y apoyar las diferentes tareas encomendadas para mejoramiento de nuestras labores. Todos sus usuarios están sujetos a esta política y a los términos de este manual. Su uso inapropiado será sancionado con la eliminación del acceso a estos recursos, la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

El uso de los recursos deberá tomar en cuenta que se respeten las medidas de seguridad que garanticen la integridad de los sistemas de cómputo, ya instalados y su accesibilidad por otros, para hacer el trabajo eficiente y productivo.

RESPONSABILIDAD

Es responsabilidad de todos los funcionarios de la Institución cumplir con las normas y procedimientos establecidos en este documento para acceso a los servicios de correo y de Internet

Usos Aceptables

Los servicios de correo electrónico y accesos a Internet se disponen lo siguiente:

- Comunicación entre investigadores y personas relacionadas con las labores desempeñadas en el ámbito nacional y extranjero, siempre y cuando exista un intercambio mutuo y en condiciones recíprocas.

- Comunicación e intercambio con la comunidad académica, universitaria u otras instituciones con el fin de tener acceso a los últimos avances relacionados con la especialidad o tareas desempeñadas

- Anuncios o servicios nuevos para el uso de los usuarios en general, pero no para publicidad de tipo comercial o personal alguno.

- Comunicación entre instituciones o empresas privadas siempre y cuanto estén vinculadas con las tareas encomendadas.

Usos Inaceptables

Queda prohibido el uso de los recursos de Internet y correo en los siguientes aspectos:

- Cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular.

- Acceso a lugares obscenos, que distribuyan libremente material pornográfico, o bien materiales ofensivos en perjuicio de terceros.

- Acceso a lugares recreativos, deporte, música, chistes, entre otros.

- Utilización de los servicios de correo para envió de información personal, chistes, pensamientos y cualquier otra información que no sea de carácter laboral.

CONTROL DEL USO DEL SERVICIO

Administración de la red

- La administración pondrá en funcionamiento herramientas de control que posibilitan analizar y detectar usos indebidos, por lo anterior se advierte que el contenido de la información es monitoreada y sujeta a controles y reportes sobre el uso.

- La administración de la red, no da garantías de ningún tipo, sean expresas o implícitas,

para el servicio que provee, por lo que no existirá ninguna responsabilidad por cualquier daño, que el usuario sufra, causado por negligencia propia o por errores u omisiones de sus usuarios.

- Cualquiera que acceda a otras redes nacionales o internacionales por medio del servidor de Internet debe acatar las reglas que rijan las mismas.

- Los mensajes que se envíen vía Internet, serán de completa responsabilidad del usuario emisor y en todo caso deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses de personas individuales, así como de ninguna otra institución.

- La institución tiene la autoridad para controlar y negar el acceso a cualquier funcionario que viole las políticas o interfiera con los derechos de otros usuarios. También tiene la responsabilidad de notificar a aquellas personas que se vean afectadas por las decisiones tomadas.

- El área de Informática, utilizará herramientas de monitoreo del uso de los recursos, por lo cual podrá establecer controles de acceso a sitios y de envío de información masivamente por la red.

- El área de informática enviará reporte del uso del servicio de correo o Internet a las Jefaturas respectivas, para que tomen medidas tendientes a mejorar su utilización.

- El administrador de la red monitorea en forma automática los sitios visitados por los funcionarios, por lo cual se advierte que se aplicaran las sanciones establecidas por el acceso indebido.

Prohibiciones:

- La transmisión de materiales, que viole cualquier regulación, queda prohibida. Esto incluye, pero no se limita, a materiales con derechos de propiedad intelectual, o que legalmente se consideren amenazantes u obscenos. Lo anterior en cumplimiento con el Decreto Nº 29915-MP Prohibiciones Material Pornográfico-Equipo Electrónico-Reglamento Autónomo de Servicio-Dirección General de Servicio Civil.

- Queda prohibido el envío de información en forma masiva a todo el personal o grupos de usuarios.

- Debido al nivel de seguridad con el que se debe de contar, las claves de acceso a Internet y correo electrónico deberán de ser estrictamente confidenciales y personales. Además de censurar la visita de páginas en la red dedicadas a áreas que no sean de interés investigativo, capacitación, legal, o del área de competencia.

- Utilizar los servicios de comunicación de Internet, incluyendo el correo electrónico o cualquier otro recurso, para intimidar, insultar o acosar a otras personas, interferir con el trabajo de los demás, provocar un ambiente de trabajo no deseable dentro del contexto de las políticas del Consejo.

- Utilizar los recursos de la Institución para obtener acceso no autorizado a redes y sistemas remotos.

- Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas.

- Poner información en la red que infrinja los derechos de los demás.

- Utilizar los servicios de red para juegos a través del servicio de Internet o Intranet.

- Utilizar los servicios de red para ver publicaciones de deportes.

- Utilizar los servicios de red para ver publicaciones de pornografía.

- Utilizar los servicios de red para enviar archivos que sean confidenciales.

- La exhibición de material pornográfico en cualquier lugar de la institución utilizando el equipo de cómputo y/o los servicios de comunicación de la institución.

- Envío de mensajes masivamente a todos los usuarios de la red o segmentos, iniciación y facilitaciones de cadenas y creación de procesos de discusión y contestación.

Para regular el uso del correo se establecen los siguientes lineamientos que son de acatamiento obligatorio:

Lectura de Correo

- Es obligatorio la utilización de carpetas personales para almacenar la información del correo que ingresa y que desea conservar.

- Si no tiene tiempo de contestar los mensajes completamente, envíe un breve mensaje para, que la persona que le envió el mensaje sepa que usted lo recibió.

- Mantenga los mensajes relacionados en carpetas aparte dentro de las carpetas personales.

- Seleccione la opción de eliminar mensajes cuando sale de la aplicación de correo para liberar espacio.

Envío de Correo

- Intente enviar mensajes bien formateados. Las personas que reciben mucho correo pueden dejar de leer un mensaje mal formateado.

- Utilice el campo asunto dentro del mensaje.

- No utilice las opciones de confirmación de entrega y lectura, a menos que sea un mensaje muy importante. Es innecesario, la mayoría de las veces provoca mucho tráfico en la red.

- No envíe mensajes ofensivos, abusivos, etc.

- No envíe mensajes a todo el personal del Consejo, a menos que sea un asunto oficial que involucre a toda la institución. Se advierte que está prohibido el envío de mensajes masivos que no estén debidamente autorizados.

- Antes de enviar el mensaje revise el texto que lo compone y los destinatarios. Esto con el fin de corregir errores de ortografía, forma o fondo.

Reenvío de Mensajes

- Cuando se reenvía un mensaje, incluya el mensaje original, para que la o las personas, hacia las que va dirigido el mensaje, conozca de que se está hablando en un momento dado.

- En muchas ocasiones se utiliza un mensaje para entremezclar una respuesta, y se eliminan las partes que son irrelevantes. Es altamente recomendable incluir el mensaje original, tal y como fue recibido.

- No envíe ni sea parte de una cadena de mensajes. Esto es considerado ilegal y puede acarrear la desactivación de la casilla, aunque no haya sido usted la persona que comenzó con la cadena.

Listas de Correos

- Queda prohibido el envío de mensajes con adjuntos a grupos de usuarios de la institución, únicamente podrán realizarlo los funcionarios debidamente autorizados.

- Si se siente ofendido por un mensaje no lo responda inmediatamente, envíe el mensaje hacia el superior inmediato con el fin de tomar las acciones respectivas.

- No haga que un tema de discusión se convierta en otro tópico. Si así lo desea comience con otro mensaje.

- No se suscriba a listas de amigos por Internet, esto provoca que gran cantidad de mensajes lleguen a su casilla de correo provocando saturación.

Tamaño de los mensajes

- El tamaño de los mensajes adjuntos no debe exceder de los XX MB, este ocasiona que el equipo responda de forma muy lenta.

- Si el adjunto excede de XX MB, debe ser compactado, para ello el encargado de brindar soporte ofrecerá las instrucciones del caso.

Mensajes con virus

- Desconfíe de todos los mensajes que vengan de Internet pues pueden estar infectados con virus, por lo cual las opciones dentro del antivirus deben de activarse de tal forma

que se chequeen todos los archivos aún los que se encuentren compactados y que la acción que debe seguirse sea la de eliminar el virus automáticamente.

