# PERÍODO PARLAMENTARIO

# 2009

# ORDEN DEL DÍA Nº 102

**COMISIÓN PARLAMENTARIA MIXTA**
**REVISORA DE CUENTAS**

**Impreso el día 8 de febrero de 2010**

Término del artículo 113: 17 de febrero de 2010

SUMARIO: **Pedido** de informes al Poder Ejecutivo sobre las medidas adoptadas en atención a las observaciones formuladas por la Auditoría General de la Nación respecto del informe referido a evaluar la Gestión de la Tecnología de la Información en la Biblioteca Nacional, para determinar debilidades y fortalezas de la administración de la información del organismo. (206-S.-2009.)

Buenos Aires, 2 de diciembre de 2009.

*Al señor presidente de la Honorable Cámara de Diputados de la Nación.*

Tengo el honor de dirigirme al señor presidente, a fin de comunicarle que el Honorable Senado, en la fecha, ha sancionado el siguiente

**Proyecto de resolución**

*El Senado y la Cámara de Diputados de la Nación*

RESUELVEN:

1. Dirigirse al Poder Ejecutivo nacional, solicitándo leinforme sobre las medidas adoptadas en atención a las observaciones formuladas por la Auditoría General de la Nación respecto del informe referido a evaluar la Gestión de la Tecnología de la Información en la Biblioteca Nacional, para determinar debilidades y fortalezas de la administración de la información del organismo.

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

Saludo a usted muy atentamente.

JUAN C. MARINO.
*Juan Estrada.*

FUNDAMENTOS

La Auditoría General de la Nación (AGN) efectuó un examen en la Biblioteca Nacional con el objeto de evaluar la gestión de la Tecnología de la Información en la Biblioteca Nacional, organismo descentralizado en la órbita de la Secretaría de Cultura de la Presidencia de la Nación, para determinar debilidades y fortalezas de la administración de la información. Período auditado: julio de 2007 a febrero de 2008.

La AGN realiza los siguientes comentarios y recomendaciones:

*Planificación y organización*

1. *Plan Estratégico de Tecnología de la Información (TI).* No hay conciencia de que se necesita una planificación estratégica de TI para respaldar las metas del organismo.

2. *Arquitectura de la información.* El conocimiento, la pericia y las responsabilidades necesarias para desarrollarla no existen en el organismo.

3. *Dirección tecnológica.* No hay conciencia de la necesidad de planificar la infraestructura tecnológica. El conocimiento y la pericia que se requieren para desarrollarla no existen.

4. *La organización y las relaciones de tecnología de la información.* La estructura organizativa del organismo no está eficazmente establecida para concentrarse en el logro de los objetivos de sus misiones y funciones.

5. *Administración de la inversión en TI.* No se ha tomado conciencia de la importancia de seleccionar y presupuestar las inversiones de TI. No se hace un seguimiento o monitoreo de las inversiones y los gastos de TI.

6. *Comunicación de los objetivos y directivas de la gerencia.* La máxima autoridad del organismo no ha establecido un ambiente positivo de control de la información. No se reconoce la necesidad de establecer un conjunto de políticas, procedimientos y normas y de controlar su cumplimiento.

7. *Administración de los recursos humanos.* No se ha tomado conciencia de la importancia de alinear la admi-

nistración de los recursos humanos de TI con el proceso de planificación de tecnología para el organismo. No hay ninguna persona o grupo formalmente responsable de la administración de recursos humanos específicos de TI.

8. *Garantía del cumplimiento de los requisitos externos.* Siguen procesos informales para mantener el cumplimiento.

9. *Evaluación de riesgos.* No se realiza una evaluación de riesgos para los procesos y las decisiones de actividades sustantivas.

10. *Administración de proyectos.* El organismo no aplica técnicas de administración de proyectos ni considera el impacto que una administración deficiente y las fallas de los proyectos pueden tener en el logro de los objetivos de la misión.

11. *Administración de la calidad.* El organismo carece de un proceso de planificación de garantía de calidad y de una metodología de ciclo de vida de desarrollo de sistemas. No se verifica la calidad de los proyectos y las operaciones.

Nivel de riesgo: alto.

