



# Auditoría General de la Nación

## INFORME DE AUDITORÍA

A Lic. Ana María Edwin  
Directora  
Instituto Nacional de Estadística y Censos.

En uso de las facultades conferidas por el artículo 118 de la Ley 24.156, la AUDITORÍA GENERAL DE LA NACIÓN efectuó un examen en el ámbito del Ministerio de Economía y Finanzas Públicas de la Nación, con el objeto que se detalla en el apartado 1.

### **1. – Objeto de la auditoría**

Evaluación de la gestión de la Tecnología de la Información (TI) en el Instituto Nacional de Estadística y Censos –INDEC–, organismo dependiente del Ministerio de Economía y Finanzas Públicas de la Nación, con el objeto de determinar la calidad de la administración de la información en el Organismo.

### **2. – Alcance del examen**

El examen fue realizado de conformidad con las normas de auditoría externa de la AUDITORÍA GENERAL DE LA NACIÓN, aprobadas por la Resolución N° 145/93, dictada en virtud de las facultades conferidas por el artículo 119, inciso d) de la Ley 24.156.

Se basó la tarea 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.

**2.1.-** En la etapa de planificación identificamos los temas de mayor exposición al riesgo realizando las siguientes actividades:



# Auditoría General de la Nación

- Relevamiento de la documentación normativa del área de tecnología informática del Organismo.
- Relevamiento de la infraestructura informática del Organismo.
- Relevamiento de los sistemas existentes en producción y desarrollo.
- Verificación de la adecuación de los sistemas, la infraestructura y la planificación para lograr las misiones y metas del Organismo y cumplir con las leyes y decretos que regulan su actividad.
- Verificación del modelo de arquitectura de la información y su seguridad.
- Relevamiento y análisis del organigrama del área de tecnología informática y su funcionamiento.
- Verificación del cumplimiento de la comunicación de los objetivos y las directivas de la Gerencia.
- Análisis de la administración de recursos humanos, el cumplimiento de los requerimientos externos, la evaluación de riesgos, la administración de proyectos, la administración de calidad y las prácticas de instalación y acreditación de sistemas y de administración de cambios.
- Análisis de:
  - la definición de los niveles de servicio,
  - la administración de los servicios prestados por terceros,
  - la administración de la capacidad y el desempeño,
  - los mecanismos que garantizan el servicio continuo y la seguridad de los sistemas,
  - la imputación de costos,
  - la educación y capacitación de los usuarios,
  - la asistencia a los clientes de la Tecnología de la Información,
  - la administración de la configuración de *hardware* y *software*,
  - la administración de problemas e incidentes,
  - la administración de datos, de instalaciones y de operaciones.
- Análisis del control de los procesos, la idoneidad del control interno y de su monitoreo.

**2.2.** - Se obtuvo información de las siguientes fuentes:



## Auditoría General de la Nación

- Entrevistas con la Directora del INDEC y el Director Técnico del INDEC, los responsables del sector informático central y responsables de desarrollo, soporte y mantenimiento. Entrevistas con los distintos Directores Nacionales del Instituto y sus respectivos responsables de sistemas.
- Cuestionario para determinar las necesidades de análisis detallado.
- Cuestionarios para el análisis detallado de los temas que lo requerían.
- Inspecciones directas en el área informática central para determinar las condiciones actuales de la administración de la información en el Organismo.

**2.3.- Limitaciones:** No se pudo verificar la implementación de la defensa de la red informática contra ataques externos. Su programación, en atención a que se le hace mantenimiento a sus bases de datos en forma remota, fue solicitada por esta Auditoría y resultó denegada por la Dirección del Instituto por nota, sin número, del 11 de noviembre de 2009. Cabe destacar que no se consideró apropiado hacer el test de penetración sugerido en dicha nota pues podría generar inconvenientes no deseados al Organismo (denegación de servicio, pérdida de datos, interferencias en las aplicaciones, etc.).

