SIGEN
Sindicatura General de la Nación
Presidencia de la Nación

NORMAS DE CONTROL INTERNO

PARA TECNOLOGÍA DE LA INFORMACIÓN

2021

IF-2021-106082452-APN-SNI#SIGEN

NORMAS DE CONTROL INTERNO
PARA TECNOLOGÍA DE LA INFORMACION

2021

NORMAS DE CONTROL INTERNO PARA TECNOLOGÍA DE LA INFORMACIÓN

SECTOR PÚBLICO NACIONAL

En el año 2005 la Sindicatura General de la Nación emitió las Normas de Control Interno para Tecnología de la Información –mediante la Resolución N°48 de ese año-, las cuales constituyeron un hito para el control de las áreas informáticas del Sector Público Nacional, induciendo desde ese momento, cambios organizativos y en la disciplina procedimental en base a las prácticas recomendadas en la materia. En ese sentido, las referidas Normas establecieron una guía de controles a ser instrumentados por los organismos del Poder Ejecutivo Nacional en cuanto a la gestión de la tecnología, que fueron y son utilizados como parámetro al momento de realizar las auditorías por parte de SIGEN, de las Unidades de Auditoría Interna y de organismos de control externo como la Auditoría General de la Nación.

Como contexto, es importante tener en cuenta que al entrar en la tercera década del Siglo XXI, la tecnología es uno de los ejes transformadores de la sociedad y de la gestión de las organizaciones, que se suman a otros cambios profundos en marcha en nuestra época, que van desde las crecientes preocupaciones por el cuidado del ambiente al rol de la mujer, entre otros. En particular, los cambios que se producen por la tecnología resultan muy profundos en todo el mundo y cubren un amplio abanico de elementos como -por ejemplo- el acelerado desarrollo de herramientas de ciencia de datos e inteligencia artificial (por ej. con algoritmos de análisis masivo de patrones de comportamiento), internet de las cosas (IoT), despliegues de tecnologías de red de 5ta. Generación – 5G, almacenamiento y procesamiento en la nube (cloud), avances en la robótica e internet satelital, criptomonedas, etc.

Por su parte, la pandemia Covid-19 ha puesto en consideración a nivel internacional, diversas cuestiones como el rol del Estado –particularmente ante situaciones de emergencia que pueden aumentar la desigualdad y la concentración de la riqueza. La pandemia ha acelerado, a su vez, el cambio tecnológico, volcando gran cantidad de actividades hacia una modalidad basada en la tecnología (teletrabajo, reuniones mediante herramientas de videollamada, cursos a distancia, etc.). Esto ha aparejado grandes desafíos para la gestión del Estado Nacional que ha debido enfrentar este período de grandes cambios, con capacidad de innovación y resiliencia, adaptando las herramientas, procedimientos y esquemas de trabajo a la nueva situación.

Todo esto, hace necesario subrayar la importancia del control sobre la gestión de la tecnología, particularmente en el ámbito del Sector Público, dada la importancia de sus funciones y servicios a la sociedad.

Los aspectos considerados, sumados a la experiencia recogida desde la emisión de las Normas de Control Interno para Tecnología de la Información de 2005, llevaron a la revisión y actualización de dichas normas, generándose durante 2020, un documento preliminar que fue puesto en consideración de especialistas y expertos en la materia –en diversas Unidades de Auditoría Interna y áreas informáticas del Estado Nacional, entre otros-, a quienes esta Sindicatura General de la Nación, agradece sus valiosos aportes.

En base a esos elementos, se ha elaborado un conjunto revisado y actualizado de las Normas de Control Interno para Tecnología de Información, en la que se especifican los objetivos de control y los riesgos que se busca cubrir a partir de cada control normado. Con esto, la Sindicatura General de la Nación, en su rol como Órgano Rector del Control Interno de los organismos del Sector Público Nacional, establece los controles que deben ser implementados en cuanto a la gestión de la tecnología de información, por los distintos organismos del Poder Ejecutivo Nacional, empresas del Estado o con participación estatal mayoritaria y Universidades Nacionales. De esta forma, y considerando la relevancia de la informática para la gestión, se propician mejoras en el control interno que repercutirán en mayor calidad en los servicios del Estado, y superiores elementos para la rendición de cuentas y transparencia.

