UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO
PROGRAMA DE POSGRADO EN AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN

# AUDITORÍA DE ADQUISICIÓN E IMPLEMENTACIÓN DEL SISTEMA BASE UNIFICADA DE CLIENTES

Trabajo Final de Investigación Aplicada, sometido a la Comisión del Programa de Estudios de Posgrado en Administración de Empresas para optar por el grado de Magíster en Auditoría de Tecnologías de Información

MARICRUZ RICHMOND CHACÓN

Ciudad Universitaria Rodrigo Facio, Costa Rica

2007

*Dedicada a mi hijo Heiner, mi novio Ricardo y a mis padres*
*por todo el apoyo y paciencia durante estos*
*tres años de ausencia y sacrificio.*

# AGRADECIMIENTOS

A Dios por haberme acompañado a lo largo de este camino y darme las fuerzas para salir adelante y permitirme seguir creciendo tanto personal como profesionalmente.

A Heiner por ser mi fuente diaria de inspiración, por ser un ejemplo de fortaleza y lucha constante, por enseñarme que siempre existe una luz el final del camino y sobre todo por su apoyo y comprensión durante la maestría.

A Ricardo por su confianza, su colaboración en todo este proceso, por creer en mí y siempre tener una palabra de aliento en los ratos más difíciles.

A mis Padres por su ayuda incondicional durante estos 3 años, porque sin ellos el camino habría sido más difícil de terminar.

A Guis, Fran, Carlitos, Luis y Walter, mi grupo a lo largo de la maestría; por tantos sábados de tertulias y estudio, por brindarme su apoyo y sobre todo por los buenos momentos.

# Índice

# CAPÍTULO I. INTRODUCCIÓN

Desde hace varias décadas las empresas han venido apoyándose en el campo de la informática para mejorar y agilizar sus procesos, al buscar que la organización sea cada vez más eficaz y eficiente. Por tal razón, la creación de sistemas informáticos ha sido fundamental para el éxito de las empresas, debido a sistemas que han sido creados para procesos simples como llevar una bitácora de los empleados y su respectiva información, hasta procesos mucho más complejos que involucran alta capacidad computacional.

El desarrollo de estos sistemas puede ser interno a la organización, externo o inclusive una mezcla de ambos. Para todos ellos se debe de contar, entre otras cosas, con un buen planeamiento que permita llevar a cabo el proyecto de principio a fin y entregar los resultados esperados, o de ser posible, superarlos. El desarrollo externo a la organización permite poder seleccionar el proveedor que mejor se adapte a las necesidades de la empresa y a la vez cumpla con los requerimientos solicitados por la empresa, para lo cual en varios casos, se debe de llevar a cabo un proceso de selección entre múltiples oferentes.

A este proceso de selección del proveedor se le conoce también como el proceso de adquisición. En la actualidad, las empresas buscan adquirir productos de manera sencilla, ágil, exacta para cumplir con las estimaciones dadas, además este proceso pueda llegar a ser repetitivo. Sin embargo, con el progreso, producto de las tecnologías, esto resulta ser complicado para las organizaciones si no cuenta con una metodología clara basada en las experiencias de adquisiciones anteriores; las cuales pueden ser aplicadas como referencia para futuras contrataciones dentro de la empresa.

En el Instituto Nacional de Seguros (INS) se aprobó el desarrollo de un Sistema Unificado de Clientes (BUC), dado que en la actualidad cuenta con múltiples

aplicaciones transaccionales en las cuales constantemente se registra información de todos los clientes quienes hacen uso de cualquiera de los servicios brindados por el INS, por lo tanto no cuenta con una sola fuente de origen de datos, esto ocasiona duplicidad de información, mayor trabajo para los funcionarios e información distinta para un mismo cliente. Por cuanto el registro de datos en cada sistema es diferente, no ha sido posible generar consultas consolidadas en las que se pueda ver cuales son los productos adquiridos por un determinado cliente, éstas son las razones de la contratación con la cual se espera crear una base única de clientes y, por ende, tener un mejor control sobre la información con la cual se cuenta.

## *Justificación*

El Instituto Nacional de Seguros, en vías de adquirir un sistema que cubra las necesidades de la Institución, ofreció por medio de un concurso, la Licitación por Registro N°306010 para la elaboración del mismo. Esta licitación fue adjudicada a la empresa Productos Informáticos para el Desarrollo S.A. (Prides S.A.), la cual a la fecha se encuentra en las etapas finales del proyecto. Es por esta razón que surge la necesidad de realizar una auditoría al proceso de adquisición e implementación del Sistema Unificado de Clientes, con el fin de que la elaboración de la licitación salvaguarde los intereses de la Institución, así como el cumplimiento de lo especificado en ella misma haya sido implementado, además de la funcionalidad del sistema para el usuario final. Adicionalmente, éste proyecto podrá servir de marco para futuras auditorias similares.

El análisis radicalmente determina los distintos mecanismos existentes en la Institución, con el fin de medir el impacto que tiene la Adquisición de Tecnologías y los medios disponibles para su regulación y control.

# CAPÍTULO II. MARCO TEÓRICO

El proyecto de Práctica Profesional se enfoca en la Auditoría de la Adquisición e Implementación de un sistema Unificado de Clientes (BUC) en el Instituto Nacional de Seguros (INS). Para llevar a cabo este estudio, se tomarán como criterios la Ley de Contratación Administrativa, el COBIT 4.1 (Control Objectives for Information Technology) específicamente en el módulo de Adquisición e Implementación y el Manual de Normas Generales para el Ejercicio de la Auditoría, los cuales buscan mejorar los procesos de contratación, sin embargo no siempre son utilizados como guía para la elaboración y el control sobre la licitación.

Es importante contar con una metodología definida para minimizar los riesgos que eventualmente se presentan durante el proceso de adquisición y durante la implementación del sistema. De lo contrario, la empresa puede desarrollar sistemas que no satisfagan ninguna necesidad ni presentar ninguna oportunidad para si misma en la asignación de recursos tanto económicos como humanos que al final no aportaran ningún valor agregado a la Institución, identificándose esto en una etapa anterior (incluso inicial) del proyecto. Se debe contar con puntos de control, los cuales también puedan ser puntos de decisión para la continuidad o no del proyecto, al considerar factores de factibilidad, funcionalidad, así como cambios repentinos en las prioridades del negocio. Es aquí en donde el auditor juega un papel crítico dado que es el encargado de validar el correcto seguimiento del proceso, así como identificar las áreas en las cuales el proceso mismo o los controles internos estén fallando, de tal manera se realicen las mejoras necesarias.

Antes de continuar con el repaso de las funciones del auditor, es importante mencionar algunos conceptos generales de Auditoria con el fin de tener un conocimiento más amplio y, por ende, un entendimiento preciso del estudio particular durante el desarrollo del proyecto.

A continuación se describen conceptos esenciales con la finalidad de ubicar al lector en el ámbito de la presente investigación:

## *Auditoría*

Es un examen crítico sistemático el cual se realiza con el objeto de evaluar la eficiencia y eficacia de una sección de una entidad y dar un valor agregado a la entidad con el fin de que mejore sus procesos. La naturaleza de la auditoría es recopilar y evaluar información cuantificable de una entidad con el propósito de determinar si son llevados acabo los criterios establecidos.

Para llevar a cabo una auditoría se necesita contar con información verificable y criterios, los cuales pueden estar compuestos por estándares, leyes, normas, políticas o disposiciones mediante las cuales el auditor evalúa la información obtenida. Es importante mencionar que existen distintos tipos de auditarías como por ejemplo: Auditaría de Estados Financieros, Auditaría de Operaciones, Auditaría de cumplimiento, Auditoría de tecnologías de Información, entre otras.

En todos los casos, el auditor debe estar capacitado para entender los criterios que se utilizan y ser competente para que determine cual es la cantidad y el tipo de evidencia por recopilar, por otro lado el auditor debe contar con total independencia, pues requiere un pensamiento objetivo para los juicios y las decisiones que deban de tomarse.

