SESIONES ORDINARIAS

2011

ORDEN DEL DÍA Nº 2054

COMISIÓN PARLAMENTARIA MIXTA REVISORA DE CUENTAS

Impreso el día 4 de mayo de 2011

Término del artículo 113: 13 de mayo de 2011

SUMARIO: **Pedido** de informes al Poder Ejecutivo sobre las medidas adoptadas respecto de las observaciones formuladas por la Auditoría General de la Nación con motivo del examen realizado en el ámbito del Instituto Nacional de Estadística y Censos (INDEC) con el objeto de evaluar la gestión de la Tecnología de la Información y cuestiones conexas.

1.– (1.716-D.-2011.)
2.– (307-O.V.-2010.)

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 O.V.-307/10, mediante el cual la Auditoría General de la Nación comunica resolución aprobando el informe referido a la "Evaluación de la gestión de la Tecnología de la Información en el Instituto Nacional de Estadística y Censos (INDEC), con el objeto de determinar la calidad 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: *a)* respecto de las observaciones formuladas por la Auditoría General de la Nación con motivo del examen realizado en el ámbito del Instituto Nacional de Estadística y Censos –INDEC–, con el objeto de evaluar la gestión de la Tecnología de la Información (TI) y determinar la calidad de la administración de dicha información en el organismo; *b)* a los fines de determinar y efectivizar las responsabilidades que pudieran haber emergido de las situaciones objeto de las referidas observaciones.

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 noviembre 2010.

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 O.V.-307/10, mediante el cual la Auditoría General de la Nación comunica resolución aprobando el informe referido a la "Evaluación de la gestión de la Tecnología de la Información en el Instituto Nacional de Estadística y Censos (INDEC), con el objeto de determinar la calidad 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 las medidas adoptadas respecto de las observaciones formuladas por la Auditoría General de la Nación con motivo del examen realizado en el ámbito del Instituto Nacional de Estadística y Censos –INDEC –, con el objeto de evaluar la gestión de la Tecnología de la Información (TI) y determinar la calidad de la administración de dicha 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, el presente dictamen pasa directamente al orden del día.

Sala de la comisión, 30 de noviembre 2010.

Nicolás A. Fernández. – Gerónimo Vargas Aignasse. – José María Díaz Bancalari.

FUNDAMENTOS

La Auditoría General de la Nación (AGN), efectuó un examen en el ámbito del Instituto Nacional de Estadística y Censos –INDEC –, organismo dependiente del Ministerio de Economía y Finanzas Públicas de la Nación, referido a la evaluación de la gestión de la Tecnología de la Información (TI) con el objeto de determinar la calidad de la administración de la información en el Organismo.

Las tareas de campo abarcaron desde agosto de 2009 hasta octubre 2009.

La AGN señala que el examen fue realizado de conformidad con las normas de Auditoría Externa de la AGN, aprobadas por la resolución 145/93, dictadas en virtud de las facultades conferidas por el artículo 119, inciso *d)* de la ley 24.156.

La tarea se basó en la verificación de los Objetivos de Control establecidos por las normas COBIT (*Control Objectives in Information Technologies*). Los Objetivos de Control describen los resultados que debe alcanzar un organismo implantando procedimientos de control en los procesos de TI. No fue objeto de la presente auditoría el análisis detallado del funcionamiento de los sistemas informáticos del Instituto ni los procedimientos de cálculo de los índices que realiza el Organismo, ni de los métodos de selección de los datos con que éstos se calculan.

La AGN, en el apartado "Aclaraciones previas", realiza una breve descripción del marco legal e institucional del INDEC, creado en 1968 mediante la ley 17.622 como organismo público técnico, encargado de unificar la orientación y ejercer la dirección superior de las actividades estadísticas oficiales que se lleven a cabo en el territorio de la República Argentina. Asimismo detalla objetivos y estructura organizativa de la Entidad.

En punto a los "Comentarios y observaciones", la AGN desarrolla los siguientes:

1. PLANIFICACIÓN Y ORGANIZACIÓN.

1.1. Definición de un Plan Estratégico de TI.

Objetivo de control: La máxima autoridad debe impulsar el proceso periódico de planificación estratégica que permita formular los planes a largo plazo. A su vez, estos planes deben traducirse oportunamente en planes operativos que definan metas claras y concretas a corto plazo.

Nivel de madurez: Inicial. La dirección reconoce la necesidad de una planificación estratégica de TI, pero no hay un proceso de decisión estructurado. La planificación estratégica está determinada por necesidades puntuales. Por lo tanto, los resultados son esporádicos, no uniformes.

Observaciones: No existe el plan estratégico del Organismo ni de la Dirección de TI.

1.2. Definición de la Arquitectura de la Información.

Objetivo de control: La información debe mantenerse acorde con las necesidades y debe ser identificada, recopilada y comunicada en tiempo y forma de modo de permitir a las personas cumplir sus responsabilidades de manera eficiente y oportuna. Se debe crear y mantener un modelo de arquitectura de información que incluya el modelo de datos del Organismo y los sistemas de información relacionados.

Nivel de madurez: Inicial. El área de TI reconoce la necesidad de una arquitectura de la información, pero no ha formalizado ni un proceso ni un plan para desarrollarla. Hay un avance aislado y reactivo de los componentes de la arquitectura de la información. Existen implementaciones aisladas y parciales de reglas de sintaxis y diagramas de datos y documentación. Las decisiones se basan en datos aislados, en lugar de basarse en información.

Observaciones: 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. Cada Dirección Nacional tiene una modalidad propia en TI no centralizada por la Dirección de Informática por lo que no existe una arquitectura de la información ni un modelo de datos común al Organismo.

1.3. Determinación de la Dirección Tecnológica.

Objetivo de control: Se debe crear y mantener un plan de infraestructura tecnológica que fije y administre expectativas claras y realistas de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de entrega.