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 (unidad de TI) que asegure la homogeneidad y unicidad de criterios y objetivos en la materia.
• Ante casos excepcionales en que esto no fuera factible –los que deben estar justificados formalmente por la máxima autoridad de la organización-, debe instrumentarse un Comité de TI o figura similar que se encargue de la coordinación de objetivos y lineamientos para inversiones en TICs, desarrollos, políticas y procedimientos, etc., asegurando que respondan a un criterio unificado.
• En aquellas organizaciones que manejen importantes volúmenes monetarios y/o gestionen información o infraestructuras de alta criticidad para el Estado Nacional, deberán asignarse las responsabilidades por la Seguridad de la Información a un área independiente de la unidad de TI, constituyendo de ese modo, un mecanismo de control por oposición.

Principales riesgos que buscan reducir estos controles:

• Dificultades para la delimitación de incumbencias y la correspondiente rendición de cuentas, lo que permite que los distintos sectores informáticos vean diluidas sus responsabilidades ante la ocurrencia de problemas.
• Falta de homogeneidad de criterios, por ejemplo, en la aplicación de métodos o técnicas de desarrollo o en la planificación estratégica de la tecnología de información.
• Compras informáticas de elementos que no contribuyen a una estrategia unificada, no compatibles entre sí, etc.
• Duplicación de esfuerzos en tareas informáticas, al existir diversos responsables, distintas áreas realizando tareas similares, o no existir la posibilidad de compartir conocimientos y recursos para el desarrollo de las tareas (módulos desarrollados, productos de software, utilitarios, bases comunes, etc.).
• En organizaciones que gestionan información de alta criticidad, si Seguridad de la Información depende de la unidad de TI pueden presentarse riesgos de conflictos de intereses.

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.

Principales riesgos que buscan reducir estos controles:

• Administración de prioridades no alineada con las necesidades y estrategia organizacional.
• Atención “preferencial” del área de TI a la gerencia usuaria de la cual depende.

1.3 [1]

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.

Principales riesgos que buscan reducir estos controles:

• Dificultades para exigir rendiciones de cuentas.
• Dificultades para el planeamiento, la ejecución y el control de las tareas.
• Dilución de responsabilidades.

[1] Relacionado con las Normas Generales de Control Interno (NGCI) Principio 3: Estructura, autoridad y responsabilidad.

De igual forma, en aquellas organizaciones que cuenten con el área de Seguridad de la Información, deben documentarse y aprobarse los puestos de trabajo, contemplando la autoridad y la responsabilidad, notificando formalmente al personal de sus deberes y responsabilidades.

1.4

La asignación de responsabilidades debe garantizar una adecuada separación de funciones, que fomente el control por oposición de intereses, propiciándose rotaciones periódicas de personal afectado a tareas críticas.

Principales riesgos que buscan reducir estos controles:

- Dificultades para detectar errores por falta de controles por oposición.
- Fraude o irregularidades por concentración de funciones.
- Dificultades para exigir rendiciones de cuentas.

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. Deben contemplarse medidas de concientización sobre la seguridad informática para todo el personal y para los usuarios de los servicios que brinda el organismo.

Principales riesgos que buscan reducir estos controles:

- Pobre aprovechamiento de recursos informáticos organizacionales.
- Falta de capacitación en tecnología por parte del personal (tanto técnicos del área de sistemas como usuarios finales).
- Por falta de actualización en materia tecnológica, la organización pierde valor en su capital humano, afectando por consiguiente, su capacidad innovadora y mecanismos para mantener los objetivos y métodos de trabajo acordes con las tecnologías informáticas vigentes.

2 > PLAN ESTRATÉGICO DE TI [2]

2.1

A partir de la definición que realicen las autoridades organizacionales respecto del nivel de soporte tecnológico que se brindará a la gestión de las actividades, 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, contemplando por su parte, el análisis pertinente de los riesgos en materia de gestión. Deben considerarse asimismo, los lineamientos estratégicos en materia de TI que se dicten desde el Gobierno Nacional.