Hay varias formas de evidencia, entre las cuales se mencionan: observaciones de parte del auditor, fotografías, testimonios verbales, comunicaciones por escrito, entre otras. Existen dos puntos importantes con respecto a la evidencia, esta debe ser competente y suficiente, para satisfacer el objetivo de la auditoría.

En la etapa final del proceso de auditoría se encuentra el informe de auditoría en donde se comunican los hallazgos a la Administración Superior de la entidad. Estos

difieren en naturaleza, pero todos los informes de auditoría dan a conocer la correspondencia que existe entre la información recopilada y los criterios establecidos.

Es aquí en donde la Administración Superior, basada en los hallazgos del auditor, debe determinar las mejoras necesarias tanto a los procesos como a los controles internos o incluso al seguimiento de los mismos. En muchas situaciones, se refiere a la auditoría como el proceso encargado de identificar quién es el culpable de que los resultados no sean los esperados, sin embargo este concepto es erróneo, por cuanto la auditoría tiene como propósito: identificar cuál aspecto no está cumpliendo su objetivo y, posteriormente sea analizado, así mismo solucionen los problemas.

## *Auditoría de Tecnologías de Información*

Se puede decir que la Auditoría de Tecnologías de Información es la revisión y la evaluación de los controles, sistemas y procedimientos de la informática, de los equipos de cómputo, su utilización, eficacia y seguridad, durante el procesamiento de la información a fin de que se logre una utilización más confiable y segura de la información; así misma para mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente.

Los principales objetivos de la auditoría informática son:

- Salvaguardar los activos.
- Integridad de los datos.
- Efectividad de sistemas.
- Eficacia de sistemas.
- Seguridad y confidencialidad.

La auditoría de TI deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistema o procesamiento específico, sino que además deberá evaluar los sistemas de información en general desde sus entradas, procedimientos, comunicación, controles, archivos, seguridad, recurso humano y obtención de información, así como los datos, el "hardware", "software" y personal también son recursos críticos de la entidad, algunas entidades tiene inversiones multimillonarias en estos aspectos por lo que una pérdida ya sea intencional o no intencional causaría daños considerables a la entidad.

Ahora bien, cuando se habla de una Auditoría de TI ésta resulta ser muy amplia, ya que, como se acaba de mencionar, abarca los diferentes elementos de TI como lo son el "hardware", "software", el recurso humano, entre otros. Por tal razón las Auditorías de TI pueden enfocarse en un aspecto o incluso en un proyecto en particular, por lo tanto se puede contar con auditorías de diversos tipos. Muchas empresas optan principalmente por este tipo de auditorías pues buscan realizarla sobre las áreas consideradas más problemáticas y, de esta forma mejorar los procesos y los controles internos. Claro está que cuando la auditoría es realizada por un ente externo y al margen del cumplimiento de ley, la empresa no dicta los parámetros por auditar.

## *Auditoría de Adquisición de Tecnologías de Información*

La Adquisición de Tecnologías de Información provee los recursos de TI, incluye personas, "hardware", "software" y los servicios cuando sea necesario y a través de la definición de procesos de aprovisionamiento, la selección adecuada de proveedores y la configuración de condiciones contractuales.

El ISACA en su Documento G11 "El Efecto de Controles Penetrantes en TI" de su Lineamiento de Auditoría de TI, en la sección 2.4 se refiere a los controles que deben de existir a lo largo de los 4 dominios del COBIT, a su vez menciona que la efectividad de los controles en los dominios de Adquisición e Implementación (AI) y

Entrega y Soporte (DS) son influenciados por la efectividad de los controles que operan en los dominios de Planeación y Organización (PO) y Monitoreo (M).

En la sección 2.4.3 se refiere a un ejemplo en el cual se indica que los controles efectivos y detallados de TI sobre el proceso de “Adquirir y Mantener Software de Aplicación” (Proceso de Referencia de COBIT AI2) son afectados por lo adecuado de los controles penetrantes de TI sobre los procesos que se incluyen:

- “Definir un Plan Estratégico de TI” (Proceso de Referencia COBIT PO1).
- “Administrar Proyectos” (Proceso de Referencia COBIT PO10).
- “Administrar la Calidad” (Proceso de Referencia COBIT PO11).
- “Monitorear los Procesos” (Proceso de Referencia COBIT M1).

Por esta razón, en la sección 2.4.4 se aclara que la auditoria de la adquisición de un sistema de aplicación debe de incluir la identificación del efecto de la estrategia de TI, el enfoque para la administración de proyectos, la administración de la calidad y el enfoque hacia el monitoreo. En cuyo caso se determine, por ejemplo, que la administración de proyecto es inadecuada, el auditor de TI debe de considerar:

- Planear trabajo adicional para asegurar efectivamente que el proyecto específico este siendo auditado y administrado de manera efectiva.
- Reportar a la gerencia las debilidades en los controles penetrantes de TI.

# CAPÍTULO III. PLANIFICACIÓN PRELIMINAR

## *Nombre de la Auditoría*

Auditoría de la Adquisición e Implementación del Sistema Unificado de Clientes (BUC).

## *Objetivo*

Determinar la existencia de una metodología eficiente para la Adquisición de un "Software" que permita determinar el mejor oferente para beneficio de la organización como un todo.

## ***Objetivos Específicos***

1. Determinar la existencia de un estudio de factibilidad para determinar la viabilidad del proyecto.
2. Verificar la utilización y el cumplimiento de la Ley de Contratación Administrativa y estándares internacionales para la realización del proceso de licitación del BUC.
3. Verificar si el personal a cargo del proceso de licitación está calificado tanto para realizarlo como recomendar la mejor opción.
4. Verificar que el proceso de desarrollo, hecho por Prides S.A., cumplió con los requerimientos indicados en la licitación.
5. Determinar si el BUC es pertinente para satisfacer las necesidades de la organización.
6. Determinar la participación de la auditoría interna en el proceso de adquisición para evaluar el cumplimiento de las recomendaciones que se hayan brindado.

## *Alcance*

El presente proyecto de práctica se limitará a revisar el proceso de adquisición e implementación del Sistema de Información Médico Administrativo (SIMA) en el Instituto Nacional de Seguros (INS).

## *Criterios Generales de Auditoría*

### ***Normas técnicas para la gestión y el control de las Tecnologías de Información***[1]

**3.1 Consideraciones Generales de la Implementación de TI**

**Criterio 1:** 3.1.a. Adoptar políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI.

**Criterio 2:** 3.1.b. Establecer el respaldo claro y explícito para los proyectos de TI tanto del jerarca como de las áreas usuarias.

**Criterio 3:** 3.1.c. Garantizar la participación activa de las unidades o áreas usuarias, las cuales deben tener una asignación clara de responsabilidades y aprobar formalmente las implementaciones realizadas.

**Criterio 4:** 3.1.d. Instaurar líderes de proyecto con una asignación clara, detallada y documentada de su autoridad y responsabilidad.

[1] Tomado de las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) , de la Contraloría General de la Republica de Costa Rica

**Criterio 5:** 3.1.f. Contar con una definición clara, completa y oportuna de los requerimientos, como parte de los cuales debe incorporar aspectos de control, seguridad y auditoría bajo un contexto de costo –beneficio.

**Criterio 6:** 3.1. g. Tomar las previsiones correspondientes para garantizar la disponibilidad de los recursos económicos, técnicos y humanos requeridos.

**Criterio 7:** 3.1. h. Formular y ejecutar estrategias de implementación que incluyan todas las medidas para minimizar el riesgo de que los proyectos no logren sus objetivos, no satisfagan los requerimientos o no cumplan con los términos de tiempo y costo preestablecidos.

### 3.2 La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos

**Criterio 8:** 3.2. b. Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación postimplementación de la satisfacción de los requerimientos.