- Si el mensaje que se detecta tiene un virus que no puede ser removido, entonces el mensaje no debe ser salvado o abierto y debe ser eliminado por completo.

- Cada usuario es responsable por los adjuntos que envía. Se tomarán las medidas respectivas en caso de que un mensaje sea enviado con virus. Es responsabilidad de cada funcionario tomar las medidas para evitar el contagio.

- El chequeo diario de virus en el correo se hará para todas las casillas en el servidor de correo, tratando de limpiar todo mensaje contagiado, si el mensaje tiene virus y no puede ser eliminado el mensaje será borrado del correo.

Vigencia de los mensajes

- Si desea mantener un mensaje, en forma permanente, debe almacenarse en una carpeta personal, en la máquina del usuario.

- El envío de mensajes a todo el personal del Consejo o áreas se autoriza únicamente para asuntos oficiales.

- Queda prohibido el envío de mensajes masivos, que no estén debidamente autorizados o que no se trate de mensajes oficiales.

El correo electrónico es privado e individual

- A menos que se utilice un dispositivo de encriptación (hardware o software), se debe asumir que el correo en el Internet no es seguro. Nunca ponga en un mensaje de correo información de carácter confidencial.

- Respete los derechos de autor en el material que reproduzca. Casi todos los países incluido el nuestro, tienen leyes para los derechos de autor.

- Si está respondiendo a un mensaje no cambie la redacción. Si el mensaje era personal y usted lo está mandando a un grupo, debería pedir permiso primero. Podría acortar el mensaje y resaltar las partes relevantes, pero asegúrese de dar las atribuciones pertinentes.

- En general, es una buena idea, por lo menos revisar todas las direcciones antes de responder un mensaje. Así mismo asegúrese de que los mensajes que responda vayan dirigidos a usted.

- Sea cuidadoso cuando direccione su correo. Hay algunas direcciones que pueden ir a un grupo, pero la dirección parece la de una persona. Sepa a quién le manda el correo.

- No mande correo no solicitado, preguntando por información a personas cuyos nombres aparecen en el campo de lista de correo.

- Los mensajes de correo deben tener un asunto que refleje el contenido del mensaje.

SANCIONES APLICABLES

La institución determinará la aplicación de la suspensión de acceso a los servicios, en atención al tipo de contravención al presente documento, las que serán cumplidas inmediatamente.

El incumplimiento de las normas establecidas podrá acarrear la suspensión de servicio de la siguiente forma:

- Si por primera vez se incumplen normas y lineamientos establecidos, se suspenderá el servicio por quince días naturales.

- Si las normas y lineamientos no se cumplen por segunda vez, se suspenderá el servicio por un mes calendario

• Tercera vez de incumplimiento, se suspenderá el servicio por dos meses o suspensión permanente.

Asimismo se establece que la acción de suspensión no impide que se establezcan procedimientos administrativos, para aplicar sanciones disciplinarias por el uso indebido del equipo electrónico y las telecomunicaciones en la institución.

VI.1.12 Políticas de seguridad para redes inalámbricas

Definición Red Inalámbrica:

Una red inalámbrica es una red de computadores que no requiere sistemas de cableado para establecer la comunicación de un computador con otro. Cada computador tiene una tarjeta que emite y recibe señales de un punto central conocido como punto de acceso, el cual se encarga de procesarlas y redirigirlas al destino esperado, sin necesidad de cables.

Puntos de acceso no autorizados (“Rogue Access Points”)

No se permite la instalación de puntos de acceso en la red interna a menos que hayan sido autorizados por el personal del área de Tecnologías de Información.

Ubicación

El punto de acceso a la red inalámbrica debe ser colocado dentro de una sala o área específica, en una ubicación que permita ser localizado por los adaptadores de red de las estaciones portátiles respectivas. Aunque la señal de radio no es necesariamente detenida por paredes y muros, el punto de acceso debe estar lejos de cualquier ventana para reducir el riesgo de que su señal sea interceptada desde fuera de la sala o área específica.

Conexión

El punto de acceso debe ser conectado a un puerto específico de un “switch”, el cual debe estar dentro de una red virtual (“VLAN”) aislada. Dicha red virtual sólo debe permitir el acceso a los servicios estrictamente requeridos para la conexión exitosa a los sistemas o servicios requeridos por la estación. Se recomienda además la implementación de filtros de IP según el RFC-2827 para la prevención de “IP spoofing”, previa autenticación a la red inalámbrica.

Servicios adicionales

De requerirse servicios adicionales de la red, deben analizarse previamente los riesgos de

seguridad para determinar si la implementación de dichos accesos no compromete la seguridad de la plataforma tecnológica. Esto deberá hacerse en conjunto y con el consentimiento del Área de Seguridad en Tecnologías de Información.

Alcance de la señal

El alcance de la señal de radio del punto de acceso no debe ser mayor a la requerida para permitir el acceso a los clientes dentro de la sala o área designadas para la red inalámbrica.

Sobre la seguridad de la red inalámbrica

Debe tener habilitados protocolos de seguridad con encriptación, y como mínimo una clave de acceso al punto de conexión. Debe implementarse el encriptado a nivel de “frames” inalámbricos.

Todo protocolo o servicio adicional que provea el punto de acceso y que no se considere seguro o sea irrelevante, debe ser deshabilitado.

Uso de firewalls (muros de fuego)

Colocar un muro de fuego que separe TODOS los puntos de acceso de la red inalámbrica de la red interna.

Seguridad de los clientes de la red inalámbrica

Los clientes que ingresan vía red inalámbrica deben utilizar protocolos seguros para tal comunicación. De la misma forma, los clientes deben tener habilitado la encriptación de archivos en los directorios de datos y temporales de sus estaciones portátiles. Los clientes deben almacenar su información sólo en estos directorios y no ser administradores de sus estaciones.

Todo protocolo o servicio adicional que provea el adaptador de red inalámbrico o la estación cliente, que no se considere seguro o sea irrelevante, debe ser deshabilitado. Esto, de acuerdo al criterio conjunto del Departamento de Ingeniería en Tecnologías y el Área de Seguridad en Tecnologías de Información.

Toda estación de trabajo portátil utilizada para interactuar en una red inalámbrica, debe

tener habilitado un firewall personal o sistema análogo que permita filtrar qué conexiones o interacciones aceptará tal estación de parte de terceros.

Ninguna de las cuentas de los usuarios puede pertenecer al grupo local de administradores de la estación de trabajo.

Restricciones sobre la estación de trabajo

Si una estación de trabajo ha sido configurada para participar en una red inalámbrica, ninguna de las cuentas de usuario utilizadas para tener acceso a dicha estación podrá formar parte del grupo de administradores locales de la misma. De no acatarse la situación anterior, se correría el riesgo de que se realicen modificaciones a la configuración de la estación de trabajo, produciendo grietas a los sistemas de seguridad implementados para tales redes. Adicionalmente, se podrían presentar situaciones de instalación de software ajeno, que igualmente podrían dar al traste con la configuración de seguridad de dichas estaciones.

Movilización de tarjetas inalámbricas

No está permitido que las tarjetas inalámbricas salgan del edificio. Esta política busca reducir significativamente la posibilidad de que las estaciones sean "hackeadas", vía otra red inalámbrica, cuando se encuentran fuera de la institución.

Otras restricciones de seguridad

Adicional a las políticas señaladas anteriormente, se aplicarán a las estaciones de trabajo (microcomputadores portátiles) que pertenezcan a redes inalámbricas, las mismas políticas de seguridad que se aplican a las estaciones fijas (desktop) de la red, con el fin de minimizar los riesgos de seguridad.

VI.1.13 Política para la adquisición de bienes y servicios informáticos

- Toda adquisición de tecnología informática se efectúa a través del Comité de informática, que está conformado por el personal de la Administración de Informática y Gerente Administrativo de la unidad solicitante de bienes o servicios informáticos.

- La adquisición de Bienes de Informática en la organización, quedará sujeta a los lineamientos establecidos en este documento.

- La Administración de Informática, al planear las operaciones relativas a la adquisición de Bienes informáticos, establecerá prioridades y en su selección deberá tomar en cuenta: el estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad.

