SESIONES ORDINARIAS

2011

ORDEN DEL DÍA Nº 1969

COMISIÓN PARLAMENTARIA MIXTA REVISORA DE CUENTAS

Impreso el día 29 de marzo de 2011

Término del artículo 113: 7 de abril de 2011

SUMARIO: **Pedido** de informes al Poder Ejecutivo sobre las medidas adoptadas para regularizar las situaciones observadas por la Auditoría General de la Nación, con motivo de su examen realizado en el ámbito de la Oficina Nacional de Control Comercial Agropecuario (ONCCA), organismo descentralizado en la órbita del Ministerio de Agricultura, Ganadería y Pesca, para determinar madurez y riesgo de la administración de la información y cuestiones conexas.

1. (518-D.-2011.)
2. (448-O.V.-2009.)

Dictamen de comisión

Honorable Cámara:

Vuestra Comisión Parlamentaria Mixta Revisora de Cuentas ha considerado el Expediente O.V.-448/09, Auditoría General de la Nación comunica resolución, aprobando el informe referido a evaluar la gestión de la tecnología de la información (TI) en la Oficina Nacional de Control Comercial Agropecuario (ONCCA), organismo descentralizado en la órbita del Ministerio de Agricultura, Ganadería y Pesca, para determinar madurez y riesgo de la administración de la información; 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 las medidas adoptadas para: *a)* regularizar las situaciones observadas por la Auditoría General de la Nación con motivo de su examen realizado en el ámbito de la Oficina Nacional de Control Comercial Agropecuario (ONCCA), organismo descentralizado en la órbita del Ministerio de Agricultura, Ganadería y Pesca; *b)* determinar el perjuicio fiscal que pueda haberse originado en las referidas situaciones; y *c)* deslindar y efectivizar las correspondientes responsabilidades.

2. Remitir copia de la presente resolución, juntamente con sus fundamentos, a la Fiscalía Nacional de Investigaciones Administrativas y a la Oficina Anticorrupción a los fines de su toma de conocimiento y a los efectos que determinen sus respectivas competencias.

3. Remitir copia de la presente resolución, juntamente con sus fundamentos, a la Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal a los fines de la toma de conocimiento de los juzgados donde tramiten causas relacionadas con dichas cuestiones.

4. Comuníquese al Poder Ejecutivo, a la Fiscalía Nacional de Investigaciones Administrativas, a la Oficina Anticorrupción, a la Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal y a la Auditoría General de la Nación, juntamente con los fundamentos de la presente.

Sala de la comisión, 2 de marzo de 2011.

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

FUNDAMENTOS

La Auditoría General de la Nación (AGN) efectuó un examen en el ámbito del Ministerio de Agricul-

tura, Ganadería y Pesca, con el objeto de evaluar la gestión de la tecnología de la información (TI) en la Oficina Nacional de Control Comercial Agropecuario (ONCCA), organismo descentralizado en la órbita del Ministerio de Agricultura, Ganadería y Pesca, para determinar madurez y riesgo de la administración de la información.

El período auditado abarcó desde mayo de 2008 a abril de 2009, habiéndose realizado las tareas de campo desde mayo de 2009 hasta agosto de 2009.

La AGN hace referencia al marco legal e institucional informando que la Oficina Nacional de Control Comercial Agropecuario se creó como organismo desconcentrado en el año 1996, mediante el decreto 1.343, unificando en un solo organismo todas las funciones que hacían a la fiscalización y al control del comercio interno y externo del sector agropecuario y cuyo objetivo primario era asegurar un marco de transparencia y libre concurrencia de estas actividades, asignándoseles funciones remanentes de las ex Juntas Nacionales de Carnes y de Granos.

Por decreto 1.067/05 del 31 de agosto de 2005, se instituye a la Oficina Nacional de Control Comercial Agropecuario la naturaleza de organismo descentralizado, con autarquía económico-financiera y técnico-administrativa, dotado de personería jurídica propia, en jurisdicción de la Secretaría de Agricultura, Ganadería, Pesca y Alimentos del entonces Ministerio de Economía y Producción.