Nivel de madurez: Inicial. No hay políticas ni procesos formales definidos para el tema. Tampoco existen políticas y procedimientos para evaluar y monitorear tendencias, ni para que dichas evaluaciones sean tenidas en cuenta durante el desarrollo y mantenimiento del plan de infraestructura tecnológica. El desarrollo de los componentes y la implementación de nuevas técnicas son realizados ad hoc. Estas tareas no figuran en las misiones y funciones. Las direcciones tecnológicas son manejadas por los planes de evolución de los organismos rectores en la materia y por la oferta de los proveedores de productos de hardware, software de sistemas y software de aplicaciones. No hay análisis ni comunicación normalizados del impacto potencial de los cambios tecnológicos.

Observaciones: No hay Plan de Infraestructura Tecnológica. Se tiene conciencia de la importancia que la planificación de infraestructura 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.

1.4. Definición de la Organización y las Relaciones de TI.

Objetivo de control: Una organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión. La organización debe estar embebida en un marco de trabajo de procesos de TI que asegure la transparencia y el control, así como el compromiso de los altos ejecutivos. Un comité estratégico debe garantizar la vigilancia de la Dirección sobre TI y uno ó más comités de dirección, en los cuales participe personal de TI, deben determinar las prioridades de los recursos de TI de manera tal de alinearlos con las necesidades del Organismo. Deben existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas y la segregación de funciones. Para garantizar el soporte oportuno de los requerimientos de la misión, TI se debe involucrar en los procesos importantes de decisión.

Nivel de madurez: Inicial. Las actividades y funciones de TI son reactivas y se implantan de forma inconsistente. Personal de TI se involucra en algunos proyectos solamente en las etapas finales. La función de TI se considera como una función de soporte, sin una perspectiva organizacional general. Existe un entendimiento explícito de la necesidad de una organización de TI; sin embargo, los roles y las responsabilidades no están formalizados, ni consolidados.

Observaciones: El Organismo no cuenta con estructura informática debidamente formalizada que abarque a todo el Instituto. No existe el comité de planificación de servicios de información, ni su estructura con misiones y funciones formalizadas. Las tareas de desarrollo informático en las Direcciones Nacionales de Estadísticas del Sector Externo, de Estadísticas y Precios de la Producción y el Comercio y en la de Estadísticas de Condiciones de Vida son realizadas con personal propio y no responden a la Dirección de Informática, que por lo tanto, no atiende la totalidad de la tarea de TI.

1.5. Administración de la Inversión en Tecnología de Información.

Objetivo de control: La máxima autoridad debe definir un presupuesto anual operativo y de inversión, establecido y aprobado por el Organismo.

Nivel de madurez: Inicial. El Organismo reconoce la necesidad de administrar la inversión en TI, pero no hay una comunicación uniforme al respecto. No hay una asignación formal de la responsabilidad de la selección de inversiones y el desarrollo de presupuestos. Los gastos que se perciben como significativos requieren justificaciones sustentatorias. En casos aislados se implementa la selección y presupuestación de inversiones, con documentación informal. La justificación de las inversiones es ad hoc. Se toman decisiones de presupuestación reactivas y concentradas en las operaciones.

Observaciones: 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 debida aprobación. No se hace un seguimiento o monitoreo de las inversiones y los gastos de TI.

1.6. Comunicación de los Objetivos y Directivas de la Gerencia.

Objetivo de control: La Dirección debe impulsar la definición de políticas y su comunicación a la comunidad de usuarios. Además, es preciso que se establezcan normas a fin de traducir las opciones estratégicas en reglas prácticas y útiles.

Nivel de madurez: No conforma. La máxima autoridad del Organismo no ha establecido un ambiente positivo de control de la información. No hay reconocimiento de la necesidad de establecer un conjunto uniforme de políticas, procedimientos y normas junto con procesos de control de su cumplimiento.

Observaciones: No hay políticas formales para establecer una comunicación clara de los intereses y objetivos de la gerencia; ni que impongan un comportamiento de los funcionarios vinculado a la ética; 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; una política de calidad ni de minimización de riesgos; una política de seguridad; sanciones disciplinarias definidas para la falta de cumplimiento de las políticas de seguridad y control interno.

1.7. Administración de los Recursos Humanos de TI.

Objetivo de control: La Dirección debe implementar prácticas sólidas, justas y transparentes de administración de personal en cuanto a selección, alineación, verificación de antecedentes, remuneración, capacitación, evaluación, promoción y despido.

Nivel de madurez: No conforma. No se ha tomado conciencia de la importancia de alinear la administración 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 de TI.

Observaciones: Los roles y responsabilidades de las distintas funciones del área informática no están formalmente definidos, lo que impide evaluar el correcto desempeño de los mismos. Existen áreas de TI que no responden a la Dirección de Informática. No existe una política formal de reclutamiento y promoción.

1.8. Garantía del cumplimiento de los requisitos externos.

Objetivo de control: Se deben establecer procedimientos para la identificación y el análisis de los requerimientos externos a fin de determinar su impacto sobre la tecnología de información y la adopción de las medidas necesarias para su cumplimiento.

Nivel de madurez: Inicial. Se ha tomado conciencia de la importancia de cumplir las regulaciones, los contratos y la legislación que afectan al Organismo. Se siguen procesos informales para mantener el cumplimiento, pero solo a medida que surge una necesidad en nuevos proyectos o en respuesta a auditorías o revisiones.

Observaciones: No existen políticas y procedimientos formales para garantizar que se adopten en forma oportuna las medidas correctivas para evaluar los requisitos externos, diseñar los resguardos y objetivos de seguridad e higiene, garantizar el cumplimiento de las exigencias de los contratos de seguros, y el cumplimiento de las normas para TI dictadas por la Oficina Nacional de Tecnología de la Información.