Precio: Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos.

Calidad: Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.

Experiencia: Presencia en el mercado nacional e internacional, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.

Desarrollo Tecnológico: Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.

Estándares: Toda adquisición se basa en los estándares, es decir la arquitectura de grupo empresarial establecida por el Comité de informática. Esta arquitectura tiene una permanencia mínima de dos a cinco años.

Capacidades: Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área.

Para la adquisición de Hardware se observará lo siguiente:

a. El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares de la organización.

b. Deberá tener un año de garantía como mínimo

c. Deberá ser equipos integrados de fábrica o ensamblados con componentes

previamente evaluados por el Comité de informática.

d. La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional e internacional, así como con asistencia técnica y refaccionaria local.

e. Tratándose de equipos microcomputadoras, a fin de mantener actualizado la arquitectura informático de la organización, el Comité de informática emitirá periódicamente las especificaciones técnicas mínimas para su adquisición.

f. Los dispositivos de almacenamiento, así como las interfaces de entrada/salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en el ciclo del proceso.

g. Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado y la organización, corroborando que los suministros (cintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.

h. Conjuntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste en el costo de la partida inicial.

i. Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país.

j. Los equipos adquiridos deben contar, de preferencia con asistencia técnica durante la instalación de los mismos.

k. En lo que se refiere a los computadores denominados servidores, equipo de comunicaciones como enrutadores y concentradores de medios, y otros que se justifiquen por ser de operación crítica y/o de alto costo; al vencer su período de garantía, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de refacciones.

l. En lo que se refiere a los computadores denominados personales, al vencer su garantía por adquisición, deben de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de refacciones.

m. Todo proyecto de adquisición de bienes de informática, debe sujetarse al análisis, aprobación y autorización del Comité de informática.

- En la adquisición de Equipo de cómputo se deberá incluir el Software vigente precargado con su licencia correspondiente considerando las disposiciones siguientes:

Para la adquisición de Software base y utilitarios, el Comité dará a conocer periódicamente las tendencias con tecnología de punta vigente, conteniendo la lista los siguientes ítem:

- Plataformas de Sistemas Operativos
- Bases de Datos
- Manejadores de bases de datos
- Lenguajes de programación:
  Los lenguajes de programación que se utilicen deben ser compatibles con las plataformas enlistadas.
- Hojas de cálculo
- Procesadores de palabras
- Diseño Gráfico
- Programas antivirus
- Correo electrónico
- Browser de Internet

- En la generalidad de los casos, sólo se adquirirán las últimas versiones liberadas de los productos seleccionados, salvo situaciones específicas que se deberán justificar ante el Comité de informática. Todos los productos de Software que se adquieran deberán contar con su licencia de uso, documentación y garantía respectivas.

- Todos los productos de Software que se utilicen a partir de la fecha en que entre en vigor el presente ordenamiento, deberán contar con su licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos ya instalados que no cuenten con la licencia respectiva.

- Para la operación del software de red se debe tener en consideración lo siguiente:

a. Toda la información institucional debe invariablemente ser operada a través de un mismo tipo de sistema manejador de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de falla del sistema de cómputo.

b. El acceso a los sistemas de información, debe contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información institucional.

c. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software. Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes para cada caso.

d. El titular de la unidad administrativa responsable del sistema de información debe autorizar y solicitar la asignación de clave de acceso al titular de la Unidad de Informática.

e. Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, rotando los dispositivos de respaldo y guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, asimismo, las cintas de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación. Detalle explicativo se aprecia en la Política de respaldos en vigencia.

f. En cuanto a la información de los equipos de cómputo personales, la Unidad de Informática recomienda a los usuarios que realicen sus propios respaldos en la red o en medios de almacenamiento alternos.

g. Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales actualizados. Uno técnico que describa la estructura interna del sistema así como los programas, catálogos y archivos que lo conforman y otro que describa a los usuarios del sistema, los procedimientos para su utilización.

h. Los sistemas de información, deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoría y Control).

i. Se deben implantar rutinas periódicas de auditoría a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

- Para la contratación del servicio de desarrollo o construcción de Software aplicativo se observará lo siguiente:

    a. Todo proyecto de contratación de desarrollo o construcción de software requiere de un estudio de factibilidad que permita establecer la rentabilidad del proyecto así como los beneficios que se obtendrán del mismo.

    b. Todo proyecto deberá ser aprobado por el Comité de informática con base en un informe técnico que contenga lo siguiente:

        - Bases del concurso (Requerimientos claramente especificados)

        - Análisis de ofertas (Tres oferentes como mínimo) y Selección de oferta ganadora

Bases del Concurso

Las bases del concurso especifican claramente los objetivos del trabajo, delimita las responsabilidades de la empresa oferente y la contratante.

De las empresas oferentes

Los requisitos que se deben solicitar a las empresas oferentes son:

- Copia de la cédula de Identidad del o los representantes de la compañía.

- Copia de los nombramientos actualizados de los representantes legales de la compañía.

- Copia de los Estatutos de la empresa en que aparezca claramente definido el objeto de la compañía; esto es para determinar si está o no facultada para realizar la obra

- Referencias de clientes (Mínimo 3)

- La carta con la oferta definitiva del contratista debe estar firmada por el representante legal de la compañía oferente.

Del contratante

Las responsabilidades del contratante son:

- Delinear adecuadamente los objetivos y alcance del aplicativo.
- Establecer los requerimientos del aplicativo
- Definir responsabilidades de la contratista y contratante
- Establecer campos de acción

Análisis de ofertas y Selección de oferta ganadora

Para definir la empresa oferente ganadora del concurso, el Comité de informática establecerá una reunión en la que se debe considerar los siguientes factores:

- Costo
- Calidad
- Tiempo de permanencia en el mercado de la empresa oferente
- Experiencia en el desarrollo de aplicativos
- Referencias comprobadas de Clientes
- Cumplimiento en la entrega de los requisitos

Aprobada la oferta se debe considerar los siguientes lineamientos en la elaboración de contratos:

Todo contrato debe incluir lo siguiente:

- Antecedentes, objeto del contrato, precio, forma de pago, plazo, obligaciones del contratista, responsabilidades, fiscalizador de la obra, garantías, entrega recepción de obra provisional y definitiva, sanciones por incumplimientos, rescisión del contrato, disposiciones supletorias, documentos incorporados, solución de controversias, entre otros aspectos.

- Las garantías necesarias para cada contrato deben ser incluidas en forma conjunta con el Departamento Legal, quienes deben asesorar el tipo de garantía necesaria en la

elaboración de cada contrato.

Las garantías que se deben aplicar de acuerdo al tipo de contrato son:

- Una garantía bancaria o una póliza de seguros, incondicional, irrevocable y de cobro inmediato por el 5% del monto total del contrato para asegurar su fiel cumplimiento, la cual se mantendrá vigente durante todo el tiempo que subsista la obligación motivo de la garantía.

- Una garantía bancaria o una póliza de seguros, incondicional, irrevocable y de cobro inmediato equivalente al 100 % (ciento por ciento) del anticipo. Esta garantía se devolverá en su integridad una vez que el anticipo se haya amortizado en la forma de pago estipulada en el contrato.

- Un fondo de garantía que será retenido de cada planilla en un porcentaje del 5 %.

Junto al contrato se deberá mantener la historia respectiva del mismo que se compone de la siguiente documentación soporte:

- Estudio de factibilidad
- Bases del concurso
- Ofertas presentadas
- Acta de aceptación de oferta firmada por los integrantes del Comité
- Informes de fiscalización

Acta de entrega provisional y definitiva

VI.2 Definición de acciones de control para el área de Tecnologías de Información

Acciones de control o mecanismos de control

Las acciones de control o mecanismos de control son aquellas medidas que se implementan en primer término para prevenir la exposición ante una amenaza, detectarla si se ha materializado en el sistema, mitigar su impacto en él sistema, o para recuperar/restaurar el sistema.

A continuación se listan algunos controles generales para el área de Tecnologías de Información, posteriormente se detallaran los controles que se deben establecer por áreas funcionales.