El texto normativo mencionado en el párrafo precedente establece el marco y los instrumentos de desenvolvimiento que permiten dotar al organismo de eficiencia suficiente en su gestión, fijándose claramente el ámbito de actuación en la órbita de la Secretaría de Agricultura, Ganadería, Pesca y Alimentos. Delimita las políticas de su administración y concede a dicha secretaría la posibilidad de extender, a través de la Oficina Nacional de Control Comercial Agropecuario, el control comercial reglado a otras cadenas agroalimentarias cuando las necesidades de fiscalización así lo aconsejen.

El objetivo de la ONCCA es garantizar el cumplimiento de las normas comerciales por parte de los operadores que participan de los mercados de ganados, carnes, granos y lácteos, a fin de asegurar transparencia y equidad en el desarrollo del sector agroalimentario en todo el territorio nacional.

La AGN en su informe formula comentarios y observaciones, los que son puestos en conocimiento del organismo para que formule las aclaraciones que estime pertinentes. En su respuesta, el organismo auditado acepta las observaciones oportunamente formuladas y consecuentemente quedan ratificadas.

La AGN formula las siguientes recomendaciones:

Planificación y organización

Definición de un plan estratégico de TI: El departamento de TI debe implementar planes a corto y largo plazo que sean compatibles con la misión y las metas de la organización aprobadas por la presidencia. En este aspecto, debe garantizar que:

–La tecnología de información forme parte del plan de la organización a corto y largo plazo.

–Se elabore un plan de TI a largo plazo.

–Se actualice el enfoque y la estructura de la planificación de TI a largo plazo.

–Se realicen los cambios del plan de TI a largo plazo.

–Se elabore la planificación a corto plazo de la función de servicios de información.

–Se comuniquen los planes de TI.

–Se controlen y evalúen los planes de TI.

–Se evalúen los sistemas existentes.

Definición de la arquitectura de la información: la máxima autoridad debe impulsar la creación y el mantenimiento de un modelo que contemple lo siguiente:

–Un modelo de arquitectura de la información.

–El diccionario de datos del organismo y reglas de sintaxis de los datos.

–Un esquema de clasificación de los datos.

–Los niveles de seguridad.

Determinación de la Dirección Tecnológica: 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.

Definición de la organización y las relaciones de TI: al ubicar la función de servicios de información dentro de la estructura del organismo, la presidencia debe garantizar autoridad, masa crítica e independencia de las áreas de usuarios en la medida necesaria para lograr soluciones de tecnología de información eficientes. En este aspecto se debe asegurar:

–La designación de un comité permanente de planificación de TI.

–La ubicación adecuada de la función de servicios de información en la estructura del organismo.

–La revisión de los logros organizacionales.

–La definición de los roles y responsabilidades.

–La responsabilidad sobre el aseguramiento de calidad.

–La responsabilidad sobre la seguridad lógica y física.

–La propiedad y custodia de los datos.

–La supervisión de las actividades de TI.

–La separación de funciones.

–La competencia del personal de TI.

–Las descripciones de los puestos del personal de TI.

–Las políticas y procedimientos relativos al personal contratado.

–Las relaciones de coordinación, comunicación y enlace.

Administración de la inversión en TI: implementar un proceso de formulación presupuestaria que contemple lo siguiente:

–Un presupuesto operativo anual de TI por centro de costos.

–El monitoreo de costos y beneficios.

–La justificación de costos y beneficios.

Comunicación de los objetivos y directivas de la gerencia: implementar un marco y un programa de concientización que propicien un ambiente de control positivo en todo el organismo. Este marco debe abordar la integridad, los valores éticos y la competencia de las personas, la filosofía de gestión, el estilo operativo y la rendición de cuentas. En este aspecto, la máxima autoridad y el departamento de TI deben garantizar:

–Las responsabilidades sobre la formulación de las políticas.

