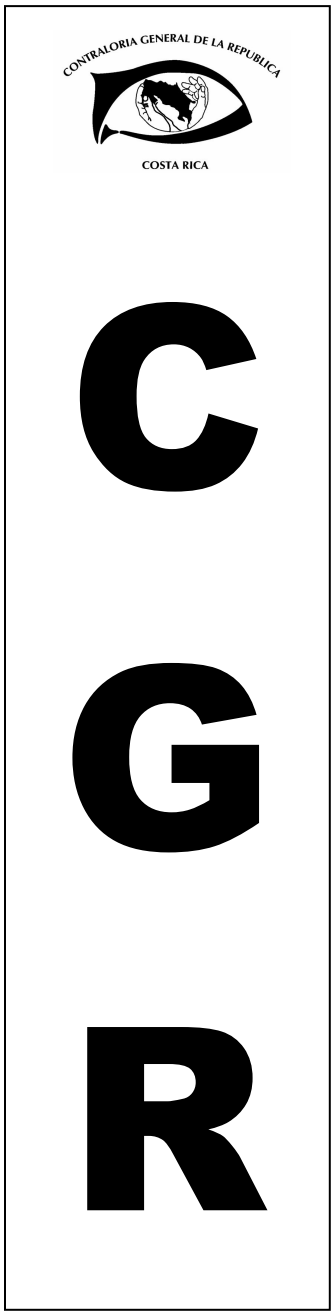

Contraloría General de la República

Normas técnicas para la gestión y el control de las Tecnologías de Información

(N-2-2007-CO-DFOE)

Aprobadas mediante Resolución del Despacho de la Contralora General de la República, Nro. R-CO-26-2007 del 7 de junio, 2007.
*Publicada en La Gaceta Nro.**119** del **21** de **junio**, 2007*

R-CO-26-2007 CONTRALORÍA GENERAL DE LA REPÚBLICA. – **DESPACHO DE LA CONTRALORA GENERAL.** – San José a las diez horas del siete de junio del 2007.

Considerando:

1º— Que el artículo 183 la Constitución Política dispone que la Contraloría General de la República es una institución auxiliar de la Asamblea Legislativa, con absoluta independencia en la vigilancia y control de la Hacienda Pública.

2º— Que los artículos 11 y 12 de la Ley Orgánica de la Contraloría General de la República, Nro. 7424, la designan como órgano rector del Ordenamiento de Control y Fiscalización Superiores de la Hacienda Pública confiriéndole, en concordancia con el artículo 24 de dicha Ley, la facultad de emitir disposiciones, normas, políticas y directrices que coadyuven a garantizar la legalidad y la eficiencia tanto de los controles internos, como del manejo de los fondos públicos de los entes sobre los cuales tiene jurisdicción.

3º— Que el artículo 3 de la Ley General de Control Interno, Nro. 8292 del 31 de julio de 2002, refuerza las facultades de la Contraloría General para emitir la normativa técnica de control interno necesaria para el funcionamiento efectivo del sistema de control interno de los entes y órganos sujetos a esa ley.

4º— Que la Contraloría General de la República publicó en La Gaceta Nro. 24 del 2 de febrero de 1996, Alcance Nro. 7, el "Manual sobre Normas Técnicas de Control Interno relativas a los Sistemas de Información Computadorizados".

5º— Que las tecnologías de información -afectadas por constantes avances tecnológicos-, se han convertido en un instrumento esencial en la prestación de los servicios y representan rubros importantes en los presupuestos del Sector Público.

6º— Que con fundamento en lo antes expuesto la Contraloría General de la República ha considerado pertinente emitir las "Normas técnicas para la gestión y el control de las tecnologías de información" para con ello fortalecer la administración de los recursos invertidos en tecnologías de información, mediante el establecimiento de criterios básicos de control que deben ser observados en la gestión institucional de esas tecnologías y que a su vez coadyuven en el control y fiscalización que realice este órgano contralor.

