INFORME DE AUDITORÍA INTERNA Nº 13/2022

EVALUACIÓN DE LA GESTION DE TECNOLOGÍA INFORMÁTICA Y SISTEMAS DE INFORMACIÓN (RESOL-2022-87-APN-SIGEN)

INFORME EJECUTIVO

Objeto

Revisión del cumplimiento de los aspectos contemplados en la RESOL-2022-87-APN-SIGEN que establece las Normas de Control Interno para Tecnología de la Información – Sector Público Nacional, en particular los aspectos vinculados con la organización, las políticas y procedimientos y el desarrollo, mantenimiento o adquisición de software de aplicación.

Alcance

Las tareas de auditoría se llevaron a cabo entre los meses de octubre y diciembre del corriente año.

El examen se realizó de acuerdo con las Normas de Auditoría Interna Gubernamental, aprobadas por Resolución SIGEN N° 152/2002, y los lineamientos fijados en el "Manual de Control Interno Gubernamental" aprobado por Resolución SIGEN N° 03/2011.

No existieron limitaciones al alcance en el presente informe de auditoría.

Observaciones

Políticas y Procedimientos

Observación N° 1: Ausencia de un Plan para afrontar Contingencias. (Observación recurrente Informe de Auditoría SIGEN N° 248/2003).

Impacto: Medio

Recomendación: Desarrollar un plan para afrontar contingencias, para lo cual se sugiere determinar, para cada sistema de información, el tiempo aceptable de recuperación ante una eventual interrupción y elaborar el plan sobre esa base. Deben especificarse los recursos necesarios y los responsables de llevar a cabo las tareas, a efectos de asegurar la continuidad de procesamiento de los sistemas críticos.

Observación N° 2: • Política de Seguridad de la Información: falta de definición de Política de Seguridad. (Observación recurrente Informe de Auditoría UAI N° 08/2016)

Impacto: Alto

Recomendación: 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.

Observación N° 3: El área no cuenta con un Manual de Procedimientos formalmente aprobado. El mismo debe especificar las tareas y controles a realizar en los distintos procesos, así como los responsables de su ejecución. En los procedimientos se deben contemplar: gestión de inventarios de recursos informáticos y licencias, generación de backups y pruebas de recuperación, tratamiento ante contingencias y continuidad operativa, soporte, administración y control de acceso a sistemas y/o aplicaciones, registro y revisión de transacciones, administración de proyectos informáticos, accesos y controles a la seguridad física sobre los recursos y control contra software malicioso.

Impacto: Medio

Recomendación: Desarrollar, aprobar e implementar los procedimientos relacionados con las actividades de la Dirección de Tecnología y Sistemas de Información. Los mismos 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.

Administración de Proyectos – Desarrollo y Mantenimiento de Software

Observación N° 4: No hay un marco formal de administración de proyectos ni de procesos de monitoreo de sus plazos y costos. No se da participación formal a los usuarios en su mayoría externos al Organismo. No existe una normativa formal para el desarrollo y mantenimiento de software. No hay una política de costos, ni normas para asegurar la calidad. (Observación recurrente Informe AGN N° 01/2009)

Impacto: Alto

Recomendación: Se debe establecer un marco de administración de proyectos que debe contemplar, como mínimo, la asignación de responsabilidades, división de tareas, presupuestación del tiempo y los recursos, plazos, puntos de verificación y aprobaciones. La presidencia y el departamento de TI deben garantizar que: - se aplique un marco de administración de proyectos, - se contemple la participación del departamento de usuarios en el inicio del proyecto, - se asignen miembros y responsabilidades del equipo del proyecto, - exista una definición del proyecto, - se aprueben las fases del proyecto, - exista un plan maestro del proyecto, - se defina un plan de garantía de calidad del sistema, - se implemente la administración formal de riesgos del proyecto, - se elabore un plan de pruebas, - se elabore un plan de capacitación, - se desarrolle un plan de revisión posterior a la implementación.

Continuidad de las Operaciones – Evaluación de Riesgo

Observación N° 5: El área de sistemas se encuentra dividida en dos sectores, uno se ocupa de la red local y el otro específicamente del SINTRA. Para la red local no se encontró un **plan de continuidad de los servicios de información**; para el SINTRA existe dentro del Documento Principal del sistema (Anexo I, punto 9) un **plan de contingencia** en el cual se enumeran las posibles causas, escenarios y procedimientos a seguir en cada caso, pero no se asignan prioridades para su recuperación y restablecimiento. Se realizó originalmente una evaluación de riesgos para el SINTRA, pero no se determinó el nivel aceptable ni está definido un procedimiento para disminuirlos o indicar cuáles son admisibles y de qué manera se solucionará el problema en caso de que se presente. No existen políticas, planes o procedimientos que incluyan capacitación o concientización de los roles individuales o grupales para asegurar la continuidad. **(Observación N° 21 recurrente Informe AGN N° 01/2009)**

