ASAMBLEA LEGISLATIVA DE LA
REPÚBLICA DE COSTA RICA

PROYECTO DE LEY

LEY MARCO SOBRE NORMAS TÉCNICAS PARA LA GESTIÓN Y EL CONTROL DE LAS TECNOLOGÍAS DE INFORMACIÓN

VARIOS SEÑORES DIPUTADOS

EXPEDIENTE N.º 17.492

DEPARTAMENTO DE SERVICIOS
PARLAMENTARIOS

PROYECTO DE LEY

LEY MARCO SOBRE NORMAS TÉCNICAS PARA LA GESTIÓN Y EL CONTROL DE LAS TECNOLOGÍAS DE INFORMACIÓN

Expediente N.º 17.492

ASAMBLEA LEGISLATIVA:

A través del tiempo se ha podido constatar que el sector público no posee una estrategia adecuada que sirva de guía para la compra y el uso de los rubros que se enmarcan dentro del concepto de tecnología de información, lo que sin duda ha originado procesos de poca eficiencia en la utilización de los recursos públicos.

Como muy bien lo señala y reconoce la Contraloría General de la República[1], 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.

Dentro de un contexto amplio, es claro que las compras públicas deben considerarse, no solamente como una simple manera de adquirir bienes y servicios, sino que componen una importante herramienta de desarrollo mediante la cual el Estado se ha convertido en uno de los más importantes compradores de tecnología, ya que adquiere desde software y hardware hasta sofisticadas redes de telecomunicaciones, así como el contrato de servicios y asistencia técnica.

En virtud de lo anterior, la Contraloría General de la República consideró necesario y pertinente emitir las “Normas técnicas para la gestión y el control de las tecnologías de información”, para fortalecer la administración de los recursos invertidos en tecnologías de información mediante criterios básicos de control. La administración de estos recursos debe ser observada por la gestión institucional de esas tecnologías para que, a su vez, coadyuve en el control y la fiscalización que realiza este órgano contralor[2].

De esta forma se aprueba, mediante resolución del despacho de la Contralora General de la República, N.º R-CO-26-2007, de 7 de junio de 2007, publicado en La Gaceta N.º 119, de 21 de junio de 2007, 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

---

[1] CGR - Normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CO-DFOE)

[2] CGR - (N-2-2007-CO-DFOE)

coadyuvar en su gestión, ya que estas son un instrumento esencial en la prestación de servicios públicos y una inversión importante en el presupuesto del Estado[3].

Ante la importancia de este documento, gestado por la Contraloría General de la República, y dados los alcances y el fondo de este, se considera necesario e imperioso llevarlo a un nivel más alto en el marco de la normativa legal costarricense.

A la luz de la realidad actual y al visualizar los años venideros, puede decirse que la Administración Pública necesita una ley marco, en esta área, que podría surgir del texto emitido por la Contralora General de la República, cuya complejidad y claridad satisfacen, sin duda, los requerimientos y las necesidades.

De lo anteriormente expuesto, y en reconocimiento al esfuerzo del ente contralor para adaptarlo al formato legislativo, se redacta el proyecto de Ley marco sobre normas técnicas para la gestión y el control de las tecnologías de información, cuyo contenido básico se plasma en seis capítulos que versan sobre lo siguiente: normas de aplicación general; planificación y organización; implementación de tecnologías de información; prestación de servicios y mantenimiento; seguimiento, control y fiscalización y, finalmente, definiciones.

Esta Ley marco no tiene más objeto que institucionalizar un conjunto de 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 estas, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de servicios públicos y de inversión importante en el presupuesto del Estado.

Por lo anteriormente expuesto se somete al conocimiento de la Asamblea Legislativa la presente iniciativa de ley.