Por tanto,

RESUELVE

Artículo 1—Aprobar el documento denominado "Normas técnicas para la gestión y el control de las tecnologías de información", normativa que establece los criterios básicos de control que deben observarse en la gestión de esas tecnologías y que tiene como propósito coadyuvar en su gestión, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de los servicios públicos, representando inversiones importantes en el presupuesto del Estado. Dicha normativa está estructurada de la siguiente manera:

Artículo 2 – Promulgar las "Normas técnicas para la gestión y el control de las tecnologías de información", Nro. N-2-2007-CO-DFOE.

Artículo 3 – Establecer que las "Normas técnicas para la gestión y el control de las tecnologías de información" son de acatamiento obligatorio para la Contraloría General de la República y las instituciones y órganos sujetos a su fiscalización, que prevalecerán sobre cualquier disposición en contrario que emita la Administración. Asimismo, que su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable.

Artículo 4 – Derogar el "Manual sobre normas técnicas de control interno relativas a los sistemas de información computadorizados", publicado en el Alcance Nro. 7 de La Gaceta No. 24 del 2 de febrero de 1996.

Artículo 5 – Informar que dicha normativa será distribuida por medio de los mecanismos pertinentes a cada institución y estarán a disposición en la dirección electrónica www.cgr.go.cr de la Contraloría General de la República.

Artículo 6 – Informar que la Administración contará con dos años a partir de su entrada en vigencia para cumplir con lo regulado en esta normativa, lapso en el cual, dentro de los primeros seis meses, deberá planificar las actividades necesarias para lograr una implementación efectiva y controlada de lo establecido en dicha normativa, contemplando los siguientes aspectos:

a. La constitución de un equipo de trabajo con representación de las unidades que correspondan.
b. La designación de un responsable del proceso de implementación, quien asumirá la coordinación del equipo de trabajo y deberá contar con la autoridad necesaria, dentro de sus competencias, para ejecutar el referido plan.
c. El estudio detallado de las normas técnicas referidas, con el fin de identificar las que apliquen a la entidad u órgano de conformidad con su realidad tecnológica y con base en ello establecer las prioridades respecto de su implementación.
d. Dicha planificación deberá considerar las actividades por realizar, los plazos establecidos para cada una, los respectivos responsables, los costos estimados, así como cualquier otro requerimiento asociado (tales como infraestructura, personal y recursos técnicos) y quedar debidamente documentada.

Artículo 7 – Comunicar que la referida normativa entrará a regir a partir del 31 de julio del 2007.

Publíquese.

Rocío Aguilar Montoya
CONTRALORA GENERAL DE LA REPÚBLICA

Contraloría General de la República

Normas técnicas para la gestión y el control de las tecnologías de información

(N-2-2007-CO-DFOE)

ÍNDICE

Normas técnicas para la gestión y el control de las tecnologías de información

N-2-2007-CO-DFOE

Introducción

Las tecnologías de información (TI) constituyen uno de los principales instrumentos que apoyan la gestión de las organizaciones mediante el manejo de grandes volúmenes de datos necesarios para la toma de decisiones y la implementación de soluciones para la prestación de servicios ágiles y de gran alcance.

Su uso ha implicado, al menos, tres situaciones relevantes: la dedicación de porciones importantes del presupuesto de las organizaciones, con el costo de oportunidad que ello conlleva, principalmente en organizaciones con recursos limitados y actividades sustantivas esenciales para la sociedad; un marco jurídico cambiante tendente a buscar su paralelismo con las nuevas relaciones que se dan a raíz del uso de esas TI; y una presión importante de proveedores y consumidores por la implementación de más y mejores servicios apoyados en estas tecnologías.

Dado el impacto de dichas situaciones, las TI deben gestionarse dentro de un marco de control que procure el logro de los objetivos que se pretende con ellas y que dichos objetivos estén debidamente alineados con la estrategia de la organización.

Con el propósito de coadyuvar con ese marco de control y procurar una mejor gestión de dichas tecnologías por parte de las organizaciones, esta Contraloría General sustituye el "Manual sobre normas técnicas de control interno relativas a los sistemas de información automatizados", mediante la promulgación de las presentes "Normas técnicas para la gestión y el control de las tecnologías de información", que se constituyen en una normativa más ajustada a la realidad y necesidad de nuestro ámbito tecnológico actual.