- Desarrollar, documentar y probar procedimientos de respaldo**.**
- Desarrollar, documentar y probar procedimientos de continuidad de las operaciones.
- Implementar mecanismos de control de accesos**.**
- Implementar mecanismos de autentificación de usuarios**.**
- Implementar mecanismos de encriptación.
- Implementar procesos de administración de la configuración para el software.
- Implementar procesos de control de versiones para la documentación.
- Preparar, distribuir y dar mantenimiento a los planes, instrucciones, guías y procedimientos estándares de operación relacionados con la seguridad en la operación del sistema**.**
- Desarrollar documentación del uso adecuado del sistema para el usuario**.**
- Impartir capacitación en el uso seguro y adecuado del sistema**.**
- Implementar mecanismos para monitorear, informar y auditar actividades que requieren revisiones independientes**.**
- Implementar controles de operación para asegurar la adecuada separación de los datos**.**
- Negociar acuerdos de mantenimiento y con proveedores para facilitar una segura continuidad operativa del sistema**.**
- Efectuar consultas con la Gerencia de Servicios generales para implementar controles físicos de seguridad que protejan el sistema**.**
- Asegurar que las investigaciones del personal de seguridad sean efectuadas adecuadamente**.**
- Implementar procedimientos de desempeño, monitoreo y prueba para el aseguramiento de la calidad**.**
- Asegurar que la Administración de redes instale software corporativo antivirus en todo el sistema**.**

- Entrenar el personal de respaldo o emergente**.**
- Solicitar el apoyo administrativo para asegurar la cooperación y coordinación de las distintas unidades de negocio**.**
- Instaurar controles en la Administración de la producción, tal como evaluar y eliminar procesos para garantizar la integridad de los almacenes de datos**.**
- Dar seguimiento a la planificación de los tiempos programados para el mantenimiento técnico**.**
- Documentar posibles exposiciones a la seguridad, como los accesos a los programas " backdoors" o también conocidos como de puerta trasera.
- Mantener sitios de respaldo (fríos o calientes) con requerimientos ya determinados y adecuadamente implementados

Gestión administrativa de recursos informáticos

Acciones de control sobre la planificación y administración de los proyectos para adquisiciones, sustituciones, implementación o mantenimiento de plataformas tecnológicas y servicios conexos.

Acciones de control

- Metodologías de administración de proyectos.
- Plan estratégico de información realizado por el Comité de Informática.
- Plan informático realizado por el Departamento de Informática.
- Plan general de seguridad física y seguridad lógica.
- Estudios de factibilidad.
- Plan de necesidades de servicios Informáticos (hardware, software, sistemas de información).
- Políticas, normas sobre utilización de recursos informáticos, Internet, equipos, claves de acceso, seguridades física, seguridad lógica, etc.

1.1 Adquisición y recepción de recursos informáticos

Acciones de control

Planeación

- Identificación de necesidades.
- Viabilidad técnica – económica.
- Definición de alternativas.
- Criterios de selección.

Especificaciones técnicas de hardware

- Dimensionamiento.
- Tecnología.
- Compatibilidad.
- Adecuaciones locativas.
- Requisitos ambientales y técnicos.

Especificaciones técnicas software

- Funciones básicas.
- Requerimientos de software.
- Versión.
- Licencias de uso.
- Soporte del vendedor.

Acuerdos contractuales / r
ecepción de bienes y servicios (Inventario)

Acciones de control

Software Contratado

- Especificaciones funcionales.
- Cronogramas de desarrollo.
- Evaluaciones periódicas.
- Responsabilidad de las partes.

1.3 Equipo sistematización

- Inventario de equipos, programas, responsable.
- Procedimientos de operación.
- Administración de medios magnéticos.
- Plan de mantenimiento preventivo correctivo.
- Control de fallas.
- Seguros.

2. Desarrollo y mantenimiento de sistemas de información

Acciones de control que consisten en una revisión de procedimientos de control en los sistemas, que posteriormente son puestos en operación, considerando amplias pruebas y corridas paralelas para reducir lo más posible, las fallas en los sistemas cuando se está usando en producción.

Acciones de control

- Estudio de viabilidad de la aplicación.
- Definición lógica de la aplicación.
- Desarrollo técnico de la aplicación.
- Metodología y estándares de desarrollo de sistemas.
- Separación de ambientes de producción y desarrollo.
- Políticas y procedimientos de mantenimiento de sistemas.
- Pruebas organizadas y documentadas.
- Manuales (usuario, técnico).

2.1 Sistemas en Producción

Acciones de control que consisten en una revisión de normas y procedimientos sobre las aplicaciones, con el propósito de establecer las medidas necesarias para ejercer el control sobre la entrada, el proceso y la salida de los datos. Asimismo, comprobar los mecanismos de control de accesos y auditabilidad del sistema.

2.1.1 Aplicaciones en funcionamiento / origen y preparación de datos

Acciones de control

- Elaboración de documentación fuente.

- Autorización de transacciones.
- Clasificación de documentos.
- Consolidación de cifras y documentos.
- Envío de documentos fuentes.
- Capacitación e instructivos para diligenciar documentos fuentes.
- Diseño de funciones.

Aplicaciones en funcionamiento (producción)

Acciones de control

- Captura o grabación de datos.
- Validación de campos en la captura.
- Generación de reportes para revisión previa.
- Proceso de corrección de errores.
- Niveles de seguridad en la entrada.

Control de documentos negociables

.

Claves de seguridad en archivos de datos

.

- Generación de archivos para interfaces.

Validación, facilidad de corrección

- , cifras de control, manejo de transacciones rechazadas, manejo de errores, otros.
- Generación de transacciones automáticas.
- Rutinas de liquidación.
- Políticas y procedimientos para la identificación, autenticación y autorización al sistema de información.
- Pistas de auditoría.
- Bitácora y políticas para la emisión y revisión de reportes de actividad.

2.3 Aplicaciones en funcionamiento / archivos de datos

Acciones de control

Comprende los procedimientos de acceso a la información de los archivos de computador especialmente:

- Perfil de autorización.
- Copias de archivos.
- Ubicación y organización física de los archivos

.

2.4 Aplicaciones en funcionamiento / acceso y seguridades de los programas

Procedimientos de acceso a los programas fuente - objeto

Acciones de control

- Solicitud del cambio.
- Priorización de los cambios.
- Solicitud del programa a modificar.
- Desarrollo del cambio.
- Pruebas.
- Autorización.
- Proceso de catalogación de cambios.
- Rastro pistas de los cambios.
- Actualización de documentación.

2.5 Aplicaciones en Funcionamiento Backup y Recuperación

Acciones de control

- Identificación de archivos importantes.
- Tiempo de retención definido para cada archivo.
- Ubicación de backups del sistema a evaluar.
- Procedimientos de reinicio en caso de cancelación de procesos

.

2.6 Aplicaciones en Funcionamiento Satisfacción del Usuario

Acciones de control

Se evaluará la aplicación o sistema de información en relación con:

- Sus expectativas.
- Exactitud y confiabilidad del procesamiento de información.
- Relación costo-beneficio (Desarrollo y Operación).
- Eficiencia técnica.
- Cumplimiento normas convenciones codificación

.

3. Bases de datos

Acciones de control para la revisión de procedimientos para una adecuada administración de las base de datos, que contemple controles sobre el acceso a la información y sobre el uso de utilitarios. Asimismo, se pueda identificar una clara definición del rol de administrador de bases de datos y de la propiedad sobre la información

Acciones de control

- Procedimientos de seguridad, integridad y confidencialidad que se le aplicarán a los datos.
- Procedimientos para recuperar los datos en casos de caída del sistema o de corrupción de los archivos.
- Procedimientos para prohibir el acceso no autorizado a los datos.
- Procedimientos para restringir el acceso no autorizado a los datos. debiendo identificar los distintos perfiles de usuario.
- Procedimientos para mantener la consistencia y corrección de la información en todo momento.
- Procedimientos para la administración de la base de datos.
- Roles del Administrador.
- Modelo y estructura de la base de datos.
- Esquema de seguridad.
- Bitácora y políticas para la emisión y revisión de reportes de actividad.

Control y seguridad de datos y software

- Políticas de seguridad lógica.
- Administración de claves acceso.
- Clasificación de información para seguridad.