[3] **CGR - (N-2-2007-CO-DFOE)**

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA
DECRETA:

LEY MARCO SOBRE NORMAS TÉCNICAS PARA LA GESTIÓN Y EL CONTROL DE LAS TECNOLOGÍAS DE INFORMACIÓN

CAPÍTULO I
NORMAS DE APLICACIÓN GENERAL

ARTÍCULO 1.- Objetivos de la ley

La presente Ley marco tiene por objeto establecer las normas técnicas para la gestión y el control de las tecnologías de información, normativa que instituye los criterios básicos que deben ser observados en la gestión institucional de esas tecnologías y que a su vez coadyuven en los procesos de control y fiscalización.

ARTÍCULO 2.- Marco estratégico de tecnologías de información

El jerarca de la institución debe traducir sus aspiraciones en materia de tecnologías de información (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.

ARTÍCULO 3.- Gestión de la calidad

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

ARTÍCULO 4.- Gestión de riesgos

La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las tecnologías de información 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.

ARTÍCULO 5.- 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:

a) La implementación de un marco de seguridad de la información.
b) El compromiso del personal con la seguridad de la información.
c) La seguridad física y ambiental.
d) La seguridad en las operaciones y comunicaciones.
e) El control de acceso.
f) La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.
g) La continuidad de los servicios de tecnologías de información.
h) Además debe establecer las medidas de seguridad relacionadas con:
i) El acceso a la información por parte de terceros y la contratación de servicios prestados por estos.
j) El manejo de la documentación.
k) La terminación normal de contratos, su rescisión o resolución.
l) 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.

ARTÍCULO 6.- 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 tecnologías de información 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.

ARTÍCULO 7.- 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 tecnologías de información. 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 tecnologías de información.
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.

ARTÍCULO 8.- Seguridad física y ambiental

La organización debe proteger los recursos de tecnologías de información 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 tecnologías de información.
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 tecnologías de información.
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.

ARTÍCULO 9.- Seguridad en las operaciones y comunicaciones

La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de tecnologías de información 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 y 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.

ARTÍCULO 10.- 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 tecnologías de información en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.
c) Definir la propiedad, custodia y responsabilidad sobre los recursos de tecnologías de información.
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 tecnologías de información.
e) Asignar los derechos de acceso a los usuarios de los recursos de tecnologías de información 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 tecnologías de información. 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.
g) Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.
h) Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las tecnologías de información.
i) Manejar de manera restringida y controlada la información sobre la seguridad de las tecnologías de información.

ARTÍCULO 11.- 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 de 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.

ARTÍCULO 12.- Continuidad de los servicios de tecnologías de información

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 tecnologías de información según su criticidad.

ARTÍCULO 13.- Gestión de proyectos

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

ARTÍCULO 14.- Decisiones sobre asuntos estratégicos de tecnologías de información

El jerarca debe apoyar sus decisiones sobre asuntos estratégicos de tecnologías de información 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 tecnologías de información a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización.

ARTÍCULO 15.- Cumplimiento de obligaciones relacionadas con la gestión de tecnologías de información

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

CAPÍTULO II
PLANIFICACIÓN Y ORGANIZACIÓN

ARTÍCULO 16.- Planificación de las tecnologías de información

La organización debe lograr que las tecnologías de información 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.

ARTÍCULO 17.- 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, solo la información que sus procesos requieren.

ARTÍCULO 18.- Infraestructura tecnológica

La organización debe tener una perspectiva clara de su dirección y condiciones en materia tecnológica, así como de la tendencia de las tecnologías de información 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 tecnologías de información.

ARTÍCULO 19.- Independencia y recurso humano de la función de tecnologías de información

El jerarca debe asegurar la independencia de la función de tecnologías de información respecto de las áreas usuarias y que esta mantenga la coordinación y comunicación con las demás dependencias tanto internas como externas. Además, debe brindar el apoyo necesario para que dicha función de tecnologías de información 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.

ARTÍCULO 20.- Administración de recursos financieros

La organización debe optimizar el uso de los recursos financieros invertidos en la gestión de tecnologías de información 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

ARTÍCULO 21.- Consideraciones generales de la implementación de tecnologías de información

La organización debe implementar y mantener las tecnologías de información 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 tecnologías de información.
b) Establecer el respaldo claro y explícito para los proyectos de tecnologías de información 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 tecnologías de información tiempo y costo preestablecidos.
i) Promover su independencia de proveedores de hardware, software, instalaciones y servicios.