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

**2.4.- Metodología:** La auditoría incluyó dos etapas: la primera, de planificación del análisis detallado; la segunda, de verificación de lo informado en la primera etapa, por medio de pruebas sustantivas y de cumplimiento.

La etapa de planificación incluyó las siguientes actividades:

- Análisis del marco legal e institucional del funcionamiento del Instituto.
- Análisis de los informes de Auditoría Interna y Externa en temas informáticos.
- Entrevistas con la Directora y con responsables del área informática.
- Análisis de las minutas de reunión para determinar las necesidades de análisis detallado.

En la etapa de verificación:

- Inspecciones in situ y entrevistas con personal subalterno, realizadas por especialistas en diversas ramas de la informática a través del trabajo directo en el campo.
- Entrevistas con usuarios internos de los servicios informáticos.

En función de la información relevada y los niveles de riesgo estimados se definieron los



# Auditoría General de la Nación

trabajos de campo convenientes para realizar las verificaciones necesarias.

## **3. – Aclaraciones previas**

### **3.1. – Marco legal e institucional**

El Instituto Nacional de Estadística y Censos, INDEC, fue creado en 1968 mediante la ley N° 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, debe coordinar el Sistema Estadístico Nacional -SEN-, bajo el principio del desarrollo de métodos de captación de datos y normas para la producción de estadísticas oficiales (censos, encuestas, registros, etc.), permitiendo de este modo la confección de indicadores con relación a diferentes áreas temáticas.

Conforme el art. 3° de la ley de creación son objetivos del Instituto Nacional de Estadística y Censos:

- a) Unificar la orientación y ejercer la dirección superior de todas las actividades estadísticas oficiales que se realicen en el territorio de la Nación;
- b) Estructurar, mediante la articulación y coordinación de los servicios estadísticos nacionales, provinciales y municipales, el sistema estadístico nacional, y ponerlo en funcionamiento de acuerdo con el principio de centralización normativa y descentralización ejecutiva.

La ley de creación establece en su Art. 10° “el secreto estadístico” de las informaciones que sean suministradas a los organismos que integran el SEN, de modo que no pueda ser violado el secreto comercial o patrimonial, ni individualizarse las personas o entidades a quienes se refieran, quedando exceptuados de aquél: nombre y apellido o razón social, domicilio y rama de la actividad.

De la Directora del INDEC dependen a través del Director Técnico:

Dirección Nacional de Cuentas Internacionales

Dirección Nacional de Cuentas Nacionales

Dirección Nacional de Estadísticas y Precios de la producción y el comercio

Dirección Nacional de Planificación y Coordinación Estadística

Dirección Nacional de Estadísticas del Sector Externo



# Auditoría General de la Nación

Dirección Nacional de Estadísticas Sociales y de Población  
Dirección Nacional de Estadísticas de Condiciones de Vida  
Dirección Nacional de Recursos Humanos y Organización  
Dirección General de Administración y Operaciones  
Dirección de Metodología Estadística  
Dirección de Informática  
Dirección de Asuntos Jurídicos  
Dirección de Difusión

Las Direcciones Nacionales son responsables de coordinar con los institutos de estadística de las provincias conformando el SEN.

## **4. – Comentarios y observaciones**

Para cada una de las Observaciones se menciona el nivel de madurez que le corresponde, conforme al Modelo de Madurez de la Capacidad incluido en el Anexo IV. En el punto 6, se encuentran las Recomendaciones para mejorar el ambiente de control y reducir los riesgos.

Además, para cada uno de los objetivos de control, se indica qué requerimientos de la información (detallados en el Anexo V) son afectados.