Principales riesgos que buscan reducir estos controles:

- Descoordinación entre las acciones del área informática y la estrategia organizacional.
- Desequilibrio en el grado de informatización de las áreas: algunos sectores muy tecnificados, otros con escaso nivel de apoyo informático.
- Incorrecta administración de prioridades para los proyectos informáticos.
- Que se encaren proyectos informáticos no autorizados o que no cuenten con presupuesto.
- Que se encaren proyectos informáticos que no responden a la estratégia dispuesta por el Gobierno Nacional.

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.

Principales riesgos que buscan reducir estos controles:

- Retraso de la organización en la capacidad informática, lo que puede redundar en menor prestación de servicios, información de menor calidad para la toma de decisiones, etc.
- Obsolescencia del equipamiento tecnológico de la organización.

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.

Principales riesgos que busca reducir este control:

- Que se encaren proyectos informáticos no autorizados.
- Proyectos informáticos incorrectamente planificados, que no se basan en análisis de costos y beneficios.
- Proyectos informáticos no integrales o aislados.

[2] Relacionado con NGCI Principio 6: Especificación de los objetivos y Principio 11: Definición e implementación de controles sobre la tecnología.

2.4

El plan informático debe mantenerse actualizado.

Principales riesgos que busca reducir este control:

- Pérdida de validez del Plan original (dando lugar a los riesgos enunciados en 2.1).
- Dificultades para detectar oportunamente los desvíos en la ejecución del Plan y para requerir rendiciones de cuentas.

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.

Principales riesgos que busca reducir este control:

- Imposibilidad de llevar a cabo los proyectos informáticos planificados por no disponer de presupuesto.

2.6

La dirección de la organización debe controlar en forma periódica, el grado de avance del plan informático, a efectos de detectar y evitar desvíos en los plazos, costos y metas previstas.

Principales riesgos que busca reducir este control:

- Que la organización no obtenga oportunamente los resultados informáticos planificados.
- Mayores costos a los previstos
- Dificultades para detectar oportunamente los desvíos en la ejecución del Plan y para requerir rendiciones de cuentas.
- Proyectos informáticos que no se finalizan en los plazos previstos, o que no logran los objetivos planificados.

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.

Principales riesgos que buscan reducir estos controles:

- Que se realicen compras que no contribuyan con los proyectos incluidos en el plan informático aprobado, sino a otro tipo de objetivos que no cuentan con aprobación.
- Que se insuma el presupuesto para informática en proyectos sin autorización.
- Compras que no responden a la estrategia informática organizacional (incompatibles, no consistentes con otros productos existentes o que se prevé incorporar, etc.).

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, adoptando todas las medidas a su alcance para que estos se encuentren disponibles para su utilización, en concordancia con las necesidades operativas de las diferentes áreas usuarias en cuanto a oportunidad, integridad 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.

Principales riesgos que buscan reducir estos controles:

- Datos inconsistentes, redundantes, no accesibles, etc. por un erróneo diseño de las bases de datos.
- Información pobre para la toma de decisiones.
- Mayores costos y dificultades para el mantenimiento de sistemas y bases de datos o archivos de información.

4 > POLÍTICA DE SEGURIDAD [3] Y PROCEDIMIENTOS DE GESTIÓN DE LA TI

4.1

Se debe garantizar el cumplimiento de las normas establecidas en cuanto al deber de disponer de una política de seguridad de la información (Decisión Administrativa N° 641/2021 y normas complementarias o modificatorias, en base al estándar IRAM - ISO/IEC 27001, 27002 y 20000-1).

Todos los aspectos de la seguridad deben definirse considerando la clasificación de los recursos y la información, de modo de establecer un adecuado balance entre los controles y el recurso a proteger.

El requisito de disponer de una política de seguridad y adecuadas medidas de seguridad de la información (en base al estándar IRAM - ISO/IEC 27001, 27002 y 20000-1), alcanza a todos los organismos, empresas, universidades y demás entidades que conforman el Poder Ejecutivo Nacional.

Principales riesgos que buscan reducir estos controles:

- Dificultades o imposibilidad para acceder a información necesaria para las operaciones o para la toma de decisiones.
- Información no confiable (datos incorrectos, faltantes, sobrantes, inconsistentes, etc.)
- Acceso a la información organizacional por parte de personas no autorizadas.
- Interrupciones a las operaciones y/o servicios informáticos.
- Exposición de información confidencial.
- Pérdidas económicas.
- Pérdida de información organizacional.
- Dificultades para exigir rendiciones de cuentas
- Fraude o irregularidades.
- Dificultades para detectar errores por falta de controles por oposición.