En razón de que dicha normativa establece criterios de control que deben ser observados como parte de la gestión institucional de las TI, el jerarca y los titulares subordinados, como responsables de esa gestión, deben establecer, mantener, evaluar y perfeccionar ese marco de control de conformidad con lo establecido en la Ley General de Control Interno Nro. 8292. Asimismo, la Función de TI debe contribuir con ello cumpliendo con dicho marco de control y facilitando la labor estratégica del jerarca.

Esta normativa es de acatamiento obligatorio para la Contraloría General de la República y las instituciones y órganos sujetos a su fiscalización, y su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable.

Capítulo I Normas de aplicación general

1.1 Marco estratégico de TI

El jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido.

1.2 Gestión de la calidad

La organización debe generar los productos y servicios de TI de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo.

1.3 Gestión de riesgos

La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable.

1.4 Gestión de la seguridad de la información

La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.

Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:

- La implementación de un marco de seguridad de la información.
- El compromiso del personal con la seguridad de la información.
- La seguridad física y ambiental.
- La seguridad en las operaciones y comunicaciones.
- El control de acceso.
- La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.
- La continuidad de los servicios de TI.

Además debe establecer las medidas de seguridad relacionadas con:

- El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.
- El manejo de la documentación.
- La terminación normal de contratos, su rescisión o resolución.
- La salud y seguridad del personal.

Las medidas o mecanismos de protección que se establezcan deben mantener una proporción razonable entre su costo y los riesgos asociados.

1.4.1 Implementación de un marco de seguridad de la información

La organización debe implementar un marco de seguridad de la información, para lo cual debe:

a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.
b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.
c. Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados.

1.4.2 Compromiso del personal con la seguridad de la información

El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.

Para ello, el jerarca, debe:

a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.
b. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.
c. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos.

1.4.3 Seguridad física y ambiental

La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos.

Como parte de esa protección debe considerar:

a. Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas.
b. La ubicación física segura de los recursos de TI.
c. El ingreso y salida de equipos de la organización.
d. El debido control de los servicios de mantenimiento.
e. Los controles para el desecho y reutilización de recursos de TI.
f. La continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas.
g. El acceso de terceros.
h. Los riesgos asociados con el ambiente.

1.4.4 Seguridad en las operaciones y comunicaciones

La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información.

Para ello debe:

a. Implementar los mecanismos de control que permitan asegurar la *no negación*, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.
b. Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.
c. Establecer medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus.

1.4.5 Control de acceso

La organización debe proteger la información de accesos no autorizados.

Para dicho propósito debe:

a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.
b. Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.
c. Definir la propiedad, custodia y responsabilidad sobre los recursos de TI.
d. Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.
e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de *necesidad de saber* o *menor privilegio*. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones.
f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.
i. Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.
j. Establecer los mecanismos necesarios (pistas de auditoría) que

permitan un adecuado y periódico seguimiento al acceso a las TI.

k. Manejar de manera restringida y controlada la información sobre la seguridad de las TI.

1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica

La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información.

Para ello debe:

a. Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura.
b. Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.
c. Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.
d. Controlar el acceso a los programas fuente y a los datos de prueba.

1.4.7 Continuidad de los servicios de TI

La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.

Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.

1.5 Gestión de proyectos

La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos.

1.6 Decisiones sobre asuntos estratégicos de TI

El jerarca debe apoyar sus decisiones sobre asuntos estratégicos de TI en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional, a establecer las prioridades de los proyectos de TI, a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización.

1.7 Cumplimiento de obligaciones relacionadas con la gestión de TI

La organización debe identificar y velar por el cumplimiento del marco jurídico que tiene incidencia sobre la gestión de TI con el propósito de evitar posibles conflictos legales que pudieran ocasionar eventuales perjuicios económicos y de otra naturaleza.

Capítulo II Planificación y organización

2.1 Planificación de las tecnologías de información

La organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes.

