SESIONES ORDINARIAS

2010

ORDEN DEL DÍA Nº 1586

COMISIÓN PARLAMENTARIA MIXTA REVISORA DE CUENTAS

Impreso el día 29 de octubre de 2010

Término del artículo 113: 9 de noviembre de 2010

SUMARIO: **Pedido** de informes al Poder Ejecutivo sobre las medidas adoptadas a fin de regularizar las situaciones observadas por la Auditoría General de la Nación, en la evaluación de la gestión informática del Ente Nacional Regulador de la Electricidad, del período junio 2007-mayo 2008.

1. (7.430-D.-2010).
2. (273-O.V.-2009).

Dictamen de comisión

Honorable Congreso:

Vuestra Comisión Parlamentaria Mixta Revisora de Cuentas ha considerado el expediente oficiales varios O.V.-273/09, mediante el cual la Auditoría General de la Nación remite resolución referido a realizar un análisis preliminar del área de tecnología informática, que permita conocer las áreas de mayor exposición al riesgo y evaluar la gestión informática del Ente Nacional Regulador de la Electricidad (ENRE) 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 a fin de regularizar las situaciones observadas por la Auditoría General de la Nación en su informe referido a evaluar la gestión informática del Ente Nacional Regulador de la Electricidad. Período auditado: junio 2007-mayo 2008.

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

De acuerdo con las disposiciones pertinentes del Reglamento del Honorable Senado de la Nación, este dictamen pasa directamente al orden del día.

Sala de la comisión, 26 de agosto de 2010.

Heriberto A. Martínez Oddone. – Luis A. Juez. – Gerardo R. Morales. – Juan C. Romero. – Ernesto R. Sanz. – Juan C. Morán. – José M. Díaz Bancalari.

FUNDAMENTOS

La Auditoría General de la Nación (AGN) efectuó un examen con el objeto de evaluar la gestión de la Tecnología de la Información (TI) en el Ente Nacional Regulador de la Electricidad (ENRE), organismo autárquico en la órbita del Ministerio de Planificación Federal, Inversión Pública y Servicios de la Nación, con el objeto de determinar las debilidades de la administración de la información en el organismo. Período auditado: junio 2007-mayo 2008.

La AGN realiza los siguientes comentarios y observaciones:

1.Planificación y organización:

a) Definición de un plan estratégico de TI: las autoridades actuales del ente no han definido un plan estratégico ni un procedimiento para su elaboración. Recién este año se está preparando un plan operativo anual del organismo que, a partir del 2009, incluiría el área de sistemas.

b) Determinación de la Dirección Tecnológica: no se definió formalmente un área para determinar la dirección tecnológica.

c) Definición de la organización y las relaciones de TI: no está conformado el comité de planificación para el área informática, ni está definida su estructura con misiones y funciones formalizadas. La cantidad

de personal del área informática es escasa y no cubre la totalidad de las funciones necesarias para operar correctamente.

d) Administración de la inversión en tecnología de información: no existe una política formal ni un procedimiento de formulación que garanticen el establecimiento de un presupuesto operativo anual y su aprobación. No se monitorean ni se siguen formalmente las inversiones y los gastos. El área de TI no tiene un presupuesto formal asegurado para cada año.

e) Comunicación de los objetivos y directivas de la gerencia: no existen, políticas formales que impongan un comportamiento de los funcionarios vinculado a la ética en el manejo de la información; áreas responsables de la formulación de políticas y procedimientos; un marco de referencia y un proceso de revisión periódica de estándares, políticas, directrices y procedimientos; políticas de calidad; políticas de minimización de riesgos y sanciones disciplinarias definidas para la falta de cumplimiento de las políticas de seguridad y control interno.

f) Evaluación de riesgos: no existe un marco de identificación y evaluación de riesgos y el enfoque es informal e incompleto.

g) Administración de proyectos: no hay un marco formal de administración de proyectos ni de procesos de monitoreo de sus plazos y costos. No existe una normativa formal para el desarrollo y mantenimiento de software. No hay una política de costos, ni normas para asegurar la calidad.

h) 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.

