Manual sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computarizados.

CONTENIDO

303.05.01 Estudio preliminar

303.05.02 Estudio de factibilidad

303.05.03 Análisis y determinación de los requerimientos de información

303.05.04 Diseño conceptual del sistema

303.05.05 Diseño físico del sistema

303.05.06 Desarrollo de la programación

303.05.07 Desarrollo de la documentación

303.05.08 Prueba del sistema

303.05.09 Implantación

303.05.10 Evaluación post-implantación

303.06 Procesamiento en paralelo

303.07 Procedimientos de control y rastros de las transacciones

303.08 Participación de los usuarios en el CVDS

303.09 Participación del auditor en el CVDS

303.10 Modificaciones a los SIC

304 DOCUMENTACIÓN

304.01 Desarrollo de la documentación de conformidad con el Manual de estándares

304.02 Documentación del sistema

304.03 Documentación del programa

304.04 Documentación del usuario

304.05 Documentación de las operaciones del computador

304.06 Documentación de otros procedimientos

305 OPERACIÓN

305.01 Procedimientos adecuados para la recepción de los datos

305.02 Seguridad física

305.03 Seguridad lógica

305.04 Supervisión adecuada

305.05 Administración de la biblioteca de archivos magnéticos

305.06 Respaldo de archivos magnéticos

305.07 Plan de contingencia

305.08 Controles del equipo

305.09 Mantenimiento del equipo

Presentación

Los grandes avances en la tecnología informática que se han dado principalmente en las dos últimas décadas, han venido a afectar el funcionamiento de las entidades y órganos públicos y de manera directa y positiva a sus sistemas de información, los cuales han venido evolucionando de un estado manual de procesamiento de datos y manejo de información, a una posición en que con el apoyo del computador, realizan tales labores en grandes volúmenes y a velocidades incomparables.

El desarrollo de los sistemas de información computadorizados (SIC) involucra necesariamente una alta inversión de recursos humanos, materiales, financieros y tecnológicos, que se debe hacer en forma ordenada para un mejor aprovechamiento de los fondos públicos.

Con especial complacencia, la Contraloría General de la República como rectora del Ordenamiento de Control y Fiscalización Superiores de la Hacienda Pública y con el propósito de contribuir en la administración eficiente y eficaz del patrimonio público, emite la primera parte del Manual sobre normas técnicas de control interno relativas a los sistemas de información computadorizados.

Si bien esta normativa es de acatamiento obligatorio por parte de las entidades y órganos que conforman la Hacienda Pública, tiene como fin fundamental ser una guía para la Administración en su responsabilidad de establecer, mantener y perfeccionar sus sistemas de control interno, tal y como está establecida en el artículo 60 de la Ley Orgánica de la Contraloría General de la República.

Con el propósito de que la presente normativa técnica se mantenga acorde con los tiempos y con el desarrollo tecnológico relativo a los SIC, la Contraloría General de la República mantendrá un programa de revisión y actualización periódica. Con ese objetivo agradecemos de antemano las sugerencias y comentarios que los auditores internos, administradores en general,

especialistas en informática y cualesquiera otros interesados en la materia, hagan llegar a la Dirección General de Planificación Interna y Evaluación de Sistemas. Las colaboraciones de la Administración activa podrán informarse por medio de sus unidades de Auditoría Interna.

Lic. Samuel Hidalgo Solano **CONTRALOR GENERAL DE LA REPUBLICA**

Noviembre, 1995

Manual Sobre Normas Técnicas de Control Interno Relativas a Los Sistemas de Información Computadorizados - Primera Parte -

300 NORMAS GENERALES

Procuran que los sistemas de información computadorizados (SIC) se lleven a cabo en un ambiente razonablemente controlado. Comprenden las actividades básicas de preinstalación (301), administración (302), desarrollo (303), documentación (304) y operación de los sistemas de información computadorizados (305).

301 PREINSTALACION

Se refiere a los procedimientos necesarios para lograr una orientación fundamentada y organizada de todas las actividades previas a la adquisición e instalación del computador y a la adquisición o desarrollo de los sistemas de información computadorizados. Comprende las normas relativas al estudio preliminar (301.01), al estudio de factibilidad (301.02), a la contratación del equipo de cómputo (301.03) y al plan de preinstalación (301.04).

301.01 Estudio preliminar

Se elaborará un estudio preliminar para la adquisición de hardware y software y para el desarrollo de nuevos SIC y se preparará el informe correspondiente de conformidad con las especificaciones emitidas.

Declaración interpretativa

Determinada la existencia de áreas problema o nuevas necesidades en cuanto a los sistemas de información de la organización, deberá llevarse a cabo un estudio preliminar, siguiendo los lineamientos que establecerá y aprobará para ese propósito el órgano competente. El objeto del estudio es determinar si el uso del computador y la adquisición o desarrollo del SIC, es viable técnica y económicamente y que por lo tanto, se justifica elaborar un estudio de factibilidad.

El estudio deberá llevarse a cabo preferiblemente con personal de la organización, y se escogerá aquel que esté familiarizado con las operaciones y las necesidades identificadas; no obstante, si no hubiera personal disponible o debidamente calificado, podrá recurrirse a servicios profesionales externos.

Entre otros asuntos, el informe deberá contener las conclusiones y recomendaciones de los responsables del estudio.

301.01.02 Se establecerán las especificaciones necesarias para el estudio preliminar.

Declaración interpretativa

La Administración, por medio del Comité Gerencial de Informática (302.09), formulará las especificaciones o guías de referencia para la elaboración del estudio preliminar y del informe correspondiente.

Entre otras especificaciones, se deberá definir lo siguiente:

a) *Las personas responsables de llevar a cabo el estudio.*

b) *El tiempo de ejecución estimado y las áreas oproblemas específicos que abarcará el estudio.*

c) *La información que deberá obtenerse para cada área o problema indicado, entre la que puede mencionarse:*

i. *Procedimientos actuales , volumen de información que se maneja, fuentes de datos, clases y destino*

de los documentos de salida.

ii. *Tiempos entre la entrada de datos y la salida de los reportes y horas pico.*

iii. *Diagrama general que muestre las relaciones entre las diferentes operaciones del procesamiento.*

iv. Costo actual del personal y equipo necesarios para llevar a cabo las operaciones que se desean

automatizar y el nuevo costo de recursos utilizando el computador.

v. El probable impacto que producirá el computador en la entidad u órgano y los requerimientos de comunicación y transmisión de datos entre las diversas unidades administrativas.

vi. Beneficios y ahorros que puedan preverse con la introducción del computador y con la implantación del SIC.

301.02 Estudio de factibilidad

301.02.01 De acuerdo con los resultados del estudio preliminar, se elaborará un estudio de factibilidad para la adquisición de hardware y software y para el desarrollo de nuevos SIC y se preparará el informe correspondiente en conformidad con las especificaciones emitidas.

Declaración interpretativa

El estudio de factibilidad se llevará a cabo en atención a las recomendaciones resultantes del estudio preliminar y tiene como propósito determinar los alcances del proyecto de desarrollo del SIC, las áreas de aplicación, las alternativas de solución a los problemas existentes y la factibilidad técnica y económica para su desarrollo e implantación.

Generalmente se relaciona con las áreas indicadas en el informe resultante del estudio preliminar, pero suministrando un grado mucho mayor de detalle en la descripción de las áreas problema, en la definición del sistema por desarrollar y en los costos y beneficios que se espera obtener. El personal seleccionado para llevar a cabo el estudio, deberá poseer suficiente experiencia y conocimiento en sistemas, métodos y equipo de procesamiento electrónico de datos, así como en análisis económico de proyectos ; en el caso de no disponerse del personal idóneo, deberá recurrirse a personal externo.

El informe de factibilidad ofrecerá un panorama claro de las opciones de procesamiento manual y automatizado posibles y de la solución recomendada para satisfacer el problema o necesidad existente.

El estudio de factibilidad se preparará tanto para la adquisición de hardware y software como para el desarrollo del SIC. Cuando se trate de un sistema nuevo, aún si éste formara parte de la planificación del SIG (302.03), debe completarse la fase de determinación de la factibilidad; si el SIC requerido no se encuentra contemplado dentro de la planificación del SIG, el estudio de factibilidad incluirá el determinar si es congruente con el plan estratégico del SIG y si deberá anteponerse a las prioridades de los otros SIC proyectados.

Al igual que para el estudio preliminar, el informe final relativo al estudio de factibilidad deberá contener, entre otra información, las conclusiones y recomendaciones necesarias, por ejemplo, si la adquisición de hardware, software o el desarrollo del nuevo SIC es factible técnica y económicamente. Es menester advertir que en determinados casos, algunos proyectos de automatización pueden no resultar económicamente factibles, no obstante por conveniencia institucional u otra similar, su desarrollo e implantación deberá llevarse acabo, lo cual debe quedar debidamente sustentado y documentado.