*Entrega y soporte*

*Administración e implementación*

1. *Soluciones automatizadas.* El organismo no exige la identificación de requerimientos funcionales y operativos para desarrollar, implementar o modificar las soluciones de sistemas, servicio, infraestructura, software y datos.

2. *Adquisición y mantenimiento del software de aplicación.* No hay un proceso formal para diseñar y especificar aplicaciones.

3. *Adquisición tecnológica.* No se trata formalmente la arquitectura tecnológica.

4. *Desarrollo y mantenimiento de procedimientos.* No hay un proceso documentado para la producción de documentación del usuario, manuales de operaciones y material de capacitación.

5. *Instalación y acreditación de aplicativos.* Se carece de procesos formales de instalación y acreditación que garanticen que el aplicativo que se libera a los usuarios satisface sus requerimientos.

6. *Administración de cambios.* No hay un proceso de administración de cambios definido y es posible introducir cambios sin control.

Nivel de riesgo: alto.

*Entrega y soporte*

1. *Definición y administración de los niveles de servicio.* La conducción no ha reconocido la necesidad de un proceso para la definición de niveles de servicio. La rendición de cuentas y las responsabilidades del monitoreo de dichos niveles no están asignadas.

2. *Administración de servicios prestados por terceros.* Las responsabilidades y la rendición de cuentas no están definidas. No hay políticas y procedimientos formales para la contratación de terceros. No hay actividades de medición ni informes de terceros. La alta gerencia no está al tanto de la calidad del servicio prestado.

3. *Administración de la capacidad y el desempeño.* No se cuenta con ningún proceso de planificación de la capacidad.

4. *Garantía de un servicio continuo.* No se comprenden los riesgos, las vulnerabilidades y las amenazas para las operaciones de TI, ni el impacto que la pérdida de servicios de TI puede tener en el organismo.

5. *Garantía de la seguridad de los sistemas.* La seguridad de la TI se encara en forma reactiva y no se realizan mediciones. Las responsabilidades no son claras.

6. *Identificación e imputación de costos.* Se carece de un proceso reconocible para identificar e imputar costos con respecto a los servicios de información prestados.

7. *Educación y capacitación de los usuarios.* Se carece de programas de educación y capacitación de los usuarios de sistemas. El organismo no encara formalmente el tema.

8. *Asistencia y asesoramiento a los usuarios de tecnología de la información.* No hay un proceso estandarizado y sólo se brinda un soporte reactivo. La alta gerencia no monitorea las consultas, problemas o tendencias. No hay un proceso de escalamiento que ayude a resolver los problemas.

9. *Administración de la configuración.* La alta gerencia no cuenta con un proceso para el tratamiento de la información y administración de la infraestructura de TI, ni para la configuración de hardware y de software.

10. *Administración de problemas e incidentes.* No se reconoce la necesidad de administrar problemas e incidentes.

11. *Administración de datos.* Los datos no están considerados como un recurso y un bien del organismo. La calidad y seguridad de los datos es escasa o nula.

12. *Administración de instalaciones.* No se ha tomado conciencia de la necesidad de proteger las instalaciones o de invertir en recursos de computación.

13. *Administración de operaciones.* El organismo no dedica tiempo ni recursos a establecer políticas y prácticas para los manuales de instrucciones y procedimientos de las operaciones de procesamiento; documentación del proceso de puesta en marcha y otras operaciones; programas de trabajo; desviaciones de los programas estándar de trabajo; continuidad del procesamiento y registro de operaciones o salvaguardia de formularios especiales y dispositivos de salida.

Nivel de riesgo: alto.

*Monitoreo*

1. *Monitoreo de los procesos.* El organismo no ha implementado procesos de monitoreo.

2. *Evaluación de la idoneidad del control interno.* El organismo carece de procedimientos para monitorear la eficacia de los controles internos.

3. *Obtención de garantía independiente.* El organismo no tiene procesos de garantía. No ha implementado políticas de seguridad. No se desarrollaron acuerdos de nivel de servicio y no se efectúa una medición de los procesos.

4. *Provisión de auditoría independiente.* No se realizan auditorías independientes.

Nivel de riesgo: alto.

Como consecuencia del análisis del descargo presentado por el organismo auditado, la AGN ratifica las observaciones oportunamente formuladas.