4.2

La unidad de TI debe desarrollar, documentar, aprobar 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.

Las políticas y/o procedimientos que deben desarrollar, documentar, aprobar y comunicar –según corresponda en cada organismo-, abarcan entre otros:

- Gestión de inventario de recursos informáticos y licencias
- Propiedad y clasificación de la información
- Generación de backups y pruebas de recuperación.

Principales riesgos que buscan reducir estos controles:

- Falta de aplicación de procedimientos y controles uniformes.
- Dificultades para delimitar responsabilidades y exigir rendiciones de cuentas.
- Dependencia de determinado personal. Desconocimiento de la operatoria por parte del personal.
- Dificultades para capacitar nuevo personal.
- Uso ineficiente de tiempo y recursos.
- Errores o fallas en las actividades por la transmisión oral de las prácticas de trabajo.
- Por la informalidad, se presentan dificultades para comprobar si se ejecutaron o no tareas o controles dentro del proceso.
- Dificultades para encarar mejoras en los procesos (ya que no se cuenta con un esquema claro del cual partir).

[3] Relacionado con NGCI Principio 11: Definición e implementación de controles sobre la tecnología, Norma específica/objetivo de control 11.3: La seguridad de la información debe ser gestionada en todos los niveles organizacionales en base a una política y procedimientos específicos, que consideren las necesidades operativas y que apunten a alcanzar los siguientes objetivos para la información: Confidencialidad, Integridad y Disponibilidad.

- Tratamiento ante contingencias y para la continuidad operativa
- Gestión de incidentes.
- Atención de la mesa de ayuda/servicios informáticos
- Administración y control de Acceso a Sistemas y Aplicaciones (considerando vínculos de comunicaciones involucrados) –abarcando la gestión de altas, bajas y modificaciones sobre los permisos de acceso, gestión de usuarios críticos y de emergencia
- Control contra software malicioso
- Registro y revisión de registros de transacciones o logs
- Administración de la configuración de software de base, de comunicaciones y seguridad
- Administración de proyectos informáticos
- Accesos y medidas de control a la seguridad física sobre los recursos informáticos –en particular sobre aquellos considerados críticos-;
- Metodología de administración sitios web y redes sociales (responsabilidades por el ABM de contenidos, periodicidad de actualización, lineamientos de imagen, etc.)
- Trabajo remoto
- Procedimientos particulares según el caso (seguridad en dispositivos móviles, criptografía, seguridad y gestión de servicios y almacenamiento en la nube, etc.)

La elaboración de procedimientos deberá sujetarse a lo establecido en el art. 101 del Dec. 1344/2007, en cuanto a que se deberá pedir opinión previa favorable de la correspondiente Unidad de Auditoría Interna, la cual verificará los criterios de contenido y forma según la Res. SIGEN N°162/2014.

5 CUMPLIMIENTO DE REGULACIONES EXTERNAS

5.1

La unidad de TI debe garantizar el cumplimiento de las regulaciones relativas a protección de datos personales, propiedad intelectual del software, seguridad de la información, utilización de estándares, sistemas o plataformas definidas en Sector Público Nacional, acceso a la información pública, así como de las demás normas que resulten aplicables.

Principales riesgos que buscan reducir estos controles:

- Litigios, juicios, sanciones o sumarios por incumplimiento de normativa.
- Perjuicio económico para la organización.
- Uso ineficiente de los recursos públicos.

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, los cuales deben ser revisados periódicamente a fin de asegurar que se mantengan actualizados.

Principales riesgos que busca reducir este control:

- Inconvenientes para delimitar responsabilidades.
- Reclamos por parte de terceros hacia la organización.
- Baja calidad o bajo nivel de servicios por parte de la contraparte.
- Incumplimientos por parte de la contraparte, dificultades para realizar los reclamos pertinentes.
- Exposición de información de la Organización por parte de terceros con los que no se suscribió un adecuado acuerdo de confidencialidad o no divulgación.

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.