Se destaca que cada objetivo de control va acompañado de su nivel de riesgo genérico (alto, medio o bajo) que le es propio, poniendo en evidencia el impacto provocado por su incumplimiento y sin estar vinculado con la situación del Organismo. Ese nivel genérico es modificado por el índice de madurez correspondiente (dependiente de las observaciones realizadas) para establecer el riesgo específico para ese objetivo, en el caso particular. Puede observarse en los gráficos del anexo que un objetivo de control que tiene implícito un riesgo genérico alto y fue calificado con un índice de madurez alto, genera un riesgo específico menor que aquel que tenga un riesgo genérico medio o bajo y un índice de madurez bajo.

### **4.1. – Planificación y organización**

#### **4.1.1. – 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



## Auditoría General de la Nación

deben traducirse oportunamente en planes operativos que definan metas claras y concretas a corto plazo.

Este objetivo de control afecta, primariamente:

- la eficacia

y en forma secundaria:

- la eficiencia.

**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. La alineación de los requerimientos del Organismo, las aplicaciones y los análisis de la dirección tecnológica, se realizan en forma reactiva y no por una estrategia para toda la organización. La posición de riesgo estratégico se identifica informalmente proyecto por proyecto.

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

**Nivel de riesgo:**                     Alto         Medio         Bajo

### 4.1.2. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia

y en forma secundaria:

- la eficiencia
- la confidencialidad
- la integridad

**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



# Auditoría General de la Nación

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.

**Nivel de riesgo:**  Alto  Medio  Bajo

## 4.1.3. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia

y en forma secundaria:

- la eficiencia

**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.



## Auditoría General de la Nación

**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.

**Nivel de riesgo:**  Alto  Medio  Bajo

### 4.1.4. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia

**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



# Auditoría General de la Nación

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.

**Nivel de riesgo:**  Alto  Medio  Bajo

## 4.1.5. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la confiabilidad

**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.

**Nivel de riesgo:**  Alto  Medio  Bajo



## Auditoría General de la Nación

### 4.1.6. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia

y en forma secundaria:

- el cumplimiento

**Nivel de madurez:** *No Conformar*. 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,
- políticas formales 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.

**Nivel de riesgo:**                     Alto                     Medio                     Bajo

### 4.1.7. – 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.



# Auditoría General de la Nación

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia

**Nivel de madurez:** *No Conformar*. 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.

**Nivel de riesgo:**  Alto  Medio  Bajo

## 4.1.8.- 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- el cumplimiento

y en forma secundaria:

- la confiabilidad

**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,



# Auditoría General de la Nación

- garantizar el cumplimiento de las exigencias de los contratos de seguros,
- cumplimiento de las normas para TI dictadas por la Oficina Nacional de Tecnología de la Información.

**Nivel de riesgo:**                     Alto         Medio         Bajo

## 4.1.9. – 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.

Este objetivo de control afecta, primariamente:

- la confidencialidad
- la integridad
- la disponibilidad

y en forma secundaria:

- la eficacia
- la eficiencia
- el cumplimiento
- la confiabilidad

**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.



# Auditoría General de la Nación

**Nivel de riesgo:**  Alto  Medio  Bajo

## 4.1.10. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia

**Nivel de madurez:** *No Conformar*. 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.

**Nivel de riesgo:**  Alto  Medio  Bajo

## 4.1.11. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia
- la integridad

y en forma secundaria:

- la confiabilidad



# Auditoría General de la Nación

**Nivel de madurez:** *No Conformar.* 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.

**Nivel de riesgo:**  Alto  Medio  Bajo

## 4.2. – Administración e implementación

### 4.2.1. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia

y en forma secundaria:

- la eficiencia

**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.



# Auditoría General de la Nación

**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.

**Nivel de riesgo:**  Alto  Medio  Bajo

## 4.2.2. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la integridad
- el cumplimiento
- la confiabilidad

**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



## Auditoría General de la Nación

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.

**Nivel de riesgo:**                     Alto             Medio             Bajo

### 4.2.3. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la integridad

**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



## Auditoría General de la Nación

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.
- 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.