*Recomendaciones*

*Planificación y organización*

La AGN recomienda implementar planes a corto y a largo plazo compatibles con la misión y las metas de la organización. La máxima autoridad debe impulsar la creación y el mantenimiento de un modelo que contemple: i) arquitectura de la información; ii) diccionario de datos del organismo y reglas de sintaxis de los datos; iii) esquema de clasificación de los datos y iv) niveles de seguridad.

Se debe crear y actualizar periódicamente un plan de infraestructura tecnológica que incluya la arquitectura de los sistemas, la dirección tecnológica y las estrategias de información.

Al incluir la función de servicios de información en la estructura del organismo para implantar soluciones de TI, la alta gerencia debe garantizar autoridad, recursos suficientes e independencia con respecto a las áreas de usuarios de TI.

Debe implementarse un proceso de formulación presupuestaria que contemple: i) un presupuesto operativo anual de TI por centro de costos; ii) monitoreo y justificación de costos y beneficios.

Se debe implementar un marco y un programa de concientización que propicien un ambiente de control positivo en todo el organismo. El organismo debe contar con una fuerza laboral con las habilidades necesarias para alcanzar sus metas. La máxima autoridad y la alta gerencia deben garantizar: i) la selección y promoción, formación y experiencia del personal; ii) la definición de roles y responsabilidades; iii) los procedimientos de verificación de antecedentes del personal, etcétera.

La máxima autoridad y la alta gerencia deben establecer y mantener procedimientos para revisar los requerimientos externos relacionados con las prácticas y controles de la TI. Además, se debe determinar en qué medida es preciso que las estrategias de TI respalden los requerimientos de cualquier tercero relacionado. Se debe establecer un marco de evaluación sistemática de riesgos. Se debe establecer un marco de administración de proyectos que contemple, como mínimo, la asignación de responsabilidades, división de tareas, estimación del tiempo y los recursos, plazos, puntos de verificación y aprobaciones.

Se debe definir el proyecto, aprobar sus fases y elaborar un plan maestro; establecer un plan de garantía de calidad del sistema; implementar la administración formal de riesgos del proyecto; elaborar un plan de pruebas, un plan de capacitación y un plan de revisión posterior a la implementación. Desarrollar y mantener periódicamente un plan general de calidad basado en los planes del organismo y de TI a largo plazo.

*Administración e implementación*

La AGN recomienda garantizar la aplicación y mejora continua de la metodología del ciclo de vida de desarrollo de sistemas (CVDS). Además, la metodología del CVDS debe contemplar un plan de estrategias de adquisición de software y de evaluación de requerimientos y especificaciones para la contratación de terceros proveedores de servicios.

Se deben establecer procedimientos y técnicas adecuadas para: i) aplicar la metodología del CVDS del organismo en coordinación estrecha con los usuarios de sistemas; ii) crear especificaciones de diseño para cada proyecto de desarrollo de un sistema nuevo y verificarlas.

Garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de TI: i) realizar evaluación del hardware y el software nuevos; ii) mantenimiento preventivo del hardware; iii) atender a la seguridad del software del sistema; iv) instalación del software del sistema; v) efectuar el mantenimiento del software y vi) realizar los controles de cambios del software del sistema.

Aplicar la metodología del CVDS del organismo de manera tal de garantizar la definición oportuna de los requerimientos operativos y niveles de servicio, la preparación de manuales de usuario y de operaciones y el desarrollo de materiales de capacitación. La alta gerencia y el responsable de la función de servicios de información deben verificar la eficacia de los procedimientos y prácticas establecidas para: i) cumplimentar los requerimientos operativos y niveles de servicio; ii) redactar manuales de procedimientos del usuario; iii) redactar el manual de operaciones y iv) elaborar los materiales de capacitación.

En todos los proyectos se deben aplicar las resoluciones del Comité de Seguridad Informática relativas a la implementación o modificación de los sistemas de aplicación.

Aplicar los procedimientos específicos para tratar los pedidos de cambios, mantenimiento de sistemas y mantenimiento del proveedor.