Una vez aceptados los resultados del estudio en referencia y aprobado por el máximo jerarca, con la asesoría del Comité Gerencial de Informática (302.09), el proyecto de automatización se continuará con las fases subsecuentes del CVDS (303.05).

301.02.02 Se establecerán las especificaciones necesarias para el estudio de factibilidad.

Declaración interpretativa

Al igual que para el estudio preliminar, la Administración, por medio del Comité Gerencial de Informática (302.09), definirá con claridad el alcance y los objetivos del estudio de factibilidad, así como las especificaciones requeridas.

Normalmente, entre otras especificaciones, se incluye lo siguiente:

a) *Las personas asignadas para efectuar el estudio.*

b) *Las áreas que deberán revisarse.*

c) La amplitud de la información y de la documentación requerida.

d) Estimación de las horas-hombre y del costo requerido para completar el estudio.

e) El tiempo de ejecución estimado y la fecha en que se iniciará el estudio y las intermedias en que deberá revisarse el avance de éste.

f) El contenido del informe resultante, por ejemplo:

i. Descripción general del SIC por desarrollar.

ii. Los costos y beneficios esperados de cada opción identificada, determinándose así su factibilidad técnica y económica.

iii. Las características del software y hardware requeridos.

iv. La calendarización y presupuestación de los recursos humanos, materiales, financieros y tecnológicos requeridos.

301.03 Contratación del equipo de cómputo

301.03.01 La contratación de hardware y software requeridos por la organización, se efectuará de conformidad con el ordenamiento jurídico vigente.

Declaración interpretativa

Presentado el informe sobre el estudio de factibilidad, la definición de criterios, selección, adjudicación, recibo y otros procedimientos necesarios para la contratación de los componentes físicos (hardware) y lógicos (software) de los sistemas de información computadorizados de la organización, determinados con base en dicho estudio de factibilidad, deberán efectuarse según lo dispuesto por el ordenamiento jurídico aplicable a cada entidad u órgano público.

301.03.02 Los convenios contractuales que se suscriban, deberán revisarse cuidadosamente en forma previa a su adjudicación y firma.

Declaración interpretativa

En los casos en que la entidad suscriba contratos con los proveedores, ya sea por concepto de mantenimiento, respaldo de equipo, arrendamiento o de cualquier otra naturaleza, éstos deberán revisarse con todo detalle desde el punto de vista legal, técnico y financiero, de manera que la entidad quede protegida de cualquier situación presente o futura que se contraponga a los intereses de la sana administración del patrimonio público.

La revisión deberá llevarse a cabo en forma previa a la adjudicación y firma del mismo, por personal competente.

301.04 Plan de preinstalación

Se identificarán y definirán todas las tareas o actividades previas a la instalación del equipo de cómputo y en general a la implantación del SIC y se preparará el plan de preinstalación.

Declaración interpretativa

Las tareas o actividades previas a la instalación de un computador y en general a la implantación del SIC (303.05.09), podrán controlarse en forma efectiva si se definen y se incorporan en un plan de preinstalación, el cual deberá contener una estimación de tiempo para cada actividad, que permita medir el grado de avance conforme se ejecuta. Podrán emplearse técnicas de programación tales como PERT (Program Evaluation and Review Technique), CPM (Critical Path Method) u otras que se consideren apropiadas para medir y controlar el avance real del proyecto respecto de lo planeado.

Algunas de las actividades que podrán incluirse en el plan de preinstalación son: determinar las necesidades de personal; reclutar, seleccionar y contratar personal cuando sea necesario; entrenar al personal; completar los requerimientos, el diseño y la preparación del local del computador; preparar los programas de prueba para correr en el computador; recepción y revisión del equipo contratado.

302 ADMINISTRACION

Tiene como propósito establecer una adecuada planificación, organización, dirección, control y evaluación de los sistemas de información computadorizados (SIC). Comprende las normas relativas al sistema de información gerencial (302.01), a la estructura conceptual (302.02), planificación (302.03), políticas (302.04), y estructura de la organización de dicho SIG (302.05), a la ubicación de la Unidad de Informática (302.06), a la segregación de funciones incompatibles dentro de la organización (302.07), a la segregación de funciones dentro de la Unidad de Informática (302.08), al Comité Gerencial de Informática (302.09) y a los estudios y auditorías internas y externas (302.10).

302.01 Sistema de información gerencial (SIG)

El desarrollo de los SIC se efectuará dentro de la filosofía de un sistema de información gerencial.

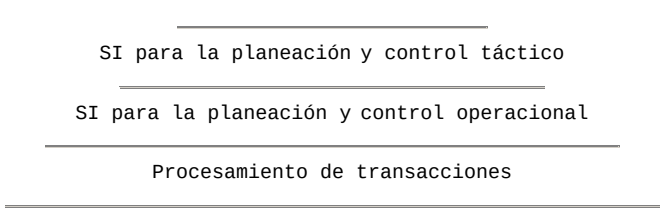
Declaración interpretativa

Se emplean diversos nombres para referirse al sistema de información gerencial (SIG) de la organización. Algunos escritores utilizan una terminología alternativa tal como sistema de información administrativa, sistema de procesamiento de información, sistema de información y de decisiones, o simplemente sistema de información.

El SIG es el sistema formal computadorizado que examina, recupera y procesa datos internos y externos a la organización para proveer información de manera eficiente y eficaz que apoye las operaciones, la administración y las funciones de toma de decisiones.

El concepto de SIG es el de una federación de subsistemas que emplea bases de datos comunes, desarrollado e implementado de acuerdo con las necesidades de la organización y constituye una orientación como concepto y filosofía integradora que guía el desarrollo y la operación de los SIC.

GRAFICO No 1 SISTEMA DE INFORMACION GERENCIAL



El SIG conforme al Gráfico Nº 1, puede describirse como una estructura piramidal en la que la parte inferior comprende un sistema de información (SI) relacionado con el procesamiento de las transacciones; el siguiente nivel comprende el SI para apoyar la planeación y el control operacional; el tercer nivel agrupa el SI para ayudar a la planeación y el control tácticos; el nivel más alto comprende el SI necesario para apoyar la planeación y el control estratégicos en los niveles determinativos y gerenciales de la Administración. Bajo esa estructura, cada nivel indicado puede utilizar la información suministrada por los niveles inferiores respectivos.

Conforme con lo descrito, el SIG desempeña un papel fundamental en la formulación de la estrategia corporativa, en el sentido de que proporciona una estructura continua y formalizada que reúne información tanto interna como externa.

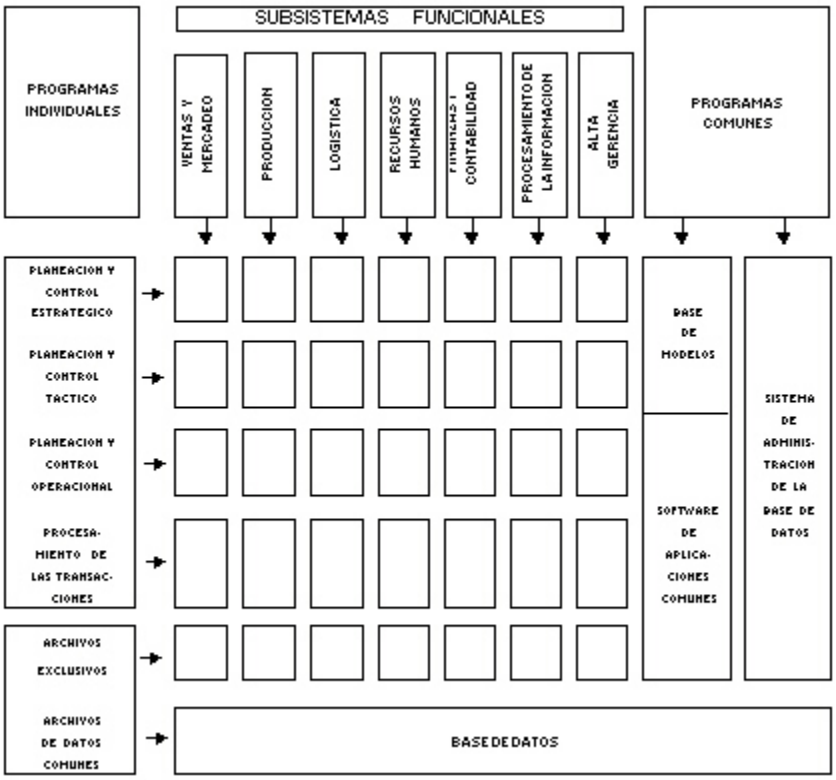
302.02 Estructura conceptual del SIG

La estructura conceptual del SIG se define como la federación de subsistemas de información para las diferentes funciones organizacionales.