**Nivel de riesgo:**                     Alto         Medio         Bajo

### 4.2.4. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la integridad
- el cumplimiento
- la confiabilidad



# Auditoría General de la Nación

**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.

**Nivel de riesgo:**  Alto  Medio  Bajo

## 4.2.5. – 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 post-implantación. Esto garantiza que los sistemas estén en línea con las expectativas convenidas y con los resultados esperados.

Este objetivo de control afecta, primariamente:

- la eficacia

y en forma secundaria:

- la integridad
- la disponibilidad

**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.



## Auditoría General de la Nación

**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 4.1.4, 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.

**Nivel de riesgo:**  Alto  Medio  Bajo

### 4.2.6. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia
- la integridad
- la disponibilidad

y en forma secundaria:

- la confiabilidad



# Auditoría General de la Nación

**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.

**Nivel de riesgo:** [ ] Alto [X] Medio [ ] Bajo

## 4.3. – Entrega y Soporte

### 4.3.1. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la confidencialidad
- la integridad
- la disponibilidad
- el cumplimiento
- la confiabilidad

**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.



# Auditoría General de la Nación

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

**Nivel de riesgo:** [ ] Alto [X] Medio [ ] Bajo

## 4.3.2. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la confidencialidad
- la integridad
- la disponibilidad
- el cumplimiento
- la confiabilidad

**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



## Auditoría General de la Nación

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.

**Nivel de riesgo:**  Alto  Medio  Bajo

### 4.3.3. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la disponibilidad

**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.

**Nivel de riesgo:**  Alto  Medio  Bajo



## Auditoría General de la Nación

### 4.3.4. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- la disponibilidad

y en forma secundaria:

- la eficiencia

**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.



## Auditoría General de la Nación

Nivel de riesgo:                     Alto         Medio         Bajo

### 4.3.5. – 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.

Este objetivo de control afecta, primariamente:

- la confidencialidad
- la integridad

y en forma secundaria:

- la disponibilidad
- el cumplimiento
- la confiabilidad

**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.



## Auditoría General de la Nación

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.

**Nivel de riesgo:**  Alto  Medio  Bajo

### 4.3.6. – 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.

Este objetivo de control afecta, primariamente:

- la eficiencia
- la confiabilidad

**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.

**Nivel de riesgo:**  Alto  Medio  Bajo

### 4.3.7. – Educación y Capacitación de los Usuarios

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

Este objetivo de control afecta, primariamente:



## Auditoría General de la Nación

- la eficacia

y en forma secundaria:

- la eficiencia

**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.

**Nivel de riesgo:**                     Alto         Medio         Bajo

### 4.3.8. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia

**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.



## Auditoría General de la Nación

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.

**Nivel de riesgo:**                     Alto             Medio             Bajo

### 4.3.9. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia

y en forma secundaria:

- la disponibilidad
- la confiabilidad

**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 entregó 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.



## Auditoría General de la Nación

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.

**Nivel de riesgo:**  Alto  Medio  Bajo

### 4.3.10. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la disponibilidad

**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.

**Nivel de riesgo:**  Alto  Medio  Bajo

### 4.3.11. – 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.

Este objetivo de control afecta, primariamente:



## Auditoría General de la Nación

- la integridad
- la confiabilidad

**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.

**Nivel de riesgo:**                     Alto             Medio             Bajo

### 4.3.12. – 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.

Este objetivo de control afecta, primariamente:

- la integridad
- la disponibilidad

**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



## Auditoría General de la Nación

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.

**Nivel de riesgo:**                     Alto             Medio             Bajo

### 4.3.13. – 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



## Auditoría General de la Nación

protección de datos de salida sensitivos, monitoreo de la infraestructura y mantenimiento preventivo del *hardware*.