2.2 Modelo de arquitectura de información

La organización debe optimizar la integración, uso y estandarización de sus sistemas de información de manera que se identifique, capture y comunique, en forma completa, exacta y oportuna, sólo la información que sus procesos requieren.

2.3 Infraestructura tecnológica

La organización debe tener una perspectiva clara de su dirección y condiciones en materia tecnológica, así como de la tendencia de las TI para que conforme a ello, optimice el uso de su infraestructura tecnológica, manteniendo el equilibrio que debe existir entre sus requerimientos y la dinámica y evolución de las TI.

2.4 Independencia y recurso humano de la Función de TI

El jerarca debe asegurar la independencia de la Función de TI respecto de las áreas usuarias y que ésta mantenga la coordinación y comunicación con las demás dependencias tanto internas y como externas.

Además, debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones.

2.5 Administración de recursos financieros

La organización debe optimizar el uso de los recursos financieros invertidos en la gestión de TI procurando el logro de los objetivos de esa inversión, controlando en forma efectiva dichos recursos y observando el marco jurídico que al efecto le resulte aplicable.

Capítulo III Implementación de tecnologías de información

3.1 Consideraciones generales de la implementación de TI

La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe:

a. Adoptar políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI.
b. Establecer el respaldo claro y explícito para los proyectos de TI tanto del jerarca como de las áreas usuarias.
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.
d. Instaurar líderes de proyecto con una asignación clara, detallada y documentada de su autoridad y responsabilidad.
e. Analizar alternativas de solución de acuerdo con criterios técnicos, económicos, operativos y jurídicos, y lineamientos previamente establecidos.
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.
g. Tomar las previsiones correspondientes para garantizar la disponibilidad de los recursos económicos, técnicos y humanos requeridos.
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.
i. Promover su independencia de proveedores de hardware, software, instalaciones y servicios.

3.2 Implementación de software

La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:

a. Observar lo que resulte aplicable de la norma 3.1anterior.
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-implantación de la satisfacción de los requerimientos.
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.
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.

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.
f. Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento.

3.3 Implementación de infraestructura tecnológica

La organización debe adquirir, instalar y actualizar la infraestructura necesaria para soportar el software de conformidad con los modelos de arquitectura de información e infraestructura tecnológica y demás criterios establecidos. Como parte de ello debe considerar lo que resulte aplicable de la norma 3.1 anterior y los ajustes necesarios a la infraestructura actual.

3.4 Contratación de terceros para la implementación y mantenimiento de software e infraestructura

La organización debe obtener satisfactoriamente el objeto contratado a terceros en procesos de implementación o mantenimiento de software e infraestructura. Para lo anterior, debe:

a. Observar lo que resulte aplicable de las normas 3.1, 3.2 y 3.3 anteriores.
b. Establecer una política relativa a la contratación de productos de software e infraestructura.
c. Contar con la debida justificación para contratar a terceros la implementación y mantenimiento de software e infraestructura tecnológica.
d. Establecer un procedimiento o guía para la definición de los "términos de referencia" que incluyan las especificaciones y requisitos o condiciones requeridos o aplicables, así como para la evaluación de ofertas.
e. Establecer, verificar y aprobar formalmente los criterios, términos y conjunto de pruebas de aceptación de lo contratado; sean instalaciones, hardware o software.
f. Implementar un proceso de transferencia tecnológica que minimice la dependencia de la organización respecto de terceros contratados para la implementación y mantenimento de software e infraestructura tecnológica

Capítulo IV Prestación de servicios y mantenimiento

4.1 Definición y administración de acuerdos de servicio

La organización debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la Función de TI según sus capacidades.

El jerarca y la Función de TI deben acordar los servicios requeridos, los ofrecidos y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño. Para ello deben:

a. Tener una comprensión común sobre: exactitud, oportunidad, confidencialidad, autenticidad, integridad y disponibilidad.
b. Contar con una determinación clara y completa de los servicios y sus atributos, y analizar su costo y beneficio.
c. Definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas.
d. Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos.
e. Definir los criterios de evaluación sobre el cumplimiento de los acuerdos.
f. Revisar periódicamente los acuerdos de servicio, incluidos los contratos con terceros.