La AGN recomienda que la dirección implemente planes a corto y largo plazo que sean compatibles con la misión y las metas de la organización. Crear y actualizar periódicamente un plan de infraestructura tecnológica que incluya la arquitectura de los sistemas, la dirección tecnológica y las estrategias de información. La dirección debe garantizar autoridad, masa crítica e independencia de las áreas de usuarios para lograr soluciones de tecnología de información eficientes. Implementar un proceso de formulación presupuestaria que contemple: un presupuesto operativo anual de TI por centro de costos; el monitoreo de costos y beneficios y la justificación de costos y beneficios. Implementar un marco y un programa de concientización que propicien un ambiente de control positivo en todo el organismo. Establecer un marco de evaluación sistemática de riesgos. Establecer un marco de administración de proyectos que contemple mínimamente la asignación de responsabilidades, división de tareas, presupuestación del tiempo y los recursos, plazos, puntos de verificación y aprobaciones. Desarrollar y mantener periódicamente un plan general de calidad basado en los planes del organismo y de tecnología de información a largo plazo.

2. Administración e implementación

a) Adquisición y mantenimiento del software de aplicación: no existe una metodología de ciclo de vida de desarrollo y mantenimiento de sistemas para la organización.

b) Adquisición y mantenimiento de la infraestructura tecnológica: no existen políticas y procedimientos que aseguren la preparación de un plan formal de evaluación del hardware y el software nuevos, a fin de determinar el impacto que pueden tener sobre el rendimiento general del sistema. No existe un manual de procedimientos para las contrataciones informáticas. No existen políticas formalmente definidas sobre el mantenimiento preventivo del hardware.

c) Desarrollo y mantenimiento de procedimientos: no existe un marco estándar, definido y monitoreado, para desarrollar la documentación y los procedimientos. No se definen ni planifican los requerimientos operativos, ni los niveles de servicio ni las expectativas de desempeño.

d) Instalación y acreditación de aplicativos: se carece totalmente de procesos formales de instalación y acreditación. No existen: el manual de calidad, el plan de calidad, la estimación de desempeño y los programas formales de capacitación. No existe un ambiente dedicado a la prueba de los desarrollos nuevos y de las modificaciones de sistemas.

La AGN recomienda definir una metodología de adquisición e implementación formal. Implementar herramientas de soporte automatizadas. Establecer una metodología para fijar qué requerimientos claves son prioritarios. Monitorear el cumplimiento del modelo de arquitectura de TI del organismo. Definir una metodología de adquisición e implementación. Realizar un inventario pormenorizado de la infraestructura de TI. Definir una metodología de ciclo de vida para seleccionar, adquirir, mantener y quitar componentes de la infraestructura de TI. Definir acuerdos de nivel de servicio. Diseñar la infraestructura y estructura organizativa para promover y compartir la documentación del usuario, los procedimientos técnicos y el material de capacitación entre los instructores, la mesa de ayuda y los grupos de usuarios. Definir los planes de capacitación del organismo y de TI mantener el inventario de aplicativos, los procedimientos del organismo y de TI utilizando herramientas automatizadas. Definir una metodología de adquisición e implementación que garantice la aplicación de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de TI: capacitación de los usuarios y del personal de mesa de ayuda; evaluación del desempeño del software de aplicación; desarrollo del plan de implementación; entre otras.

3. Entrega y soporte

a) Definición y administración de los niveles de servicio: el directorio del organismo no les asigna los recursos necesarios a los servicios de TI. El proceso

de planificación es informal. No existe ningún proceso formal para la definición y administración de niveles de servicio.

b) Administración de servicios prestados por terceros: existen contratos formales para la contratación de servicios con terceros que siguen, en algunos casos, las recomendaciones de la Oficina Nacional de Tecnologías de Información (ONTI). No hay procedimientos para garantizar su eficacia y su cumplimiento.

c) Garantía de un servicio continuo: no hay documentación sobre la realización de pruebas del plan en su conjunto ni de la calidad de los respaldos, ni de un inventario confiable de sistemas y componentes críticos.

d) Garantía de la seguridad de los sistemas: el organismo cuenta con una política de seguridad informática formalmente aprobada pero no existen manual ni procedimientos formales al respecto y la responsabilidad de aplicarla le corresponde a la persona encargada de desarrollo de sistemas no habiendo de esta forma una adecuada separación de roles. No hay un procedimiento formal de altas, bajas y autenticación de usuarios. No están definidos perfiles de seguridad. La seguridad de TI se encara en forma reactiva y no se realizan monitoreos.

