NORMAS DE CONTROL INTERNO PARA TECNOLOGÍA DE LA INFORMACIÓN - SECTOR PÚBLICO NACIONAL

Res. 48/2005 SIGEN

- **Dirigidas a:**
  - ✓ Responsables de organismos
  - ✓ Responsables Informáticos
  - ✓ Auditores

Utilidad

Resp. de Organismos y Resp. Informáticos

- Son los encargados de cumplir las normas
- Les ofrece un detalle de controles mínimos que se deben cumplir en la gestión de TI

Auditores Informáticos

- Son los encargados de verificar el cumplimiento de las normas por parte de los responsables.
- Identifica que deben incluir en las revisiones de la gestión informática. Brinda una guía para las revisiones

Aspectos considerados en la Norma

1. ORGANIZACIÓN INFORMÁTICA
2. PLAN ESTRATÉGICO DE TI
3. ARQUITECTURA DE LA INFORMACIÓN
4. POLÍTICAS Y PROCEDIMIENTOS
5. CUMPLIMIENTO DE REGULACIONES EXTERNAS
6. ADMINISTRACIÓN DE PROYECTOS
7. DESARROLLO, MANTENIMIENTO O ADQUISICIÓN DE SOFTWARE DE APLICACIÓN
8. ADQUISICIÓN Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA
9. SEGURIDAD
10. SERVICIOS DE PROCESAMIENTO Y/O SOPORTE PRESTADOS POR TERCEROS
11. SERVICIOS DE INTERNET / EXTRANET / INTRANET
12. MONITOREO DE LOS PROCESOS
13. AUDITORÍA INTERNA DE SISTEMAS

1. ORGANIZACIÓN INFORMÁTICA

1.1. La responsabilidad por las actividades de Tecnología de la Información (TI) de la organización debe recaer en una única unidad o comité de sistemas (unidad de TI) que asegure la homogeneidad y unicidad de criterios y objetivos en la materia.

1.2. La ubicación de la unidad de TI dentro de la estructura orgánica debe garantizar su independencia respecto de las áreas usuarias, asegurando la atención de todos los sectores de la organización.

1.3. Debe existir una descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de TI, la cual debe contemplar tanto la autoridad como la responsabilidad. El personal de TI debe notificarse de sus deberes y responsabilidades.

1. ORGANIZACIÓN INFORMÁTICA

1.4. La asignación de responsabilidades debe garantizar una adecuada separación de funciones, que fomente el control por oposición de intereses

1.5. En concordancia con el plan estratégico, la dirección de la organización debe establecer y mantener procedimientos para identificar y documentar las necesidades de capacitación de todo el personal que utiliza los servicios de información. Se debe establecer un plan de capacitación para cada grupo de empleados, tanto los usuarios finales como el personal técnico informático.

2. PLAN ESTRATÉGICO DE TI

2.1. La unidad de TI debe elaborar e implementar un plan informático estratégico, el cual deberá estar alineado con el plan estratégico y el presupuesto de la organización. Para la elaboración de dicho plan se deben considerar, evaluar y priorizar los requerimientos de todas las áreas de la organización.

2.2. La unidad de TI debe incluir en el plan informático, consideraciones respecto de la evolución de la infraestructura tecnológica, contemplando un esquema de actualización orientado a evaluar la conveniencia de incorporar nuevas tecnologías disponibles en el mercado y evitar la obsolescencia tecnológica.

2.3. El plan informático debe ser aprobado por la dirección de la organización considerando, para cada uno de los proyectos involucrados, la razonabilidad de los plazos, beneficios a obtener y costos asociados.

2. PLAN ESTRATÉGICO DE TI

2.4. El plan informático debe mantenerse actualizado.

2.5. La unidad de TI debe elaborar un presupuesto asociado a la ejecución del plan informático y el desarrollo de sus actividades, el cual debe ser evaluado y aprobado por la dirección, e incorporado al presupuesto anual de la organización.

2.6. La dirección de la organización debe controlar en forma periódica, el grado de avance del plan informático

2.7. Las adquisiciones de hardware, software u otros servicios informáticos, deben responder a los proyectos incluidos en el plan informático de la organización. Las situaciones de excepción deben ser autorizadas por la dirección de la organización y auditadas por la unidad de auditoría interna.

3. ARQUITECTURA DE LA INFORMACIÓN

3.1. La unidad de TI debe definir el modelo de arquitectura de la información de la organización, orientado a asegurar que los datos se encuentren organizados eficientemente y de manera homogénea, garantizando que estarán disponibles para su utilización, en concordancia con las necesidades operativas de las diferentes áreas usuarias en cuanto a oportunidad, integridad, exactitud o formato, entre otras. Este modelo de arquitectura de la información debe documentarse y mantenerse actualizado en un diccionario de datos corporativo, especificando los controles de consistencia, integridad, confidencialidad y validación aplicables.