Declaración interpretativa

La estructura conceptual definida, permite la descripción y comprensión del SIG como concepto y filosofía integradora y se fundamenta por una parte, en la clasificación de los subsistemas conforme con las funciones principales de la organización tales como ventas y mercadeo, producción, logística, recursos humanos, finanzas y contabilidad, procesamiento de información, alta gerencia, etc., y por otra parte en la clasificación de los subsistemas de las actividades de procesamiento de transacciones, planeación y control operacional, planeación y control administrativo y planeación y control estratégico, tal como se expone en el Gráfico Nº 2.

GRAFICO No. 2



ESTRUCTURA CONCEPTUAL DEL SIG

Cada uno de los subsistemas funcionales del SIG dispone de archivos individuales de datos; también se emplean archivos de datos comunes como lo son las bases de datos institucionales y los programas comunes para funciones múltiples entre los que se citan la base de modelos, software de aplicación comunes y el sistema de administración de la base de datos.

302.03 Planificación del SIG

302.03.01 Se establecerá un sistema de planificación institucional para la actividad relativa al SIG, que coadyuve con un eficiente y eficaz desarrollo del mismo.

Declaración interpretativa

La planificación es la primera actividad en todo proceso administrativo y surge como esencial en materia de informática, ante la complejidad de los sistemas de información computadorizados y ante su relevancia fundamental dentro de la organización.

Se requiere por lo tanto que se planifique el desarrollo del SIG, integrado por los subsistemas de información computadorizados de la organización, con el propósito de alcanzar niveles adecuados de eficiencia y eficacia y sobre la adquisición y el empleo de los recursos necesarios para ello. La planificación provee la base para la asignación de recursos y el control relativo al desarrollo informático institucional por lo que requiere de su actualización periódica. Mediante el proceso de planificación se definen los objetivos, metas y acciones organizacionales del SIG, la arquitectura informática objetivo, la estructura de la organización del SIG y de la plataforma tecnológica requerida.

Los objetivos, metas y acciones constituyen los criterios orientadores para dirigir el desarrollo informático, los cuales deberán ser concordantes y derivados de los objetivos, estrategias y metas organizacionales.

La arquitectura informática objetivo o estructura conceptual del SIG (302.02), constituye el conjunto de subsistemas de información computadorizados con sus interfaces internas y externas que la organización requiere y su definición exige la realización de los estudios preliminar (301.01) y de factibilidad (301.02).

La definición de la estructura de la organización del SIG (302.05) se refiere entre otros asuntos, a la ubicación jerárquica de la Unidad de Informática, su organización interna, funciones, procedimientos y estandarización del trabajo, necesarios para un eficiente y eficaz desarrollo del SIG.

Finalmente, la plataforma tecnológica constituye el hardware, el software y las comunicaciones requeridas por la organización.

302.03.02 El sistema de planificación institucional del SIG se constituirá por un plan estratégico y un plan anual operativo.

Declaración interpretativa

El propósito básico de la planificación estratégica para el SIG, es establecer objetivos, metas y acciones, de mediano y largo plazo acordes con y derivados de los objetivos y metas organizacionales establecidas para el cumplimiento de la misión institucional. El proceso de planificación estratégica puede subdividirse en dos fases: formular la estrategia general y formular los pasos, tiempos y costos que se requieren para implantar la estrategia, que en forma conjunta constituyen el plan estratégico el cual involucra la planeación de mediano y largo plazo.

La ejecución del plan estratégico del SIG, que también forma parte del plan estratégico corporativo, se realizará mediante la formulación y ejecución del plan anual del SIG como parte integrante del plan anual operativo institucional (PAO) que deberá formularse y ejecutarse de conformidad con el ordenamiento jurídico y la normativa técnica vigente sobre el particular.

Tanto el plan estratégico como los planes anuales operativos relativos al SIG, requerirán la aprobación del máximo jerarca, sea este unipersonal o colegiado, de la entidad u órgano, quien podrá obtener la asesoría del Comité Gerencial de Informática (302.09).

302.04 Políticas relativas al SIG

Se definirán y se darán a conocer las políticas relativas al sistema de información gerencial.

Declaración interpretativa

Las políticas son lineamientos o criterios generales dictados por la autoridad superior, que tienen como propósito orientar la acción, en este caso, de los sistemas de información computadorizados como componentes del SIG, para el cumplimiento de los objetivos y metas de la organización. Las políticas que se dicten deberán ser documentadas y divulgadas en los niveles pertinentes de la organización y objeto de actualización permanente.

El jerarca del ente u órgano público, con el apoyo del Comité Gerencial de Informática, conforme se comenta en la norma 302.09, y de la Unidad de Informática, deberá dictar políticas para áreas

como las siguientes: centralización o descentralización de los recursos informáticos, adquisición del hardware y software, prioridades en el desarrollo de los sistemas, la protección de información confidencial, telecomunicaciones, compatibilidad de hardware y software, mantenimiento de equipo, el entrenamiento del personal y en general para la administración del SIG.

302.05 Estructura de la organización del SIG

Se establecerá una adecuada estructura de la organización del Sistema de Información Gerencial que coadyuve en el logro eficiente y eficaz de su finalidad.

Declaración interpretativa

De conformidad con las normas 302.01 y 302.02, el SIG tiene como propósito el examinar, recuperar y procesar datos internos y externos a la organización para proveer información de manera eficiente y eficaz para la planeación y el control en los niveles operacional, táctico y estratégico, así como para el procesamiento de las transacciones.

Para el logro de la finalidad indicada, la Administración definirá y establecerá la estructura de la organización del SIG que considere más apropiada, sea esta centralizada, departamental, personal o del usuario final, o una combinación de las anteriores. La diferencia principal entre las citadas estructuras, radica en la posesión de la función y de las personas designadas para ejecutar las tareas de operación y desarrollo de los SIC, de planeación y control globales y demás tareas vinculadas al SIG.

La estructura centralizada se concibe como la organización tradicional del SIG, constituida por una Unidad de Informática que administra los recursos del computador y sirve a usuarios multi-organizacionales y a necesidades heterogéneas, la cual típicamente la integran las unidades de desarrollo de sistemas, operación del computador y soporte técnico, entre otras.

En la estructura departamental, el equipo de cómputo que generalmente consiste en un minicomputador o una red de área local, se localiza en el área del usuario, satisfaciendo de esa manera necesidades homogéneas del mismo. En esta modalidad, el personal de apoyo del usuario es reducido y puede consistir de uno o dos operadores del computador y un

programador; como resultado una sola persona podría realizar diversas funciones consideradas incompatibles, lo cual hace necesario establecer otros controles compensatorios.

La estructura personal o del usuario final se caracteriza porque los recursos del computador, que consisten básicamente en microcomputadores o estaciones de trabajo, están dedicados a un usuario individual quien podrá recibir algún soporte técnico de la Unidad de Informática, cuando esta exista.

302.06 Ubicación de la Unidad de Informática

La Unidad de informática deberá estar ubicada en un nivel jerárquico adecuado dentro de la organización, que le permita realizar de manera independiente y objetiva, la función de servicio que le corresponde.

Declaración interpretativa

La Unidad de Informática, constituida bajo una filosofía de una estructura de la organización centralizada, debe brindar servicio a toda la institución, de apoyo a los sistemas de recursos o adjetivos, operativos o sustantivos y de administración, por lo que requiere de una ubicación adecuada dentro de la estructura organizacional de la institución, que le permita actuar con objetividad e independencia en su relación con todos los sectores usuarios del servicio que ofrece, tales como el desarrollo de sistemas, la operación del computador, el soporte técnico y demás actividades vinculadas.

302.07 Segregación de funciones incompatibles dentro de la organización

Se mantendrá una segregación efectiva de las funciones de iniciación, autorización, ejecución y registro de transacciones dentro de la organización.

Declaración interpretativa

Las funciones incompatibles son aquellas que colocan a cualquier persona en una situación en la que pueda cometer y ocultar errores o irregularidades en el curso normal de sus obligaciones. Consecuentemente, los controles dependen en gran grado de la eliminación de la oportunidad de encubrimientos, de manera que los procedimientos diseñados para detectar errores o irregularidades, deben desempeñarse por personas distintas de aquellas que están en posición de cometerlos, esto es, por personas que no realicen funciones incompatibles.

De conformidad con lo anterior, la Unidad de Informática en su condición de servidora o de apoyo a las otras unidades de la organización, se limitará al registro y procesamiento de los datos. Como regla, no deberá originar ni autorizar transacciones, ejecutar la preparación inicial de los datos para su procesamiento y tener autoridad para iniciar los cambios en los sistemas computadorizadas, con excepción de las actividades necesarias para cumplir con su competencia. Tampoco deberá tener acceso a los registros contables preparados manualmente, excepto a los documentos fuente que serán necesarios para la entrada y el procesamiento de los datos.