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la integridad
- la disponibilidad

**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.

**Nivel de riesgo:**                     Alto             Medio             Bajo



# Auditoría General de la Nación

## 4.4. – Monitoreo

### 4.4.1. – 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.

Este objetivo de control afecta, primariamente:

- la eficacia

y en forma secundaria:

- la eficiencia
- la confidencialidad
- la integridad
- la disponibilidad
- el cumplimiento
- la confiabilidad

**Nivel de madurez:** *No Conformar*. 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.

**Nivel de riesgo:**                     Alto         Medio         Bajo

### 4.4.2. – 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.



# Auditoría General de la Nación

Este objetivo de control afecta, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la confidencialidad
- la integridad
- la disponibilidad
- el cumplimiento
- la confiabilidad

**Nivel de madurez:** *No Conformar*. 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.

**Nivel de riesgo:**                     Alto             Medio             Bajo

## **5. – Comunicación del proyecto de informe y análisis de los descargos formulados por el Instituto Nacional de Estadística y Censos**

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 (que consta como Anexo VI), se ratifican las observaciones oportunamente formuladas.



# Auditoría General de la Nación

## 6. – Recomendaciones

### 6.1. – Planificación y organización

**6.1.1. – 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.

**6.1.2. – 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.

**6.1.3. – 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.

**6.1.4. – 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,



# Auditoría General de la Nación

- 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.

**6.1.5. – 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.

**6.1.6. – 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:

- la 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,



## Auditoría General de la Nación

- 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.

**6.1.7. – 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.

**6.1.8. – 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.



## Auditoría General de la Nación

**6.1.9. – 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 riesgos 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.

**6.1.10. – 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.

**6.1.11. – 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:



# Auditoría General de la Nación

- 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.

## **6.2. – Administración e implementación**

**6.2.1. – 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



## Auditoría General de la Nación

- Implementar un proceso estructurado de análisis de requerimientos.
- Considerar los requerimientos de seguridad y control desde el principio.

**6.2.2. – 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

**6.2.3. – 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.

**6.2.4. – 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.

**6.2.5. – 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,



## Auditoría General de la Nación

- 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.

**6.2.6. – 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.



# Auditoría General de la Nación

## **6.3. – Entrega y Soporte**

**6.3.1. – 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.

**6.3.2. – 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.

**6.3.3. – 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,



## Auditoría General de la Nación

- la realización de pronósticos de la carga de trabajo,
- administración de la capacidad de los recursos,
- establecer la disponibilidad de recursos,
- planificación de recursos.

**6.3.4. – 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.

**6.3.5. – 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,



## Auditoría General de la Nación

- 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.

**6.3.6. – 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.

**6.3.7. – 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.



## Auditoría General de la Nación

**6.3.8. – 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.

**6.3.9. – 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*.

**6.3.10. – 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.

**6.3.11. – 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:



## Auditoría General de la Nación

- 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.



## Auditoría General de la Nación

**6.3.12. – 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.

**6.3.13. – 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



# Auditoría General de la Nación

- salvaguardia de formularios especiales y dispositivos de salida
- operaciones remotas

## **6.4. – Monitoreo**

**6.4.1. – 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.

**6.4.2. – 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.

## **7. – 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



## Auditoría General de la Nación

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.



## Auditoría General de la Nación

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” (ver Anexo IV). El nivel de riesgo promedio (ver Anexo II) 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.



# Auditoría General de la Nación

## 8. – LUGAR Y FECHA

BUENOS AIRES, 11 DE AGOSTO DE 2010.