4.2 Administración y operación de la plataforma tecnológica

La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:

a. Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.
b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.
c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas.
d. Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas.
e. Controlar la ejecución de los trabajos mediante su programación, supervisión y registro.
f. Mantener separados y controlados los ambientes de desarrollo y producción.
g. Brindar el soporte requerido a los equipos principales y periféricos.
h. Definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración.
i. Controlar los servicios e instalaciones externos.

4.3 Administración de los datos

La organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura.

4.4 Atención de requerimientos de los usuarios de TI

La organización debe hacerle fácil al usuario el proceso para solicitar la atención de los requerimientos que le surjan al utilizar las TI. Asimismo, debe atender tales requerimientos de manera eficaz, eficiente y oportuna; y dicha atención debe constituir un mecanismo de aprendizaje que permita minimizar los costos asociados y la recurrencia.

4.5 Manejo de incidentes

La organización debe identificar, analizar y resolver de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TI. Además, debe darles el seguimiento pertinente, minimizar el riesgo de recurrencia y procurar el aprendizaje necesario.

4.6 Administración de servicios prestados por terceros

La organización debe asegurar que los servicios contratados a terceros satisfagan los requerimientos en forma eficiente. Con ese fin, debe:

a. Establecer los roles y responsabilidades de terceros que le brinden servicios de TI.
b. Establecer y documentar los procedimientos asociados con los servicios e instalaciones contratados a terceros.
c. Vigilar que los servicios contratados sean congruentes con las políticas relativas a calidad, seguridad y seguimiento establecidas por la organización.
d. Minimizar la dependencia de la organización respecto de los servicios contratados a un tercero.
e. Asignar a un responsable con las competencias necesarias que evalúe periódicamente la calidad y cumplimiento oportuno de los servicios contratados.

Capítulo V Seguimiento

5.1 Seguimiento de los procesos de TI

La organización debe asegurar el logro de los objetivos propuestos como parte de la gestión de TI, para lo cual debe establecer un marco de referencia y un proceso de seguimiento en los que defina el alcance, la metodología y los mecanismos para vigilar la gestión de TI. Asimismo, debe determinar las responsabilidades del personal a cargo de dicho proceso.

5.2 Seguimiento y evaluación del control interno en TI

El jerarca debe establecer y mantener el sistema de control interno asociado con la gestión de las TI, evaluar su efectividad y cumplimiento y mantener un registro de las excepciones que se presenten y de las medidas correctivas implementadas.

5.3 Participación de la Auditoría Interna

La actividad de la Auditoría Interna respecto de la gestión de las TI debe orientarse a coadyuvar, de conformidad con sus competencias, a que el control interno en TI de la organización proporcione una garantía razonable del cumplimiento de los objetivos en esa materia.