–La comunicación de las políticas del organismo.

–La disponibilidad de los recursos para la implementación de políticas.

–El mantenimiento de políticas.

–El cumplimiento de las políticas, los procedimientos y las normas.

–El compromiso con la calidad.

–La política marco de seguridad y control interno.

–La observancia de los derechos de propiedad intelectual.

–La comunicación de la concientización en materia de seguridad.

Administración de los recursos humanos: el organismo debe contar con una fuerza laboral que tenga las habilidades necesarias para lograr sus metas. La máxima autoridad y el departamento de TI deben garantizar:

–El cumplimiento de los períodos de vacaciones.

–La selección y promoción del personal.

–La formación y experiencia del personal.

–La definición de roles y responsabilidades.

–La capacitación del personal.

–La capacitación cruzada o personal de reemplazo.

–Los procedimientos de verificación de antecedentes del personal.

–La evaluación del desempeño laboral.

–El cambio de puestos y la seguridad en la extinción de la relación laboral.

Garantía del cumplimiento de los requerimientos externos: la máxima autoridad y la jefatura de TI deben establecer y mantener procedimientos para la revisión de los requerimientos externos que permitan identificar los relacionados con las prácticas y controles de la TI. Además, se debe determinar en qué medida es preciso que las estrategias respalden los requerimientos de cualquier tercero relacionado. En este aspecto, la máxima autoridad y la jefatura de TI deben garantizar:

–La revisión de los requerimientos externos.

–Las prácticas y procedimientos para garantizar el cumplimiento de los requerimientos externos.

–El cumplimiento de la normativa en materia de seguridad y ergonomía.

–La privacidad de datos y la propiedad intelectual.

–El cumplimiento de la legislación en las actividades de comercio/gobierno electrónico.

–El cumplimiento de los contratos de seguro.

Evaluación de riesgos: se debe establecer un marco de evaluación sistemática de riesgos. El mismo debe incorporar una evaluación periódica de los riesgos de información relacionados con la consecución de los objetivos del organismo, que constituya una base para determinar cómo deben administrarse los riegos a un nivel aceptable. El departamento de TI debe garantizar que se realice:

–Una evaluación de riesgos de la actividad.

–La identificación de riesgos.

–La medición de riesgos.

–Un plan de acción de reducción de riesgos.

–La aceptación de riesgos.

Administración de proyectos: 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.

Administración de la calidad: debe desarrollarse y mantenerse periódicamente un plan general de calidad basado en los planes del organismo y de tecnología de información a largo plazo. La presidencia y el departamento de TI deben garantizar que exista:

–Un plan general de calidad.

–Un enfoque de garantía de calidad.

–Una planificación de garantía de calidad.

–La revisión de garantía de calidad en cuanto al cumplimiento de las normas y procedimientos de TI.

–Una metodología del ciclo de vida del desarrollo de sistemas.

–Una metodología del ciclo de vida del desarrollo de sistemas para la introducción de cambios importantes en la tecnología existente.

–La actualización de la metodología del ciclo de vida del desarrollo de sistemas.

–La coordinación y comunicación entre los usuarios y el personal de TI.

–Un marco de adquisición y mantenimiento de la infraestructura tecnológica.

–Un marco para las relaciones con terceros a cargo de la implementación.

–La observación de las normas de documentación de programas, verificando que:

–Se cumplan las normas de prueba de programas.

–Se cumplan las normas de prueba de sistemas.

–Se utilicen pruebas en paralelo/piloto.

–La documentación de pruebas de sistemas.

Administración e implementación

Identificación de soluciones automatizadas: se deben definir prácticas que contemplen la solidez del diseño, la robustez de la funcionalidad y también la operabilidad (que incluye desempeño, escalabilidad e integración), la aceptabilidad (que cubre administración, mantenimiento y soporte) y la sustentabilidad (que considera costo, productividad y aspecto).

–Se deben definir los criterios para evaluar las opciones de desarrollo interno, soluciones compradas y tercerización.