Impacto: Medio

Recomendación: Se debe crear un marco de continuidad que defina los roles, las responsabilidades, el enfoque y las normas y estructuras para documentar un plan de contingencia que garantice el servicio continuo La presidencia y el departamento de TI deben garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI: - un marco de continuidad de TI, - definir estrategias y filosofía del plan de continuidad de TI, - establecer contenido del plan de continuidad de TI, - reducción de los requerimientos de continuidad de TI, - mantenimiento del plan de continuidad de TI, - realizar la prueba del plan de continuidad de TI, - capacitación en el plan de continuidad de TI, - distribución del plan de continuidad de TI, - resguardo de la posibilidad de procesamiento alternativo para el usuario, - identificar recursos críticos de TI, - definir el sitio y equipamiento alternativos, - almacenamiento de resguardo en sitio alternativo, - reevaluación periódica del plan.

Observación N° 6: No existen procedimientos formalmente definidos de administración de problemas. Si bien se confeccionan partes de trabajo no existe un control sistemático. No se realizan estadísticas de ninguna clase. **(Observación N° 27 recurrente Informe AGN N° 01/2009)**

Impacto: Alto

Recomendación: El departamento de TI debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI: - sistema de administración de problemas, - escalamiento de problemas, - seguimiento de problemas y pistas de auditoría, - autorizaciones de emergencia y acceso temporario, - establecer las prioridades de procesamiento de emergencia.

Cambios a programas

Observación N° 7: Los cambios a los programas de trabajo no son estrictamente controlados. No existe un procedimiento formal de aceptación de nuevos programas de tareas, incluyendo la documentación presentada (…). **(Observación N° 30 recurrente Informe AGN N° 01/2009)**

Impacto: Medio

Recomendación: Resulta necesario tener documentado de manera correcta la formulación y documentación de los requerimientos por parte de las áreas usuarias, el criterio de establecimiento de las prioridades, la aprobación por parte de las áreas usuarias, la participación de la Unidad de Auditoría Interna durante el desarrollo, la realización de pruebas y la etapa de implementación, para evitar cambios a programas que no satisfacen el área usuaria, conflictos entre áreas, sistemas que no incorporan suficientes controles, entre otros..

Desarrollo, mantenimiento y adquisición de software

Observación N° 8: • Desarrollo, mantenimiento o adquisición de Software de Aplicación: el área se encuentra trabajando en el proyecto del Manual de Organización, Políticas y Procedimientos de la Dirección de Sistemas. **(Observación N° 6 recurrente Informe UAI N° 08/2016)**

Impacto: Medio

Recomendación: 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 de administración de proyectos, el que debe incluir la etapa de formulación y documentación de requerimientos, criterios para establecer prioridades entre los requerimientos, aprobación por parte de las áreas usuarios, participación de la Unidad de Auditoría Interna, documentación de las etapas de prueba e implementación, control de versiones, documentación de soporte para personal de técnico y usuarios y la etapa de capacitación.

Conclusiones

Sobre la base de las tareas realizadas detalladas en el punto 2.3. Verificaciones y Hallazgos y con el alcance descripto en el punto 1.2., se concluye que en cuanto al cumplimiento de los aspectos contemplados en la RESOL-2022-87-APN- SIGEN Normas de Control Interno para Tecnología de la Información, en particular los aspectos vinculados con la organización, las políticas y procedimientos y el desarrollo, mantenimiento o adquisición de software de aplicación, la Dirección de Tecnología y Sistemas de Información cumple con salvedades, y se encuentra realizando las acciones tendientes a subsanar y corregir las situaciones descriptas en los puntos 2.3 y 2.4.

No obstante, esta UAI considera que, para mejorar el ambiente de control, la evaluación de riesgos y las actividades de control, dentro de los controles y de la propia operatoria de la Dirección de Tecnología y Sistemas de Información, existen puntos que requieren ser atendidos.

Si bien se evidencia un avance con el desarrollo de los manuales de procedimientos y políticas de seguridad informática, estos requieren ser aprobados formalmente y en el marco de la normativa vigente.

Adicionalmente resulta necesario la elaboración de un plan para afrontar contingencias y un plan de capacitación en materia de TI para el personal del organismo, y los usuarios externos.

Es importante destacar que la UAI y la DTySI se reúnen de manera regular con el objetivo de darle tratamiento a las observaciones pendientes de regularización originadas en los distintos informes de auditoría emitidos por los órganos de control, definiendo un plan de trabajo que permite darle un seguimiento a las acciones encaradas, fortaleciendo las actividades de supervisión de manera conjunta, lo cual pone de manifiesto un compromiso por parte del área auditada respecto al interés por el fortalecimiento del ambiente y de las actividades de control.

Finalmente es necesario el desarrollo de una Política de Seguridad de la Información, en la que participen todas las áreas del organismo.

Ciudad de Buenos Aires, 22 de diciembre de 2022.

KOMAID VAN GELDEREN Jose Alberto

Firmado digitalmente por KOMAID VAN GELDEREN Jose Alberto
Fecha: 2022.12.28 16:56:27 -03'00'