*Entrega y soporte*

La AGN recomienda garantizar la eficacia de las políticas y prácticas establecidas para: i) establecer marco de acuerdos de nivel de servicio; ii) definir procedimientos de ejecución; iii) realizar el monitoreo y los informes; iv) revisar los contratos y acuerdos de nivel de servicio y v) 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.

La máxima autoridad y la alta gerencia deben garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas de TI: i) identificar requerimientos de disponibilidad y desempeño; ii) establecer un plan de disponibilidad; iii) monitorear el desempeño de los recursos de TI y realizar informes; iv) utilizar herramientas para la creación de modelos; v) administrar el desempeño de manera proactiva; vi) pronosticar la carga de trabajo; vii) administrar la capacidad de los recursos; viii) establecer la disponibilidad de recursos y ix) planificar los recursos.

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 alta gerencia y el responsable de la función de servicios de información deben garantizar la eficacia de las políticas y prácticas establecidas para: i) administración de las medidas de seguridad; ii) identificación, autenticación y acceso; iii) garantizar la seguridad del acceso en línea a los datos; iv) administrar las cuentas de usuarios; v) revisión de la gerencia de cuentas de usuarios; vi) el control ejercido por el usuario en sus propias cuentas, etcétera.

La máxima autoridad y la alta gerencia deben garantizar la eficacia de las políticas y prácticas establecidas para: i) identificar ítem imputables; ii) definir procedimientos de determinación de costos y iii) utilizar procedimientos de cargos e imputación de costos al usuario.

El funcionario principal de servicios de información debe garantizar la eficacia de las políticas y prácticas establecidas para: i) soporte al usuario a través de la mesa de ayuda; ii) registro completo de consultas de usuarios; iii) escalamiento de consultas de usuarios; iv) monitoreo de soluciones y v) análisis e informe de tendencias.

El funcionario principal de la función servicios de información debe garantizar la eficacia de las políticas y prácticas establecidas para: i) establecer el nivel mínimo necesario de la configuración de hardware y software; ii) registrar el estado de la configuración; iii) efectuar el control de la configuración; iv) detectar el software no autorizado; v) almacenar el software; vi) administrar la configuración y vii) efectuar el seguimiento y el control de las versiones de software.

El responsable de la función de servicios de información debe garantizar la eficacia de las políticas y prácticas establecidas para: i) optimizar el sistema de administración de problemas; ii) efectuar el escalamiento de problemas; iii) realizar el seguimiento de problemas y de las pistas de auditoría; iv) aprobar las autorizaciones de emergencia y el acceso temporario y v) establecer las prioridades de procesamiento de emergencia.

La alta gerencia, los responsables de programas y actividades y el responsable de la función de servicios de información deben garantizar la eficacia de los procedimientos y prácticas establecidas para: i) preparación de datos; ii) autorizar los documentos fuente; iii) recopilar datos de documentos fuente; iv) manejar errores de documentos fuente, etcétera.

El responsable de la función de servicios de información debe garantizar la eficacia de las políticas y prácticas establecidas para: i) proveer la seguridad física; ii) asegurar la discreción del sitio de TI; iii) acompañar a las visitas del centro de cómputos con personal del área; iv) proveer a la salud y la seguridad del personal y v) protección contra factores ambientales.

El responsable de la función de servicios de información debe garantizar la eficacia de las políticas y prácticas establecidas para: i) desarrollar manuales de instrucciones y procedimientos de las operaciones de procesamiento; ii) documentar el proceso de puesta en marcha y otras operaciones; iii) fijar los programas de trabajo, etcétera.

La alta gerencia es responsable de garantizar: i) la recopilación de los datos de monitoreo; ii) la evaluación continua del desempeño; iii) la evaluación de la satisfacción del usuario y iv) la elaboración de informes de gestión.

La alta gerencia y el funcionario principal de servicios de información son responsables de monitorear la eficacia de los controles internos en el curso normal de las operaciones. Las desviaciones graves deben informarse a la máxima autoridad del organismo.

La alta gerencia debe obtener la garantía independiente de la seguridad y controles internos de los servicios de TI, de la eficacia de sus proveedores y del cumplimiento de requisitos legales y regulatorios y de los compromisos contractuales. Además, debe garantizar que la función de auditoría interna posea la competencia técnica y las capacidades y conocimientos necesarios para llevar a cabo dichas revisiones de un modo eficaz, eficiente y económico.