e) Identificación e imputación de costos: el área de sistemas realiza una estimación no formal sobre los recursos que necesitará para el ejercicio siguiente, pero los montos, proyectos y objetivos pueden ser cambiados por el directorio durante el año.

f) Educación y capacitación de los usuarios: no existe un plan formal de capacitación.

g) Asistencia y asesoramiento a los usuarios de tecnología de la información: la función de mesa de ayuda está soportada por una aplicación Help Desk implementada sobre tecnología Lotus Notes. La obligación de utilizar este aplicativo está formalizada aunque no se controla su cumplimiento. La jefatura de sistemas no monitorea las consultas, problemas o tendencias. No se llevan estadísticas sobre tipos de problemas ocurridos ni sobre la eficiencia del sector.

h) Administración de la configuración: no se han definido procedimientos de trabajo estándares, se depende de los conocimientos y la experiencia del personal técnico. El contenido de los datos de configuración es limitado y no es utilizado por procesos interrelacionados, como la administración de cambios y la administración de problemas.

i) Administración de problemas e incidentes: si bien los pedidos que se hacen a través del aplicativo Help Desk quedan registrados, no se realiza un control sistemático, estadísticas ni informes sobre las mismas.

j) Administración de datos: no existe un diccionario de datos, ni esta definida la función de DBA que permitiría una adecuada administración.

k) Administración de operaciones: los cambios a los programas de trabajo no son debidamente controlados. No existe un procedimiento estricto de aceptación de nuevos programas de tareas. No se establecieron procedimientos escritos completos, claros y concisos de detección, inspección y escalamiento de problemas. No existen normas de desempeño ni acuerdos de nivel de servicio del usuario ni se encontraron procedimientos formales de mantenimientos de equipos.

La AGN recomienda garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas de TI: establecer el marco de acuerdos de nivel de servicio; procedimientos de ejecución; monitoreo e informes; revisión de los contratos y de los acuerdos de nivel de servicio y establecer un programa de mejora del servicio. Verificar que los servicios prestados por terceros se identifiquen de modo adecuado y que la interrelación técnica y funcional con los proveedores esté documentada. Crear un marco de continuidad que defina los roles, las responsabilidades, el enfoque y las normas y estructuras necesarias para documentar un plan de contingencia que garantice el servicio continuo. Garantizar la eficacia de las políticas y prácticas establecidas para las siguientes 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; entre otras. El director y la jefatura de TI deben garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas: administración de las medidas de seguridad; identificación, autenticación y acceso; la seguridad del acceso en línea a los datos; administración de cuentas de usuarios; entre otras. El director y la jefatura de TI deben garantizar la eficacia de las políticas y prácticas establecidas para las siguientes actividades: identificar ítems imputables; definir procedimientos de determinación de costos; utilizar procedimientos de cargos e imputación de costos al usuario. Garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas de TI: identificación de necesidades de capacitación; organización de sesiones de capacitación; capacitación y concientización en los principios de seguridad. Garantizar la eficacia de las políticas y prácticas establecidas para las siguientes actividades de TI: registro completo de consultas de usuarios; escalamiento de consultas de usuarios; monitoreo de soluciones; análisis e informe de tendencias. Garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas de TI: registro de la configuración; establecer el nivel básico de configuración; registro del estado de la configuración; control de la configuración; detectar el software no autorizado; almacenamiento del software; administración de configuración y seguimiento y control de versiones de software. Garantizar la eficacia de las políticas y prácticas establecidas para las siguientes actividades de TI: sistema de administración de problemas; escalamiento de problemas; seguimiento de problemas y pistas de auditoría; autorizaciones de emergencia y acceso temporario y establecer las prio-

ridades de procesamiento de emergencia. El director y la jefatura de TI deben garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de TI: preparación de datos; autorización de documentos fuente; recopilación de datos de documentos fuente; manejo de errores de documentos fuente; conservación de documentos fuente; autorización de entrada de datos; entre otras. La jefatura de TI debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas de TI: desarrollo de manuales de instrucciones y procedimientos de las operaciones de procesamiento; documentación del proceso de puesta en marcha y otras operaciones; fijación de programas de trabajo; control de las desviaciones de los programas estándar de trabajo; asegurar la continuidad del procesamiento; registración de operaciones; salvaguardia de formularios especiales y dispositivos de salida y realización de operaciones remotas.