Glosario

Activos informáticos	Véase "Recursos informáticos"
Acuerdos de confidencialidad	Convenio suscrito entre la entidad y sus funcionarios, o bien, entre instituciones que comparten datos o sistemas, para garantizar el manejo discreto de la información. También se utiliza el concepto "cláusulas de confidencialidad", que son aquellas que imponen una obligación negativa: de no hacer o de abstenerse; es decir, de no utilizar la información recibida con fines distintos a los estipulados. (Véanse los artículos 71 del Código de Trabajo)
Acuerdos de servicio	Los acuerdos de servicios, mejor conocidos como convenios o acuerdos de nivel de servicio ("SLA's" por sus siglas en inglés de "Service Level Agreement") son contratos escritos, formales, desarrollados conjuntamente por el proveedor del servicio de TI y los usuarios respectivos, en los que se define, en términos cuantitativos y cualitativos, el servicio que brindará la dependencia responsable de TI y las responsabilidades de la contraparte beneficiada por dichos servicios.
Ambiente de desarrollo	Conjunto de componentes de hardware y software donde se efectúan los procesos de construcción, mantenimiento (v.gr. ajustes, cambios y correcciones) y pruebas de sistemas de información.
Ambiente de producción	Conjunto de componentes de hardware y software donde se efectúan los procesos normales de procesamiento de datos, con sistemas e información reales.
Base de datos	Colección de datos almacenados en un computador, los cuales pueden ser accedidos de diversas formas para apoyar los sistemas de información de la organización.
Calidad	Propiedad o conjunto de propiedades inherentes a algo, que permiten juzgar su valor. / Conjunto de características que posee un producto o servicio obtenidos en un sistema productivo, así como su capacidad de satisfacción de los requerimientos del usuario.
Confidencialidad de la información	Protección de información sensible contra divulgación no autorizada.
Contingencia	Riesgo que afecta la continuidad de los servicios y operaciones.
Continuidad de los servicios y operaciones	Implica la prevención, mitigación de las interrupciones operacionales y la recuperación de las operaciones y servicios.
Contraseñas	Véase "password".
Conversión de datos	Proceso mediante el cual se cambia el formato de los datos.
Cumplimiento	Proceso de respetar y aplicar las leyes, reglamentaciones y disposiciones contractuales a las que está sujeta la organización.
Datos	Objetos en su sentido más amplio (es decir, internos y externos), estructurados y no estructurados, gráficos, sonido, entre otros.
Desarrollo	Etapa del ciclo de vida del desarrollo de sistemas que implica la construcción de las aplicaciones.

Disponibilidad de la información	Se vincula con el hecho de que la información se encuentre disponible (v.gr. utilizable) cuando la necesite un proceso de la organización en el presente y en el futuro. También se asocia con la protección de los recursos necesarios y las capacidades asociadas. Implica que se cuente con la información necesaria en el momento en que la organización la requiere.
Efectividad de la información	Que la información sea cierta, oportuna, relevante y pertinente para la organización.
Eficiencia	Provisión de información efectiva a la organización mediante el uso óptimo (el más productivo y económico) de los recursos.
Función de TI	Unidad organizacional o conjunto de componentes organizacionales responsable de los principales procesos relacionados con la gestión de las tecnologías de información en apoyo a la gestión de la organización.
Gestión de las TI	Conjunto de acciones fundamentadas en políticas institucionales que, de una manera global, intentan dirigir la gestión de las TI hacia el logro de los objetivos de la organización. Para ello se procura, en principio, la alineación entre los objetivos de TI y los de la organización, el balance óptimo entre las necesidades de TI de la organización y las oportunidades que sobre ello existen, la maximización de los beneficios y el uso responsable de los recursos, la administración adecuada de los riesgos y el valor agregado en la implementación de dichas TI. Tales acciones se relacionan con los procesos (planificación, organización, implementación, mantenimiento, entrega, soporte y seguimiento), recursos tecnológicos (personas, sistemas, tecnologías, instalaciones y datos), y con el logro de los criterios de fidelidad, calidad y seguridad de la información. También se entiende como "Gobernabilidad de TI".
Hardware	Todos los componentes electrónicos, eléctricos y mecánicos que integran una computadora, en oposición a los programas que se escriben para ella y la controlan (software).
Información	Conjunto de datos que han sido capturados y procesados, que se encuentran organizados y que tienen el potencial de confirmar o cambiar el entendimiento sobre algo.
Infraestructura tecnológica	Conjunto de componentes de hardware e instalaciones en los que se soportan los sistemas de información de la organización.
Instalaciones	Edificaciones y sus aditamentos utilizados para alojar los recursos informáticos.
Integridad	Precisión y suficiencia de la información, así como su validez de acuerdo con los valores y expectativas del negocio.
Jerarca	Superior jerárquico, unipersonal o colegiado del órgano o ente quien ejerce la máxima autoridad.
Marco de seguridad de la información	Conjunto de componentes asociados a la gestión de la seguridad dentro de los cuales cuentan, entre otros: Principios y términos definidos para un uso uniforme en la organización; un sistema de gestión que implica la definición de actividades, productos y responsables del proceso de definición, implementación y seguimiento de acciones para la seguridad de la información; el conjunto de controles; las guías de implementación; métricas para seguimiento y la consideración de riesgos.
Menor Privilegio	Principio utilizado para la asignación de perfiles de usuario según el cual a éste se