**Criterio 9:** 3.2. c. Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.

**Criterio 10:** 3.2.d. Controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración.

**Criterio 11:** 3.2. e. Definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.

## ***Control Objectives for Information Technology - COBIT 4.1***[2]

### Adquisición e Implementación

**Criterio 12:** AI1 – Identificar Soluciones Automatizadas

La necesidad de una nueva aplicación o función requiere de análisis antes de la adquisición o creación para asegurar que los requerimientos de negocio son satisfechos con un enfoque efectivo y eficiente. Este proceso cubre la definición de las necesidades, consideración de fuentes alternativas, revisión de la factibilidad tecnológica y económica, ejecución de un análisis de riesgos y de costo-beneficio y la conclusión de una decisión final de “hacer” o “comprar”. Todos estos pasos ayudan a las organizaciones a minimizar el costo de adquirir e implementar soluciones mientras asegura que permiten al negocio alcanzar sus objetivos.

**Criterio 13:** AI2 – Adquirir y mantener el Software de Aplicación

Las aplicaciones se hacen disponibles conforme a los requerimientos de negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión adecuada de los controles de la aplicación y los requerimientos de seguridad, así como el desarrollo y la configuración de acuerdo con los estándares. Esto permite a las organizaciones brindar el soporte adecuado a las operaciones de negocio con la aplicación automatizada correcta.

[2] Tomado del Control Objectives for Information Technology - COBIT 4.1 del IT Governance Institute.

**Criterio 14:** AI3 – Adquirir y mantener la Infraestructura de Tecnología

Las organizaciones tienen procesos para la adquisición, implementación y mejora de la infraestructura tecnológica. Esto requiere un enfoque planificado para la adquisición, el mantenimiento y la protección de la infraestructura de acuerdo con las estrategias de tecnología previamente aprobadas y la provisión de ambientes de desarrollo y pruebas. Esto asegura que hay soporte tecnológico continuo para las aplicaciones de negocio.

**Criterio 15:** AI4 – Habilitar la Operación y su uso

El conocimiento de nuevos sistemas se hace disponible. Este proceso requiere la producción de documentación y manuales de usuarios y de TI, provee entrenamiento para asegurar el uso apropiado y la operación de las aplicaciones e infraestructura.

**Criterio 16:** AI5 – Obtener Recursos de TI

Los recursos de TI, incluyendo persona, “hardware”, “software” y servicios deben de ser obtenidos. Esto requiere la definición y el seguimiento de procesos de obtención, la selección de proveedores la definición de acuerdos contractuales y la adquisición en sí. Llevar a cabo lo anterior asegura que la organización cuenta con todos los recursos de TI de manera oportuna y de costo apropiado.

**Criterio 17:** AI6 – Administrar los cambios

Todos los cambios, incluyendo mantenimientos y parches de emergencia relacionados a la infraestructura y las aplicaciones dentro del ambiente de producción son administradas formalmente y de manera controlada. Los cambios (incluyendo aquellos a procedimientos, procesos, parámetros de sistema y servicio) son registrados, evaluados y autorizados previos a la implementación y revisados contra el resultado

esperado posterior a la implementación. Esto asegura la mitigación de los riesgos de impactar negativamente la estabilidad o la integridad del ambiente de producción.

**Criterio 18:** AI7 – Instalar y Acreditar Soluciones y Cambios

Los sistemas nuevos deben de hacerse operacionales una vez que se complete el desarrollo, lo cual requiere pruebas apropiadas en un ambiente dedicado con datos de pruebas relevantes, definición de las instrucciones de implantación y migración, planeamiento de la liberación y la puesta en producción, así como una revisión post implementación, lo cual asegura que los sistemas operacionales están en línea con las expectativas y resultados acordados previamente.

## ***Ley de Contratación Administrativa***[3]

**Criterio 19:** Artículo 5.- Principio de igualdad y libre competencia.

*"En los procedimientos de contratación administrativa, se respetará la igualdad de participación de todos los oferentes potenciales. Los reglamentos de esta Ley o las disposiciones que rijan los procedimientos específicos de cada contratación, no podrán incluir ninguna regulación que impida la libre competencia entre los oferentes potenciales…"*

[3] Tomado de la Ley No. 7494, Ley de Contratación Administrativa, publicada en Gaceta No. 110, Alcance No. 20.

**Criterio 20:** Artículo 6.- Principio de publicidad.

*"Los procedimientos de contratación se darán a la publicidad por los medios correspondientes a su naturaleza.*

*Todo interesado tendrá libre acceso al expediente de contratación administrativa y a la información complementaria.*

*En el primer mes de cada período presupuestario, los órganos y los entes sujetos a las regulaciones de esta Ley darán a conocer, por medio del Diario Oficial, el programa de adquisiciones proyectado, lo cual no implicará ningún compromiso de contratar.*

*En el Diario Oficial se insertará un boletín que funcionará como sección especial dedicada exclusivamente a la contratación administrativa."*

**Criterio 21:** Artículo 27.- Determinación del procedimiento.

*"Cuando la ley no disponga un procedimiento específico en función del tipo de contrato, el procedimiento se determinará de acuerdo con las siguientes pautas: ... para las contrataciones superiores a ciento ochenta millones de colones (¢ 180.000.000,00); la licitación por registro para las contrataciones entre ciento ochenta millones de colones (¢180.000.000,00) y ochenta millones de colones (¢ 80.000.000,00)…"*

**Criterio 22:** Artículo 33.- Garantía de participación.

*"La Administración exigirá, a los oferentes, una garantía de participación, entre un uno por ciento (1%) y un cinco por ciento (5%) del monto de la propuesta, el cual se definirá en el cartel o pliego de condiciones respectivo, de acuerdo con la complejidad del contrato.*

*La administración deberá solicitar al oferente corregir defectos formales, como: falta de timbres, de copias, de autenticación de firmas o de documentos. Los defectos deberán subsanarse en el plazo que indique el Reglamento de esta Ley, siempre que no se afecte el contenido de la oferta en cuanto a los bienes y los servicios ofrecidos, sus precios, los plazos de entrega ni las garantías."*

**Criterio 23:** Artículo 34.- Garantía de cumplimiento.

*"La Administración exigirá una garantía de cumplimiento, entre un cinco por ciento (5%) y un diez por ciento (10%) del monto de la contratación. Este monto se definirá en el cartel o en el pliego de condiciones respectivo, de acuerdo con la complejidad del contrato, para asegurar el resarcimiento de cualquier daño eventual o perjuicio ocasionado por el adjudicatario.*

*La garantía se ejecutará hasta por el monto necesario para resarcir, a la Administración, los daños y perjuicios imputables al contratista.*

*Cuando exista cláusula penal por demora en la ejecución, la garantía no podrá ejecutarse con base en este motivo, salvo la negativa del contratista para cancelar los montos correspondientes por ese concepto.*

*La ejecución de la garantía de cumplimiento no exime al contratista de indemnizar a la Administración por los daños y perjuicios que no cubre esa garantía."*

**Criterio 24:** Artículo 45.- Estructura mínima.

*"En la licitación por registro, se invitará a participar a todos los proveedores del bien o el servicio, acreditados en el registro correspondiente. De ello, se dejará constancia en el expediente respectivo.*

*Cuando el número de proveedores inscritos para un determinado objeto sea superior a diez, se faculta a la Administración para invitar a participar, en la licitación, por medio de una publicación en el Diario Oficial y, facultativamente, en dos diarios de circulación nacional.*

*Cuando el número de proveedores inscritos para un determinado objeto sea inferior a cinco, la Administración deberá invitar a participar en la licitación, por medio de una publicación en el Diario Oficial y, facultativamente, en dos diarios de circulación nacional por lo menos."*

**Criterio 25:** Artículo 66.- Criterios.

*"Las condiciones personales, profesionales o empresariales de los participantes determinarán la adjudicación. El precio no constituirá el único factor determinante para comparar las ofertas."*

## ***Constitución Política de la República de Costa Rica***

**Título VII – La Educación y la Cultura**
**Capítulo Único**

**Criterio 26:** Artículo 76.

*"El español es el idioma oficial de la Nación…"*

## *Metodología*

En la investigación se analizará la metodología aplicada, el proceso de licitación, determinar el grado de participación que tuvo la Auditoría Interna en el proceso de adquisición, validar si para este proceso se contó con representación adecuada de la parte técnica y del negocio, así como también, validar los controles que se tuvieron a lo largo del desarrollo del software hasta la conclusión del mismo, para esto se hará:

- Revisión de la Licitación y documentación.
- Revisión de la Ley de Contratación Administrativa vigente a la fecha de contratación.
- Revisión de estándares internacionales para la adquisición de aplicaciones.
- Realización de entrevistas.
- Aplicación de listas de chequeo.