4. POLÍTICAS Y PROCEDIMIENTOS

4.1. La unidad de TI debe desarrollar, documentar y comunicar políticas y procedimientos respecto de las actividades relacionadas con la TI. Tales políticas y procedimientos deben mantenerse actualizados. Deben especificar las tareas y controles a realizar en los distintos procesos, así como los responsables y las sanciones disciplinarias asociadas con su incumplimiento.

5. CUMPLIMIENTO DE REGULACIONES EXTERNAS

5.1. La unidad de TI debe garantizar el cumplimiento de las regulaciones relativas a privacidad de la información, propiedad intelectual del software, seguridad de la información así como de las demás normas que resulten aplicables.

5.2. La unidad de TI debe establecer convenios o contratos formales con aquellos terceros con los que existan intercambios de información o prestación de servicios relacionados con la TI.

6. ADMINISTRACIÓN DE PROYECTOS

6.1. La unidad de TI debe disponer de una metodología de administración de proyectos que se aplique en todos los proyectos informáticos encarados y que contemple, mínimamente, lo siguiente:

6.1.1. La documentación y aprobación de la justificación que origina el proyecto, así como la definición clara del plan, especificando sus objetivos, alcance, asignación de responsabilidades y facultades a los miembros del grupo de proyecto, y el presupuesto de los recursos a utilizar en el mismo. Se debe contemplar la elaboración del plan de pruebas y de capacitación que fueran necesarios.

6.1.2. La realización de los estudios de factibilidad pertinentes y del análisis de los riesgos del proyecto.

6.1.3. La participación formal de todas las áreas involucradas en el proyecto y de la unidad de auditoría interna.

6.2. Se debe monitorear la ejecución del plan del proyecto considerando el cumplimiento de los objetivos planteados, plazos y costos.

7. DESARROLLO, MANTENIMIENTO O ADQUISICIÓN DE SOFTWARE DE APLICACIÓN

7.1. La unidad de TI debe disponer de un procedimiento o metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas, que debe estar documentado y aprobado, y debe aplicarse en forma complementaria a las normas relativas a administración de proyectos. Debe contemplar procedimientos detallados, mínimamente para :

7.1.1. La formulación y documentación de requerimientos por parte de las áreas usuarias, ya sea para nuevos desarrollos, adquisiciones o cambios a los sistemas existentes, incluyendo la definición detallada de las necesidades que motivan el requerimiento y la especificación de los niveles de servicio esperados.

7.1.2. El criterio para el establecimiento de prioridades entre los distintos requerimientos recibidos por la unidad de TI.

7.1.3. El tratamiento de solicitudes de emergencia, incluyendo la autorización del responsable de la unidad de TI, el registro y monitoreo de las tareas realizadas

7.1.4. La aprobación por parte de los responsables de las áreas usuarias afectadas, de las especificaciones de diseño elaboradas.

7. DESARROLLO, MANTENIMIENTO O ADQUISICIÓN DE SOFTWARE DE APLICACIÓN

7.1. La unidad de TI debe disponer de un procedimiento o metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas, que debe estar documentado y aprobado, y debe aplicarse en forma complementaria a las normas relativas a administración de proyectos. Debe contemplar procedimientos detallados, mínimamente para :

7.1.5. La participación de la unidad de auditoría interna durante el desarrollo.

7.1.6. La utilización de estándares de diseño, programación y documentación.

7.1.7. La realización de pruebas suficientes en las distintas etapas del desarrollo, conforme a un plan de pruebas y de control de calidad aprobado, en un ambiente específico representativo del ambiente operativo futuro y distinto del ámbito de producción. Se deben establecer los criterios para concluir el proceso de prueba y dar por aceptada la implementación del sistema. Dichas pruebas deben contemplar la participación y aprobación formal del usuario solicitante.

7. DESARROLLO, MANTENIMIENTO O ADQUISICIÓN DE SOFTWARE DE APLICACIÓN

7.1. La unidad de TI debe disponer de un procedimiento o metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas, que debe estar documentado y aprobado, y debe aplicarse en forma complementaria a las normas relativas a administración de proyectos. Debe contemplar procedimientos detallados, mínimamente para :

7.1.8. El pasaje del sistema aprobado desde el ambiente de desarrollo/prueba al de producción.

7.1.9. El control de las versiones del software por parte del área responsable de las tareas de desarrollo y mantenimiento de sistemas.

7.1.10. La preparación de documentación de soporte para el usuario y el personal técnico.

7.1.11. La capacitación al personal de las áreas usuarias y de la unidad de TI.

7. DESARROLLO, MANTENIMIENTO O ADQUISICIÓN DE SOFTWARE DE APLICACIÓN

7.2. La contratación de servicios externos de desarrollo de sistemas debe estar justificada por escrito y autorizada por el responsable de la unidad de TI. El contrato debe estipular que el software, la documentación y demás ítems adquiridos se sometan a prueba y revisión antes de la aceptación por parte de la unidad de TI y de las áreas usuarias. Salvo justificación documentada y aprobada en contrario, la propiedad intelectual del software resultante debe pertenecer a la organización contratante, lo cual debe constar en el contrato. Asimismo, deben establecerse en el citado contrato, los criterios de aceptación del producto.