1.9. Evaluación y Administración de Riesgos.

Objetivo de control: La máxima autoridad debe definir un proceso por el cual el Organismo se ocupa de identificar los riesgos de Tecnología de la Información y analizar su impacto, involucrando funciones multidisciplinarias y adoptando medidas eficaces en función de costos a fin de mitigarlos.

Nivel de madurez: Inicial. El Organismo conoce sus responsabilidades legales y contractuales, pero considera los riesgos de TI en forma ad hoc, sin seguir procesos o políticas definidas. Se llevan a cabo evaluaciones informales del riesgo de los proyectos. Es poco probable que se identifiquen evaluaciones de riesgo dentro de un plan. La Dirección de Informática no especifica la responsabilidad por la administración de riesgos en las descripciones de puestos. Los riesgos que afectan la seguridad, disponibilidad e integridad, se consideran sobre la base de cada proyecto. Los riesgos relacionados con las operaciones diarias son un tema tratado informalmente en reuniones de gestión.

Observaciones: No existe un marco formal de identificación y evaluación de riesgos. Este proceso se complica por la independencia informática que se verifica en las direcciones nacionales mencionadas.

1.10. Administración de Proyectos.

Objetivo de control: La máxima autoridad debe establecer un proceso por el cual el Organismo identifique y priorice los proyectos en concordancia con el plan operativo. El Organismo debe adoptar y aplicar técnicas bien concebidas de administración de proyectos para cada uno que se inicie.

Nivel de madurez: No conforma. No se usan técnicas de administración de proyectos y el Organismo no considera el impacto que una administración deficiente y las fallas de los proyectos pueden tener en el logro de los objetivos.

Observaciones: 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.

1.11. Administración de la Calidad.

Objetivo de control: Se debe elaborar un sistema de administración de calidad con procesos y estándares probados de desarrollo y de adquisición. Los requerimientos de calidad se deben relevar y documentar con indicadores cuantificables y alcanzables. La mejora continua se logra por medio del constante monitoreo, corrección de errores y la comunicación de los resultados a los interesados.

Nivel de madurez: conforma. El Organismo carece de un proceso de planificación de garantía de calidad y de una metodología de ciclo de vida de desarrollo de sistemas. La alta gerencia y el personal de TI reconocen la necesidad de un programa de calidad. Nunca se verifica la calidad de los proyectos y de las operaciones.

Observaciones: No se aplican criterios de calidad y no existe metodología formal del ciclo de vida para el desarrollo y mantenimiento de los sistemas.

2. ADMINISTRACIÓN E IMPLEMENTACIÓN.

2.1. Identificación de Soluciones Automatizadas.

Objetivo de control: La necesidad de una nueva aplicación o función requiere de análisis antes de la compra o desarrollo para garantizar que las misiones del Organismo se satisfacen con un enfoque efectivo y eficiente. Este proceso cubre su definición, considera las fuentes alternativas, realiza una revisión de la factibilidad tecnológica y económica, ejecuta un análisis de riesgo y de costo-beneficio y concluye con una

decisión final de desarrollar o comprar. Todos estos pasos permiten a las organizaciones minimizar el costo para adquirir e implantar soluciones, mientras que al mismo tiempo facilitan el logro de los objetivos de la organización.

Nivel de madurez: Inicial. Se tomó conciencia de la necesidad de definir requerimientos e identificar soluciones de tecnología. Sin embargo, los enfoques no son uniformes y no se basan en una metodología específica de adquisición e implementación. Cada grupo se reúne para analizar las necesidades informalmente y los requerimientos no suelen quedar documentados. Las soluciones son identificadas sobre la base de un conocimiento limitado del mercado o en respuesta a las propuestas de los proveedores. El análisis estructurado y la investigación de la tecnología disponible son escasos o nulos.

Observaciones: El Organismo no posee políticas y procedimientos para identificar requerimientos funcionales y operativos para el desarrollo, implementar y modificar las soluciones de sistemas. No existen 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 evaluación de la tercerización de desarrollos de software en comparación con los desarrollos propios.

Por otra parte, existen estructuras informáticas autónomas en tres direcciones nacionales que no siguen directivas de la Dirección de Informática en lo referente al tema.

2.2. Adquisición y Mantenimiento del Software de Aplicación.

Objetivo de control: Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del Organismo. Este proceso cubre su diseño, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, el desarrollo y la configuración en sí de acuerdo a los estándares. Esto permite a las organizaciones apoyar el cumplimiento de sus objetivos de forma apropiada con las aplicaciones automatizadas correctas.

Se deben establecer estrategias de adquisición de software y evaluación de requerimientos y especificaciones para la contratación de terceros proveedores de servicios.

La adquisición y mantenimiento del software aplicativo debe realizarse por medio de la definición específica de requerimientos funcionales y operativos con una implementación por etapas de prestaciones claras.

Nivel de madurez: Inicial. Se tomó conciencia de que se necesita un proceso para adquirir y mantener las aplicaciones. Sin embargo, los enfoques varían de proyecto a proyecto sin uniformidad. No existe una metodología de adquisición formal, aceptada, entendida y aplicada. No existen políticas ni procedimientos que aseguren que la instalación y el mantenimiento del software se realicen de acuerdo con un marco definido y debidamente aprobado.

Observaciones: No existe una metodología para el desarrollo y mantenimiento de sistemas para la organización. Existen estructuras informáticas autónomas en tres direcciones del Organismo, que desarrollan, mantienen y pasan a producción aplicaciones sin cumplir con los requisitos necesarios para asegurar su correcto funcionamiento, y sobre las cuales la Dirección de Informática no tiene control.

2.3. Adquisición y Mantenimiento de la Infraestructura Tecnológica.

Objetivo de control: La organización debe contar con procesos para adquirir, implantar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del Organismo.