## *Conocimiento de la Organización*

El **Instituto Nacional de Seguros** fue creado mediante la Ley No.12, del 30 de octubre de 1924 con el propósito de responder a las necesidades de protección de la sociedad costarricense.

En sus inicios se formó como Banco de Seguros y posteriormente en el año 1948, cambió el nombre a INSTITUTO NACIONAL DE SEGUROS; el seguro de vida fue su primera póliza el cual se puso a la venta el 05 de noviembre de 1925.El 17 de febrero de 1926, se autoriza al Banco a manejar el Seguro de Incendio y en junio de ese mismo año, por medio de Decreto Ejecutivo No.16, se asumió la administración del Seguro sobre Accidente de Trabajo. Fueron estos los primeros productos que el INS puso a disposición de los costarricenses.

El **INSTITUTO NACIONAL DE SEGUROS** ofrece una amplia gama de productos y servicios, junto con una fuerte proyección social con programas de beneficio como por

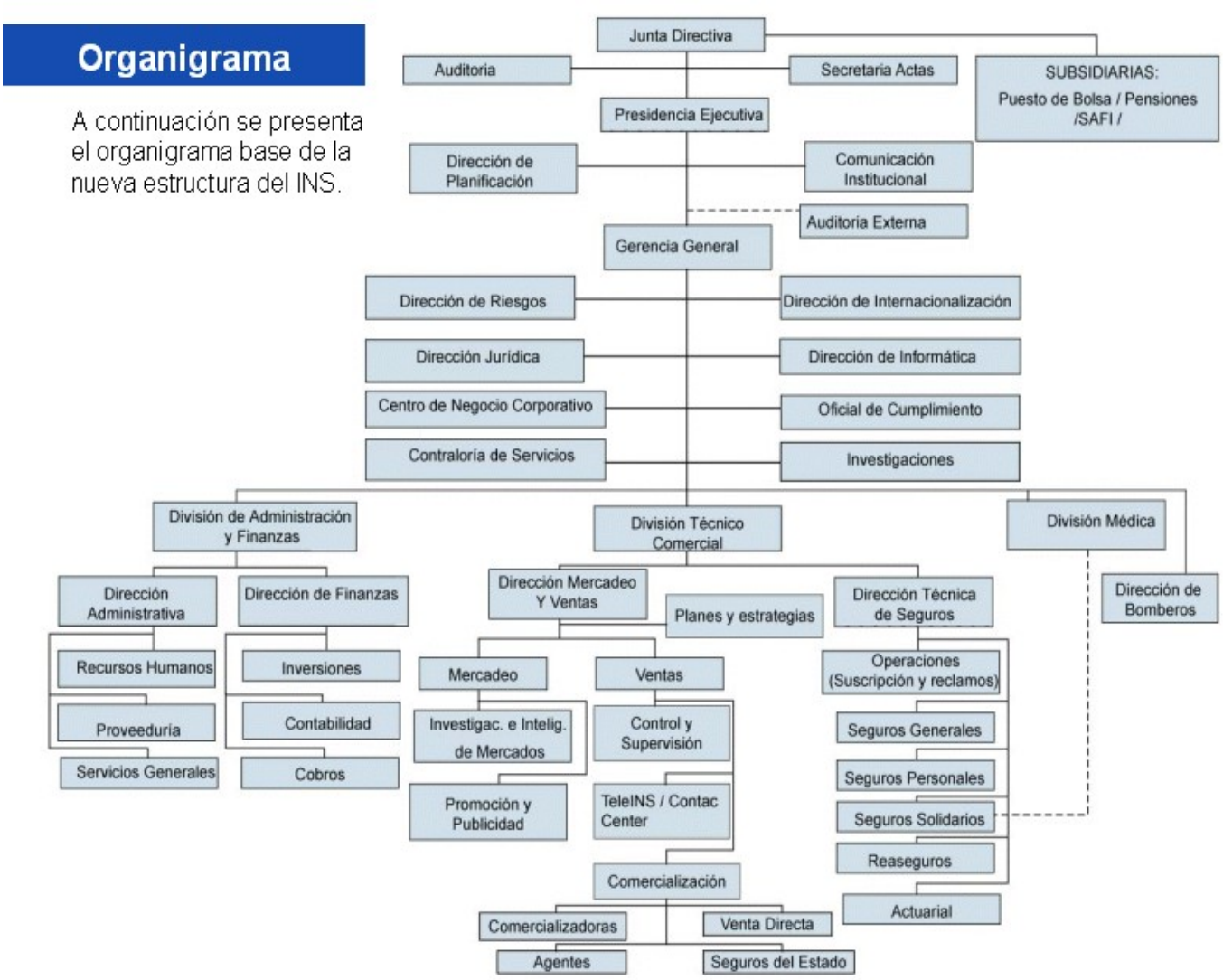
ejemplo; el Benemérito Cuerpo de Bomberos, el Programa Infantil de Brigadas de Seguridad, las Campañas de Prevención de Riesgos del Trabajo, Accidentes de Tránsito e Incendios Forestales.

Cuenta con oficinas administrativas como centros de salud en todo el territorio nacional, con el fin de brindar un mejor servicio a los clientes y solventar las necesidades que se presenten en un menor tiempo de espera.

## ***Ubicación***

- Oficinas Centrales: se encuentra situada en las calles 9 y 11, avenida 7.
- Agencias y Dispensarios Médicos: se encuentran en todo el territorio nacional.

## ***Organigrama Institucional***




## ***Misión***

"Brindar soluciones de protección personal y patrimonial al mercado, con seguros y servicios competitivos y con responsabilidad social."

## ***Visión***

“Seremos la empresa de seguros líder en el mercado nacional y con proyección comercial internacional.”

## ***Valores***

1. **Integridad**: en el INS lo más importante es que actuamos conforme a nuestros valores personales e institucionales. Para nosotros la integridad consiste en que haya concordancia entre el hacer y el decir. Al ser el primer valor, será la integridad lo que, ante cualquier circunstancia, rija nuestras decisiones.

2. **Compromiso:** creer en lo que hacemos, hacerlo de la mejor forma, defender nuestra posición y sentirnos orgullosos de nuestro trabajo y de nuestra empresa, es el significado que tiene el valor del compromiso para los colaboradores del INS.

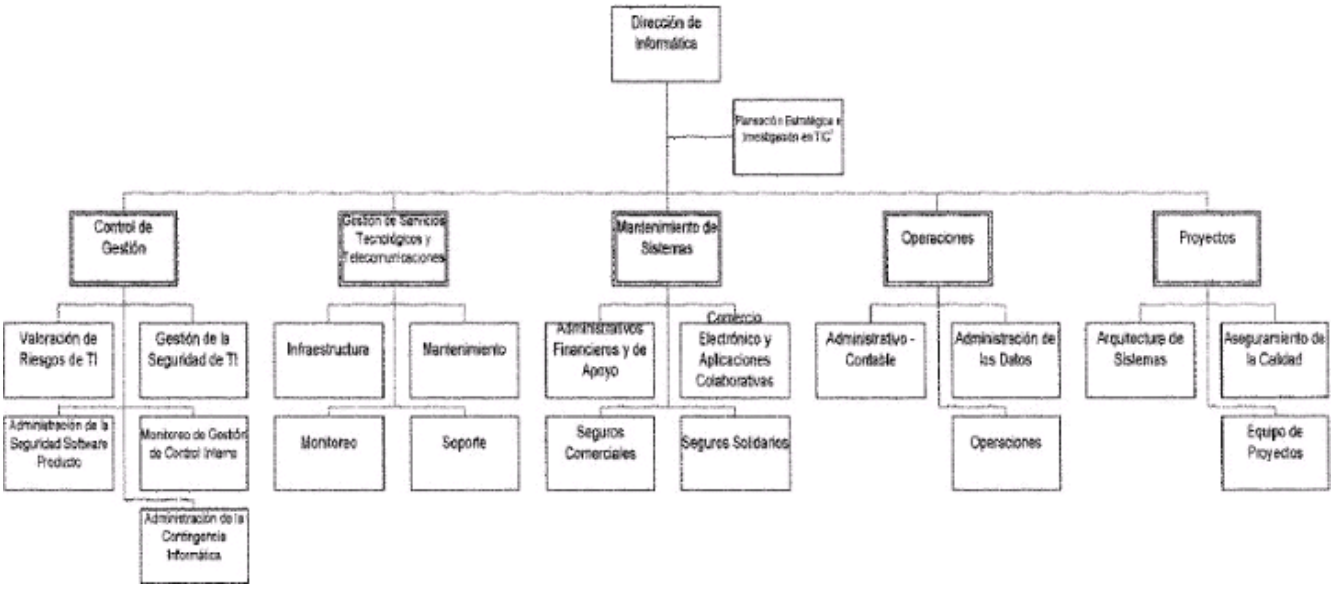
3. **Solidaridad:** vivimos la solidaridad porque nuestro quehacer tiene que ver con el bienestar de las personas. La esencia del INS es brindar protección a todos, y trabajar siempre en la búsqueda de nuevos y mejores servicios.