302.08 Segregación de funciones dentro de la Unidad de Informática

Se segregarán las funciones de análisis y diseño de sistemas, programación, operación del equipo, control de los datos y manejo de la cintoteca.

Declaración interpretativa

El control interno se verá fortalecido si dentro de la estructura de la organización de la Unidad de Informática, existe una segregación adecuada de funciones incompatibles, lo cual también dará como resultado, una mayor eficiencia operacional debido al diferente nivel de entrenamiento, conocimiento y habilidad requeridos en cada función.

Con el propósito de mantener la segregación requerida, el análisis de los sistemas y el diseño de éstos, hasta donde sea posible lo realizarán personas diferentes, quienes no intervendrán en la programación y en la operación del equipo; estas dos últimas funciones también deberán estar segregadas. Los grupos de control de datos pueden formar parte de la unidad usuaria, pero con frecuencia son parte integrante de la Unidad de Informática, en cuyo caso deberán ser independientes de los grupos de análisis de sistemas, programación y operación.

El acceso a la biblioteca de discos, cintas y otros archivos magnéticos y de otra naturaleza, deberá estar permitido sólo al personal autorizado. La disposición de los archivos magnéticos por parte de los operadores del computador para la ejecución de sus funciones, se realizará respetando procedimientos formales de control.

En forma adicional, es necesario establecer otros procedimientos apropiados como la rotación de tareas y el disfrute de vacaciones anuales.

La segregación de tareas en una organización pequeña puede ser difícil de ponerse en práctica en razón del poco personal que labora dentro de la Unidad de Informática, en cuyo caso deberán implantarse controles compensatorios.

302.09 Comité Gerencial de Informática

Se constituirá un Comité Gerencial de Informática coadyuvante de la administración superior del SIG.

Declaración interpretativa

El Comité Gerencial de Informática constituye la instancia técnica entre el máximo jerarca y la Unidad de Informática, brindando una asesoría al primero en lo relativo a la administración del SIG y de los recursos humanos, materiales y financieros que se destinen para su desarrollo.

Como parte de sus responsabilidades específicas le corresponde dictar las especificaciones necesarias para los estudios preliminar (301.01.02) y de factibilidad (301.02.02), asesorar al nivel jerárquico superior en la aprobación de los resultados de los estudios de factibilidad (301.02), de los planes estratégico y operativo anual de la función de informática (302.03) y en la emisión de políticas relativas al SIG (302.04), controlar y evaluar la ejecución de los planes aprobados, evaluar la necesidad de disponer de hardware y software adicional y asegurar que el nuevo equipo sea contratado bajo los criterios de oportunidad y con una relación adecuada de beneficio-costo.

El Comité Gerencial de Informática se conformará por acuerdo del máximo jerarca, unipersonal o colegiado, y estará presidido por un representante de este. Usualmente lo integran además, un representante de las unidades de Planificación Institucional, Financiera e Informática como secretaría técnica, así como dos representantes de otras unidades usuarias. Eventualmente el Comité podrá convocar a otros representantes de unidades usuarias, en consideración de los asuntos por tratar.

302.10 Estudios y auditorías internas y externas

302.10.01 La Unidad de Auditoría Interna evaluará el cumplimiento, la suficiencia y la validez del control interno en los SIC.

Declaración interpretativa

Para cumplir con su competencia, la Auditoría Interna deberá planear y ejecutar auditorías de los sistemas de información computadorizados y como parte de ellas, evaluar el cumplimiento, la suficiencia y la validez del sistema de control interno teniendo como marco de referencia la normativa expuesta en el presente Manual.

La Auditoría Interna verificará que los sistemas operen en forma eficiente y eficaz y que brinden información útil y confiable; deberá emplear las técnicas y herramientas computadorizadas que considere convenientes y oportunas.

302.10.02 Las auditorías y estudios especiales de auditoría por parte de la Contraloría General de la República, relativos a los SIC, se realizarán en coordinación con la Unidad de Auditoría Interna.

Declaración interpretativa

El propósito de la coordinación entre la Contraloría General de la República y la Unidad de Auditoría Interna para la realización de auditorías y estudios especiales relativos a los SIC, es minimizar la duplicidad de esfuerzos y hacer un uso más eficiente de los recursos públicos, todo dentro de la filosofía del Ordenamiento de Control y Fiscalización Superiores de la Hacienda Pública.

La coordinación involucra actividades como reuniones previas para planear la labor por realizar y determinar las áreas de mayor interés, obtener el acceso a los programas de auditoría, papeles de trabajo e informes emitidos, e incluso para la utilización de personal capacitado, de técnicas de auditoría con ayuda del computador (TAAC) y de métodos y herramientas de empleo mutuo en poder de la Auditoría Interna.

La labor de la auditoría externa a cargo del Organo Contralor, involucra evaluar tanto la gestión de la Auditoría Interna en relación con los SIC, como la evaluación misma de tales sistemas. La evaluación del trabajo ejecutado por el auditor interno constituye un elemento coadyuvante en la determinación de la naturaleza, oportunidad y alcance de los procedimientos del auditor externo. Una función de auditoría interna adecuada y eficaz justificará con frecuencia una reducción de los procedimientos ejecutados por el auditor externo.

302.10.03 El auditor deberá poseer el entrenamiento técnico y capacidad profesional relativa a la auditoría de los SIC.

Declaración interpretativa

El enunciado anterior se fundamenta en la norma personal de auditoría relativa al entrenamiento técnico y capacidad profesional.

A efecto de darle cumplimiento a la norma en comentario, el auditor, en especial aquel designado a realizar auditorías de los SIC, debe tener suficiente conocimiento y experiencia sobre hardware, software y sistemas de procesamiento automatizado de datos, así como de la aplicación de los procedimientos de auditoría incluyendo las técnicas de auditoría con ayuda del computador (TAAC), que le permita llevar a cabo las auditorías y estudios especiales de auditoría requeridos para los sistemas de información computadorizados de la organización que integran el SIG. A manera de ejemplo, deberá poseer conocimientos y adquirir experiencia en las áreas de administración, seguridad, desarrollo y control sobre el mantenimiento de los SIC; planes de contingencia; administración de bases de datos; telecomunicaciones y software de sistemas.

Cuando el auditor, no disponiendo de las habilidades necesarias para llevar a cabo estudios muy técnicos, requiera del apoyo de uno o varios especialistas en la materia, seguirá siendo responsable de los resultados de dichos estudios, por lo que deber dirigir, supervisar y revisar el trabajo de sus colaboradores.

303 DESARROLLO DE SISTEMAS

Está orientado a lograr un desarrollo y mantenimiento eficiente, eficaz y controlado de los SIC. Incluye las normas relativas al desarrollo en concordancia con Los planes y políticas del SIG (303.01), al Manual de estándares para el desarrollo de los SIC (303.02), al proyecto de desarrollo del SIC (303.03), al administrador del proyecto de desarrollo del SIC (303.04), al ciclo de vida para el desarrollo de sistemas (303.05), al procesamiento en paralelo (303.06), a los procedimientos de control y rastros de las transacciones (303.07), a la participación de los usuarios en el CVDS (303.08), a la participación del auditor en el CVDS (303.09) y a las modificaciones a los SIC (303.10).

303.01 Desarrollo en concordancia con los planes y las políticas del SIG

El desarrollo de los SIC se efectuará teniendo como base fundamental el plan estratégico, el plan anual operativo y las políticas relativas al SIG.

Declaración interpretativa

El desarrollo de los SIC constituye el conjunto de actividades predefinidas y estructuradas sistemáticamente, para la obtención de sistemas con un alto nivel de calidad, que permitan el logro de los objetivos o fines especificados por el usuario. Los sistemas de información computadorizados que se desarrollen, por principio, deben estar enunciados en el plan estratégico y en el plan anual operativo relativo al SIG, conforme lo establecen las normas 302.03.01 y 302.03.02 del presente Manual.

Asimismo, debe tomarse como referencia las políticas que en materia del SIG haya dictado la autoridad superior con el apoyo del Comité Gerencial de Informática y de la Unidad de Informática, tal como se establece en la norma 302.04.

303.02 Manual de estándares para el desarrollo de los sistemas de información computadorizados (SIC)

Se establecerá y mantendrá actualizado un Manual de estándares para el desarrollo de los SIC.

Declaración interpretativa

Para un adecuado control interno en el desarrollo de los SIC, es indispensable disponer de un Manual de estándares, entendido como el conjunto de procedimientos necesarios para guiar dicha actividad, preparados tomando como referencia las políticas institucionales relativas al SIG (302.04) y demás normativa técnica contenida en el presente Manual sobre normas técnicas. El Manual de estándares que en el mayor de los casos es preparado por la Unidad de Informática, deberá ser aprobado por la autoridad máxima de la entidad u órgano; también requerirá la actualización permanente y la divulgación necesaria. Como parte del contenido del Manual se deben incluir las etapas del ciclo de vida para el desarrollo de sistemas.