Nivel de madurez: Inicial. Si bien se reconoce que la infraestructura de la TI es importante, no hay un enfoque general uniforme. El Organismo carece de políticas y procedimientos referentes a la adquisición, implementación y mantenimiento de hardware y software. Los cambios de infraestructura se introducen para cada nueva necesidad sin un plan general.

Observaciones: 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. Se pudo observar que las adquisiciones en la materia no alcanzan a compensar el nivel de obsolescencia y el crecimiento de la infraestructura y servicios, con lo cual el problema se agravará en el futuro. No existe un manual de procedimientos para las contrataciones informáticas. El inventario de la configuración no está debidamente actualizado.

No existen políticas ni procedimientos relacionados con: análisis de impacto de la incorporación de hardware y el software nuevos; análisis de integración entre distintas plataformas; análisis de tercerización con aprovechamiento de infraestructura interna o externa; el manejo de casos en los que se depende de un proveedor de única fuente; y el mantenimiento preventivo del hardware.

Es de destacar el estado de la red de datos, la cual puede definirse como precaria, no solo por su antigüedad tecnológica, sino también por la falta de mantenimiento adecuado que pone en riesgo la continuidad de los servicios que presta.

2.4. Desarrollo y Mantenimiento de Procedimientos.

Objetivo de control: Se debe aplicar un enfoque estructurado para el desarrollo de procedimientos del usuario y de operaciones, requerimientos de servicios y materiales de capacitación. La metodología del Ciclo

de Vida de Desarrollo de Sistemas del Organismo debe garantizar la definición oportuna de los requerimientos operativos y niveles de servicio, la preparación de manuales del usuario y de operaciones y el desarrollo de materiales de capacitación.

Nivel de madurez: Inicial. La organización ha tomado conciencia de la necesidad de generar un marco estándar, definido y monitoreado, para el desarrollo de la documentación y los procedimientos. Ocasionalmente se produce documentación, pero está dispersa, es inconsistente y sólo está disponible para grupos limitados. Gran parte de la documentación y los procedimientos son incompletos, están desactualizados y prácticamente no hay integración de éstos entre distintos sistemas y unidades sustantivas. Los materiales de capacitación son aislados y de calidad variable.

Observaciones: No existe un marco estándar, definido y monitoreado, para el desarrollo de la documentación y de 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.

2.5. Instalación y Acreditación de Aplicativos.

Objetivo de control: Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación y la transición en sí al ambiente de producción, y revisar la posimplantación. Esto garantiza que los sistemas estén en línea con las expectativas convenidas y con los resultados esperados.

Nivel de madurez: Inicial. Se ha tomado conciencia de la necesidad de verificar y confirmar que las soluciones implementadas sean adecuadas para la finalidad prevista. Se efectúan pruebas para algunos proyectos, pero éstas iniciativas quedan a criterio de cada equipo de proyecto y los enfoques adoptados pueden variar. La acreditación y aprobación formal es escasa o nula.

Observaciones: Se carece de procesos formales de instalación y acreditación. Si bien en la Dirección de Informática se han separado los entornos de desarrollo, pruebas (llamado internamente "curso") y producción, éstos no son totalmente independientes ya que los desarrolladores pasan el software entre desarrollo y pruebas y un jefe de proyecto hace lo propio entre 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, previo a la etapa de pruebas por parte del usuario involucrado.

Por otra parte, las estructuras informáticas autónomas existentes en las direcciones nacionales, mencionadas en 1.4, realizan el desarrollo, el mantenimiento y el pase a producción utilizando criterios independientes y fuera del control de la Dirección Informática. En éstos casos suelen ser las mismas personas las que realizan el desarrollo, las pruebas y la puesta en producción.

2.6. Administración de Cambios.

Objetivo de control: Todos los cambios, incluyendo el mantenimiento de emergencia y soluciones transitorias, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse de manera formal y controlada. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación; y comparar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente en la estabilidad o integridad del ambiente de producción.

Nivel de madurez: Inicial. Se reconoce que los cambios deberían ser administrados y controlados, pero no hay un procedimiento uniforme que pueda seguirse. Las prácticas varían y es probable que ocurran cambios no autorizados. La documentación de los cambios es escasa o nula y la documentación de la configuración es incompleta y poco confiable. Esto podría dar lugar a deficiencias e interrupciones en el ambiente de producción.

Observaciones: No se han establecido procedimientos formales para administrar cambios de manera estándar para todas las solicitudes que se realizan. Además las estructuras informáticas autónomas existentes en tres direcciones están fuera del control de la Dirección de Informática.

3. ENTREGA Y SOPORTE.

3.1. Definición y Administración de los Niveles de Servicio.

Objetivo de control: La máxima autoridad debe definir un marco para promover el establecimiento de acuerdos de nivel de servicio que formalicen los criterios de desempeño en virtud de los cuales se medirá su cantidad y calidad.

Nivel de madurez: Inicial. La dirección reconoce la necesidad de administrar los niveles de servicio, pero el proceso es informal y reactivo. La responsabilidad y rendición de cuentas por el monitoreo del desempeño tienen una definición informal. Las medidas del desempeño son cualitativas, con metas vagamente definidas. La presentación de informes sobre el desempeño es infrecuente e inconsistente.

Observaciones: No existe una política que promueva la definición de acuerdos de nivel de servicios, ni acciones que impulsen la participación de los usuarios en su definición. La responsabilidad de los usuarios se formaliza mediante un documento donde se establecen las condiciones para el uso de los sistemas pero no existe control del cumplimiento del mismo. La res-

ponsabilidad de los proveedores está definida caso por caso, sin una política general en los contratos.

3.2. Administración de Servicios Prestados por Terceros.

Objetivo de control: La dirección debe implementar medidas de control orientadas a la revisión y al monitoreo de los contratos y procedimientos existentes para garantizar su eficacia y el cumplimiento de la política del Organismo.