Principales riesgos que buscan reducir estos controles:

- Cada proyecto informático se gestiona de acuerdo a la capacidad del responsable, sin requisitos mínimos unificados. Resultados inciertos en cada caso.
- Responsabilidades no claras para las tareas dentro del proyecto.
- Se encaran proyectos no autorizados o sin presupuesto.
- Las recomendaciones de la UAI llegan una vez finalizado el proyecto (por no haber participado desde etapas tempranas).
- Proyectos informáticos que no son aprovechados por todas las áreas involucradas.
- Insuficiente planificación para los proyectos.

6.2

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

Principales riesgos que busca reducir este control:

- No se alcanzan las expectativas de las autoridades organizacionales por no cumplirse los objetivos del proyecto, por no cumplirse los plazos previstos y/o excederse en costos.
- Desvíos en la ejecución de proyectos informáticos que no se detectan, o se detectan tarde.
- Mayores costos.

7.1

La unidad de TI debe disponer de un procedimiento o metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas (incluyendo sus distintas modalidades: web, aplicaciones móviles, etc.), 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:

Principales riesgos que buscan reducir estos controles:

- Las tareas de desarrollo de sistemas se llevan a cabo de acuerdo al criterio y capacidad del responsable de turno.
- Dependencia del personal que desarrolla cada sistema.
- Inconvenientes para delimitar responsabilidades.

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.

Principales riesgos que buscan reducir estos controles:

- Se desarrollan sistemas que no satisfacen los requerimientos del usuario o que no fueron requeridos ni consensuados con ningún usuario.
- Cambios a programas que no fueron solicitados por el área usuaria del sistema.
- Conflictos entre el área de Sistemas y las Áreas.

7.1.2

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

Principales riesgos que buscan reducir estos controles:

- Se encaran desarrollos que no responden a la estrategia organizacional.
- Sistemas atiende primero los pedidos de las áreas “amigas”.
- Conflictos en la relación con las áreas porque todos solicitan sistemas “urgentes” y no está claro cómo deben ser administrados.

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

Principales riesgos que buscan reducir estos controles:

- Tratamiento de los cambios de emergencia de acuerdo al criterio y capacidad del responsable (puede obstaculizar su ejecución pidiendo formalidades y otros controles propios de cambios de rutina, o realizar los cambios sin ningún tipo de control o registraciones).
- Dificultades para reconstruir la situación previa en caso de fallas, o imposibilidad de determinar responsables.
- Cambios a programas o datos que no dejan rastros, son fraudulentos o encubren otras situaciones irregulares.

7.1.4

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

Principales riesgos que buscan reducir estos controles:

- Se desarrollan sistemas que no satisfacen los requerimientos del usuario.
- Conflictos entre el área de Sistemas y las Áreas.

7.1.5

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

Principales riesgos que buscan reducir estos controles:

- Se desarrollan sistemas que no incorporan controles suficientes, o bien no contemplan requerimientos del área de Auditoría como registros de transacciones o logs, alertas automáticas, etc.
- Las recomendaciones de la Auditoría Interna llegan con el sistema en funcionamiento, y obligan a reformular y modificar el sistema.

7.1.6

La utilización de estándares de diseño, programación y documentación.

Principales riesgos que buscan reducir estos controles:

- El diseño, programación o documentación del sistema se realiza de acuerdo al criterio, conocimientos y capacidad del responsable de turno. Pueden resultar inentendibles para otros agentes del área.
- Dependencia del personal de sistemas afectado a la labor.
- Dificultades para controlar y auditar el sistema.

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.

Principales riesgos que buscan reducir estos controles:

- Se implementan sistemas que no satisfacen los requerimientos del usuario.
- Se implementan sistemas que funcionan incorrectamente, arrojan errores o no responden a lo esperado.
- Se pierden o afectan datos de las bases de datos, por sistemas que funcionan erróneamente.

7.1.8

La apropiada segregación de ambientes y el pasaje del sistema aprobado desde el ambiente de desarrollo/prueba al de producción.

Principales riesgos que buscan reducir estos controles:

- Se implementan sistemas o versiones de programas fraudulentos, irregulares y/o que no se encuentran autorizados.
- Se agregan, borran o modifican datos de las bases de datos, por cambios a programas que no fueron probados y aprobados.