303.03 Proyecto de desarrollo del SIC

Se preparará un proyecto para cada SIC que se pretenda desarrollar, así como para los que sean objeto de modificaciones importantes.

Declaración interpretativa

El proyecto que se preparará para cada SIC objeto de desarrollo o de modificación importante, lo conforma el plan detallado de actividades técnicas y administrativas orientadas a desarrollar e implantar dicho sistema, conforme a la planificación del SIG (302.03), a las políticas relativas al SIG (302.04) y al Manual de estándares (303.02).

Un proyecto se define por un objetivo a alcanzar en cierto tiempo y con un presupuesto determinado, lo cual lo caracteriza como un proceso delimitado en el tiempo y en el costo.

Se entenderá por modificaciones importantes, aquellas requeridas para el mejoramiento de los sistemas automatizados que estén en operación en la entidad u órgano pertinente y que por su naturaleza y alcance, modifican sustancialmente el sistema actual, justificándose por lo tanto un adecuado planeamiento y control de dichas modificaciones.

Las actividades técnicas del plan están constituidas por las tareas involucradas en cada una de las etapas del ciclo de vida del desarrollo de sistemas, y las actividades administrativas son las referidas a la estimación de los tiempos y recursos humanos, materiales, financieros y tecnológicos necesarios para el desarrollo del proyecto. Como elementos coadyuvantes en la labor de planeación del proyecto, podrán emplearse las técnicas de programación por redes

conocidas como PERT (Program Evaluation and Revew Technique), CPM (Critical Path Method), ABC (Analysis Bar Charting), el gráfico de Gantt u otras técnicas y herramientas que se consideren apropiadas.

El proyecto de desarrollo, como plan que es, deberá documentarse y requerirá la aprobación por parte de la Jefatura de la Unidad de Informática como unidad técnica especializada y la comunicación necesaria al Comité Gerencial de Informática.

303.04 Administrador del proyecto de desarrollo del SIC

Se nombrará un funcionario que tendrá la responsabilidad directa de planear, organizar, dirigir, coordinar y controlar el proyecto de desarrollo del SIC.

Declaración interpretativa

Esta norma tiene su fundamento doctrinario en el principio de control interno sobre la responsabilidad delimitada, con lo cual se fortalece la estructura del control interno. Por consiguiente se nombrará un funcionario competente quien tendrá la responsabilidad de planear, organizar, dirigir, coordinar y controlar el proyecto de desarrollo del SIC (303.03) y fungirá como enlace entre los usuarios, analistas, programadores y la jefatura de la Unidad de Informática. Su responsabilidad termina una vez realizada la evaluación post-implantación (303.05.10) del sistema en forma satisfactoria.

La planificación comprende tanto el desarrollo del plan de trabajo general del proyecto, como el plan detallado correspondiente a cada etapa comprendida dentro del ciclo de vida para el desarrollo de sistemas. La organización del proyecto deberá también basarse en la metodología del ciclo de vida (303.05), considerando las necesidades de recurso humano en cada una de sus etapas; en todo caso se deberá dar participación activa a la unidad o unidades usuarias del sistema ideado; para tal propósito se definirán en forma precisa las funciones y responsabilidades entre los diversos integrantes del equipo del proyecto. Las funciones administrativas de dirección, coordinación y control son básicas para la ejecución adecuada del proyecto.

Es menester indicar que el control del proyecto involucra la implantación y seguimiento de los mecanismos de retroalimentación apropiados, tendentes a procurar el logro eficiente y eficaz de los objetivos establecidos en la planificación del sistema objeto de desarrollo para una

satisfacción plena de usuario y en general de la Administración. En este sentido el administrador del proyecto deberá establecer los controles y medidas necesarias para contrarrestar los posibles riesgos inherentes relativos a los proyectos y al sistema, tales como alcance inadecuado, costo y tiempo excesivo, inoportunidad e inadecuada funcionalidad, tecnología y mantenimiento del sistema una vez desarrollado.

303.05 Ciclo de vida para el desarrollo de sistemas (CVDS)

Los sistemas de información computadorizados se desarrollarán siguiendo la metodología del ciclo de vida para el desarrollo de sistemas (CVDS).

Declaración interpretativa

El ciclo de vida para el desarrollo de sistemas constituye el conjunto de etapas que los usuarios, analistas, diseñadores de sistemas y otros funcionarios involucrados, realizan para desarrollar e implantar un sistema de información computadorizado.

Las etapas del CVDS son descritas por diversos autores pero con diferencias en cuanto al número, denominación y detalle de las mismas, no obstante en el fondo coinciden entre sí. Para los efectos de emplear una metodología común, las etapas del CVDS se definen como estudio preliminar (303.05.01), estudio de factibilidad (303.05.02), análisis y determinación de los requerimientos de información (303.05.03), diseño conceptual del sistema (303.05.04), diseño físico del sistema (303.05.05), desarrollo de la programación (303.05.06), desarrollo de la documentación (303.05.07), prueba del sistema (303.05.08), implantación (303.05.09) y evaluación post-implantación (303.05.10).

La metodología del CVDS permite una mejor administración de los sistemas en desarrollo y por lo tanto facilita el control del avance del proyecto y de los recursos humanos, materiales, financieros y tecnológicos que se destinan para su ejecución.

303.05.01 Estudio preliminar

El proyecto de desarrollo del SIC se iniciará con un estudio preliminar y se preparará el informe correspondiente en conformidad con las especificaciones que se emitan.

Declaración interpretativa

Ver la declaración interpretativa para las normas 301.01.01 y 301.01.02.

303.05.02 Estudio de factibilidad

De acuerdo con los resultados del estudio preliminar, se elaborará un estudio de factibilidad y se preparará el informe correspondiente en conformidad con las especificaciones que se emitan.

Declaración interpretativa

Ver la declaración interpretativa para las normas 301.02.01 y 301.02.02.

303.05.03 Análisis y determinación de requerimientos de información

Se realizará un análisis del sistema actual y se determinarán y documentarán los requerimientos de información del sistema de información en desarrollo.

Declaración interpretativa

Esta tercera etapa del CVDS consiste en efectuar un análisis exhaustivo del sistema actual, cuando exista en la organización, sea este manual o computadorizado y determinar y documentar los nuevos requerimientos de procesamiento e información del sistema en desarrollo.

Las técnicas básicas para reunir datos son entrevistas, cuestionarios, recopilación de documentos y manuales o formularios de operación del sistema, y las observaciones personales acerca de los procedimientos actuales. El análisis comprende la investigación detallada acerca de lo que está sucediendo en el sistema actual y del por qué ello ocurre.

Tomando como base el análisis efectuado, se procederá a definir los requerimientos de información y de cualquier otra naturaleza para el nuevo sistema, considerando por lo menos las necesidades de corto y mediano plazo. Entre otros, se definirán los requerimientos del origen y entrada de las transacciones en el procesamiento de datos, de comunicación, procesamiento, almacenamiento y recuperación de los datos, así como los requerimientos para la salida de información y para el control y seguridad de los datos y de la información que se genere, todo lo cual deberá quedar documentado.

Debe advertirse que parte de la información requerida en esta etapa ya ha sido obtenida, aunque de manera general, en la etapa relativa al estudio de factibilidad

303.05.04 Diseño conceptual del sistema

El diseño conceptual del SIC deberá documentarse y responderá a los requerimientos de información determinados.

Declaración interpretativa

Durante la etapa de diseño conceptual o de diseño lógico como también se le denomina, se llevará a cabo la descripción funcional y del procesamiento de los datos del sistema en desarrollo y se efectuará con base en los requerimientos definidos en la etapa de análisis y determinación de los requerimientos de información (303.05.03).

Entre otros asuntos, se describirán las entradas del sistema, incluyendo los tipos de transacciones, documentos fuente, formularios y ediciones; los resultados que producirá el sistema; los controles y las funciones, técnicas y métodos de procesamiento; las interfases del sistema; la estructura de los archivos y los requerimientos de hardware y software de sistemas.

303.05.05 Diseño físico del sistema

El diseño físico del SIC deberá documentarse y ofrecer las especificaciones necesarias y suficientes para el desarrollo de los programas.

Declaración interpretativa

Esta etapa también es conocida con el nombre de diseño físico, interno o detallado y consiste en una ampliación y extensión de las características generales incluidas en el diseño conceptual.

El diseño físico del sistema de información computadorizado se compone de especificaciones completas y detalladas concernientes a todo lo relativo al sistema, que serán utilizadas para el desarrollo de los programas computadorizados. Para ese propósito se emplearán las técnicas más adecuadas que se consideren posibles.