4. **Equidad**: el trabajo del INS se caracteriza por brindar satisfacción a las partes involucradas, de manera justa. El trato con los diferentes públicos relacionados con la empresa se fundamenta en el respeto de los alcances acordados.

## *Conocimiento del Área de Tecnologías de Información*

El área de tecnologías de Información del Instituto Nacional de Seguros es la responsable de proveer la tecnología necesaria para soportar los objetivos y la estrategia comercial de la Organización que se formulan para dar cumplimiento a la misión y visión institucionales, la gestión informática se agrupa en tres categorías las cuales son: a corto, mediano y largo plazo.

## ***Organigrama de la Dirección de Informática***



## ***Misión***

Como ente rector en materia de tecnología de información y comunicaciones, facilitamos soluciones integrales, de alta calidad y oportunas, para el apoyo a la toma de decisiones a todos los niveles de la organización. Dentro de un ambiente que promueva el mejoramiento continuo, trabajo en equipo, y una actitud proactiva hacia la solución de problemas de nuestros clientes.

## ***Visión***

En el 2008, seremos reconocidos como la dirección de apoyo, líder en facilitar el fortalecimiento institucional, mediante la aplicación de tecnología de la información y comunicación

## ***Objetivos***

### Soporte tecnológico acorde con los objetivos y las estrategias del negocio.

- Establecer una arquitectura abierta y consolidada, bajos costos, portable, escalable, alta capacidad, alta disponibilidad, contingente, segura, confiable, independencia del proveedor.
- Garantizar una eficiente gestión de TI.
- Aplicación de procedimientos de adquisición de hardware y Software para reducción de costos y oportunidad en la atención de requerimientos.
- Proveer el mantenimiento adecuado a los servicios de TI.
- Contar con la estructura organizacional adecuada para proveer los servicios TI.

**Compromiso para proveer soluciones oportunas y eficientes.**

- Contar con una infraestructura para la atención y control del servicios
- Contar con personal motivado para garantizar su compromiso en el desempeño de sus funciones

## Satisfacción de necesidades.

- Atención integral

# CAPÍTULO IV. PLANIFICACION DETALLADA

| ***PROCESO DE CONTRATACIÓN*** | | |
|---|---|---|
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Políticas, procedimientos y manuales para el proceso de adquisición de tecnologías | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Verifique si la empresa cuenta con políticas, procedimientos y manuales para el proceso de adquisición de tecnologías determine si:<br>.a Se encuentran revisados y aprobados por la gerencia.<br>.b Si fueron divulgados a todo el personal.<br>.c Se encuentran accesibles.<br>.d Si son actualizados constantemente. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Proceso de elaboración de la licitación | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Verifique si están definidos los responsables de la elaboración de la licitación.<br>• Determine si dentro del proceso de elaboración de la licitación se toma en cuenta tanto la parte técnica como la legal de la organización.<br>• Verifique si se encuentran definidos los responsables de analizar y determinar el proveedor. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Validación de Garantía | **Comentarios:** |

| | | |
|---|---|---|
| | *Detalle/Pruebas*<br>Verifique si la licitación cuenta con los siguientes aspectos:<br>a. Garantía.<br>b. Tiempo de respuesta.<br>c. Lugar en donde se presta la garantía.<br>d. Vigencia. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Validación de Documentación técnica, manual de usuario y manual operacional por entregar | **Comentarios:** |
| | *Detalle/Pruebas*<br>Verifique si la licitación cuenta con los siguientes aspectos:<br>a. Formato de entrega de la documentación.<br>b. Idioma.<br>c. Plazo de entrega.<br>d. Pertinente. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Validación de Forma de Pago | **Comentarios:** |
| | *Detalle/Pruebas*<br>Verifique si la licitación cuenta con los siguientes aspectos:<br>a. Frecuencia y monto del pago.<br>b. Criterio para realizar el pago. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Validación de Sanciones | **Comentarios:** |
| | *Detalle/Pruebas*<br>Verifique si la licitación cuenta con los siguientes aspectos:<br>a. Especificación de Sanciones.<br>b. Monto de las sanciones. | |

| Obtener Información Preliminar | **Paso de Procedimiento:**<br>Validación de Requerimientos | **Comentarios:** |
|---|---|---|
| | *Detalle/Pruebas*<br>Verifique si la licitación cuenta con los siguientes aspectos:<br>a. Claridad de los requerimientos.<br>b. Completitud de los requerimientos. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Validación del Equipo de Trabajo | **Comentarios:** |
| | *Detalle/Pruebas*<br>Verifique si la licitación cuenta con los siguientes aspectos:<br>a. Formación académica del equipo de trabajo.<br>b. Experiencia en trabajos similares.<br>c. Funciones definidas. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Validación de Confidencialidad, Propiedad Intelectual y Código Fuente | **Comentarios:** |
| | *Detalle/Pruebas*<br>Verifique si la licitación cuenta con los siguientes aspectos:<br>a. Entrega de código fuente.<br>b. Cláusula de confidencialidad.<br>c. Cláusula sobre propiedad intelectual. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Validación de Metodología y Herramientas de Desarrollo | **Comentarios:** |
| | *Detalle/Pruebas*<br>Verifique si la licitación cuenta con los siguientes aspectos:<br>a. Metodología de desarrollo definida.<br>b. Indica las herramientas de desarrollo a utilizar.<br>c. Responsable de proveer las licencias del software. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Validación de Evaluación de las Ofertas | **Comentarios:** |

| | | |
|---|---|---|
| | *Detalle/Pruebas*<br>Verifique si la licitación cuenta con los siguientes aspectos:<br>a. Criterios de evaluación.<br>b. Objetividad en la evaluación. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Validación de Capacitación | **Comentarios:** |
| | *Detalle/Pruebas*<br>Verifique si la licitación cuenta con los siguientes aspectos:<br>a. Capacitación practica.<br>b. Responsable de la Capacitación.<br>c. Cantidad de personas por capacitar.<br>d. Lugar en donde se impartirá la capacitación<br>e. Contenido de la capacitación. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Validación de Disolución | **Comentarios:** |
| | *Detalle/Pruebas*<br>Verifique si la licitación cuenta con:<br>a. Cláusula de disolución de la licitación.<br>b. Motivos para la disolución. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Validación de Pruebas del Sistema | **Comentarios:** |

| | | |
|---|---|---|
| | *Detalle/Pruebas*<br>Verifique si la licitación cuenta con los siguientes aspectos:<br>a. Pruebas del sistema.<br>b. Frecuencia de las pruebas.<br>c. Responsables.<br>d. Criterio de aceptación. | |
| ***ESTÁNDARES DE DESARROLLO*** | | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Desarrollo de acuerdo con los planes y políticas | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Verifique si la empresa cuenta con un Plan Estratégico para el área de Tecnologías de Información.<br>• Si cuentan con un plan estratégico para el área de TI determine si:<br>.a Se encuentra éste alineado con el plan estratégico de la compañía.<br>.b Fue divulgado al personal de la empresa. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Manual de Estándares | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Verificar si existe un manual de estándares para el desarrollo de los proyectos.<br>• Verificar si los manuales se encuentran actualizados.<br>• Verificar si estos manuales se utilizan. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Proyecto de Desarrollo | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Verificar que los requerimientos y su documentación se encuentran claros y fáciles de entender. | |

