SESIONES ORDINARIAS

2011

ORDEN DEL DÍA Nº 2638

COMISIÓN PARLAMENTARIA MIXTA REVISORA DE CUENTAS

Impreso el día 20 de octubre de 2011

Término del artículo 113: 31 de octubre de 2011

SUMARIO: Pedido de informes al Poder Ejecutivo sobre las medidas adoptadas a los efectos de regularizar las situaciones observadas por la Auditoría General de la Nación en ocasión de la evaluación de gestión de la tecnología de la información, en el Instituto Nacional Central Único Coordinador de Ablación e Implante (INCUCAI), y otras cuestiones conexas.

1. (4.885-D.-2011.)

2. (192-O.V.-2009.)

I. **Dictamen de mayoría.**

II. **Dictamen de minoría.**

I

Dictamen de mayoría

Honorable Cámara:

Vuestra Comisión Parlamentaria Mixta Revisora de Cuentas ha considerado el expediente Oficiales Varios O.V. 192/09, mediante el cual la Auditoría General de la Nación remite resolución 133/09 aprobando el informe de auditoría referido a "evaluar la gestión de la tecnología de la información (TI) en el Instituto Nacional Central Único Coordinador de Ablación e Implante (Incucai), organismo descentralizado en la órbita del Ministerio de Salud, para determinar debilidades y fortalezas de la administración de la información; y, por las razones expuestas en sus fundamentos, os aconseja la aprobación del siguiente

Proyecto de resolución

La Cámara de Diputados de la Nación

RESUELVE:

1) Dirigirse al Poder Ejecutivo nacional, solicitándole informe sobre las medidas adoptadas para: a) regularizar las situaciones observadas por la Auditoría General de la Nación, en ocasión de la evaluación de gestión de la tecnología de la información, en el Instituto Nacional Central Único Coordinador de Ablación e Implante (Incucai), b) determinar y efectivizar las responsabilidades que pudieran haber emergido de las aludidas situaciones.

2) Comuníquese al Poder Ejecutivo nacional y a la Auditoría General de la Nación, juntamente con sus fundamentos.

De acuerdo con las disposiciones pertinentes, el presente dictamen pasa directamente al orden del día.

Sala de la comisión, 30 de junio de 2011.

Heriberto A. Martínez Oddone. – Luis A. Juez. – Gerardo R. Morales. – Juan C. Romero. – Ernesto R. Sanz. – Juan C. Morán. – Walter A. Agosto.

II

Dictamen de minoría

Honorable Cámara:

Vuestra Comisión Parlamentaria Mixta Revisora de Cuentas ha considerado el expediente Oficiales Varios O.V. 192/09, mediante el cual la Auditoría General de la Nación remite resolución 133/09 aprobando el informe de auditoría referido a evaluar la gestión de la tecnología de la información (TI) en el Instituto Nacional Central Único Coordinador de Ablación e Implante (Incucai), organismo descentralizado en la órbita del Ministerio de Salud, para determinar debilidades y fortalezas de la administración de la información; y, por las razones expuestas en sus fundamentos, os aconseja la aprobación del siguiente

Proyecto de resolución

La Cámara de Diputados de la Nación

RESUELVE:

1) Dirigirse al Poder Ejecutivo nacional, solicitándole informe sobre las medidas adoptadas para regularizar las situaciones observadas por la Auditoría General de la Nación, en ocasión de la evaluación de gestión de la tecnología de la información, en el Instituto Nacional Central Único Coordinador de Ablación e Implante (Incucai).

2) Comuníquese al Poder Ejecutivo nacional y a la Auditoría General de la Nación, juntamente con sus fundamentos.

De acuerdo con las disposiciones pertinentes, el presente dictamen pasa directamente al orden del día.

Sala de la comisión, 30 de junio de 2011.

Nicolás A. Fernández.

FUNDAMENTOS

La Auditoría General de la Nación (AGN) procedió a evaluar la gestión de la tecnología de la información (TI) en el Instituto Nacional Central Único Coordinador de Ablación e Implante (Incucai) con el fin de determinar debilidades y fortalezas de la administración de la información.

Las tareas de campo se desarrollaron entre los meses de febrero y abril del año 2009.

La AGN resolvió otorgar el carácter de reservado al Anexo VI del presente informe por tratarse de información relacionada con el área de sistemas, cuya difusión podría llegar a comprometer la seguridad informática del organismo auditado.

Los auditores señalan que no pudieron analizar la calidad de los datos almacenados en las bases de datos a fin de conocer de manera indirecta el funcionamiento del sistema de información nacional sobre trasplantes, siendo consecuencia de la entrega de datos incompletos por parte del Incucai.