4. Redes y telecomunicaciones

Acciones de control para la revisión de controles sobre la transmisión de datos por medio de computadores, con el propósito de garantizar la privacidad y confidencialidad de la información ante posibles accesos, sobre todo externos, así como frente a virus por diferentes vías de infección, incluyendo correo electrónico.

Acciones de control

- Procedimientos de implantación y mantenimiento de Hardware y Software.
- Manual de estándares y operación de la red.
- Esquema de seguridad.
- Política de seguridad física.
- Política de acceso.
- Políticas y procedimientos para el uso de correo electrónico e Internet

5. Continuidad de operaciones

Acciones de control para asegurar que las funciones vitales de la organización que dependen del área de Tecnologías de Información, puedan seguir funcionando durante períodos de emergencia, causado por defectos en los equipos, pérdida de las bases de datos, errores de programación y otras situaciones parecidas.

Acciones de control

- Procedimientos para respaldo y recuperación de datos.
- Respaldo eléctrico.
- Seguridad física.
- Plan de Contingencias Informáticas.
- Seguros.
- Centro alterno para la recuperación en caso de desastres.

Planes de Contingencia

- Propiedad del Plan.
- Recursos críticos.

- Entrenamiento y seguridad del personal en procedimientos de emergencia.
- Procedimientos de respaldo

y recuperación de datos.

Controles ambientales y seguridades físicas

- Planes políticas sobre control ambiental y seguridad física.
- Responsables de la seguridad física.
- Ubicación física.
- Acceso físico.
- Medidas de protección contra incendios - inundaciones

.

VI.3 Estándar de Administración de Riesgos

Este estándar esta basado en el estándar de administración de riesgos AS/NZS 4360. El mismo provee una estructura genérica para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos.

Sección 1: Vista general del proceso de administración de riesgos

1.1 General

La administración de riesgos es una parte integrante del proceso de administración. Administración de riesgos es un proceso multifacético, aspectos apropiados del cual son a menudo llevados a cabo por un equipo multidisciplinario. Es un proceso iterativo de mejora continua que es mejor incorporarlo en las prácticas o procesos de negocio existentes.

1.2 Elementos principales

Los elementos principales del proceso de administración de riesgos, son los siguientes:

Comunicar y consultar

Comunicar y consultar con interesados internos y externos según resulte apropiado en cada etapa del proceso de administración de riesgos y concerniendo al proceso como un todo.

Establecer el contexto

Establecer los contextos estratégico, organizacional y de administración de riesgos en los cuales tendrá lugar el resto de los procesos. Deberán establecerse los criterios contra los cuales se evaluarán los riesgos y definirse la estructura del análisis.

Identificar riesgos

Identificar qué, por qué, dónde, cuándo y cómo los eventos podrían impedir, degradar, demorar o mejorar el logro de los objetivos estratégicos y de negocio de la organización.

Analizar riesgos

Determinar los controles existentes y analizar los riesgos en términos de consecuencia y probabilidad en el contexto de tales controles. El análisis debería considerar el rango de consecuencias potenciales y cuan probable es que esas consecuencias puedan ocurrir. Consecuencia y probabilidad pueden ser combinadas para producir un nivel estimado de riesgo.

Evaluar riesgos

Comparar los niveles estimados de riesgo contra los criterios preestablecidos y considerar el balance entre beneficios potenciales y resultados adversos. Esto permite realizar apreciaciones sobre prioridades gerenciales.

Tratar riesgos

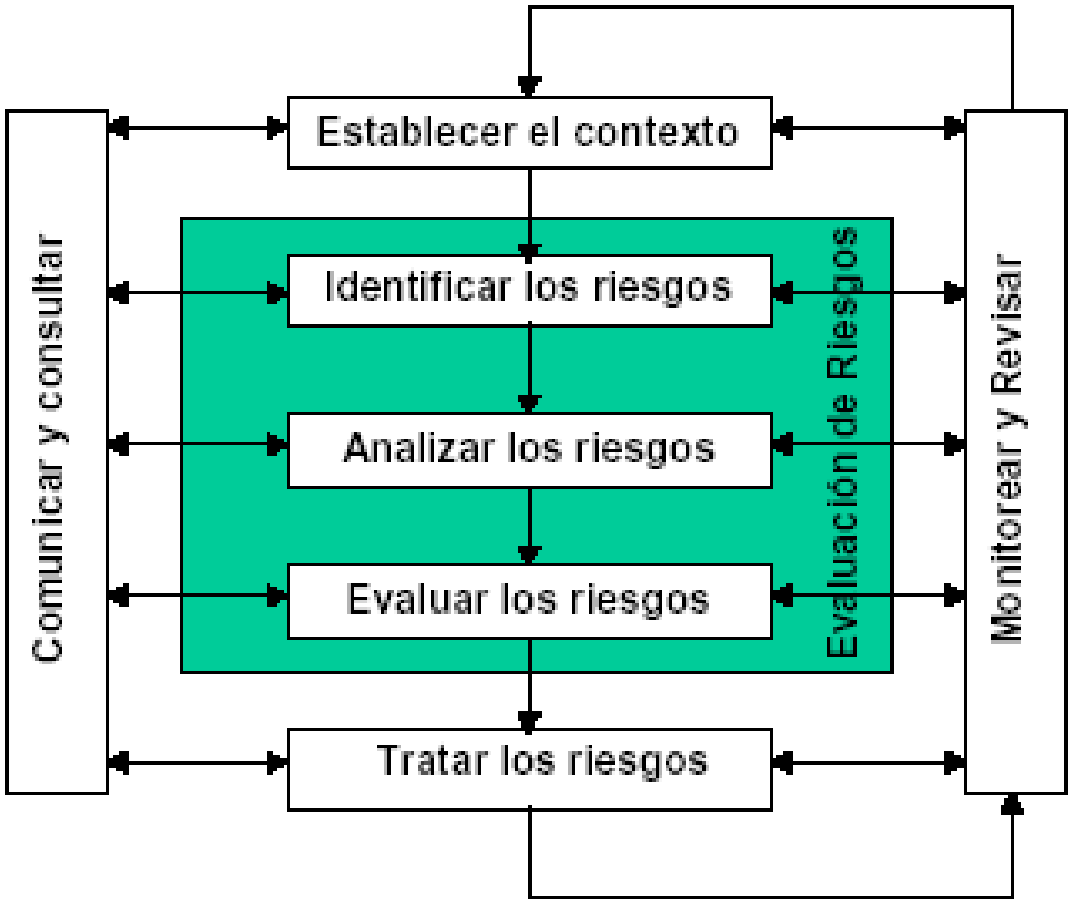
Si los niveles de riesgo establecidos son bajos y son tolerables entonces no se requiere tratamiento. Para otros riesgos desarrollar e implementar estrategias y planes de acción específicos costo-eficaces para aumentar los beneficios potenciales y reducir los costos

potenciales.