La alta gerencia debe establecer la responsabilidad primaria y las acciones para la función de auditoría interna que resuman la responsabilidad, facultad y rendición de cuentas de la función de auditoría informática. Además, este marco debe ser revisada periódicamente para garantizar que se mantenga la independencia, facultad y responsabilidad de la función de auditoría informática.

De acuerdo a las observaciones y recomendaciones realizadas la AGN concluye que ninguno de los cuatro objetivos de control considerados alcanza el nivel mínimo necesario para cumplir con los objetivos y las acciones que la legislación le asigna al organismo, ni para garantizar la conservación de la información digital disponible en la actualidad. La evaluación realizada con el modelo genérico de madurez indica que el 100 % de los objetivos de control se encuentran en los niveles más bajos del modelo. La conducta del organismo en los temas de TI es reactiva y genera los inconvenientes típicos de la falta de planificación. El departamento de sistemas no cuenta con una estructura propia aprobada, ni con un jefe nombrado por concurso, ni con personal de planta o con los perfiles necesarios. El sistema de aplicación usado para atender al público es un catálogo de publicaciones con datos sólo de los libros recibidos hasta el año 2004. Los libros posteriores al 2004 figuran en un inventario ad hoc en otro banco de datos a la espera de la contratación del Sistema de Gestión Bibliotecaria, en vías de licitación, que permitirá catalogarlos junto al resto de los materiales en existencia. Los sistemas usados en Administración son provistos por una empresa pequeña (sociedad de hecho), la institución no cuenta con copias de los programas fuente ni de sus datos históricos para permitir resguardarse de su eventual desaparición. La carencia de normas de seguridad, continuidad y resguardo pone en riesgo la información digital disponible, los niveles de riesgo promedio se encuentran entre el 83 y el 94 % siendo el máximo aceptable un piso del 20 %. Respecto al análisis del sitio web de la BN las páginas examinadas no alcanzan el nivel mínimo de calificación definido por las normas competentes.

*Recomendaciones adicionales:* A la Dirección de la Biblioteca: asignar la más alta prioridad y urgencia a formar un área profesionalizada de informática. A la Secretaría de Cultura: proveer el presupuesto necesario, permitiendo a la institución cumplir con eficacia y eficiencia con sus objetivos específicos. Se estima imposible cumplir con lo recomendado sin una adecuación de los recursos disponibles para tecnología de la información.

*Nicolás A. Fernández. – José J. B. Pampuro. – Gerardo R. Morales. – Juan J. Álvarez. – Miguel Á. Pichetto. – Carlos D. Snopek.*

ANTECEDENTES

1

**Dictamen de comisión**

*Honorable Congreso:*

Vuestra Comisión Parlamentaria Mixta Revisora de Cuentas ha considerado el expediente Oficiales Varios 7/09, mediante el cual la Auditoría General de la Nación remite resolución referida a evaluar la gestión de la tecnología de información en la Biblioteca Nacional, con el objeto de determinar debilidades y fortalezas de la administración de la información en el organismo; y, por las razones expuestas en sus fundamentos, os aconseja la aprobación del siguiente

**Proyecto de resolución**

*El Senado y la Cámara de Diputados de la Nación*

RESUELVEN:

1. Dirigirse al Poder Ejecutivo nacional solicitándole informe sobre las medidas adoptadas en atención a las observaciones formuladas por la Auditoría General de la Nación respecto del informe referido a evaluar la gestión de la tecnología de la información en la Biblioteca Nacional, para determinar debilidades y fortalezas de la administración de la información en el organismo.

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, este dictamen pasa directamente al orden del día.

Sala de la comisión, 3 de septiembre de 2009.

*Nicolás A. Fernández. – José J. B. Pampuro. – Gerardo R. Morales. – Juan J. Álvarez. – Miguel Á. Pichetto. – Ernesto R. Sanz. – José M. Á. Mayans. – Carlos D. Snopek.*

2

Ver expediente 206-S.-2009.

* Los fundamentos corresponden a los publicados con la comunicación del Honorable Senado.