Asimismo, el órgano de control formula comentarios y observaciones que se detallan a continuación:

Su análisis se ha basado en la verificación de los objetivos de control establecidos por las normas COBIT (Control Objectives in Information Technologies), destacando el nivel de madurez correspondiente según el modelo de madurez de la capacidad y su consecuente nivel de riesgo implícito.

I. Planificación y organización

Definición de un plan estratégico de TI: sólo existe la planificación a un año tanto para el organismo como para TI, realizada sin metodología formal.

Definición de la arquitectura de la información: existe conciencia de la importancia de la arquitectura de la información, pero no se avanzó en el tema, no se ha definido el sector responsable ni se crearon sus misiones y funciones; no existe un modelo al respecto ni políticas y procedimientos al efecto.

Determinación de la dirección tecnológica: se tiene conciencia de la importancia que la planificación de infraestructura tecnológica reviste para el organismo pero no se ha definido formalmente un área para determinar la dirección tecnológica. A la fecha, no existe normativa formal para la función.

Definición de la organización y las relaciones de TI: no existe el comité de planificación de la función servicios de información, ni su estructura con misiones y funciones formalizadas.

Administración de la inversión en tecnología de información: no existe en el organismo una política formal ni un procedimiento de formulación presupuestaria que garanticen el establecimiento de un presupuesto operativo anual y su aprobación. Tampoco existen los planes estratégicos del organismo y de TI. No se hace un seguimiento o monitoreo de las inversiones y los gastos de TI.

Comunicación de los objetivos y directivas de la gerencia: no hay: a) políticas formales que impongan un comportamiento de los funcionarios vinculado a la ética, b) áreas responsables de la formulación de políticas y procedimientos, c) un marco de referencia y un proceso de revisión periódica de estándares, políticas, directrices y procedimientos, d) una política de calidad ni de minimización de riesgos, e) sanciones disciplinarias definidas para la falta de cumplimiento de las políticas de seguridad y control interno.

Administración de los recursos humanos: los roles y responsabilidades de las distintas funciones del área informática no están formalmente definidos. No existe una dotación de personal suficiente y sólo el jefe del área es de planta permanente. No existe una política formal de reclutamiento y promoción. No hay un proceso adecuado de evaluación de desempeño del personal que ocupa los cargos del área informática.

Garantía del cumplimiento de los requisitos externos: no existen políticas y procedimientos formales para: a) garantizar que se adopten en forma oportuna las medidas correctivas para evaluar los requisitos externos, b) diseñar los resguardos y objetivos de seguridad e higiene, c) garantizar el cumplimiento de las exigencias de los contratos de seguros.

Evaluación de riesgos: no existe un marco formal de identificación y evaluación de riesgos.

Administración de proyectos: 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.

Administración de la calidad: no se aplican criterios de calidad y no existe metodología formal del ciclo de vida del desarrollo y mantenimiento de sistemas.

II. Administración e implementación

Identificación de soluciones automatizadas: el organismo no posee políticas y procedimientos para identificar requerimientos funcionales y operativos para el desarrollo, implementar y modificar las soluciones de sistemas. No se obtuvo evidencia de políticas definidas que satisfagan los requerimientos de desempeño, confiabilidad, compatibilidad y legislación. No existen políticas para la identificación de alternativas a las soluciones de tecnología ni de la evaluación de la tercerización de desarrollos de software en comparación con los desarrollos propios.

Adquisición y mantenimiento del software de aplicación: no existe una metodología para el desarrollo y mantenimiento de sistemas para la organización.

Adquisición y mantenimiento de la infraestructura tecnológica: la organización no ha elaborado un plan de adquisición y mantenimiento de la infraestructura tecnológica que permita asegurar que la configuración, la instalación y el mantenimiento del software de base no pongan en peligro los datos y programas que se almacenan. No existe un manual de procedimientos para las contrataciones informáticas. No existen políticas ni procedimientos relacionados con: a) análisis de impacto de la incorporación del hardware y el software nuevos, b) análisis de integración entre distintas plataformas, c) análisis de tercerización con aprovechamiento de infraestructura interna o externa, d) el manejo de casos en los que se depende de un proveedor de única fuente, e) el mantenimiento preventivo del hardware.

Desarrollo y mantenimiento de procedimientos: no existe un marco estándar, definido y monitoreado, para la documentación y los procedimientos. No se evalúan los requerimientos operativos tomando como base los datos históricos. No se definen ni planifican los requerimientos operativos, ni los niveles de servicio ni las expectativas de desempeño.