8. ADQUISICIÓN Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA

8.1. Las adquisiciones de bienes y servicios informáticos deben basarse en los estándares vigentes para la Administración Pública. Se debe garantizar el cumplimiento de la normativa de contrataciones aplicable.

8.2. Los productos deben ser analizados y probados antes de proceder a su aceptación definitiva.

8.3. La unidad de TI debe planificar y realizar el mantenimiento preventivo periódico del hardware, a fin de reducir la frecuencia y el impacto de las fallas en su desempeño.

8.4. Deben existir procedimientos documentados para la gestión de licencias de software a fin de asegurar que en la organización solamente se utilicen productos adquiridos por vías oficiales.

9. SEGURIDAD

9.1. Se debe garantizar el cumplimiento de las normas establecidas en cuanto al deber de disponer de una política de seguridad de la información.

Capitulos Introductorios

1. Introducción
2. Términos y Definiciones
3. Estructura de la Política modelo
4. Evaluación y tratamiento de riesgos

Capitulos Cláusulas

Politicas x cláusula

Objetivo = resultado deseado
Controles = para mitigar riesgos

Politica de Seguridad

5. Política de Seguridad
6. Organización
7. Clasificación de Activos
8. Recursos Humanos
9. Seguridad Física Ambiental
10. Gestión de Comunicaciones /Operaciones
11. Gestión de Accesos
12. Adquisición, Desarrollo y mantenimiento de sistemas
13. Gestión de Incidentes de Seguridad
14. Gestión de la Continuidad
15. Cumplimiento

Cláusulas
Aspecto o dominio particular de la seguridad de la información

Categoría
Grupo de controles de cada claúsula

Control
Punto de evaluación

Política de Seguridad de la Información Modelo
Disposición 3/2013

10. SERVICIOS DE PROCESAMIENTO Y/O SOPORTE PRESTADOS POR TERCEROS

10.1. La decisión de contratar servicios a terceros debe estar debidamente justificada, documentada y respaldada por el análisis de costo/beneficio y la evaluación de riesgos pertinentes.

10.2. La dirección de la organización debe definir procedimientos específicos para garantizar que cada vez que se implementen relaciones con proveedores externos de servicios, se defina y se acuerde un contrato formal antes de que comience el trabajo, el cual debe identificar claramente los objetivos a alcanzar y servicios a proveer, las obligaciones de ambas partes, los métodos y responsables de las interacciones y las políticas de la organización que deben ser respetadas por el tercero. Tales procedimientos deben asegurar el cumplimiento de la normativa para las Contrataciones aplicables.

10. SERVICIOS DE PROCESAMIENTO Y/O SOPORTE PRESTADOS POR TERCEROS

10.3. Los contratos con terceros proveedores de servicios deben incluir la especificación formal de acuerdos de nivel de servicio, identificando explícitamente los respectivos a seguridad -por ejemplo los acuerdos de no divulgación- y al cumplimiento de los requisitos legales aplicables. Se debe aclarar expresamente que la propiedad de los datos corresponde a la organización contratante.

10.4. La dirección de la organización debe monitorear el servicio prestado por los terceros contratados, para garantizar que se cumplan las obligaciones comprometidas.

10.5. En caso de contrataciones de servicios externos en los que el proveedor realice el procesamiento de la información de la organización mediante sistemas que pertenecen al tercero, careciendo la organización de los programas fuente, deben tomarse las previsiones necesarias para asegurar la disponibilidad de los mismos por parte de la organización en caso de alguna contingencia o salida del mercado del proveedor -por ejemplo, dejando una copia de los fuentes bajo custodia de escribano para el caso de una eventual quiebra del proveedor-.

11. SERVICIOS DE INTERNET / EXTRANET / INTRANET

11.1. El contenido y la estructura del sitio web de la organización deben basarse en un modelo aprobado por las autoridades, en el que estén documentados los siguientes aspectos: contenido y estructura del sitio web, fuentes de ingreso de datos, frecuencia de las actualizaciones, necesidades de disponibilidad del sitio, recursos afectados, responsable de los contenidos y todo otro dato atinente al contenido y funcionamiento del sitio.

11.2. Debe establecerse un acuerdo de nivel mínimo de servicios con los proveedores de los servicios de comunicaciones, a fin de asegurar que la prestación de los mismos se corresponda con los requerimientos de la organización.

12. MONITOREO DE LOS PROCESOS

12.1. Se deben definir indicadores de desempeño para monitorear la gestión y las excepciones de las actividades de TI.

12.2. La unidad de TI debe presentar informes periódicos de gestión a la dirección de la organización para que esta supervise el cumplimiento de los objetivos planteados.

13. AUDITORÍA INTERNA DE SISTEMAS

13.1. Las unidades de auditoría interna definidas en la ley 24.156, deben contemplar la ejecución de auditorías de sistemas, debiendo reunir los responsables de llevarlas a cabo, los requisitos de competencia técnica, independencia y autoridad para efectuar revisiones objetivas de los controles informáticos y preparar informes sobre sus hallazgos y recomendaciones.