–Definir formalmente un método general de adquisición e implementación o metodología de ciclo de vida de desarrollo de sistemas.

–Definir formalmente un proceso para la planificación, iniciación y aprobación de soluciones.

–Implementar un proceso estructurado de análisis de requerimientos.

–Considerar los requerimientos de seguridad y control desde el principio.

Adquisición y mantenimiento del *software* de aplicación: Definir una metodología de adquisición e implementación formal.

–Implementar herramientas de soporte automatizadas.

–Establecer una metodología para fijar qué requerimientos clave son prioritarios.

–Monitorear el cumplimiento con la arquitectura de TI del organismo, incluyendo un proceso formal de aprobación de las desviaciones.

Adquisición y mantenimiento de la infraestructura tecnológica: definir una metodología de adquisición e implementación.

–Realizar un inventario pormenorizado de la infraestructura de TI (hardware y software).

–Definir una metodología de ciclo de vida para seleccionar, adquirir, mantener y quitar componentes de la infraestructura de TI.

Desarrollo y mantenimiento de procedimientos: 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 el proceso de desarrollo asegurando el uso de procedimientos operativos estándar y una apariencia estándar.

–Definir un marco estándar para la documentación y los procedimientos.

Instalación y acreditación de sistemas de aplicación: 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 personal de servicios de información.

–Evaluación del desempeño del software de aplicación.

–Desarrollo del plan de implementación.

–Conversión de sistemas de aplicación.

–Conversión de datos.

–Definición de la estrategia y los planes de prueba.

–Realización de la prueba de cambios.

–Aplicación de criterios de ejecución de pruebas paralelas/piloto.

–Realización de la prueba de aceptación final.

–Realización de las pruebas de acreditación de seguridad.

–Realización de la prueba de funcionamiento.

–Transición a producción.

–Evaluación del cumplimiento de los requerimientos del usuario.

–Revisión de la gerencia posterior a la implementación.

Administración de cambios: definir e implementar políticas y procedimientos de administración de cambios.

–Integrar la administración de cambios con la administración de las versiones de software y de la administración de la configuración.

–Definir un proceso de planificación, aprobación e iniciación que cubra la identificación, categorización, evaluación de impacto y fijación de prioridades para los cambios.

–Definir un proceso formal para la transición desde el ambiente de desarrollo al de producción.

–Establecer un procedimiento de emergencias que permita llevar la solución de un problema en el menor tiempo posible alterando o agilizando alguno de los pasos del procedimiento estándar.

–Todos estos procedimientos de administración de cambios deben contemplar, por último, una etapa de cierre que incluya la documentación de usuario y un proceso de revisión para garantizar la implantación completa de los cambios. Pueden también ser revisados los costos ejecutados.

Entrega y soporte

Definición y administración de los niveles de servicio: Garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

–Establecer marco de acuerdos de nivel de servicio.

–Procedimientos de ejecución.

–Monitoreo e informes.

–Revisión de los contratos y acuerdos de nivel de servicio.

–Establecer un programa de mejora del servicio.

Administración de servicios prestados por terceros: se debe 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 y/o actividades de TI:

–Interrelación con proveedores de TI.

–Asignar la responsabilidad por tales relaciones.

–Formalización de contratos con terceros.

–Evaluación del conocimiento y la experiencia de terceros.

–Formalización de contratos de tercerización.

–Asegurar la continuidad de los servicios.

–Acordar las relaciones de seguridad.

–Monitoreo de la prestación del servicio.

Administración de la capacidad y el desempeño: 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:

–Identificación de requerimientos de disponibilidad y desempeño.

–Establecer un plan de disponibilidad.

–Monitoreo e informes del desempeño de los recursos de TI.

–Utilización de herramientas para la creación de modelos.

–Administración proactiva del desempeño.

–La realización de pronósticos de la carga de trabajo.

–Administración de la capacidad de los recursos.

–Establecer la disponibilidad de recursos.

–Planificación de recursos.