303.05.06 Desarrollo de la programación

Los programas requeridos por el SIC se desarrollarán de conformidad con las especificaciones definidas en el diseño físico y se preparará la documentación respectiva.

Declaración interpretativa

Esta etapa del proyecto de desarrollo comprende la codificación, compilación, prueba y depuración de los módulos que integran los programas, con el propósito de detectar y corregir los errores de sintaxis y de lógica, así como el desarrollo de la documentación necesaria.

Como requisito fundamental, el programador debe estudiar y analizar las especificaciones preparadas por el analista durante la etapa de diseño físico (303.05.05) y con base en ellas, desarrollará el programa utilizando técnicas adecuadas que promuevan el control, la eficiencia y la eficacia del sistema, tales como la modularidad y la programación estructurada. También debe procurarse el empleo de un lenguaje de programación adecuado para la entidad u órgano público.

303.05.07 Desarrollo de la documentación

La documentación del SIC deberá concluirse antes de la prueba del mismo.

Declaración interpretativa

El desarrollo de la documentación del SIC constituye una etapa clave del CVDS y debe de concluirse antes de la prueba del sistema (303.05.08), con el propósito de validar los procedimientos establecidos.

La documentación requerida y el contenido de la misma se expone de manera general en el grupo de normas 304 referidas a la documentación de los sistemas en desarrollo.

En la práctica la documentación de los SIC debe comenzarse desde el inicio del CVDS, a efecto de que el desarrollo de la misma sea oportuna e incluya todos los detalles requeridos. Su preparación requiere de una estrategia combinada en la que los analistas de sistemas y usuarios trabajen en mutua colaboración para producir de esa manera una documentación técnicamente correcta, completa y comprensible.

303.05.08 Prueba del sistema

Se realizarán las pruebas necesarias al SIC de previo a su implantación y se documentarán adecuadamente.

Declaración interpretativa

La prueba del SIC consiste en una prueba tanto individual o unitaria, como integral de los diferentes programas y de todas las fases y procedimientos manuales y automatizados que conforman el sistema, con el propósito de que este resulte confiable, funcional y en conformidad con las especificaciones establecidas originalmente.

Las pruebas deberán ser planificadas y documentadas adecuadamente e incluir entre otros procedimientos, la corrida en el computador de un grupo de datos de prueba con resultados predeterminados. Su preparación y ejecución deberá ser un esfuerzo conjunto de los usuarios y del personal de la Unidad de Informática.

303.05.09 Implantación

La implantación del SIC se llevará a cabo conforme a un plan establecido y bajo un control adecuado.

Declaración interpretativa

La implantación del SIC entre otras actividades, comprende la instalación del hardware y del software de sistemas requerido (sistema operativo, compiladores, intérpretes, utilitarios), la instalación del sistema de información computadorizado que ha sido desarrollado, la conversión de los archivos, el entrenamiento adicional para los usuarios y operadores del nuevo sistema, la revisión y actualización de la documentación en los casos requeridos.

Son diversas y delicadas las actividades comprendidas dentro de esta etapa, por lo que se requiere de una planeación adecuada y un control efectivo de las mismas, tal y como se dispone en la norma 301.04 relativa a la preinstalación.

303.05.10 Evaluación post-implantación

Posterior a la implantación del SIC, deberá realizarse una evaluación del mismo a fin de determinar si ha logrado satisfacer los objetivos establecidos dentro de la relación de beneficio-costo esperada.

Declaración interpretativa

La evaluación post-implantación es la última fase del CVDS y consiste en una revisión que se realiza después de que el SIC haya estado en operación durante un período razonable, por ejemplo un año, bajo la responsabilidad del administrador del proyecto de desarrollo del SIC (303.04), el cual podrá apoyarse en un grupo conformado con representantes de los usuarios, analistas y operadores de sistemas.

La evaluación post-implantación estará orientada a medir el logro de los objetivos del SIC y por ende a la atención de los requerimientos establecidos en las etapas iniciales del CVDS, así como a realizar un análisis de los beneficios y costos estimados originalmente en comparación con los beneficios y costos reales.

303.06 Procesamiento en paralelo

Se ejecutará el procesamiento en paralelo del antiguo sistema con el nuevo SIC, cuando este último sea complejo, de importancia estratégica o según el criterio del administrador del proyecto.

Declaración interpretativa

El procesamiento en paralelo del sistema nuevo con el anterior, constituye una ampliación de las pruebas ya realizadas de conformidad con la norma 303.05.08. Tal procedimiento resulta muy efectivo para el control de la conversión de los archivos y operaciones iniciales de los nuevos sistemas.

No obstante los beneficios y la confiabilidad que brinda, en razón del costo elevado que representa su ejecución tanto en equipo como en personal adicional requerido, el procesamiento en paralelo sólo resulta obligatorio para los sistemas complejos o que son de importancia estratégica para la institución, siempre considerándose la relación beneficio-costo, sin embargo, el administrador del proyecto de desarrollo del SIC (303.04) podrá decidir otros casos en los cuales sea necesario el procesamiento en paralelo.

Por importancia estratégica se entenderá aquel sistema que es básico o fundamental para el cumplimiento de los objetivos y metas de la organización y que por tal característica debe brindar información oportuna y confiable.

303.07 Procedimientos de control y rastros de las transacciones

Los SIC incluirán los procedimientos de control y los rastros de las transacciones que sean necesarios.

Declaración interpretativa

Durante el desarrollo de los sistemas de información computadorizados, deberán considerarse especialmente los procedimientos y rutinas de control que sean necesarios, tanto manuales como automatizados, para que el sistema brinde información confiable para la planificación, el control y la toma de decisiones. Con tal propósito deberán incorporarse los controles establecidos en las normas de aplicación, normas adicionales y otras relacionadas del presente Manual.

Asimismo, los SIC deberán diseñarse de tal forma que se facilite el rastreo y la comprobación de una transacción original hacia adelante a un total de resumen, o a la inversa, para investigar un total resumen hacia la transacción original.

303.08 Participación de los usuarios en el CVDS

Se requerirá la participación activa de los usuarios en las diversas etapas del CVDS.

Declaración interpretativa

La participación activa de los usuarios en el desarrollo de los sistemas de información computadorizados, resulta imprescindible para la obtención de un sistema que satisfaga las necesidades de información de la organización, por lo que cuando sea requerido, cada unidad usuaria deberá participar en las diferentes etapas del CVDS ya que está involucrada su área de responsabilidad.

Los productos resultantes de las etapas de análisis y determinación de los requerimientos de información (303.05.03), diseño conceptual (303.05.04), desarrollo de la documentación (303.05.07), prueba del sistema (303.05.08) e implantación (303.05.09), requerirán la aprobación de la unidad usuaria respectiva, la cual se hará constar en la documentación que se genere de cada etapa indicada.

303.09 Participación del auditor en el CVDS

Durante el CVDS el auditor fungirá como asesor o consejero del administrador del proyecto y en general del equipo de desarrollo.

Declaración interpretativa

La participación del auditor como asesor o consejero del administrador del proyecto de desarrollo del SIC (303.04) y del equipo a cargo de su desarrollo, no sólo le permitirá cumplir en forma oportuna y eficiente con su servicio constructivo y de protección a la Administración, sino que además le dará una seguridad razonable de que los SIC incluyan procedimientos de control necesarios y confiables.

La responsabilidad y limitaciones del auditor sólo deben ser calificadas en su función de asesor, no de gestor o administrador y como tal, ayuda a prevenir la implantación de sistemas con riesgos considerables. De manera general y con el propósito de mantener su independencia y objetividad, sus revisiones deberán llevarse a cabo en forma posterior a la conclusión de cada etapa del CVDS y como resultado de ello, preparará el informe correspondiente.

Entre otros asuntos, el auditor evaluará que el proyecto de desarrollo del SIC, se lleve a cabo con la participación activa de los usuarios y en conformidad con las restantes normas establecidas para el desarrollo de sistemas, asimismo que se incluyan los procedimientos de control y los rastros de las transacciones que sean necesarios (303.07).

303.10 Modificaciones a los SIC

Las modificaciones a los SIC en operación deberán ser autorizadas, controladas, aprobadas y documentadas adecuadamente.

Declaración interpretativa

Como parte del procedimiento formal que debe implantar la Administración para el mantenimiento de los SIC en operación, se requerirá que la iniciación y la autorización de los cambios en los mismos sea llevada a cabo por los usuarios, así como la aprobación de dichas modificaciones.

Adicionalmente, las modificaciones importantes deberán ser autorizadas y aprobadas por el máximo jerarca de acuerdo con la recomendación del Comité Gerencial de Informática. De conformidad con la norma 303.03, tales modificaciones importantes requerirán la elaboración del proyecto de desarrollo y por ende, cumplir con las etapas del CVDS.