Nivel de madurez: Repetible. El proceso de supervisión de los proveedores de servicios y la prestación de los servicios es informal. Se usa un contrato firmado con términos y condiciones estándares para los proveedores y una descripción de los servicios a prestar.

Observaciones: 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 para los elementos informáticos. No se encontraron en las órdenes de compra analizadas documentación que defina la relación entre contratistas y subcontratistas. En la documentación recibida no se encontraron informes sobre el desempeño de los proveedores. Durante el período auditado se hizo cargo de la administración de las bases de datos del Organismo una persona contratada, que hace el mantenimiento de las mismas fuera del horario de trabajo o en forma remota.

3.3. Administración de la Capacidad y el Desempeño.

Objetivo de control: Se debe implementar un proceso de administración orientado a la recopilación de datos, al análisis y a la generación de informes sobre el desempeño de los recursos de tecnología de la Información, la dimensión de los sistemas de aplicación y la demanda de cargas de trabajo.

Nivel de madurez: Inicial. La administración de la capacidad y el desempeño es reactiva y esporádica. Los usuarios suelen diseñar sus propios métodos para solucionar las limitaciones del desempeño y la capacidad. La gestión de TI conoce la necesidad de una administración del desempeño y la capacidad pero la acción tomada suele ser reactiva o incompleta. El proceso de planificación es informal.

Observaciones: El equipamiento informático del Organismo no está acorde con sus necesidades. Los servidores, las PC de escritorio, elementos de conectividad de redes e instalaciones son en su mayor parte obsoletos y están desactualizados. No se realizan tareas de evaluación sobre capacidad y desempeño en forma sistemática. Se observó que en varias máquinas no puede utilizarse el antivirus contratado por el Organismo porque su exigua potencia (consecuencia de su antigüedad) impide la instalación.

No existen plazos ni niveles de servicio definidos para las prestaciones del área de sistemas. No se utilizan herramientas para monitorear el desempeño. No se pide información a los usuarios para establecer plazos o definiciones de servicios No se realizan informes de desempeño y se hace un control informal del mismo.

3.4. Garantía de un Servicio Continuo.

Objetivo de control: Se debe implementar un plan probado y operativo de continuidad de TI que concuerde con el plan de continuidad general del Organismo y con sus requerimientos.

Nivel de madurez: Inicial. Las responsabilidades del servicio continuo son informales, con autoridad limitada. La máxima autoridad y la alta gerencia se están dando cuenta de los riesgos relacionados y la necesidad de un servicio continuo. El foco está puesto en la función de TI y no en la función de las actividades del Organismo. Los usuarios implementan formas de solucionar las interrupciones. La respuesta a las grandes interrupciones es reactiva y carece de planificación. Se programan interrupciones para satisfacer las necesidades de TI y no para adaptarse a las necesidades vinculadas con las actividades del Organismo.

Observaciones: No se encontró un plan de continuidad de los servicios de información del Organismo ni planes de contingencia que analicen posibles causas, escenarios y riesgos asociados. Tampoco se encontraron procedimientos para resolver los problemas que pudieran presentarse.

No está definido un sitio de procesamiento alternativo para el caso de que el centro de cómputos dejara de funcionar.

El edificio de la calle Julio A. Roca cuenta con una UPS que puede alimentar al centro de cómputos en caso de corte del suministro de energía el tiempo necesario para dar de baja los sistemas en forma ordenada. En el edificio de la calle Carlos Calvo si bien hay un grupo electrógeno no hay UPS lo que trae como consecuencia la salida de servicio en forma abrupta de los servidores en caso de corte de energía. El grupo electrógeno tarda aproximadamente un minuto a partir de la puesta en marcha para estar operativo.

No existen políticas, planes o procedimientos que incluyan capacitación o concientización de los roles individuales o grupales para asegurar la continuidad.

3.5. Garantía de la Seguridad de los Sistemas.

Objetivo de control: La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades, así como de políticas, procedimientos estándares que contemplen la seguridad y pruebas periódicas para verificar las repuestas. Se deben realizar acciones correctivas sobre las debilidades o incidentes identificados.

Nivel de madurez: Inicial. El Organismo reconoce la necesidad de la seguridad de TI pero la concientización depende de cada persona. La seguridad de TI se encara en forma reactiva y no se realizan mediciones. Las

violaciones a la seguridad de TI, si son detectadas, no logran señalar a los culpables porque las responsabilidades no son claras. Las respuestas a las violaciones de la seguridad de TI son impredecibles.

Observaciones: La red interna del Organismo está protegida por un firewall que bloquea páginas de Internet potencialmente peligrosas e impide el acceso a páginas web de chat y el uso de mensajería instantánea No se realizan reportes o informes de seguridad. Se monitorea pero no en forma sistemática. No existe una política de contraseñas, las mismas una vez definidas no caducan para los usuarios ubicados en el edificio de Av. Roca y tienen un año de validez para los usuarios del edificio de la calle Carlos Calvo. No se muestra al usuario la fecha y hora del último acceso. No hay límite de tiempo por inactividad, una vez autenticado el usuario no debe volver a hacerlo.

El Organismo tiene contratada la provisión de antivirus, pero este no puede ser instalado en todas las máquinas, dada la obsolescencia de algunas. Para solucionar en parte este problema se instala una versión de prueba de otro proveedor (normalmente 90 días), que solo se actualiza durante ese lapso.

Existen usuarios de PC que son administradores de sus equipos, esto les permite instalar sin control de la Dirección de Informática software que puede contener virus o cuya licencia no sea legal. Esta circunstancia, no solo pone en riesgo la red de datos, sino que también deja al Organismo expuesto a sanciones judiciales.

3.6. Identificación e Imputación de Costos.

Objetivo de control: Se debe implementar un sistema de imputación de costos que garantice que se registren, calculen y asignen los costos de acuerdo con el nivel de detalle requerido y el ofrecimiento de servicio adecuado.