Garantía de un servicio continuo: 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.

Garantía de la seguridad de los sistemas: 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:

–Administración de las medidas de seguridad.

–Identificación, autenticación y acceso.

–La seguridad del acceso en línea a los datos.

–Administración de cuentas de usuarios.

–Revisión de la gerencia de cuentas de usuarios.

–El control ejercido por el usuario en sus propias cuentas.

–La supervisión de la seguridad.

–Clasificación de los datos.

–Administración centralizada de identificaciones y derechos de acceso.

–Realizar informes de violación y actividades de seguridad.

–Manejo de incidentes.

–Acreditación de soluciones.

–Normar la confianza en la contraparte.

–Autorización de transacciones.

–Establecer la imposibilidad de rechazo.

–Definir ruta de acceso confiable.

–Protección de las funciones de seguridad.

–Administración de claves criptográficas.

–Prevención, detección y corrección de software malicioso.

–Establecer arquitectura de *firewalls* y conexiones con redes públicas.

–Protección del valor electrónico.

Identificación e implementación de costos: 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:

–Identificar ítems imputables.

–Definir procedimientos de determinación de costos.

–Utilizar procedimientos de cargos e imputación de costos al usuario.

Educación y capacitación de los usuarios: 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:

–Identificación de necesidades de capacitación.

–Organización de sesiones de capacitación.

–Capacitación y concientización en los principios de seguridad.

Asistencia y asesoramiento a los usuarios de TI: el departamento de TI debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

–Registro completo de consultas de usuarios.

–Escalamiento de consultas de usuarios.

–Monitoreo de soluciones.

–Análisis e informe de tendencias.

Administración de la configuración: el departamento de TI debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades 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.

–Seguimiento y control de versiones de software.

Administración de problemas e incidentes: 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.

Administración de datos: la jefatura de TI, los responsables de programas y actividades y el jefe de operaciones 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.

–Verificación de exactitud, integridad y autorización.

–Manejo de errores de entrada de datos.

–Asegurar la integridad del procesamiento de datos.

–Validación y edición del procesamiento de datos.

–Manejo de errores del procesamiento de datos.

–Manejo y conservación de salidas.

–Distribución de salidas de datos.

–Balanceo y conciliación de salidas de datos.

–Revisión y manejo de errores de salidas de datos.

–Seguridad de los informes de salida.

–Protección de información crítica durante la transmisión y el transporte.

–Protección de información crítica eliminada.

–Administración del almacenamiento.

–Establecer períodos de conservación y condiciones de almacenamiento.

–Establecer un sistema de administración de biblioteca de medios.

–Definir las responsabilidades de administración de la biblioteca de medios.

–Resguardo y restauración.

–Tareas de resguardo.

–Almacenamiento de resguardos.

–Administración de archivos.

–Protección de mensajes críticos.

–Autenticación e integridad.

Administración de instalaciones: 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:

–Seguridad física.

–Asegurar la discreción del sitio de tecnología de información.

–Acompañamiento de visitas.

–Salud y seguridad del personal.

–Protección contra factores ambientales.

Administración de operaciones: el departamento de TI debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades 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.

–Realización de operaciones remotas.

Se deben establecer y documentar los procedimientos estándar para las operaciones que garanticen la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

–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 estándares de trabajo.

–Continuidad del procesamiento.

–Registro de operaciones.

–Salvaguardia de formularios especiales y dispositivos de salida.

–Operaciones remotas.

Monitoreo

Monitoreo de los procesos: la presidencia y el departamento de TI son responsables de que se definan los indicadores de desempeño pertinentes y que se 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. En este aspecto, la alta gerencia es responsable de garantizar:

–Que se recopilan los datos de monitoreo.

–Que se evalúa el desempeño en forma continua.

–Que se evalúa la satisfacción del usuario.

–Que se elaboran informes de gestión.

Evaluación de la idoneidad del control interno: la presidencia y el departamento 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. La alta gerencia y el funcionario principal de servicios de información son responsables de garantizar:

–El monitoreo del control interno.