	le deben asignar, por defecto, únicamente los permisos estrictamente necesarios para la realización de sus labores.
Migración	Proceso de traslado de datos o sistemas entre plataformas o entre sistemas.
Modelo de arquitectura de información	Véase "Modelo de Información".
Modelo de información	Representación de los procesos, sistemas y datos, y sus interrelaciones, mediante los cuales fluye toda la información organizacional.
No negación	Condición o atributo que tiene una transacción informática que permite que las partes relacionadas con ella no puedan aducir que la misma transacción no se realizó o que no se realizó en forma completa, correcta u oportuna.
Necesidad de saber	Principio utilizado para la definición de perfiles de usuario según el cual a éste se le deben asignar los permisos estrictamente necesarios para tener acceso a aquella información que resulte imprescindible para la realización de su trabajo.
Pistas de auditoría	Información que se registra como parte de la ejecución de una aplicación o sistema de información y que puede ser utilizada posteriormente para detectar incidencias o fallos. Esta información puede estar constituida por atributos como: la fecha de creación, última modificación o eliminación de un registro, los datos del responsable de dichos cambios o cualquier otro dato relevante que permita dar seguimiento a las transacciones u operaciones efectuadas. Las pistas de auditoría permiten el rastreo de datos y procesos; pueden aplicarse progresivamente (de los datos fuente hacia los resultados), o bien regresivamente (de los resultados hacia los datos fuente).
Plataforma tecnológica	Término que resume los componentes de hardware y software (software de base, utilitarios y software de aplicación) utilizados en la organización.
Prestación de servicios de TI	Entrega o prestación eficaz de los servicios de TI requeridos por la organización, que comprenden desde las operaciones tradicionales sobre aspectos de seguridad y continuidad, hasta la capacitación. Para prestar los servicios, debe establecerse los procesos de soporte necesarios. Como parte de esta prestación, se incluye el procesamiento real de los datos por los sistemas de aplicación, a menudo clasificados como controles de aplicaciones.
Propiedad de la información	Tiene la propiedad de la información la unidad responsable o que puede disponer sobre dicha información.
Recursos de TI	Aplicaciones, información, infraestructura (tecnología e instalaciones) y personas que interactúan en un ambiente de TI de una organización.
Recursos informáticos	Véase “recursos de TI”.
Seguimiento de las TI	Evaluación regular de todos los procesos de TI a medida que transcurre el tiempo para determinar su calidad y el cumplimiento de los requerimientos de control. Es parte de la vigilancia ejercida por la función gerencial sobre los procesos de control de la organización y la garantía independiente provista por la auditoría interna y externa u obtenida de fuentes alternativas.
Seguridad	Conjunto de controles para promover la confidencialidad, integridad y disponibilidad de la información.
Seguridad física	Protección física del hardware, software, instalaciones y personal relacionado con

	los sistemas de información.
Servicios prestados por terceros	Servicios recibidos de una empresa externa a la organización. Por lo general, requiere de una contraparte interna de la organización que garantice que el producto desarrollado cumple con los estándares establecidos por ésta. También es conocido como "*outsourcing"*.
Software	Los programas y documentación que los soporta que permiten y que facilitan el uso de la computadora. El software controla la operación del hardware.
Software de aplicación	Programa de computadora con el que se automatiza un proceso de la organización y que principalmente está diseñado para usuarios finales. También conocido como sistemas de aplicación.
Software de base	También conocido como software de sistemas que es la colección de programas de computadora usados en el diseño, procesamiento y control de todas las aplicaciones, los programas y rutinas de procesamiento que controlan el hardware de computadora. Incluye el sistema operativo y los programas utilitarios.
Tecnologías de información (TI)	Conjunto de tecnologías dedicadas al manejo de la información organizacional. Término genérico que incluye los recursos de: información, software, infraestructura y personas relacionadas.
Titular Subordinado	Funcionario de la administración activa responsable de un proceso, con autoridad para ordenar y tomar decisiones.