Al igual que para el desarrollo de sistemas, deberán existir controles, pruebas y documentación adecuada sobre los cambios efectuados. Un elemento adicional importante es el de disponer de un registro de cambios a los programas que indique las modificaciones efectuadas, la justificación respectiva y la fecha en que se realizaron.

304 DOCUMENTACION

Tiene como objetivo básico mantener una descripción suficiente y oportuna de los sistemas de información computadorizados, necesaria para la comprensión, operación, mantenimiento y control eficiente y efectivo de los mismos. Comprende las normas relativas al desarrollo de la documentación de conformidad con el Manual de estándares (304.01), a la documentación del sistema (304.02), a la documentación del programa (304.03), a la documentación del usuario (304.04), a la documentación de las operaciones del computador (304.05) y a la documentación de otros procedimientos (304.06).

304.01 Desarrollo de la documentación de conformidad con el Manual de estándares

La documentación de los SIC se desarrollará de acuerdo con lo establecido en el Manual de estándares.

Declaración interpretativa

El Manual de estándares para el desarrollo de los SIC contiene los procedimientos básicos que guían a los analistas y programadores para desarrollar la documentación del sistema, del programa, del usuario, de las operaciones del computador y de otros procedimientos pertinentes al sistema de información computadorizado en particular. Esto permitirá que la organización disponga de documentación completa, adecuada y actualizada para todos los sistemas que se desarrollen.

La documentación es parte vital de todo SIC y debe elaborarse desde el inicio de su ciclo de vida, con el fin de que se incorporen todos los detalles necesarios que podrían perderse si se posterga para el final del proyecto.

304.02 Documentación del sistema

Se elaborará en forma adecuada y suficiente y se mantendrá actualizada, la documentación del sistema para cada SIC que se desarrolle.

Declaración interpretativa

La documentación del sistema tiene como finalidad, dar a conocer y describir el SIC. Por ello comprenderá lo que hace el sistema, su ámbito, los controles incorporados y sus limitaciones. Debe estar orientada a proporcionar a todos los interesados, una comprensión clara y confiable del SIC y a facilitar su mantenimiento y modificaciones requeridas en forma posterior.

La documentación del sistema también conocida como el Manual del sistema, debe contener, entre otros asuntos, la información relativa a los objetivos y antecedentes del SIC, los estudios preliminar (301.01) y de factibilidad (301.02) y las aprobaciones respectivas, la descripción, diseño general y diagrama del sistema y subsistemas o aplicaciones que lo conforman, los objetivos y funciones de los programas, el diseño de la entrada y salida de datos, el diseño de los archivos y forma de acceso.

En general el Manual del sistema documenta toda la labor realizada a través del CVDS, con excepción de la relativa a los programas la cual es de uso restringido como medida preventiva de control.

304.03 Documentación del programa

La documentación de cada programa del SIC deberá mantenerse en forma adecuada, suficiente y actualizada.

Declaración interpretativa

Una comprensión clara de los programas relativos al SIC en particular y un control efectivo sobre la modificación, revisión y corrección a los mismos, así como proveer un medio aceptable para que otros interesados lleven a cabo revisiones, sólo podrá darse si existe una documentación adecuada y suficiente de los programas que conforman dicho SIC.

La documentación del programa, también conocida como Manual del programa, por lo general incluye el código y título o nombre del programa o programas que integran el SIC, la descripción del programa en forma narrativa, el diagrama de lógica o algoritmo y tabla de decisiones si las hubiera, formato y descripción de los archivos, listado del programa fuente, listado de los controles, instrucciones de operación, registro de cambios a los programas y su autorización, listado de la última corrida de prueba y demás información pertinente.

La documentación de los programas constituye un activo valioso, por ello su acceso debe restringirse, deberá conservarse en una biblioteca especial y mantener un registro sobre su uso. Su acceso sólo deberá estar permitido al personal de programación y a otros funcionarios por excepción, tales como auditores y analistas de sistemas en el cumplimiento de sus respectivas competencias.

304.04 Documentación del usuario

Deber mantenerse en forma adecuada, suficiente y actualizada, la documentación del usuario del SIC.

Declaración interpretativa

La documentación del usuario o Manual del usuario, como su nombre lo indica, está orientada al usuario o usuarios del SIC y debe explicar en forma detallada los servicios que brinda el mismo y cómo se pueden obtener. Debe estar organizada de manera que los usuarios sean autosuficientes en el manejo del sistema y presentada en lenguaje corriente, evitando la jerga computacional.

La documentación del usuario deberá contener al menos los objetivos y la descripción del SIC y de las entradas y salidas de datos al mismo, los procedimientos de control, los procedimientos para la corrección de errores, la descripción de cómo la unidad usuaria deberá revisar los reportes para constatar su veracidad y confiabilidad, así como la descripción de otros procedimientos requeridos por el usuario.

304.05 Documentación de las operaciones del computador

Se elaborará en forma adecuada y suficiente y se mantendrá actualizada, la documentación de las operaciones del computador relativas al SIC.

Declaración interpretativa

Para cada programa o conjunto de programas que integran el SIC, deberán elaborarse las instrucciones necesarias de operación de tal forma que cualquier operador del equipo de computación pueda ejecutar las labores diversas que requiere la corrida de tales programas, aún cuando no tenga experiencia previa acerca de los programas en particular.

El Manual de procedimientos del operador, como también se le denomina, deberá comprender al menos el diagrama general del sistema, el código y nombre de los programas que se ejecutarán, una breve descripción de la finalidad del programa, la descripción y diagrama general de procesos, el calendario de procesos, el esquema de la operación que muestre las entradas y salidas del proceso, instrucciones especiales de operación relativas a la preparación de la operación del computador y los procedimientos finales de operación, información sobre las interrupciones programadas y mensajes en caso de haberlos así como la acción correctiva correspondiente para proseguir el proceso, instrucciones de conclusión del trabajo, interfaces con otros sistemas y procedimientos de respaldo de la información procesada.

Su importancia reside en que, generalmente, el operador debe procesar diversos programas en el transcurso de un día o período determinado y no se puede esperar que recuerde los requerimientos de operación para cada uno de ellos. Además, una sana medida de control señala la rotación de los operadores, con el fin de que no tengan bajo su responsabilidad siempre la ejecución de los mismos programas.

304.06 Documentación de otros procedimientos

Deberá elaborarse en forma adecuada y suficiente y se mantendrá actualizada, la documentación de otros procedimientos relacionados con los SIC.

Declaración interpretativa

Como parte de otra documentación requerida para la operación adecuada de los sistemas de información computadorizados, deben existir procedimientos por escrito y actualizados para el mantenimiento, control y protección de los archivos, para el control de calidad de la entrada de datos para su procesamiento y salida de la información, para el control de la utilización del equipo de procesamiento electrónico de datos, así como de otros procedimientos relacionados.

305 OPERACION

Contempla los métodos y procedimientos que deben ponerse en práctica para la operación del equipo de los SIC, orientados a crear un ambiente que procure la efectividad y el control en la producción de la unidad de operaciones, así como proporcionar seguridad física sobre los archivos magnéticos de manera que sea factible mantener la operación continua del equipo y de los sistemas de información computadorizados.

Comprende las normas relativas a los procedimientos adecuados para la recepción de los datos (305.01), la seguridad física (305.02), la seguridad lógica (305.03), supervisión adecuada (305.04), la administración de la biblioteca de archivos magnéticos (305.05), el respaldo de archivos magnéticos (305.06), el plan de contingencia (305.07), los controles de equipo (305.08) y el mantenimiento del equipo (305.09).

305.01 Procedimientos adecuados para la recepción de los datos

Se establecerán procedimientos adecuados que procuren que los datos recibidos para su procesamiento están autorizados y completos.

Declaración interpretativa

Como parte de los procedimientos requeridos, usualmente se constituye una función específica de control de calidad a cargo de una unidad, grupo de personas o de un funcionario ubicado dentro de la unidad usuaria del SIC o formando parte de la Unidad de Informática, con la responsabilidad de recibir todos los datos que se van a procesar y verificar que cumplan con los

requisitos necesarios. Asimismo, debe controlar que los errores detectados durante el procesamiento sean corregidos y que toda información de salida se distribuya adecuadamente.

Adicionalmente a los controles manuales, deberán implantarse controles automatizados que también coadyuven en el procesamiento total, correcto y autorizado de los datos.

305.02 Seguridad física

305.02.01 El acceso físico a la sala del computador y a las áreas de equipo de soporte esencial, sólo se permitirá al personal autorizado.

Declaración interpretativa

En general, el acceso a la sala del computador se permitirá únicamente a los operadores del equipo de cómputo. Todas las demás personas que requieran ingresar al área indicada, tales como representantes de proveedores, personal de mantenimiento de equipo y otros, lo harán bajo un control adecuado y acompañados del supervisor o funcionario similar del área de operación. Tales restricciones también deberán mantenerse para el acceso físico a las áreas de albergue de equipos de soporte como aire acondicionado, tableros de control de fuerza eléctrica y a las áreas de almacenamiento de discos y cintas magnéticas, entre otras.