Instalación y acreditación de aplicativos: se carece totalmente de procesos formales de instalación y acreditación. No se han separado los entornos de desarrollo, pruebas y producción. No hay mecanismos de aprobación formal de las pruebas por parte de los usuarios involucrados que permitan poner a disposición los aplicativos para el pasaje a producción. No se hace gestión de aseguramiento de la calidad de las aplicaciones a instalar, previa a la etapa de pruebas por parte del usuario involucrado.

Administración de cambios: no se han establecido procedimientos formales para administrar cambios de manera estándar para todas las solicitudes de cambio.

III. Entrega y soporte

Definición y administración de los niveles de servicio: no existe una política que promueva la definición de acuerdos de nivel de servicios. Ni existen acciones que promuevan la participación de los usuarios en su definición. No hay documentación que defina la responsabilidad de los usuarios. La responsabilidad de los proveedores está definida caso por caso, sin una política general en los contratos.

Administración de servicios prestados por terceros: no existen políticas formalmente definidas referidas a las relaciones con terceros. El organismo realiza las adquisiciones cumpliendo con la Ley de Compras del Estado y las recomendaciones de la ONTI en las compras de elementos informáticos. No se encontró evidencia de un manual de compras propio del organismo. No se encontró en las órdenes de compra analizadas documentación que defina la relación entre contratistas y subcontratistas.

Administración de la capacidad y el desempeño: el equipamiento informático del organismo está acorde con sus necesidades, los servidores y las PC de escritorio están actualizados, pero la definición de sus características no resultó de un análisis estandarizado de capacidades y procesamiento. No se realizan tareas de evaluación sobre la capacidad y desempeño en forma sistemática. No existen plazos ni niveles de servicio definidos para los servicios prestados por el área de sistemas. No se pide información a los usuarios para establecer plazos o definiciones de servicios. No se realizan informes de desempeño, se hace un control informal del mismo. No se utilizan herramientas específicas para monitorear el desempeño.

Garantía de un servicio continuo: el área de sistemas se encuentra dividida en dos sectores, uno se ocupa de la red local y el otro específicamente del Sistema Nacional de Información sobre Trasplantes (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.

Garantía de la seguridad de los sistemas: la red interna del organismo carece de bloqueos en su acceso a Internet. Tiene permitidos la navegación sin restricciones y el acceso a programas de mensajería instantánea. No se realizan reportes o informes de seguridad. Se monitorea pero no en forma sistemática. La política de contraseñas incluye su cambio al primer uso y debe tener como mínimo 8 caracteres. Después de 5 intentos fallidos la cuenta se bloquea. No se muestra al usuario

la fecha y hora del último acceso. El tiempo de inactividad está limitado a 15 minutos, pasado ese tiempo el usuario debe volver a identificarse. El acceso de los usuarios del SINTRA utiliza un protocolo de seguridad para la autenticación de usuarios.

Identificación e imputación de costos: si bien se reconoce la importancia de llevar los costos, no se realizan informes ni se hace imputación por centro de costos.

Educación y capacitación de los usuarios: no existen políticas y procedimientos referentes a la concientización permanente en seguridad de la información. Años anteriores se realizaron cursos sobre seguridad, pero no fueron realizados en 2008 y no tienen fecha de realización para 2009. Los cursos realizados no fueron obligatorios para todo el personal. No hay políticas ni procedimientos referidos a la capacitación del personal de sistemas.

Asistencia y asesoramiento a los usuarios de tecnología de la información: el proceso de asistencia y asesoramiento a usuarios no está definido. Existe superposición de funciones entre la Dirección Científico Técnica y el área de sistemas en cuanto a la función de mesa de ayuda del SINTRA. No está definida formalmente una única función de mesa de ayuda. No existe un sistema informatizado que registre las consultas para permitir una rápida identificación de los problemas comunes y establecer tendencias. No hay encuestas de satisfacción de usuarios.

Administración de la configuración: no se encontró evidencia de la existencia de procedimientos de administración de la configuración ni procedimientos de mantenimiento de inventarios de hardware y software.

Administración de problemas e incidentes: 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.

Administración de datos: la carga inicial de los datos no es responsabilidad del organismo sino de los otros actores del proceso de trasplantes, como ser los equipos médicos y los organismos de trasplantes jurisdiccionales. El control de los documentos fuentes está asignado a los organismos provinciales quedando fuera de la responsabilidad del Incucai. No existe un diccionario de datos, ni está definida la función de administrador de la base de datos. Para realizar correcciones se accede utilizando las herramientas propias del motor de la base, desde afuera de la aplicación, lo que puede generar falta de integridad y/o registro de auditoría sobre los cambios realizados.