4. Monitoreo

a) Monitoreo de los procesos: no se realizan monitoreos de los recursos de TI. Los recursos humanos son insuficientes. No se utilizan indicadores claves a fin de medir el desempeño de la función servicios de información. No existe un plan formal de mejora del desempeño con políticas y procedimientos documentados. No existe el análisis formal de satisfacción del usuario.

b) Evaluación de la idoneidad del control interno: no existen controles internos formales ni procedimientos para su evaluación.

La AGN recomienda que el director y la jefatura de TI definan los indicadores de desempeño pertinentes y recopilen datos para la elaboración de informes de gestión e informes de excepción con respecto a estos indicadores. La evaluación de la función servicios de información se debe llevar a cabo en forma continua. El director y la jefatura de TI son responsables de monitorear la eficacia de los controles internos en el curso normal de las operaciones. Además, las desviaciones graves deben informarse a la máxima autoridad del organismo. Asimismo son responsables de garantizar: el monitoreo del control interno; la operación oportuna del control interno y los informes del nivel de control interno.

Teniendo en cuenta las observaciones y recomendaciones realizadas, la AGN concluye que la operatoria del ENRE es dependiente de los servicios de TI y muchas de sus tareas de control serían impracticables sin el aporte de esta tecnología, dificultando el correcto cumplimiento de la misión del organismo. Algunos de los rubros inexistentes son: planes estratégicos para el organismo y para tecnología y presupuestos anuales formales y detallados; políticas y procedimientos formales para abordar los resguardos y objetivos de seguridad e higiene; políticas de cálculo e imputación de costos; políticas de capacitación y control de datos.

La falta de personal, capacitación y herramientas tecnológicas, sumada a la circunstancia de no poseer una adecuada asignación de gastos por centros de costo se traduce en una confusión respecto a las inversiones que realiza el organismo. Se asigna al área de TI el costo de las áreas usuarias y consecuentemente se reduce el presupuesto real del sector debilitando su estructura y disminuyendo la cantidad de personal. Asimismo, la falta de nivel jerárquico del departamento sistemas y de sus responsables internos ocasiona que las tareas que deberían corresponder a la dirección o gerencia de sistemas estén recayendo actualmente en el directorio del organismo y la de los jefes de sector en el jefe de departamento. La evaluación realizada con el modelo genérico de madurez indica que el 65,6 % de los objetivos de control se encuentran en los niveles más bajos del modelo: "No conforma" e "Inicial", y ninguno alcanza el valor mínimo recomendable de "Proceso Definido". En síntesis:

a) Existen riesgos altos de falta de eficiencia y aun de falta de eficacia en la concreción de los objetivos.

b) En general, la información del organismo está sometida a riesgos que superan los valores aceptables.

c) Resulta necesario darle prioridad a: i) la redefinición de la estructura y del nivel jerárquico del área de TI junto con sus misiones y funciones, la definición de las políticas y procedimientos a cumplir, en particular los de nivel gerencial y el nombramiento del personal idóneo; ii) lograr que la madurez de la calidad de la gestión se aproxime al nivel de "Procesos definidos"; iii) superar a la brevedad las limitaciones de los procesos ponderados en niveles "No conforma" e "Inicial", particularmente en los casos en que la estimación del riesgo es alta.

Para superar las falencias detectadas, es imprescindible un fuerte compromiso de las máximas autoridades del ENRE en organizar los servicios de TI a través la jerarquización del área, su reestructuración interna y un mayor presupuesto que, en conjunto, permitan: mejor planificación, correcta distribución de funciones y el debido control.

Heriberto A. Martínez Oddone. – Luis A. Juez. – Gerardo R. Morales. – Juan C. Romero. – Ernesto R. Sanz. – Juan C. Morán. – José M. Díaz Bancalari.

ANTECEDENTE

Ver expedientes 7.430-D.-2010 y 273-O.V.-2009.