ARTÍCULO 22.- 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 del artículo 21 anterior.
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.

ARTÍCULO 23.- 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 del artículo 21 y los ajustes necesarios a la infraestructura actual.

ARTÍCULO 24.- 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 los artículos 21, 22 y 23 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 mantenimiento de software e infraestructura tecnológica.

CAPÍTULO IV
PRESTACIÓN DE SERVICIOS Y MANTENIMIENTO

ARTÍCULO 25.- 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 tecnologías de información según sus capacidades.

El jerarca y la función de tecnologías de información 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.

ARTÍCULO 26.- 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 tecnologías de información 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.

ARTÍCULO 27.- Administración de los datos

La organización debe asegurarse de que los datos que son procesados mediante tecnologías de información 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.

ARTÍCULO 28.- Atención de requerimientos de los usuarios de tecnologías de información

La organización debe hacerle fácil al usuario el proceso para solicitar la atención de los requerimientos que le surjan al utilizar las tecnologías de información. 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.

ARTÍCULO 29.- Manejo de incidentes

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

ARTÍCULO 30.- 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 tecnologías de información.
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

ARTÍCULO 31.- Seguimiento de los procesos de tecnologías de información

La organización debe asegurar el logro de los objetivos propuestos como parte de la gestión de tecnologías de información 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 tecnologías de información. Asimismo, debe determinar las responsabilidades del personal a cargo de dicho proceso.

ARTÍCULO 32.- Seguimiento y evaluación del control interno en tecnologías de información

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

ARTÍCULO 33.- Participación de la auditoría interna

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

CAPÍTULO VI
CONTROL Y FISCALIZACIÓN

ARTÍCULO 34.- Participación de la Contraloría General de la República

Conforme al artículo 183 la Constitución Política le corresponde a la Contraloría General de la República en su carácter de institución auxiliar de la Asamblea Legislativa, la vigilancia y control de la Hacienda Pública y por ende que coadyuve en el control y fiscalización de la presente normativa.

CAPÍTULO VI
DEFINICIONES

ARTÍCULO 35.- Glosario

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. Para los efectos véase el artículo 71 del Código de Trabajo, Ley N.º 2, de 27 de agosto de 1943.

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 tecnologías de información y los usuarios respectivos, en los que se define, en términos cuantitativos y cualitativos, el servicio que brindará la dependencia responsable de tecnologías de información 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.

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 tecnologías de información: 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 tecnologías de información: Conjunto de acciones fundamentadas en políticas institucionales que, de una manera global,

intentan dirigir la gestión de las tecnologías de información hacia el logro de los objetivos de la organización. Para ello se procura, en principio, la alineación entre los objetivos de tecnologías de información y los de la organización, el balance óptimo entre las necesidades de tecnologías de información 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 tecnologías de información. 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 Tecnologías de Información”.

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 tecnologías de información 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.

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 que 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 este 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 o 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 tecnologías de información 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 este 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 tecnologías de información: Entrega o prestación eficaz de los servicios de tecnologías de información 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 tecnologías de información, activos o recursos informáticos: Aplicaciones, información, infraestructura (tecnología e instalaciones) y personas que interactúan en un ambiente de tecnologías de información de una organización.

Seguimiento de las tecnologías de información: Evaluación regular de todos los procesos de tecnologías de información a medida que transcurre las tecnologías de información 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 esta. 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.

ARTÍCULO 36.- El Poder Ejecutivo reglamentará todo lo concerniente a la aplicación de esta Ley, durante los seis meses siguientes a su sanción.

Rige a partir de su publicación.

Federico Tinoco Carmona Edine von Herold Duarte

DIPUTADOS

24 de agosto de 2009.

NOTA: Este proyecto pasó a estudio e informe de la Comisión Permanente de Asuntos Jurídicos.