| | | |
|---|---|---|
| | • Verificar que exista un patrocinador.<br>• Verificar que exista un Director de proyectos asignado.<br>• Determinar que el equipo de analistas y programadores disponibles tengan el perfil necesario para llevar a cabo el proyecto.<br>• Revisar que exista un cronograma de actividades.<br>• Revisar que las áreas de pruebas en los equipos de computo, sea el necesario para tal trabajo.<br>• Analizar las plantillas definidas de control de riesgos para poder llevar el control de los mismos.<br>• Determinar que se encuentre bien definido e indicado en el contrato cual será la forma de pago. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Administración del Proyecto | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Controlar y evaluar los riesgos que pongan en peligro la continuidad del proyecto para mitigarlos o bien eliminarlos.<br>• Verificar si cumplen el cronograma existente.<br>• Verificar si presentan informes indicando los avances del proyecto.<br>• Analizar si se encuentran bien definidas las responsabilidades y funciones al equipo de trabajo.<br>• Verificar si las reuniones entre los programadores y usuarios se tomaron en cuenta en el cronograma de actividades. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Ciclo de Vida | **Comentarios:** |

| | | |
|---|---|---|
| | *Detalle/Pruebas*<br>• Existe una metodología de desarrollo definida a ser utilizada en el CVDS y aprobada por el departamento de TI y la Gerencia.<br>• Si existe esta metodología determinar si incluye las siguientes etapas:<br>.a Estudio Preliminar.<br>.b Estudio de Factibilidad.<br>.c Análisis y determinación de requisitos.<br>.d Diseño conceptual del sistema.<br>.e Diseño físico del sistema.<br>.f Desarrollo de la programación.<br>.g Desarrollo de la documentación.<br>.h Pruebas del sistema.<br>.i Implementación.<br>.j Evaluación post-implementación.<br>• Verificar si se definieron etapas de evaluación para determinar la aplicación de esta metodología. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Investigación Preliminar | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Revisar si cuentan con una guía del proyecto.<br>• Verificar si han identificado los riesgos que pueda causar este proyecto para la empresa.<br>• Verifique si se cuenta con un cronograma de las actividades y fechas de entrega y conclusión del proyecto.<br>• Analizar si los altos jerarcas están comprometidos con el proyecto para poder destinar todo el recurso humano necesario y poder patrocinarlo.<br>• Revisar si se han identificado las áreas a las que se van a tomar en cuenta para este nuevo proyecto. | |

| | | |
|---|---|---|
| | • Determinar si se ha designado un Gerente para el proyecto.<br>• Verifique si se tiene una guía del proyecto. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>**Estudio de Factibilidad** | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Analizar si se hizo un estudio costo/beneficio del proyecto.<br>• Estudiar si con el nuevo sistema se reducen los tiempos de respuesta.<br>• Analizar los tipos de mejora que brindara el sistema. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>**Desarrollo Conceptual** | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Verificar que exista un estudio para determinar si la creación de un nuevo proyecto o sistema de cómputo es apropiado.<br>• Verificar si se cuenta con la documentación adecuada de:<br>.a La que genere el analista a la hora arrancar el proyecto.<br>.b Las pruebas de los usuarios, programadores y base de datos.<br>.c Los errores tanto de los programadores, base de datos como de los usuarios.<br>.d Diseño de la base de datos.<br>.e Los requerimientos que definen el diseño del sistema.<br>.f Corrección de errores ocurridos en el sistema.<br>.g Nuevos componentes en el diseño.<br>.h Para pruebas del diseño del sistema.<br>.i Para el visto bueno del sistema.<br>.j Determinar si la documentación es aprobada y analizada por el personal adecuado.<br>• Verificar las pantallas de entrada que se tienen que tener, para | |

| | | |
|---|---|---|
| | la entrada de datos en el sistema. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Desarrollo de la documentación | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Toda la información que se ha obtenido para la fase de planeación es información actualizada.<br>• Se han creado documentos de diseño bien detallados.<br>• Se han documentado todos los requerimientos, solicitados tanto por la alta gerencia como por los usuarios.<br>• Se lleva documentación de los errores encontrados a lo largo del desarrollo del proyecto.<br>• Existe el control de las versiones actualizadas de la documentación. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Desarrollo de las pruebas | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Se hacen pruebas de unidad, donde el mismo desarrollador prueba el código que desarrollo para ver si funciona bien.<br>• Se hacen pruebas de rendimiento para poder ver si el sistema puede soportar la carga de los usuarios de la compañía.<br>• Se hacen pruebas de funcionalidad para poder verificar que los requerimientos estén funcionando de acuerdo con los que se pidió.<br>• Se hacen pruebas de aceptación en donde son los mismos usuarios los que revisan los requerimientos y dan la aprobación. | |

| | | |
|---|---|---|
| | • Existen reuniones para revisar lo que se encontró en las pruebas y ver si se corrigió.<br>• Existen pruebas post-implementación. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Implementación | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Verificar la documentación de los procesos para pasar a producción.<br>• Verificar la documentación del pase a producción de los programas.<br>• Verificar y Analizar la documentación de pase de las bases de datos en producción.<br>• Verificar y Analizar la documentación de la revisión de las pruebas finales en producción del sistema nuevo o cambio a realizar.<br>• Verificar y Analizar la documentación que los usuarios deben llenar para revisar el sistema nuevo en producción.<br>• Verificar y Analizar la documentación de los vistos buenos del sistema en la implantación por parte de todas las partes involucradas. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Evaluación Post-Implementación | **Comentarios:** |

| | | |
|---|---|---|
| | *Detalle/Pruebas*<br>• Verificar si existe una metodología para medir la satisfacción de los usuarios por indicadores.<br>• Verificar si se formaliza la satisfacción por escrito de los sistemas ya implantados.<br>• Existe una guía de revisión para los usuarios. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Control y Rastreo de Transacciones | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Estudie si se incluyen los rastros de auditoria de las transacciones realizadas en el sistema.<br>• Analice si se establecen los controles necesarios para la manipulación de errores.<br>• Revise si se establecen procedimientos de seguridad para salvaguardar la información.<br>• Verifique si definen los procedimientos de respaldo y recuperación en caso de fallo. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Participación de Usuarios | **Comentarios:** |
| | *Detalle/Pruebas*<br>• Verifique si tienen planeadas reuniones con los usuarios para poder ir revisando el avance del proyecto.<br>• Analice si tomaron en cuenta los usuarios de las áreas donde se implementara el nuevo sistema, de todos los niveles de estos departamentos.<br>• Determine si existe un proceso de capacitación práctico para los usuarios en el cual se puedan evacuar dudas y sirva de aceptación para el sistema. | |

| | | |
|---|---|---|
| | • Estudie si se tomaron en cuenta a los usuarios al momento del levantamiento de los requerimientos. | |
| **DOCUMENTACÓN** | | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Documentación del Manual de Usuario | **Comentarios:** |
| | • Determine que existe un manual de usuario que explica la forma de ejecución del sistema.<br>  • Descripción general del sistema.<br>  • Ejecución del sistema.<br>  • Arranque el sistema.<br>  • Control de acceso y seguridad en el sistema.<br>  • Descripción de componentes del sistema.<br>  • Descripción del menú principal.<br>  • Descripción de submenús.<br>  • Descripción de interfaces gráficas de usuario.<br>  • Uso del sistema.<br>  • Operaciones por cada interfaz gráfica de usuario.<br>  • Captura.<br>  • Consulta.<br>  • Modificación.<br>  • Eliminación.<br>  • Descripción de productos del sistema.<br>  • Descripción de condiciones de error y su manejo. | |