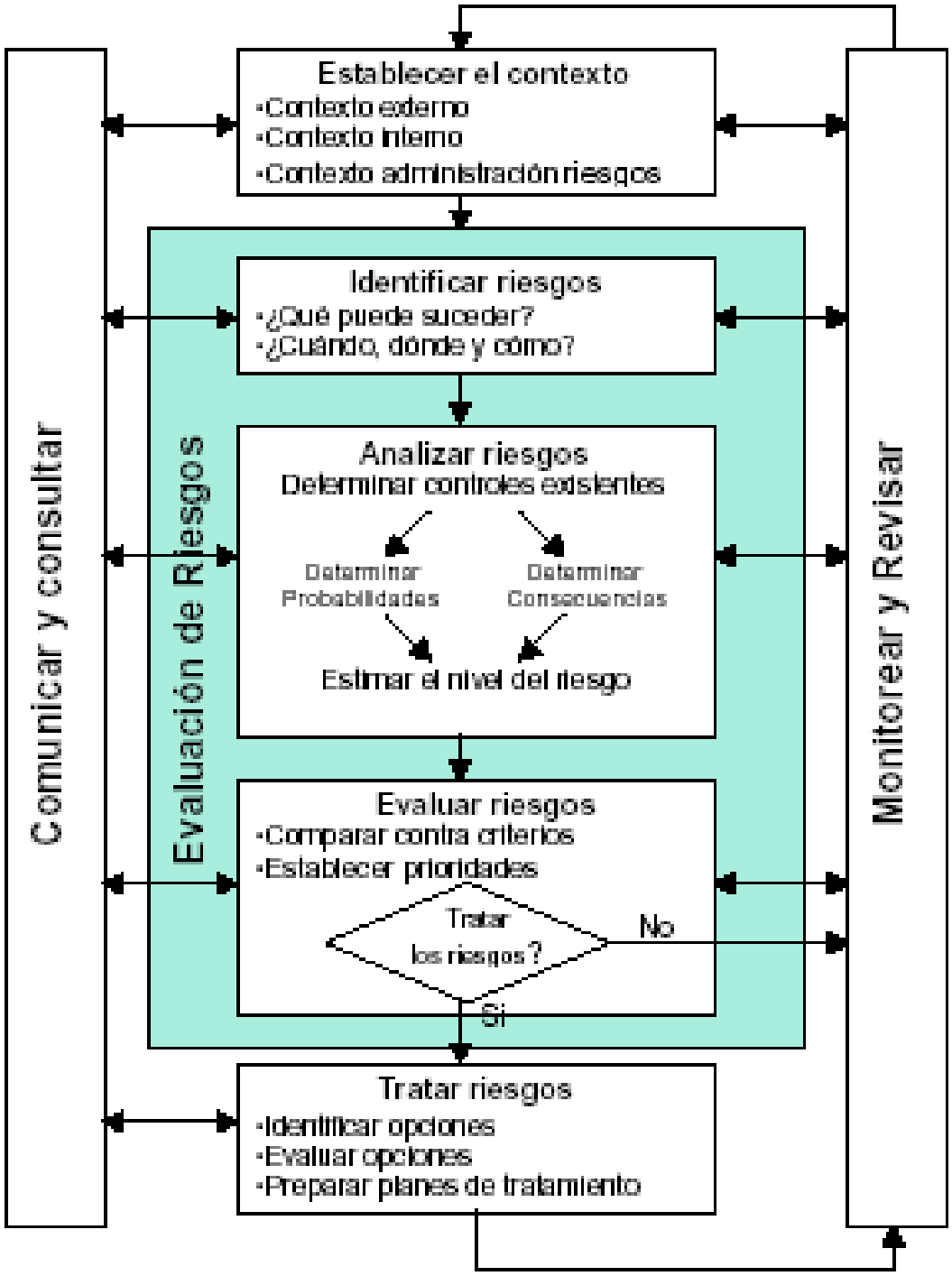
Monitorear y revisar

Monitorear y revisar el desempeño de las estrategias de control de riesgos y procurar detectar cambios que pudieran afectar la adecuación o eficacia de costo de los controles.

La administración de riesgos puede ser aplicada a muchos niveles en una organización. Puede ser aplicada a un nivel estratégico y a niveles tácticos y operacionales. Pueden ser aplicados a proyectos específicos, para sustentar decisiones específicas o para administrar áreas específicas de riesgo reconocidas.
Para cada etapa del proceso deberían mantenerse registros adecuados.



Sección 2: Proceso de Administración de Riesgos



2.1 Comunicación y consultas

La comunicación y consulta son consideraciones importantes a cada paso del proceso de administración de riesgos.

Comunicación y consulta involucra un diálogo con los interesados con esfuerzos

focalizados en la consulta más que en un flujo de información de una sola vía desde el tomador de decisiones hacia los interesados.

Es útil un enfoque de equipo de consulta para ayudar a definir el contexto en forma apropiada, para ayudar a que los riesgos sean identificados eficazmente, para reunir distintas áreas de especialidad en el análisis de riesgos, para asegurar que se consideran distintos puntos de vista en la evaluación de los riesgos y para una administración apropiada de cambios durante el tratamiento de los riesgos.

Es importante desarrollar un plan de comunicación tanto para los interesados internos como externos en la etapa más temprana del proceso. Este plan debería considerar aspectos relativos tanto al riesgo en si mismo, como al proceso para administrarlo.

Son importantes las comunicaciones internas y externas eficaces para asegurar que aquellos responsables por implementar administración de riesgos, y aquellos con un interés establecido, comprendan la base sobre la cual se toman las decisiones y por qué se requieren determinadas acciones.

2.2 Establecer el contexto

2.2.1 General

El proceso de administración de riesgos se produce dentro de la estructura del contexto estratégico, interno, externo y de administración de riesgos de una organización. Establecer el contexto consiste en definir los parámetros básicos dentro de los cuales se deben administrar los riesgos y establecer el alcance para el resto del proceso de administración de riesgos.

2.2.2 Establecer el contexto interno

Antes de comenzar una actividad de administración de riesgos, a cualquier nivel, es necesario comprender la organización, su estructura y sus capacidades, como asimismo, sus metas y objetivos y las estrategias que están vigentes para lograrlos.

Este es importante por las siguientes razones:

- la administración de riesgos tiene lugar en el contexto de las metas y objetivos de la organización;
- el riesgo principal para la mayoría de las organizaciones es fallar en el logro de sus objetivos estratégicos, de negocio o de proyectos, o que sean percibidos como fallados por los interesados;
- las políticas y metas organizacionales ayudan a definir la política de riesgo de la organización; y
- los objetivos y criterios específicos de un proyecto o actividad deben considerarse a la luz de los objetivos de la organización como un todo.

2.2.3 Establecer el contexto externo

Este paso define el entorno en que opera la organización. La organización debería procurar establecer los conductores críticos del negocio y los valores de los interesados.

Definir la relación entre la organización y el entorno externo de negocios, social y político, identificando las fortalezas, debilidades, oportunidades y amenazas de la organización. El contexto incluye los aspectos financieros, operacionales, competitivos, políticos (percepciones e imagen pública), sociales, de clientes, culturales y legales de las funciones de la organización. Identificar los interesados internos y externos, y considerar sus objetivos, tomar en cuenta sus percepciones, y establecer políticas de comunicación con esas partes.

Debe llevarse a cabo un análisis estratégico. El mismo debe ser aprobado a nivel ejecutivo, establecer los parámetros básicos y proveer una guía para los procesos de administración de riesgos más detallados.

Debería existir una relación estrecha entre la política y objetivos de administración de riesgos de una organización y su misión u objetivos estratégicos.

2.2.4 Establecer el contexto de administración de riesgos

Deben establecerse las metas, objetivos, estrategias, alcance y parámetros de la actividad, o parte de la organización al cual se está aplicando el proceso de administración de riesgos.
El proceso debería ser llevado a cabo con plena consideración a la necesidad de balancear costos, beneficios y oportunidades. También deberían especificarse los recursos requeridos y los registros a mantener.

Establecer el alcance y los límites de una aplicación del proceso de administración de riesgos involucra:

- definir el proyecto o actividad y establecer sus metas y objetivos;
- especificar la naturaleza de las decisiones que deben tomarse;
- definir la amplitud de la actividad o función del proyecto en términos de tiempo y localización;
- identificar cualquier estudio de estructuración o alcance requerido y el alcance, objetivos y recursos requeridos; y
- definir la profundidad y amplitud de las actividades de administración de riesgos a llevar a cabo.
- Los aspectos específicos que también deberían ser discutidos incluyen:
- Los roles y responsabilidades de las distintas partes de la organización que participan en el proceso de administración de riesgos.
- Las relaciones entre el proyecto o actividad y otros proyectos o partes de la organización.

2.2.5 Desarrollar criterios de evaluación de riesgos

Decidir los criterios contra los cuales se van a evaluar los riesgos.

Las decisiones concernientes a si se requiere un tratamiento del riesgo deberían estar basadas en criterios operacionales, técnicos, financieros, legales, sociales, humanitarios u otros. Esto a menudo depende de las políticas internas, metas y objetivos de una organización y de los intereses de los distintos interesados.

Los criterios podrían estar afectados por las percepciones de los interesados y por requerimientos legales o reglamentarios. Es importante que se determinen los criterios apropiados desde el comienzo.

Aunque los criterios de riesgo son inicialmente desarrollados como parte del establecimiento del contexto de administración de riesgos, los mismos deben ser posteriormente desarrollados y refinados a medida que se identifiquen los riesgos particulares y se escojan técnicas de análisis de riesgos, ej: los criterios de riesgo deberían corresponder al tipo de riesgos y la forma en que se expresan los niveles de riesgo.