## 9. – FIRMA



# Auditoría General de la Nación

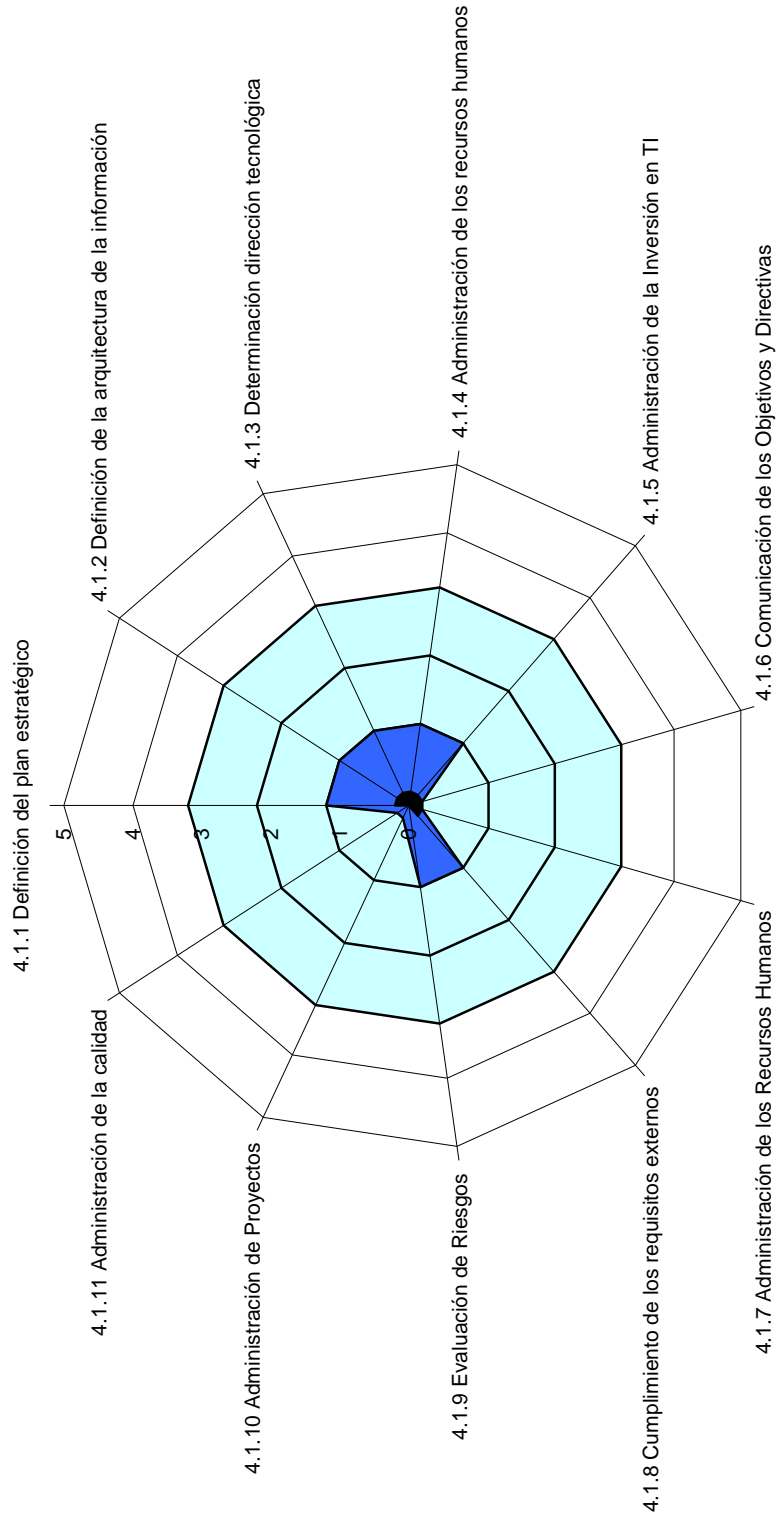
## Anexo I

**Gráficos de brecha para los niveles de madurez de los objetivos de control evaluados.**



# Auditoría General de la Nación