Nivel de madurez: Inicial. Hay un entendimiento general de los costos globales de los servicios de información, pero no hay un desglose de costos por usuario, departamento, grupos de usuarios, funciones de servicio, proyectos o prestaciones. Prácticamente no hay monitoreo de costos y solo se informan a la máxima autoridad los costos totales. No hay proceso ni sistema de imputación a los usuarios de los costos incurridos en la prestación de servicios de información.

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

3.7. Educación y Capacitación de los Usuarios.

Objetivo de control: Se debe establecer y mantener un plan integral de capacitación y desarrollo.

Nivel de madurez: Inicial. Hay evidencia de que el Organismo reconoció la necesidad de un programa de educación y capacitación, pero no hay procesos estandarizados. En ausencia de un programa organizado, los empleados identifican y asisten a cursos de capacitación por cuenta propia. El enfoque global de la dirección carece de cohesión y la comunicación de los temas y abordajes de la educación y capacitación es solo esporádica y poco coherente.

Observaciones: No existen políticas y procedimientos referentes a la concientización permanente en seguridad de la información. La capacitación se basa en la oferta de cursos que realiza el INAP (en su mayoría sobre gobierno electrónico y uso de software de oficina), y de ser necesario con proveedores externos en el caso de software especializado como, por ejemplo, el SAS Enterprise. No hay cursos internos sobre seguridad informática.

No hay obligación para el personal de realizar cursos de capacitación. No hay políticas ni procedimientos referidos a la capacitación del personal de sistemas.

3.8. Asistencia y Asesoramiento a los Usuarios de Tecnología de la Información.

Objetivo de control: Se debe establecer una función de mesa de ayuda que brinde soporte y asesoramiento de primera línea.

Nivel de madurez: Inicial. El Organismo reconoció que se necesita un proceso apoyado por herramientas y personal para responder a las consultas de los usuarios y administrar la resolución de problemas. No obstante, no se cuenta con un proceso estandarizado y solo se brinda un soporte reactivo. La alta gerencia no monitorea las consultas, inconvenientes o tendencias. No hay un proceso de escalamiento que ayude a resolver los problemas.

Observaciones: El proceso de asistencia y asesoramiento a usuarios no está definido.

Los usuarios se comunican con el sector de Mesa de Ayuda mediante dos números telefónicos que están publicados en la Intranet del Organismo, o por medio de notas internas. De acuerdo al tipo de problema, de ser necesaria la intervención de un técnico se genera una orden de trabajo en forma manual donde queda registrado el problema y luego el cierre del incidente.

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.

3.9. Administración de la Configuración.

Objetivo de control: Se deben implementar controles que identifiquen y registren todos los bienes de Tecnología de la Información y su ubicación física, y un programa de verificación regular que confirme su existencia.

Nivel de madurez: Inicial. Se reconoce la necesidad de administración de la configuración. Se realizan tareas básicas de administración de la configuración, como mantenimiento del inventario de hardware y software, en forma individual. No se aplican prácticas estándares.

Observaciones: No se encontró evidencia de la existencia de procedimientos de administración de la configuración ni procedimientos de mantenimiento de inventarios de hardware y software. Se entrego un inventario completo de los servidores del Organismo que muestra una gran diversidad de tecnologías y plataformas. Muchos de los servidores que se ocupan de tareas auxiliares son PC potenciadas y con una antigüedad excesiva para el uso que se les está dando.

El Organismo reconoció no disponer de un inventario completo y actualizado del equipamiento informático de sus oficinas. De las visitas realizadas se obtuvo como conclusión que la mayor parte del parque de equipos es obsoleta.

En la información suministrada por el Organismo se observa una gran cantidad de sistemas operativos, algunos de los cuales, dada su antigüedad, ya no tienen soporte por parte del fabricante.

3.10. Administración de Problemas e Incidentes.

Objetivo de control: Se debe implementar un sistema de administración de problemas que registre y de respuesta a todos los incidentes.

Nivel de madurez: Inicial. El Organismo reconoce que hay una necesidad de resolver problemas y evaluar incidentes. Hay especialistas clave dentro del Organismo que ayudan a resolver los problemas relacionados con su área de conocimiento y responsabilidad. La información no se comparte con otros y las soluciones varían de una persona de soporte a otra, con lo cual se crean problemas adicionales y se pierde tiempo productivo mientras se buscan las respuestas. La dirección suele cambiar el foco y la orientación del personal de soporte técnico y operaciones.

Observaciones: 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.

3.11. Administración de Datos.

Objetivo de control: La máxima autoridad debe establecer y mantener una combinación eficaz de controles generales y de aplicación sobre las operaciones de Tecnología de la Información para asegurar que los datos permanezcan durante su entrada, actualización y almacenamiento completos, precisos y válidos.

Nivel de madurez: Inicial. El Organismo reconoce la necesidad de tener datos precisos. Se desarrollan algunos métodos a nivel de cada persona para prevenir y detectar los errores en la entrada, el procesamiento y la salida. El proceso de identificación y corrección de errores es un trabajo manual realizado individualmente y las reglas y requerimientos no se transmiten de un empleado a otro cuando hay movimientos o rotación de personal.

Observaciones: No existe un diccionario de datos, ni está centralizada ni definida formalmente la función de administrador de la base de datos. Para realizar correcciones se las puede acceder utilizando las herramientas propias del motor de la base, desde afuera de la aplicación, lo que genera falta de integridad y/o registro de auditoría sobre los cambios realizados.

El Organismo recibe datos de distintas fuentes como ser encuestas propias, datos de organismos oficiales nacionales y provinciales. Estos llegan en una gran variedad de formatos porque el Organismo no define ni impone un estándar para los mismos. En el caso de las encuestas manuales, se procesan de esa forma cada uno de los cuestionarios, y una vez cargados son controlados de manera no automatizada.