2.2.6 Definir la estructura para análisis de riesgo

Esto involucra formular la actividad, proyecto o cambio en un conjunto de elementos o pasos. Estos elementos proveen una estructura lógica para análisis que ayuda a asegurar que no se pasen por alto riesgos significativos. La estructura escogida depende de la naturaleza de los riesgos y del alcance del proyecto o actividad.

2.3 Identificación de riesgos

2.3.1 General

Este paso procura identificar los riesgos a administrar. Es crítica la identificación amplia utilizando un proceso sistemático bien estructurado, porque un riesgo potencial no identificado en esta etapa quedaría excluido de análisis posteriores. La identificación debería incluir todos los aspectos de los riesgos, estén o no bajo control de la organización.

2.3.2 ¿Qué puede suceder, dónde y cuándo?

El propósito es generar una lista amplia de fuentes riesgos y eventos que podrían tener un impacto en el logro de cada uno de los objetivos estratégicos, de negocio o de proyecto referidos en la Cláusula 4.2.3. Estos eventos podrían impedir, degradar, demorar o mejorar el logro de esos objetivos. Estos son luego considerados en mayor detalle para identificar lo que puede suceder.

2.3.3 ¿Cómo y por qué puede suceder?

Habiendo identificado lo que podría suceder, es necesario considerar las causas y escenarios posibles. Hay muchas formas en que puede suceder un evento. Es importante que no se omita ninguna causa significativa.

2.3.4 Herramientas y técnicas

Los enfoques utilizados para identificar riesgos incluyen *checklists*, juicios basados en la experiencia y registros, diagramas de flujo, técnicas de *brainstorming*, análisis de sistemas, análisis de escenarios y técnicas de ingeniería de sistemas.

El enfoque utilizado dependerá de la naturaleza de las actividades bajo revisión, de los tipos de riesgos y del contexto organizacional.

2.4 Análisis de riesgo

2.4.1 General

El objetivo del análisis de riesgos es proveer un ingreso de datos a las decisiones sobre si los riesgos necesitan ser tratados y sobre las estrategias más apropiadas y costo-eficaces de tratamiento de los riesgos.

El análisis de riesgos involucra considerar las fuentes de riesgo, sus consecuencias positivas y negativas y las probabilidades de que esas consecuencias puedan ocurrir.

Pueden identificarse los factores que afectan a las consecuencias y probabilidades. El riesgo es analizado combinando consecuencias y probabilidades, tomando en cuenta las medidas de control existentes.

Se puede llevar a cabo un análisis preliminar para combinar riesgos similares o excluir del estudio detallado a los riesgos de bajo impacto. Siempre que sea posible, los riesgos excluidos deberían ser listados para demostrar la integridad del análisis de riesgo.

2.4.2 Determinar estrategias y controles existentes

Identificar los procesos, dispositivos o prácticas existentes que actúan para minimizar los riesgos negativos o mejorar las oportunidades positivas y evaluar sus fortalezas y debilidades. Pueden ser apropiadas las herramientas utilizadas en 4.3.4, como asimismo, los enfoques tales como inspecciones y auto-evaluaciones del control (CSA). Los controles pueden surgir como resultado de actividades previas de tratamiento del riesgo.

2.4.3 Consecuencia y probabilidad

La magnitud de las consecuencias de un evento, en el caso de que el mismo ocurriera, y la probabilidad del evento y sus consecuencias asociadas, son evaluadas en el contexto de la eficacia de las estrategias y controles existentes.

Las consecuencias y probabilidades se combinan para producir un nivel de riesgo.
Las consecuencias y probabilidades pueden ser determinadas utilizando cálculos y análisis estadístico.

Alternativamente, cuando no se dispone de datos anteriores confiables o relevantes, se pueden realizar estimaciones subjetivas que reflejan el grado de convicción de un individuo o grupo de que pueda ocurrir un evento o resultado particular.

Para evitar prejuicios subjetivos, cuando se analizan las consecuencias y probabilidades deberían utilizarse las fuentes de información y técnicas más pertinentes. Las fuentes de información podrían incluir:

- los registros anteriores.
- la práctica y experiencia relevante.
- la literatura relevante publicada.
- investigaciones de mercado.
- experimentos y prototipos.
- modelos económicos, de ingeniería u otros.
- los juicios de especialistas y expertos.

Las técnicas incluyen:

- entrevistas estructuradas con expertos en el área de interés;
- uso de grupos multidisciplinarios de expertos;
- evaluaciones individuales utilizando cuestionarios; y
- uso de modelos y simulaciones.

Siempre que sea posible, debería incluirse la confianza depositada en las estimaciones de los niveles de riesgo.

2.5 Evaluación de riesgo

El objetivo de la evaluación de riesgos es tomar decisiones, basadas en los resultados del análisis de riesgo, acerca de los riesgos que requieren tratamiento y sus prioridades.

La evaluación de riesgo involucra comparar el nivel de riesgo detectado durante el proceso de análisis con los criterios de riesgo previamente establecidos.

Deberían considerarse los objetivos de la organización y la gama de oportunidades que podrían resultar del riesgo. Cuando deba realizarse una selección entre distintas opciones, el mayor potencial de pérdidas debería asociarse con los mayores beneficios potenciales y la selección apropiada dependerá del contexto de la organización.

Las decisiones deberían tomar en cuenta al amplio contexto del riesgo e incluir consideraciones a la tolerancia a los riesgos por parte de terceras partes distintas de la organización que se benefician del mismo.

Los riesgos bajos o tolerables podrían ser aceptados con un tratamiento futuro mínimo. Los mismos deberían ser monitoreados y revisados periódicamente para asegurar que se mantienen igual.

Si los riesgos no son bajos o tolerables, los mismos deberían ser tratados utilizando una o más de las opciones consideradas en la Cláusula 4.6.

En algunas circunstancias, la evaluación de riesgos podría conducir a la decisión de llevar a cabo un mayor análisis.

2.6 Tratamiento del riesgo

2.6.1 General

El tratamiento del riesgo involucra identificar el rango de opciones para tratar el riesgo, evaluar esas opciones, preparar planes de tratamiento del riesgo e implementarlos.

2.6.2 Identificar opciones para tratamiento del riesgo

Las opciones de tratamiento de riesgos, que no son necesariamente mutuamente excluyentes o apropiadas en todas las circunstancias, incluyen:

- Evitar el riesgo decidiendo no seguir adelante con la actividad que probablemente crea el riesgo (cuando esto sea practicable).

El escape al riesgo puede ocurrir inadecuadamente a raíz de la tendencia de alguna gente u organizaciones a tener aversión a los riesgos. El escape inadecuado al riesgo puede aumentar la significación de otros riesgos o podría conducir a la pérdida de oportunidades de obtener beneficios.

- Cambiar la probabilidad de ocurrencia, para mejorar la probabilidad de resultados beneficiosos y reducir la probabilidad de pérdidas.

- Cambiar las consecuencias, para aumentar la magnitud de los beneficios y reducir la magnitud de las pérdidas. Esto también podría incluir respuesta a la emergencia, planes de contingencia y de recupero de desastres.

- Transferir el riesgo.

Esto involucra a otra parte sosteniendo o compartiendo alguna parte del riesgo. Los mecanismos incluyen el uso de contratos, acuerdos de seguros y estructuras organizacionales tales como sociedades y *joint ventures*. Generalmente hay algún costo financiero o beneficio asociado a la transferencia de parte del riesgo a otra organización, tal como el premio pagado por los seguros. Idealmente, las responsabilidades por el tratamiento de los riesgos debería ser asignado a las partes más aptas para controlarlos. Las responsabilidades deberían ser acordadas entre las partes en el momento más temprano posible. La transferencia de un riesgo a otras partes, o la transferencia física a otros lugares, reducirá el riesgo para la organización original, pero podría no disminuir el nivel global de riesgo para la sociedad. A menudo, tal transferencia de riesgo sólo cambia un tipo de riesgo por otro, de forma tal, que ambas partes terminan con los tipos de riesgos que están más aptos para tolerar, tratar o retener. Cuando los riesgos son total o parcialmente transferidos, la organización que transfiere el riesgo ha adquirido un nuevo riesgo, y es que la organización a la cual se ha transferido el riesgo no pueda administrar el riesgo eficazmente.