| Obtener Información Preliminar | Paso de Procedimiento:<br>Documentación del Manual de Operación | Comentarios: |
|---|---|---|
| | • Determine que existe un manual de operación que explica la forma de instalación y operación del sistema.<br>  • Requerimientos del sistema.<br>  • Configuración de ambiente.<br>  • Proceso de instalación.<br>  • Monousuario.<br>  • Red.<br>  • Web.<br>  • Proceso de respaldo de la información.<br>  • Proceso de recuperación de la información.<br>  • Proceso de actualización.<br>  • Descripción de errores.<br>  • Seguridad. | |
| **Obtener Información Preliminar** | **Paso de Procedimiento:**<br>Documentación del Manual Técnico | **Comentarios:** |
| | • Compruebe la existencia de un manual de técnico que detalla todos los aspectos técnicos del sistema de información.<br>  • Diagrama General.<br>  • Diagrama de la Base de Datos.<br>  • Diccionario de Datos.<br>  • Campos de Relación entre Tablas.<br>  • Definición de variables de ambiente y librerías.<br>  • Programas Especiales y de Ambiente.<br>  • Estándares de Diseño y Programación.<br>  • Restricciones o límites de la programación.<br>  • Flujograma Información/Proceso/Actividad. | |

| | | |
|---|---|---|
| | • Programas utilizados por proceso/actividad.<br>• Relación Programa/Archivo(s).<br>• Relación Archivo/Programa(s).<br>• Descripción y Relación de Programas. | |

# CAPÍTULO V. ELABORACIÓN DE HALLAZGOS E INFORME

| REF P/T | |
|---|---|
| | **TÍTULO:**<br>Estándares de desarrollo. |
| | **CONDICIÓN:**<br>Carecen de estándares para el desarrollo. |
| | |
| | **CRITERIO:**<br>COBIT - PLANEACIÓN Y ORGANIZACIÓN<br>**PO8.3 Estándares de Desarrollo y Adquisición**<br>Adoptar y dar mantenimiento a estándares para todos los desarrollos y las adquisiciones que siguen el ciclo de vida del entregable final, y que incluye la aceptación de entregables claves basados en los criterios de aceptación acordados anteriormente. Considerar estándares para la codificación de "software"; convenciones de nombramiento, formatos de archivos, estándares de diseño del esquema y diccionario de datos, así los estándares de interfaz de usuario, interoperabilidad, eficiencia del rendimiento del sistema, escalabilidad, estándares para desarrollo y pruebas; validación contra requerimientos, planes de prueba y pruebas de unidad, regresión e integración. |
| | |
| | **CAUSA:**<br>La Dirección de Informática no había puesto en práctica un estándar para el desarrollo de sistemas; actualmente existe un proyecto interno para definir los estándares de desarrollo, los cuales servirán como guía para futuros desarrollos y adquisiciones. |
| | |

| | |
|---|---|
| | **EFECTO:**<br>Al carecer de una guía al momento para realizar un desarrollo de sistemas, estos se desarrollan según el criterio del grupo de trabajo, lo cual impacta el nivel de complejidad para el mantenimiento del mismo, ya que depende en gran medida del conocimiento de los desarrolladores y de los manuales técnicos que elaboren, así mismo la interoperabilidad entre sistemas se ve afectada, porque no se desarrollaron bajo ningún estándar. |
| | |
| | **RECOMENDACIÓN:**<br>1. A LA DIRECCIÓN DE INFORMÁTICA<br>Adoptar un estándar de desarrollo que sirva de guía al momento de adquirir y desarrollar los sistemas de información. |

| REF P/T | |
|---|---|
| | **TÍTULO:**<br>Especificar el idioma de la documentación en la licitación. |
| | **CONDICIÓN:**<br>En el cartel de licitación no se indica el idioma en el que el proveedor debe entregar la documentación solicitada como parte del desarrollo de la aplicación. |
| | |
| | **CRITERIO:**<br>Constitución Política de la República de Costa Rica.<br>Título VII – La Educación y la Cultura.<br>Capítulo Único<br>**Artículo 76.-** "El español es el idioma oficial de la Nación…" |
| | |
| | **CAUSA:**<br>Los responsables de elaborar el cartel de licitación no tomaron en cuenta la importancia de indicar el idioma en el cual se necesita la documentación entregada por el proveedor. |
| | |
| | **EFECTO:**<br>Al no especificar el idioma de la documentación esto causaría que tanto los usuarios como técnicos no comprendan la documentación a su disposición para la aplicación. |
| | |

| | |
|---|---|
| | **RECOMENDACIÓN:**<br>1. AL DIRECTOR DE PROYECTO<br>Revisar que toda la documentación entregada por el proveedor, generada a raíz de la BUC, sea en el idioma español.<br><br>2. A LA DIRECCIÓN DE INFORMÁTICA<br>Especificar el idioma en que se quiere la documentación del sistema adquirido, en futuras contrataciones. |

| REF P/T | |
|---|---|
| | **TÍTULO:**<br>Participación del área usuaria durante el proceso de desarrollo del sistema. |
| | **CONDICIÓN:**<br>Los usuarios únicamente fueron tomados en cuenta en la etapa inicial del desarrollo. |
| | |
| | **CRITERIO:**<br>Normas técnicas para la gestión y el control de las Tecnologías de Información.<br>3.1 Consideraciones Generales de la Implementación de TI.<br>3.1.c. Garantizar la participación activa de las unidades o áreas usuarias, las cuales deben tener una asignación clara de responsabilidades y aprobar formalmente las implementaciones realizadas. |
| | |
| | **CAUSA:**<br>Según indica el director de proyecto, en esta etapa no es importante la participación de los usuarios, esto debido a que el sistema es únicamente de consulta. |
| | |
| | **EFECTO:**<br>No hacer partícipes a los usuarios en todas las etapas del proyecto puede implicar que no se tomen en cuenta los requerimientos, al mismo tiempo éstos se conozcan hasta el momento en el cual dicho sistema se encuentre en producción. Adicionalmente, provocaría una interrupción en la utilización del sistema, pues este no se adapta a las necesidades ni a las expectativas de la Institución. |
| | |
| | **RECOMENDACIÓN:**<br>1. AL DIRECTOR DE PROYECTOS<br>Incluir a los usuarios dentro de las pruebas para la aprobación del sistema y para la aprobación de la implementación del mismo.<br>Tomar en cuenta la participación de los usuarios en todas las etapas del sistema y en las pruebas para futuros proyectos. |

| REF P/T | |
|---|---|
| | **TÍTULO:**<br>Análisis de Riesgo. |
| | **CONDICIÓN:**<br>Carecen de un plan de soluciones en caso de que ocurra alguno de los riesgos previamente identificados por el equipo de trabajo del proyecto. |
| | |
| | **CRITERIO:**<br>COBIT<br>ADQUISICIÓN E IMPLEMENTACIÓN.<br>AI1.2 Reporte del Análisis de Riesgo<br>Identificar, documentar y analizar los riesgos asociados con los requerimientos de negocio y diseño de las soluciones como parte del proceso de la organización para el desarrollo de los requerimientos. |
| | |
| | **CAUSA:**<br>El Director de Proyecto comenta que el equipo de trabajo dedicado al desarrollo del sistema únicamente identifica los riesgos, pero no elabora un plan de soluciones en caso de que estos se materialicen. |
| | |
| | **EFECTO:**<br>Carecer de un plan para mitigar los riesgos o las soluciones en caso de que se materialicen podría arriesgar la continuidad del negocio y la ejecución exitosa del proyecto lo cual ocasionaría una posible pérdida cuantiosa de dinero a la Institución. |
| | |

| | |
|---|---|
| | **RECOMENDACIÓN:**<br>1. AL DIRECTOR DE PROYECTO<br>Elaborar un plan de soluciones para mitigar los riesgos identificados y, además un plan de contingencias en caso de que estos se materialicen.<br><br>2. A LA DIRECCIÓN DE INFORMÁTICA<br>Diseñar un procedimiento de análisis de riesgos que establezca, tanto la identificación de los riesgos, el manejo de los mismos, responsables, así como la determinación de soluciones en cuyo caso se materialicen. |