No hay políticas ni procedimientos formalmente definidos para la entrega de datos, ya sea internamente entre distintas áreas del Organismo o con otros organismos de la Administración Pública Nacional o administraciones provinciales.

3.12. Administración de Instalaciones.

Objetivo de control: Se deben instalar controles ambientales y físicos adecuados cuya revisión se efectúe periódicamente a fin de determinar su correcto funcionamiento.

Nivel de madurez: Inicial. El Organismo reconoce el requerimiento de la actividad de brindar un entorno físico adecuado que proteja los recursos y el personal contra los peligros generados por la naturaleza y el hombre. No existen procedimientos estándares y la administración de las instalaciones y los equipos dependen de la idoneidad y capacidad de ciertas personas clave. No se revisan las actividades de maestranza en las instalaciones y la gente se desplaza sin restricciones. La dirección no monitorea los controles ambientales de las instalaciones ni el movimiento del personal.

Observaciones: 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 se encuentra ubicado en un lugar que no cumple con los requerimientos mínimos de seguridad. No posee un sistema de automático de extinción de incendios, y el de detección no funciona por falta de mantenimiento.

Las puertas traseras de los racks se encuentran abiertas con cables de datos saliendo y cables de alimentación eléctrica con sus correspondientes tomacorrientes sueltos.

El Centro de Cómputos no posee piso técnico, se encuentra alfombrado y en mal estado de conservación.

Existe una heladera y un horno microondas en las proximidades de los servidores.

El depósito de equipos informáticos se encuentra desordenado. No cumple con las medidas de higiene y seguridad.

La disposición del equipamiento no facilita los trabajos de mantenimiento y existe el riesgo de que un movimiento involuntario desconecte de la red eléctrica a los equipos instalados. No se puede acceder de manera sencilla a equipos de aire acondicionado para su control y mantenimiento.

3.13. Administración de Operaciones.

Objetivo de control: Un procesamiento completo y apropiado de información requiere de una administración de su tratamiento y del mantenimiento del hardware. Este incluye la definición de políticas y procedimientos de operación para una gestión efectiva de la protección de datos de salida sensitivos, monitoreo de la infraestructura y mantenimiento preventivo del hardware.

Nivel de madurez: Inicial. El Organismo reconoce la necesidad de estructurar las funciones de soporte de TI. Sin embargo, no hay procedimientos estándares establecidos, las actividades de operación no están programadas y las respuestas son de tipo reactivo. La mayoría de las operaciones no están formalmente programadas y los pedidos de procesamiento se aceptan sin validación previa. Las computadoras que dan soporte a los procesos del Organismo, con frecuencia tienen interrupciones, demoras o no están disponibles. Los empleados pierden tiempo por tener que esperar los recursos.

Observaciones: No existen procedimientos formalmente definidos para operaciones de TI. No se encontró evidencia de la existencia de la programación de tareas que permita maximizar el rendimiento y la mejor utilización de los recursos informáticos.

No hay normas de desempeño, acuerdos de nivel de servicio del usuario ni procedimientos formales de mantenimientos de equipos.

No existe un plan de capacitación permanente para mantener sus competencias.

Por razones de fallas en los equipos de almacenamiento no se llevan copias de resguardo en forma regular, en el centro de cómputos del edificio ubicado en la calle Carlos Calvo dichas copias se realizan en discos rígidos de PC por estar fuera de servicio el equipo correspondiente.

4. MONITOREO.

4.1. Monitoreo de los Procesos.

Objetivo de control: La máxima autoridad debe impulsar la definición de indicadores del desempeño relevantes, el informe sistemático y oportuno y la acción inmediata en caso de desviaciones.

Nivel de madurez: No conforma. El Organismo no tiene ningún proceso de monitoreo implementado. La función de TI no realiza el monitoreo de los proyectos y procesos en forma independiente. No se cuenta con informes útiles, puntuales y precisos. No se reconoce la necesidad de fijar objetivos de gestión concretamente expresados.

Observaciones: No se realizan monitoreos de la utilización de los recursos informáticos 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.

4.2. Evaluación de la idoneidad del control interno.

Objetivo de control: Debe existir el compromiso del funcionario principal de servicios de información de monitorear los controles internos, evaluar su eficacia y realizar informes en forma periódica.

Nivel de madurez: No conforma. El Organismo carece de procedimientos para monitorear la eficacia de los controles internos. No se cuenta con métodos de informes de gestión en el área del control interno. La dirección y los empleados no ponderan la importancia del monitoreo de los controles internos.

Observaciones: Dada la inexistencia de controles internos formales tampoco existen procedimientos para su evaluación.

El proyecto de informe de auditoría fue enviado al organismo auditado para que formule las observaciones y/o comentarios que estime pertinentes, con fecha 3 de diciembre de 2009, por nota AGN N° 209/09-PCSPPEyCI. Los mismos fueron remitidos por el Instituto Nacional de Estadística y Censos, luego de la prórroga otorgada, a través de nota INDEC N° 00459 con fecha 19 de marzo de 2009. Como consecuencia del análisis del descargo presentado por el Organismo auditado, se ratifican las observaciones oportunamente formuladas.

La AGN efectúa las siguientes "Recomendaciones" a la Entidad:

1. PLANIFICACIÓN Y ORGANIZACIÓN.

1.1. Definición de un plan estratégico de TI: La Dirección de Informática debe implementar planes a corto y largo plazo que sean compatibles con la misión y las metas de la organización aprobadas por la dirección del Instituto. 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.

1.2. 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.

1.3. 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.

1.4. Definición de la organización y las relaciones de TI: Al ubicar la función de servicios de información dentro de la estructura del Organismo, la dirección debe garantizar autoridad, unicidad, 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.

1.5. Administración de la Inversión en TI: Debe implementarse 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.

1.6. Comunicación de los Objetivos y Directivas de la Gerencia: Se debe 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 la Dirección de Informática 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.