- Retener el riesgo.

Luego que los riesgos han sido reducidos o transferidos, podrían existir riesgos residuales que sean retenidos. Los riesgos también podrían ser retenidos en forma predeterminada, ej: cuando hay una falla para identificar o transferir adecuadamente, o bien tratar los riesgos.

2.6.3 Evaluar opciones de tratamiento de riesgos

Las opciones deberían ser evaluadas sobre la base del grado de reducción de las pérdidas, y el alcance de cualquier beneficio adicional u oportunidades creadas, tomando en cuenta los criterios desarrollados. Pueden considerarse y aplicarse una cantidad de opciones, ya sea individualmente o combinadas.

La selección de la opción más apropiada involucra balancear el costo de implementar cada opción contra los beneficios derivados de la misma. En general, el costo de administrar los riesgos necesita ser conmensurado con los beneficios obtenidos.

Cuando grandes cambios en el riesgo puede obtenerse con un costo relativamente bajo, tales opciones deberían ser implementadas.

Otras opciones de mejora podrían ser antieconómicas y se necesita ejercitar el juicio para determinar si las mismas son justificables.

Las decisiones deberían tomar en cuenta la necesidad de considerar cuidadosamente los riesgos raros pero severos que podrían justificar acciones de tratamiento de riesgos que no serían justificables en el terreno de lo estrictamente económico
.

Cuando se realizan esos juicios de costos versus beneficios, es importante considerar todos los costos y perjuicios, como asimismo, todos los beneficios y oportunidades. Mientras que un control en particular puede ser muy eficaz en la reducción de la probabilidad de un tipo específico de pérdida, el mismo también puede quitar la oportunidad de beneficios.

En muchos casos, es improbable que cualquier opción de tratamiento de riesgos sea una solución completa para un problema en particular. A menudo la organización se beneficiará sustancialmente por una combinación de opciones tales como cambiar la probabilidad de los riesgos, cambiar sus consecuencias, y transferir o retener cualquier riesgo residual. Un ejemplo es el uso eficaz de contratos y financiamiento de riesgos sustentado por un programa de reducción de riesgos.

Cuando el costo acumulativo de implementar todos los tratamientos de riesgos excede el presupuesto disponible, el plan debería identificar claramente el orden de prioridad en el cual deberían ser implementados los tratamientos individuales de riesgo. El ordenamiento de prioridades puede ser establecido utilizando distintas técnicas, incluyendo análisis de importancia de los riesgos y de costo-beneficio. Los requerimientos de cumplimiento legal podrían estar por encima de los análisis de costo-beneficio.

Los tratamientos de riesgos que pueden ser implementados dentro del límite del presupuesto disponible pueden esperar la disponibilidad de recursos futuros o, si por cualquier razón algunos o todos los tratamientos restantes son considerados importantes, deberá analizarse el caso para lograr financiación adicional. En todos los casos es importante comparar el costo total de no tomar ninguna acción contra el aparente ahorro presupuestario.

Las opciones de tratamiento de riesgos deberían considerar los valores y percepciones de los interesados y las formas más apropiadas de comunicarse con ellos.

Las estrategias de tratamiento de riesgos podrían por si mismas introducir nuevos riesgos. Estos riesgos necesitan ser identificados, evaluados, tratados y monitoreados como porte del proceso iterativo.

Si luego de un tratamiento hay un riesgo residual, debería tomarse una decisión sobre si retener este riesgo o repetir el proceso de tratamiento de riesgos.

2.6.4 Preparar e implementar planes de tratamiento

Los planes deberían documentar cómo serán implementadas las opciones escogidas.

Los planes de tratamiento deberían identificar las responsabilidades, las fechas programadas, los resultados esperados de los tratamientos, el presupuesto, las medidas del desempeño y el proceso de revisión a poner en práctica.

Los planes también deberían incluir mecanismos para evaluar la implementación de las opciones respecto de criterios de desempeño, las responsabilidades individuales y otros objetivos, y procesos para monitorear los logros respecto de mojones críticos de implementación.

La implementación exitosa del plan de tratamiento del riesgo requiere un sistema de administración eficaz que especifique los métodos escogidos, asigne responsabilidades individuales por las acciones y las monitoree en relación a criterios especificados.

2.7 Monitoreo y revisión

Es necesario monitorear la eficacia de todos los pasos del proceso de administración de riesgos. Este es un paso importante para la mejora continua.

Los riesgos y la eficacia de las medidas de tratamiento necesitan ser monitoreados para asegurar que las circunstancias cambiantes no alteren las prioridades. La auto evaluación del control provee un medio para la revisión continua de los riesgos y de sus controles.

Es esencial la revisión sobre la marcha para asegurar que el plan de administración se mantenga relevante. Los factores que podrían afectar la probabilidad y consecuencia de un resultado podrían cambiar, como también los factores que afectan la conveniencia o costo de las opciones de tratamiento. Es en consecuencia necesario repetir el ciclo de administración de riesgos regularmente. La revisión es una parte integral de los planes de tratamiento de la

administración de riesgos.

El progreso real respecto de los planes de tratamiento de los riesgos provee una medida importante de desempeño y deberían ser incorporados en el sistema de información, medición y administración de desempeño de la organización.

El monitoreo también involucra aprender de los eventos y de sus resultados.

2.8 Registrar el proceso de administración de riesgos

Debería registrarse en forma adecuada cada etapa del proceso de administración de riesgos. Deberían registrarse las presunciones, hipótesis, métodos, fuentes de datos, análisis, resultados y razones para las decisiones.

Los registros de tales procesos son también un aspecto importante de un buen gobierno corporativo.

Las decisiones concernientes al alcance y método de registro podrían involucrar costos y beneficios y deberían tomar en cuenta las razones para mantener la documentación.

Bibliografía

Arellano G; F. Jaime (1990). Elementos de investigación: la investigación a través de su informe. Editorial EUNED. Costa Rica.

Cubillos M. Euclides (1999). Manual de la metodología diseño de controles para sistemas de información computadorizados. Editorial AUDISIS. Colombia.

Echenique Antonio José (1990). Auditoria en Informática. Editorial Mc Graw Hill. México.

González Saénz, Néstor (1996). Comunicaciones y Redes. Editorial Prentice Hall Hispanoamericana. México.

Gómez, Miguel (2003). Elementos de estadística descriptiva. Editorial UNED. Costa Rica.

Hernández Hernández, Enrique (2002). Auditoría en informática, Editorial CECSA. México.

Hernández Sampieri, Roberto; Fernández Collado, Carlos y Baptista Lucio, Pilar (2003). Metodología de la investigación. Editorial Mc Graw Hill. México

Mantilla B, Samuel Alberto (2002). Control Interno Estructura Conceptual Integrada. Editorial ECOE. Colombia.

Sauvé Jacques Philippe; Ferreira Giozza William (1996). Redes Locales de Computadores. Editorial Mc Graw Hill. Brasil.

Tanenbaum, Andrew S. (1998). Redes de Ordenadores. Editorial Prentice Hall Hispanoamericana. México.

La Asamblea Legislativa de la República de Costa Rica (2002). Ley general de control interno, La gaceta N°169. Costa Rica.

Contraloría General de la República (2002). Manual de normas generales de control interno para la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización. La Gaceta Nº 107. Costa Rica.

Comité Directivo de COBIT y la Information System audit. And Control Foundation (1998). COBIT Objetivos de Control para la Información y Tecnologías Relacionada.

Instituto Latinoamericano y del Caribe de Planificación Económica y Social – ILPES Dirección de Gestión del Desarrollo Local y Regional (2002) www.enlac.cl/ilpes/publicaciones.html

[1] COSO.— Corresponde a las siglas de “Committee of Sponsoring Organizations of the Treadway Commision” (Comité de Organizaciones Patrocinadoras de la Comisión Treadway, agrupación que reunió la información sobre tendencias y conocimientos relativos a control interno a nivel mundial y presentó una visión actualizada de la materia, incluyendo el concepto que se encuentra vigente en los Estados Unidos de América y que ha logrado reconocimiento en diversos países y organizaciones internacionales.