–La operación oportuna del control interno.

–Los informes del nivel de control interno.

La AGN concluye su informe, expresando lo siguiente:

La ONCCA es un organismo creado en 1996 y con nuevas funciones y recursos desde 2005. La estructura orgánica interna y las misiones y funciones correspondientes a TI no han sido aprobadas a la fecha de los trabajos de campo. El cúmulo de tareas que se le asignan en los últimos años y la importancia de las mismas hicieron que se firme en marzo de 2009 un convenio marco de cooperación en temas de informática y comunicaciones con AFIP.

En función de dicho convenio y en la práctica, AFIP ha asumido la conducción del área, sin precisiones de tiempos y responsabilidades, y administra no sólo los recursos humanos de ONCCA sino también los equipos informáticos.

Señala la AGN que esta circunstancia limitó el trabajo de auditoría por no incluir las tareas que están a cargo de ese organismo.

Las debilidades que presenta el convenio entre ambas instituciones pone en riesgo el funcionamiento de la TI en la ONCCA ya que en las actuales condiciones depende de la buena voluntad de la AFIP.

Por otra parte, el rol de la Fundación Argeninta que es responsable de realizar las contrataciones del personal de TI y de gestionar las compras de equipamiento por fuera de la órbita de la ONTI hace posible que no siempre se satisfagan sus requisitos.

La AGN expresa que la falta de una estructura formal genera entre otros inconvenientes:

a) La inexistencia de una auditoría interna que garantice el funcionamiento de los controles necesarios para el correcto desempeño de la TI.

b) La inexistencia formal del área de sistemas, impidiendo el nombramiento del responsable y de los

subordinados (la tarea de jefatura es ejercida inorgánicamente por un agente de AFIP).

c) El 100 % del personal de TI es contratado utilizando los servicios que le presta la Fundación Argeninta.

En síntesis, señala la AGN, existen riesgos altos de falta de eficiencia y aun de falta de eficacia en la concreción de los objetivos y, en general, la información está sometida a riesgos que superan los valores aceptables.

Sigue diciendo el órgano de control externo que para superar el actual estado de situación, es necesario darle prioridad a:

–La definición de la estructura de tecnología de información, de sus misiones y funciones, de las políticas y procedimientos a cumplir y el nombramiento del personal idóneo, responsable de cumplirlas satisfactoriamente.

–Tender a que la madurez de la calidad de la gestión se aproxime, cuanto menos, al nivel de "procesos definidos".

–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, reformular el convenio vigente con AFIP, estipulando la naturaleza y duración del soporte de TI que se le brinda a la ONCCA, con el objeto de garantizar la continuidad del servicio prestado, respetando, como mínimo, los niveles de calidad requeridos por AFIP en sus instalaciones.

La evaluación realizada con el modelo genérico de madurez indica que el 89,6 % 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".

Para corregir las falencias detectadas es imprescindible un fuerte compromiso de las máximas autoridades de la ONCCA para organizar los servicios de TI y de las autoridades del ministerio para proveer los recursos necesarios y una urgente formalización de la estructura.

En atención a lo informado por la AGN y teniendo en cuenta lo dispuesto por la resolución 1/06 de la Comisión Parlamentaria Mixta Revisora de Cuentas que establece que esta comisión, en relación a las resoluciones de la AGN, "emitirá dictamen, recomendando a las Cámaras del Honorable Congreso… *d)* Otros destinos que resuelva la comisión", se estima conveniente comunicar oportunamente la resolución que adopte el Honorable Congreso a la Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal. Ello en relación al expediente 11.997/09, obrante en el Juzgado Nacional de Primera Instancia en lo Criminal y Correccional Nº 8, así como también para su eventual remisión a otros expedientes judiciales que puedan estar relacionados con la presente cuestión.

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

ANTECEDENTES

Ver expedientes 518-D.-2011 y 448-O.V.-2009.

anexo