Administración de instalaciones: no existen procesos formalmente definidos de revisión periódica de perfiles, ni de análisis de violaciones de seguridad, ni registros de visitas ni pases temporarios. No hay procedimientos para el control de parámetros climáticos. No se aborda el tema de la seguridad física en el plan de contingencia general. El centro de cómputos es de dimensiones reducidas para el tamaño de los *racks* de comunicaciones allí almacenados. La disposición del equipamiento no facilita los trabajos de mantenimiento, resulta posible que debido a un movimiento involuntario se desconecten de la red eléctrica los equipos instalados. No se puede acceder de manera sencilla a equipos de aire acondicionado para su control y mantenimiento. En la oficina de soporte técnico se encontró una gran cantidad de equipamiento obsoleto que dificulta el movimiento de personal y el normal desarrollo de las tareas.

Administración de operaciones: 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. No se establecieron procedimientos formales de detección, inspección y escalamiento de problemas. No hay normas de desempeño, acuerdos de nivel de servicio del usuario ni procedimientos formales de mantenimientos de equipos. Los operadores no cambian de turnos, las vacaciones pueden ser interrumpidas según la necesidad del área y no existe un plan de capacitación permanente para mantener sus competencias.

IV. Monitoreo

Monitoreo de los procesos: no se realizan monitoreos de los recursos de la función servicios de información ni se utilizan indicadores claves a fin de medir su desempeño. No existen informes internos referentes a la utilización de los recursos de la función servicios de información (personal, instalaciones, sistemas de aplicación, tecnología y datos). No existe un plan formal de mejora del desempeño con políticas y procedimientos documentados. No se cuenta con un análisis formal de la satisfacción del usuario.

Evaluación de la idoneidad del control interno: dada la inexistencia de controles internos formales no existen procedimientos para su evaluación.

La AGN concluye que existen graves falencias que colocan al SINTRA en una situación de riesgo inaceptable dado que:

El único personal de planta en el área informática es la coordinadora del Departamento de Informática y Sistemas. Tanto el coordinador del SINTRA como todo el personal que lo opera, desarrolla y mantiene es contratado y con ingresos muy inferiores a los equivalentes de mercado.

La cantidad total de personal subalterno del Departamento TI es de 4 personas en soporte de PC y 5 en administración de datos y desarrollo de sistemas, siendo de alta rotación por tratarse de agentes contratados. No resultan suficientes para encarar la generación de políticas y procedimientos, modelos de datos, documentación y actualización. Son inexistentes: la estructura formal del área informática, los planes estratégicos para el organismo y para tecnología, las políticas y

procedimientos formales para abordar los resguardos y objetivos de seguridad e higiene, las políticas sobre cálculo de costos, las políticas de capacitación y el control de datos.

La misma persona que realiza la coordinación del área se ocupa de tareas de programación y administración de la base de datos haciendo de ese agente un elemento indispensable para la continuidad del sistema e impidiendo el control por oposición y el monitoreo interno.

Asimismo, el órgano de control elaboró recomendaciones en función de las observaciones efectuadas a fin de mejorar el ambiente de control y reducir los riesgos implícitos. Establece darle prioridad a: a la definición de la estructura de TI, de sus misiones y funciones, de las políticas y procedimientos a cumplir y el nombramiento del personal idóneo, responsable de cumplirlas satisfactoriamente, b) tender a que la madurez de la calidad de la gestión se aproxime al valor mínimo recomendable, c) superar a la brevedad las limitaciones de los procesos ponderados en los niveles más bajos del modelo, particularmente en los casos en que la estimación del riesgo es alta, d) superar los inconvenientes detallados en el Anexo VI.

La evaluación efectuada conforme al modelo de madurez de la capacidad, a fin de determinar el impacto de las observaciones, indica que el 78,1% de los objetivos de control observados se encuentran en los niveles más bajos del modelo y ninguno alcanza el valor mínimo recomendable.

Asimismo, mediante nota AGN 128/11 de fecha 14 de marzo de 2011, los auditores informan a esta comisión que en su sesión del 2/03/11 se decidió levantar la reserva otorgada al Anexo VI del presente informe.

Heriberto A. Martínez Oddone. – Gerardo R. Morales. – Juan C. Romero. – Juan C. Morán. – Walter A. Agosto.

ANTECEDENTES

Ver expedientes 4.885-D.-2011 y 192-O.V.-2009.