7.1.9

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

Principales riesgos que buscan reducir estos controles:

- Se pierde el registro y control sobre las versiones de los programas implementados, con lo que puede desconocerse sobre cuál versión deben realizarse las próximas modificaciones.
- Se implementa una versión de un programa que –si bien incluye el cambio requerido en esta oportunidad- no incluye arreglos que fueron realizados previamente.

7.1.10

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

Principales riesgos que buscan reducir estos controles:

- Dependencia del personal técnico que desarrolló el sistema (único que conoce los detalles de programación y diseño del sistema).
- Dificultades para efectuar el mantenimiento y actualización del sistema.
- Dificultades para capacitar usuarios para operar el sistema. Los procedimientos se transmiten solo oralmente, con el consiguiente riesgo de errores, olvidos, etc.
- Dificultades para integrar nuevo personal técnico al equipo de trabajo.

7.1.11

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

Principales riesgos que buscan reducir estos controles:

- Usuarios no capacitados para operar el sistema, que cometen errores o no lo pueden aprovechar al máximo.
- Personal técnico encargado de funciones de desarrollo, que no se actualiza, no conoce nuevas técnicas de diseño, programación, lenguajes, etc.

7.1.12

El criterio a seguir según envergadura, características e interacciones con terceros del sistema, para el registro de la propiedad intelectual del sistema a favor del Estado Nacional, así como los pasos a seguir para dicho registro.

Principales riesgos que buscan reducir estos controles:

- Reclamos o pérdidas económicas por la falta de registro oportuno de la propiedad del sistema en caso de acceso y registro por parte de un tercero o un agente no autorizado.

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, incluyendo aspectos relativos a la seguridad de los desarrollos. 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.

Principales riesgos que buscan reducir estos controles:

- Dependencia de terceros para el uso de un sistema organizacional.
- Compras informáticas de elementos que no contribuyen a una estrategia unificada, no compatibles entre sí, etc.
- Duplicación de esfuerzos en tareas informáticas, al existir diversos responsables, distintas áreas realizando tareas similares, o no existir la posibilidad de compartir conocimientos y recursos para el desarrollo de las tareas (módulos desarrollados, productos de software, utilitarios, bases comunes, etc.).
- Sistemas que funcionan incorrectamente o presentan debilidades de control.
- La información que produce el sistema no resulta confiable.
- Litigios, reclamos económicos con terceros.
- Aceptación de sistemas provistos por terceros que no cumplen lo requerido por la organización o no responden a lo que se contrató

7.3 [4]

En el desarrollo de sistemas debe procurarse incluir controles automatizados que contribuyan a reducir los riesgos que puedan afectar el logro de los objetivos, debiendo contemplarse particularmente controles de:

- Integridad: debe asegurarse el tratamiento, procesamiento y registro de la totalidad de las transacciones u operaciones.
- Exactitud: debe asegurarse la registración oportuna y correcta de las operaciones.
- Validez: las transacciones registradas deben representar con precisión las operaciones ejecutadas, considerando los procedimientos establecidos.

Principales riesgos que buscan reducir estos controles:

- Sistemas que funcionan incorrectamente o presentan debilidades de control.
- La información que produce el sistema no resulta confiable.
- Errores en los controles manuales.
- Pérdidas de tiempo por no contar con controles automatizados.

7.4

El desarrollo de sistemas, particularmente en el caso de sistemas que contengan algoritmos de análisis masivos de datos (inteligencia artificial, análisis de patrones, ubicación geográfica, datos de salud, etc.), debe contemplar reglas éticas de diseño y funcionamiento, que aseguren la apropiada protección de los derechos de los ciudadanos.

[4] Relacionado con NGCI Principio 10: Definición e implementación de actividades de control.

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, y deben estar debidamente justificadas, documentadas y respaldadas por el análisis de costo/beneficio y la evaluación de riesgos pertinentes. Se debe garantizar el cumplimiento de la normativa de contrataciones aplicable.