1.7. 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 la Dirección de Informática 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.

1.8. Garantía del cumplimiento de los requerimientos externos: La máxima autoridad y el Director de Informática 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 gobierno electrónico.

– El cumplimiento de los contratos de seguro.

1.9. Evaluación de Riesgos: Se debe establecer un marco de evaluación sistemática de riesgos. Dicho marco 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. La Dirección de Informática 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.

1.10. 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 dirección del Instituto 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.

1.11. 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 Dirección del Instituto y el director de Informática 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.

2. ADMINISTRACIÓN E IMPLEMENTACIÓN.

2.1. 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.

2.2. 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.

2.3. 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.

2.4. 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.

2.5. 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.

2.6. 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.

3. ENTREGA Y SOPORTE.

3.1. 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.

3.2. 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.

3.3. Administración de la Capacidad y el Desempeño: La dirección del Instituto y la Dirección de Informática 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.

3.4. 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 Dirección del Instituto y el director de Informática 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.

3.5. Garantía de la Seguridad de los Sistemas: La dirección del Instituto y la Dirección de informática 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.

3.6. Identificación e Implementación de Costos: La dirección del Instituto y la Dirección de Informática 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.

3.7. Educación y capacitación de los Usuarios: La Dirección del Instituto y la Dirección de Informática 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.

3.8. Asistencia y Asesoramiento a los Usuarios de TI: La Dirección de Informática 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.

3.9. Administración de la Configuración: La Dirección de Informática 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.

3.10. Administración de Problemas e Incidentes: La Dirección de Informática 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.

3.11. 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.

3.12. Administración de Instalaciones: La Dirección del Instituto y la Dirección de Informática 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.

3.13. Administración de Operaciones: La Dirección de Informática 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 debe 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.

4. MONITOREO.

4.1. Monitoreo de los Procesos: La Dirección del Organismo y la Dirección de Informática 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.

4.2. Evaluación de la idoneidad del control interno: La Dirección del Organismo y la Dirección de Informática 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, como resultado de las observaciones efectuadas, análisis del descargo del organismo y de las recomendaciones formuladas, arriba a las siguientes conclusiones:

El INDEC es un organismo con más de 40 años de existencia, creado en 1968 por la ley 17.622 donde se la asigna la dirección superior de todas las actividades estadísticas oficiales y la coordinación del Sistema Estadístico Nacional. Su función es básicamente recabar grandes volúmenes de información y procesarla para obtener estadísticas de nivel nacional por lo cual es recomendable una utilización esmerada de las mejores prácticas en Tecnología de la Información. Y si bien, en esa época el desarrollo de la informática era muy incipiente por lo cual tal tecnología no es mencionada ni en la ley y ni en sus decretos reglamentarios, tal circunstancia no debería ser motivo para que el Organismo no esté debidamente equipado con elementos de última generación y capacitado para cumplir correctamente con sus misiones y funciones.

Como resultado de la auditoría se concluye entre otros hallazgos, que:

– El equipamiento, en promedio, está desactualizado diez años y existe una política arbitraria de distribución de equipos nuevos.

– La red de datos está desactualizada tres generaciones, lo que pone en riesgo la información que circula por ella. De hecho, ya no era de última tecnología cuando se procedió a su instalación en el año 1993.

– La dispersión que existe entre diferentes tecnologías de bases de datos que se utilizan, algunas discontinuadas desde hace años, impide su integridad y la compatibilidad entre los sistemas del Instituto.

Agrava la situación la falta de un correcto mantenimiento de la red, del hardware y del software.

En cuanto a su organización aparece como internamente descentralizado en el tema informático. De las siete direcciones nacionales que dependen de la Dirección del Organismo, tres de ellas tienen su propio sector de desarrollo de sistemas:

– Dirección Nacional de Estadísticas del Sector Externo (Comercio Exterior).

– Dirección Nacional de Estadísticas y Precios de la Producción y el Comercio.

– Dirección Nacional de Estadísticas de Condiciones de Vida (IPC).

Estas direcciones no responden al director de Informática, programan y mantienen sus aplicaciones y operan sus datos manteniendo un nivel de independencia, que impide un funcionamiento orgánico del conjunto y provoca un riesgo adicional a los mencionados.

La auditoría interna se realiza desde el Ministerio de Economía y no tiene el impacto necesario en el Organismo.

En síntesis, existen riesgos altos de falta de eficiencia y aun de falta de eficacia en la concreción de las responsabilidades del Organismo y, en general, la información está sometida a riesgos que superan los valores aceptables.

Para superar el actual estado de situación, es necesario darle prioridad a:

– La definición de la estructura organizativa 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, apuntando fundamentalmente a la unicidad de mando, centralizándolo en la dirección del área informática.

– La actualización tecnológica del Organismo para superar rápidamente el estado de obsolescencia en que se encuentra.

– Tender a que la madurez de la calidad de la gestión se aproxime, cuanto menos, al nivel de “Procesos definidos” (ver Anexo IV Niveles del Modelo Genérico de Madurez).

– 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.

– La actualización de la ley de creación del Organismo en forma que incluya, por lo menos, la arquitectura de la información y el modelo de datos básico a emplear para la gestión del sistema estadístico nacional y los niveles de calidad mínima y de obsolescencia máxima de los soportes tecnológicos y de la infraestructura operativa.

La evaluación realizada con el modelo genérico de madurez indica que el 96,9 % 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". El nivel de riesgo promedio para los 7 requerimientos de la información calculado para los 32 objetivos de control ponderados resultó de 74 % cuando lo aceptable es no superar el 20 %.

Para corregir las falencias detectadas es imprescindible un fuerte compromiso de las máximas autoridades del INDEC para organizar los servicios de TI y de las autoridades del Ministerio para proveer los recursos necesarios.

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

ANTECEDENTES

Ver expedientes 1.716-D.-2011 y 307-O.V.-2010.