El acceso se restringe por medio de guardias, tarjetas de acceso y otros dispositivos que identifiquen al personal autorizado. Asimismo, las puertas de ingreso al área deben estar equipadas con cerraduras y las paredes, suelos y similares, construidas con material adecuado.

305.02.02 Se mantendrán procedimientos y medidas efectivas para la protección del hardware, del software y de los datos de los SIC.

Declaración interpretativa

La seguridad física de los SIC, además del control del acceso físico indicado en la norma anterior, incluye también disponer de procedimientos y medidas que contrarresten los riesgos a los daños que puedan causar el fuego, el agua, los cortes o variaciones de la corriente eléctrica que alimenta a los equipos, así como por la presencia de químicos y otros elementos que afecten el ambiente normal de operación de las máquinas y del estado físico de los archivos magnéticos.

Recursos tan valiosos no sólo desde el punto de vista económico, sino también estratégico, como son los SIC, justifican el mantenimiento de sistemas de protección física que aseguren razonablemente la operación continua de tales sistemas. Se requieren, por lo tanto, procedimientos y dispositivos orientados a prevenir, detectar y combatir la presencia de los citados riesgos.

En atención a lo anterior, deberá disponerse de dispositivos de detección de fuego y humedad, así como de extintores de fuego apropiados, todos los cuales deberán probarse periódicamente para asegurar su uso en el momento requerido, otorgándose el entrenamiento necesario al personal que garantice su adecuada utilización.

La sala del computador también deberá estar ubicada en un nivel alto, en una zona que no corra el riesgo de inundaciones y en donde no esté expuesta a derramamientos de agua, y se separará de las áreas adyacentes con paredes resistentes al fuego. Fuentes de poder alternativas, controladores y reguladores de las variaciones de la electricidad son también necesarias para procurar un procesamiento continuo y adecuado de los datos.

305.03 Seguridad lógica

El acceso a los archivos de datos y programas dentro del computador, sólo se permitirá al personal autorizado.

Declaración interpretativa

Existe el riesgo que personas no autorizadas tengan acceso a los archivos de datos y a los programas de los SIC puestos en operación para el procesamiento de datos, y efectúen cambios no autorizados a los datos o información procesada y a los programas mencionados. Para mantener un control adecuado sobre lo anterior, debe emplearse y hacerse un buen uso de software de seguridad, que entre otras funciones, limite el acceso a los diversos elementos del sistema que interese controlar, tales como archivos de datos, terminales, programas de producción, tablas de claves de acceso, utilitarios y editores on-line; defina las vías de acceso autorizadas para su utilización y las funciones que puede llevar a cabo una persona; controle el sistema de claves de acceso y genere informes especiales relativos a la violación de la seguridad lógica, para su revisión posterior.

305.04 Supervisión adecuada

Se establecerá y mantendrá una supervisión adecuada de todas las operaciones y procedimientos seguidos en la sala del computador.

Declaración interpretativa

La jefatura de la unidad de operaciones en colaboración con el nivel de supervisión, deberá llevar a cabo una revisión permanente de todos los procedimientos seguidos y operaciones realizadas en la sala del computador y velar porque se cumplan con las políticas y los estándares establecidos.

La supervisión podrá llevarse a cabo por simple observación del personal que opera las máquinas y ejecuta los programas, y también por medio de una revisión de la bitácora de utilización del equipo de cómputo, de los impresos de consola, de los listados de salida y de otros registros de control disponibles.

La supervisión se hace más necesaria cuando la estructura de la organización del Sistema de Información Gerencial es de reducido tamaño y por ende la separación de funciones se ve limitada.

305.05 Administración de la biblioteca de archivos magnéticos

Se asignará un encargado de la biblioteca, responsable de la entrega, recepción y custodia de los archivos magnéticos.

Declaración interpretativa

Los archivos que se mantienen fuera de línea normalmente se encuentran en cintas magnéticas o en paquetes removibles de discos, u otro medio de almacenamiento, deben ser guardados en un recinto independiente y cerca de la sala del computador.
La administración de la biblioteca de archivos de datos y programas, estará a cargo de un funcionario que sea independiente de las personas que laboran como programadores u operadores del computador.

Como parte de la responsabilidad del funcionario encargado del manejo de la biblioteca, está la de mantener un registro detallado sobre los medios de almacenamiento magnético custodiados, proporcionar a los usuarios autorizados los archivos que requieren para el ejercicio de sus labores manteniendo un control de las entregas y devoluciones, asignar una identificación externa para cada medio de almacenamiento magnético que lo identifique y ejercer un control sobre las fechas en las cuales estos requieren de limpieza.

Asimismo, deberán efectuarse inventarios periódicos y mantenerse otros procedimientos adicionales tendentes a garantizar la integridad y disponibilidad de la información y software custodiados en la biblioteca de archivos magnéticos.

305.06 Respaldo de archivos magnéticos

Se mantendrán respaldos actualizados de los archivos de datos, de los programas y del software de sistemas.

Declaración interpretativa

Los respaldos de los archivos magnéticos empleados por la organización, constituyen una necesidad para procurar la continuidad de operaciones cuando se presenten interrupciones causadas por una destrucción significativa de los mismos. En relación con los archivos de datos, deberá emplearse la técnica conocida como "abuelo-padre-hijo".

Un respaldo de los archivos críticos deberá ser mantenido en un lugar externo de la Unidad de Informática y en los casos necesarios, también deberá mantenerse otro en un sitio remoto. El acceso de personas a estos archivos será restringido y controlado.

305.07 Plan de contingencia

Se elaborará un plan de contingencia que procure la continuidad de la operación normal de los SIC cuando se presenten eventualidades inesperadas que afecten su funcionamiento.

Declaración interpretativa

El disponer de un plan de contingencia es parte de la implantación y mantenimiento de procedimientos adecuados para la seguridad física y operacional del equipo de cómputo, de los

archivos magnéticos y en general de los SIC, ante eventualidades como el fuego, inundaciones, terremotos, robos, desperfectos del equipo, terrorismo y otros riesgos presentes.

El plan de contingencia, que deberá prepararse principalmente para los sistemas críticos o relevantes para la operación normal de la entidad u órgano, estará constituido por un plan de prevención y por un plan de recuperación. El primero se refiere a los procedimientos necesarios para la prevención de los riesgos presentes y el segundo trata sobre los procedimientos por seguir en caso de que la eventualidad suceda.

El plan deberá estar documentado, actualizado, aprobado por el máximo jerarca de la entidad u órgano y debe ser puesto a prueba.

305.08 Controles del equipo

Se utilizarán al máximo posible los controles incorporados en el equipo de procesamiento electrónico de datos.

Declaración interpretativa

En general, el equipo de procesamiento electrónico de datos cuenta con dispositivos de control, proporcionados por su fabricante o proveedor, que puestos en práctica, detectarán las fallas relacionadas con los componentes electrónicos y con su operación mecánica, asegurando que la información sea leída y registrada en forma correcta por el equipo periférico del computador y que no se originarán errores por defectos en la unidad central de procesamiento, en la memoria o en otro componente.

Los controles del equipo generalmente se apoyan en el concepto de redundancia y pueden dividirse en cinco tipos: prueba de carácter redundante, prueba de duplicación del proceso, prueba de eco, prueba de validez y prueba del equipo.

305.09 Mantenimiento del equipo

Se establecerán procedimientos adecuados para el mantenimiento del equipo de computación.

Declaración interpretativa

El mantenimiento del equipo de procesamiento electrónico de datos, es un factor de importancia significativa para garantizar la operación continua de los SIC. Se requiere por lo tanto disponer de procedimientos adecuados para un mantenimiento efectivo y periódico, tomando en consideración, las horas de uso del equipo, los riesgos y las consecuencias de interrupciones operacionales que puedan surgir por fallas del equipo, las características propias de cada componente, así como los costos y beneficios que involucra poner en práctica los planes de mantenimiento.

Este es un asunto que deberá ser considerado desde la fase de contratación de los equipos y las condiciones bajo las cuales operará un servicio de mantenimiento externo deberán estar claramente indicadas en un contrato suscrito. La Administración también deber definir y asignar los niveles de responsabilidad internos para establecer y ejecutar los planes adecuados de mantenimiento.

Este Manual sobre normas técnicas de control interno relativas a los sistemas de información computarizados, se imprimió en la Oficina de Publicaciones de la Contraloría General de la República. El tiraje consta de 500 ejemplares. Se elaboró y revisó en la Dirección General de Planificación Interna y Evaluación de Sistemas.