Las adquisiciones deben responder a los proyectos contemplados en el Plan estratégico y operativo informático, debiendo las excepciones, encontrarse justificadas y autorizadas por los niveles pertinentes.[5]

Principales riesgos que buscan reducir estos controles:

- Sanciones y/o inconvenientes por incumplimiento de la normativa.
- Adquisiciones que no respetan los estándares vigentes en la Administración Pública o que no responden a la estrategia informática organizacional (incompatibles, no consistentes con otros productos existentes o que se prevé incorporar, etc.).
- Adquisiciones informáticas incorrectamente planificadas, que no se basan en análisis de costos y beneficios.
- Que la organización no obtenga oportunamente los resultados informáticos planificados.
- Mayores costos a los previstos
- Que se realicen compras que no contribuyan con los proyectos incluidos en el plan informático aprobado, sino a otro tipo de objetivos que no cuentan con aprobación.
- Que se insuma el presupuesto para informática en compras sin autorización.

8.2

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

Principales riesgos que buscan reducir estos controles:

- Pagos a proveedores de equipamiento sin verificar la entrega de todos los productos comprometidos.
- Incorporación de productos informáticos fallados o que no responden a lo contratado.

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.

Principales riesgos que buscan reducir estos controles:

- Fallas en el equipamiento o dispositivos de hardware.
- Interrupciones en operaciones –a mayor o menor escala- por fallas en el equipamiento (Ej. deja de funcionar un servidor relevante, o inconvenientes porque falla una impresora de menor relevancia).

[5] Tener en cuenta punto 2. PLAN ESTRATÉGICO DE TI

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.

Principales riesgos que buscan reducir estos controles:

- Litigios, reclamos económicos, conflictos con terceros.
- Instalación y/o utilización de software no autorizado y/o que no responde a los objetivos organizacionales (software de oficina sin licencia, software para otros fines como juegos, etc.). Esto acarrea riesgos de virus informáticos o la inclusión de debilidades en la seguridad informática.
- Dificultades para planificar actualizaciones de productos de software.
- Sanciones y/o inconvenientes por incumplimiento de normas aplicables.
- Dificultades para obtener el inventario de licencias de software adquiridas por la Organización, y para su adecuado registro patrimonial y contable.

8.5

Las bajas de equipamiento y Residuos de Aparatos Eléctricos y Electrónicos (RAEES) deben enmarcarse en criterios preestablecidos considerando el borrado seguro de datos y la política ambiental organizacional –de corresponder- los mecanismos aplicables de gestión de residuos que puedan afectar el ambiente.

Principales riesgos que buscan reducir estos controles:

- Exposición no autorizada de información organizacional.
- Afectación negativa del ambiente.

9 SERVICIOS DE PROCESAMIENTO, SOPORTE Y/O ALMACENAMIENTO PRESTADOS POR TERCEROS

9.1

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.

Principales riesgos que buscan reducir estos controles:

- Contrataciones innecesarias o que no responden a una relación de costo - beneficio adecuada.
- Dependencia de terceros, exposición de información de la organización, etc. por la falta de análisis de riesgos.

9.2

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, incluyendo los aspectos de confidencialidad y soberanía sobre los datos, de ser aplicables. Tales procedimientos deben asegurar el cumplimiento de la normativa para las Contrataciones aplicables.

Principales riesgos que buscan reducir estos controles:

- Incumplimiento por parte del proveedor, baja calidad de los servicios recibidos.
- Litigios o conflictos, dificultades para determinar responsabilidades.
- Sanciones por incumplimientos normativos.

9.3

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.

Principales riesgos que buscan reducir estos controles:

- Interrupciones a los servicios contratados, fallas en la seguridad informática (corrupción de datos, información no confiable, accesos no autorizados, etc.)
- Incumplimiento por parte del proveedor, baja calidad de los servicios recibidos.
- Exposición no autorizada de la información de la organización.

9.4

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

Principales riesgos que buscan reducir estos controles:

- Pérdidas / perjuicio económico para la organización por pagos a proveedores que no prestan adecuadamente el servicio.
- Incumplimiento por parte del proveedor, baja calidad de los servicios recibidos. Interrupciones o inconvenientes en las operaciones informáticas de la organización.
- Dificultades para detectar desvíos o incumplimientos de terceros.

9.5

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-, o bien estableciendo otro mecanismo de contingencia para la continuidad operativa.