| REF P/T | |
|---|---|
| | **TÍTULO:**<br>Actualización de documentación. |
| | **CONDICIÓN:**<br>La documentación que se generó de las etapas de planeación y análisis del proyecto se encuentra desactualizada. |
| | |
| | **CRITERIO:**<br>COBIT<br>ADQUISICIÓN E IMPLEMENTACIÓN.<br>AI6.5 Finalización y documentación de cambios<br>En el momento en que los cambios son implementados, actualizar los sistemas y la documentación de usuarios y procedimientos asociados, de acuerdo con el cambio.<br><br>LICITACIÓN POR REGISTRO N°306010<br>G. DOCUMENTACIÓN<br>Durante el período de servicio, el adjudicatario debe mantener actualizada la documentaron relacionada (Modelo de datos, modelo entidad-relación, diagramas de diseño (arquitectura), documentación de análisis, programas, diccionario de datos, manuales técnicos, de operación y de usuario, material de capacitación y cualquier otra documentaron relacionada). |
| | |
| | **CAUSA:**<br>El proveedor, quien según la licitación, es el responsable de mantener actualizada la documentación generada por el desarrollo del sistema, no ha actualizado tal información. |
| | |

| | |
|---|---|
| | **EFECTO:**<br>Carecer de la documentación actualizada puede hacer más complejo el proceso de recreación de un elemento del proyecto o el proyecto en sí, así mismo el mantenimiento se puede ver impactado por no contar con documentación que guía al individuo quien realiza la labor y el traspaso de conocimiento, podría generar un costo elevado a la Institución tanto en tiempo, recurso humano y dinero. |
| | |
| | **RECOMENDACIÓN:**<br>1. A LA DIRECCIÓN DE INFORMÁTICA<br>Notificar al proveedor del incumplimiento de lo pactado en la licitación y aplicar las sanciones respectivas.<br><br>2. AL DIRECTOR DEL PROYECTO<br>Considerar dentro del cronograma del proyecto de la BUC así como en futuros proyectos, los tiempos necesarios para la actualización de la documentación generada a lo largo del mismo. |

| REF P/T | |
|---|---|
| | **TÍTULO:**<br>Medición de la satisfacción de usuarios post-implementación. |
| | **CONDICIÓN:**<br>Carecen de un plan para medir la satisfacción de los usuarios post-implementación. |
| | |
| | **CRITERIO:**<br>Normas técnicas para la gestión y el control de las Tecnologías de Información.[4]<br>3.2 La organización debe implementar el "software" que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos.<br>3.2. b. Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación post-implementación de la satisfacción de los requerimientos. |
| | |
| | **CAUSA:**<br>Al momento de la planeación, los usuarios fueron tomados en cuenta únicamente en la etapa inicial del proyecto y no se valoró la necesidad de conocer su satisfacción una vez implementado el sistema. |
| | |
| | **EFECTO:**<br>No medir la satisfacción de los usuarios post-implementación podría generar rechazo al sistema por parte de estos, así como el riesgo de que el sistema desarrollado no cubra las necesidades de la Institución. |
| | |

[4] Tomado de las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) , de la Contraloría General de la Republica de Costa Rica

| | |
|---|---|
| | **RECOMENDACIÓN:**<br>1. AL DIRECTOR DEL PROYECTO<br>Definir las reuniones con los usuarios para medir la satisfacción del sistema post-implementación.<br><br>En futuros proyectos se debe tomar en cuenta la participación de los usuarios en todas las etapas del proyecto y diseñar un plan para medir la satisfacción de los mismos posterior a la implementación. |

# CAPÍTULO VI. CONCLUSIONES DE LA PRÁCTICA PROFESIONAL

En los últimos años, el avance tecnológico ha ido en un constante crecimiento, el cual se ha visto reflejado en la mayoría de las organizaciones, indistintamente al negocio que se dedique. Hoy en día, las organizaciones han adquirido pequeñas computadoras las cuales cuentan con una alta capacidad de procesamiento; acortan procesos y crean acceso a la información más exacta, utilizada para la toma de decisiones.

Si se analiza la inversión efectuada por las organizaciones en compra de tecnología, se observa la importancia que tiene, para la “Alta Gerencia”, mantener un estricto control sobre la adecuada utilización de estas herramientas, así como mantener la integridad de la información que viaja por estos medios.

Para lograr esta evaluación, la organización requiere que el auditor cuente con la capacitación técnica en materia de sistemas de información e informática, para lo cual debe realizar una serie de auditorias periódicas y contar con un adecuado seguimiento de las recomendaciones para así dar un valor agregado a la organización. El auditor velará por los intereses de la organización al indicar las inconsistencias encontradas, tanto por parte del personal interno como del personal de empresas subcontratadas.

En la implementación y la adquisición de sistemas de información, el auditor es el encargado de validar que el proyecto se realice o, se haya realizado, apegado al proceso de desarrollo determinado por la empresa, y en caso contrario, presentar las recomendaciones necesarias para que la situación sea corregida, tanto en el proyecto actual como en futuras adquisiciones. Aún cuando, existe la función de Director de Proyecto, por la misma urgencia de poner el sistema en producción, se pueden ignorar aspectos del desarrollo del proyecto que son necesarios, como por ejemplo la

actualización de la documentación, al ser éste un ejemplo de un posible hallazgo determinado por el auditor.

Adicionalmente, el auditor en sistemas de información debe contar con el conocimiento actualizado en las áreas auditadas; por el contrario no podrá formular las recomendaciones adecuadas al obviar situaciones en las que existe alguna inconsistencia o al indicar errores cuando en realidad no los hay, cuyo resultando es la pérdida de credibilidad del auditor.

Finalmente, el apoyo de la Gerencia para con la función del auditor de tecnologías de información es fundamental para lograr que la auditoría identifique las áreas en las cuales se encuentran irregularidades, por medio de la participación de los empleados involucrados, así como la información y la evidencia asociada a la auditoría, de lo contrario, la auditoría podría determinarse incompleta.

# BIBLIOGRAFÍA


- Arens, Alvin A; Loebbecke, James K. Auditoría un Enfoque Integral. Sexta Edición.
- Echenique García, José A. Auditoría en Informática. McGraw-Hill. 2da. Edición.
- Davis, Chris. IT Auditing: Using Controls to Protect Information Assets. McGraw-Hill. 2007.
- IT Governance Institute. COBIT 4.1 – Control Objectives for Information Technology. 2005.
- Information Systems Audit and Control Association. IS Auditing Guideline: Effect of Pervasive IS Controls. Document G11.
- Contraloría General de la Republica de Costa Rica. Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).
- Ley de Contratación Administrativa, Ley N° 7494 del 02/05/1995. Gaceta N° 110, Alcance N° 20 del 08/06/1995.
- Constitución Política de la República de Costa Rica.


## Nodos de Internet


- http://www.network-sec.com/COBIT_AI
- http://www.isaca.org

# ANEXOS

## *Glosario de Términos*

### Aplicaciones

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

### 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.

### Confidencialidad

Es la protección de la información sensible contra divulgación no autorizada.

### Cumplimiento

Se refiere al cumplimiento de las leyes, regulaciones y acuerdos contractuales a los cuales el proceso del negocio esta sujeta.

### Disponibilidad

Se refiere a la disponibilidad de la información cuando es requerida por el proceso del negocio ahora y en el futuro.

### Efectividad

Se refiere a que la información debe ser pertinente, oportuna, correcta, consistente y utilizable.

## Eficiencia

Es la provisión de la información en una manera más productiva y económica de los recursos.

## Evidencia

Es la información obtenida por el auditor para llegar a las conclusiones sobre las cuales se basa la opinión de la auditoría. La evidencia de auditoría debe cumplir con dos características indispensables como lo son: competente y suficiente.

## Integridad

Precisión y suficiencia de la información, así como su validez de acuerdo con los valores y expectativas del negocio.

## Tecnología

Al hablar de tecnología se refiere a “hardware”, “software”, sistemas de administración de base datos, redes, multimedia, sistemas operativos, etc.