En caso de tratarse de algún tipo de procesamiento o almacenamiento en la "nube", debe constar la autorización formal correspondiente, incluyendo el análisis de riesgos y beneficios (considerando la criticidad de la información en cuestión, la posible exposición de la misma a terceros, los costos asociados, las implicancias en cuanto a disponibilidad y agilidad, la modalidad que se utilizará para asegurar la eliminación de los datos una vez que sea necesario, etc.). La información tratada en estos casos debe estar formalmente clasificada, en base a los criterios definidos en la Política de Seguridad de la Información.

Principales riesgos que buscan reducir estos controles:

- Interrupciones a las operaciones organizacionales.
- Dependencia de terceros.
- Exposición de información del Estado Nacional.

10 PUBLICACIÓN DE INFORMACIÓN DIGITAL

10.1

Deben asignarse formalmente las responsabilidades por la publicación de contenidos en medios digitales (sitios web institucionales, redes sociales organizacionales, etc.), debiendo seguir, dichas publicaciones, los criterios aprobados por las autoridades.

Principales riesgos que buscan reducir estos controles:

- Publicación de información no autorizada, incorrecta, no actualizada, contradictoria, inconsistente, etc.
- Impacto negativo en la imagen pública de la organización por incorrecto funcionamiento del sitio Web, o problemas en la información publicada. Sanciones, inconvenientes o litigios.

10.2

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.

Principales riesgos que buscan reducir estos controles:

- Interrupciones en los servicios de comunicaciones, o baja calidad de los servicios. Incumplimiento por parte del proveedor.
- Dificultades para detectar desvíos o incumplimientos, o para delimitar responsabilidades.

11 MONITOREO DE ACTIVIDADES DE TI [6]

11.1

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

Principales riesgos que buscan reducir este control:

- Los sectores dentro del área no responden adecuadamente a las tareas asignadas o planificadas. Trabajo descoordinado entre sectores.
- Aprovechamiento ineficiente de los recursos.
- Existencia de riesgos no administrados en la gestión informática.
- Los desvíos en la ejecución de tareas no se detectan, o se detectan en forma inoportuna.
- Gestión informática ineficaz o ineficiente.

11.2

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. De igual forma, deben elevarse reportes periódicos sobre la situación de la seguridad de la información.

Principales riesgos que buscan reducir estos controles:

- Inadecuada gestión de prioridades para los proyectos informáticos
- Mayores costos o plazos respecto a lo previsto.
- Descoordinación entre las actividades informáticas y la estrategia organizacional.
- Dificultades para detectar y corregir desvíos en la ejecución de proyectos informáticos.

[6] Relacionado con NGCI Principio 2 Responsabilidades de supervisión: Norma específica u Objetivo de Control: 2.2. Las autoridades superiores deben propiciar la generación de información de gestión precisa y confiable, con indicadores y reportes completos y oportunos, de modo de poder realizar la supervisión de la gestión monitoreando el grado de cumplimiento de los objetivos.

12.1

Las unidades de auditoría interna definidas en la ley 24.156, deben ejecutar auditorías de sistemas con una periodicidad acorde al nivel de informatización organizacional, 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.

Principales riesgos que buscan reducir este control:

- La autoridad no obtiene información independiente sobre el control interno de la tecnología y sistemas informáticos que funcionan en la organización (los cuales cada vez abarcan más procesos organizacionales).
- "Sensación" de impunidad por parte del personal de sistemas, porque "nadie audita".

República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Hoja Adicional de Firmas
Anexo

Número: IF-2021-106082452-APN-SNI#SIGEN

CIUDAD DE BUENOS AIRES
Miércoles 3 de Noviembre de 2021

Referencia: NORMAS DE CONTROL INTERNO PARA TECNOLOGÍA DE LA INFORMACIÓN

El documento fue importado por el sistema GEDO con un total de 25 pagina/s.

Digitally signed by KUNSTLER Horacio Ubaldo
Date: 2021.11.03 11:52:29 ART
Location: Ciudad Autónoma de Buenos Aires

Horacio Ubaldo KUNSTLER
Secretario
Secretaría de Normativa e Innovación
Sindicatura General De La Nación

Digitally signed by Gestion Documental Electronica
Date: 2021.11.03 11:52:45 -03:00