## Diagrama de brechas en Planificación y Organización

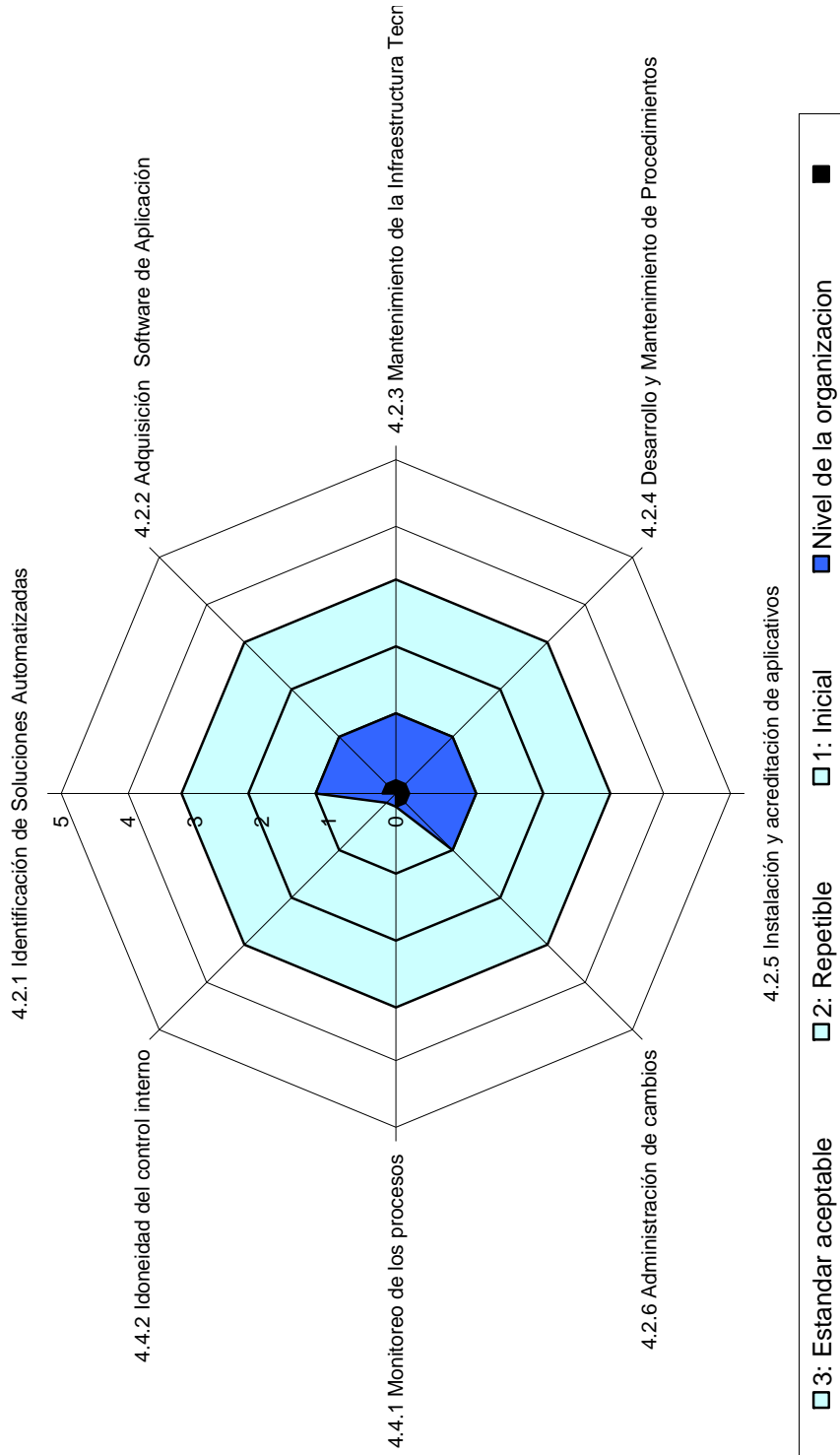


■ 3: Estandar aceptable    □ 2: Repetible    □ 1: Inicial    ■ Nivel de la organización



# Auditoría General de la Nación

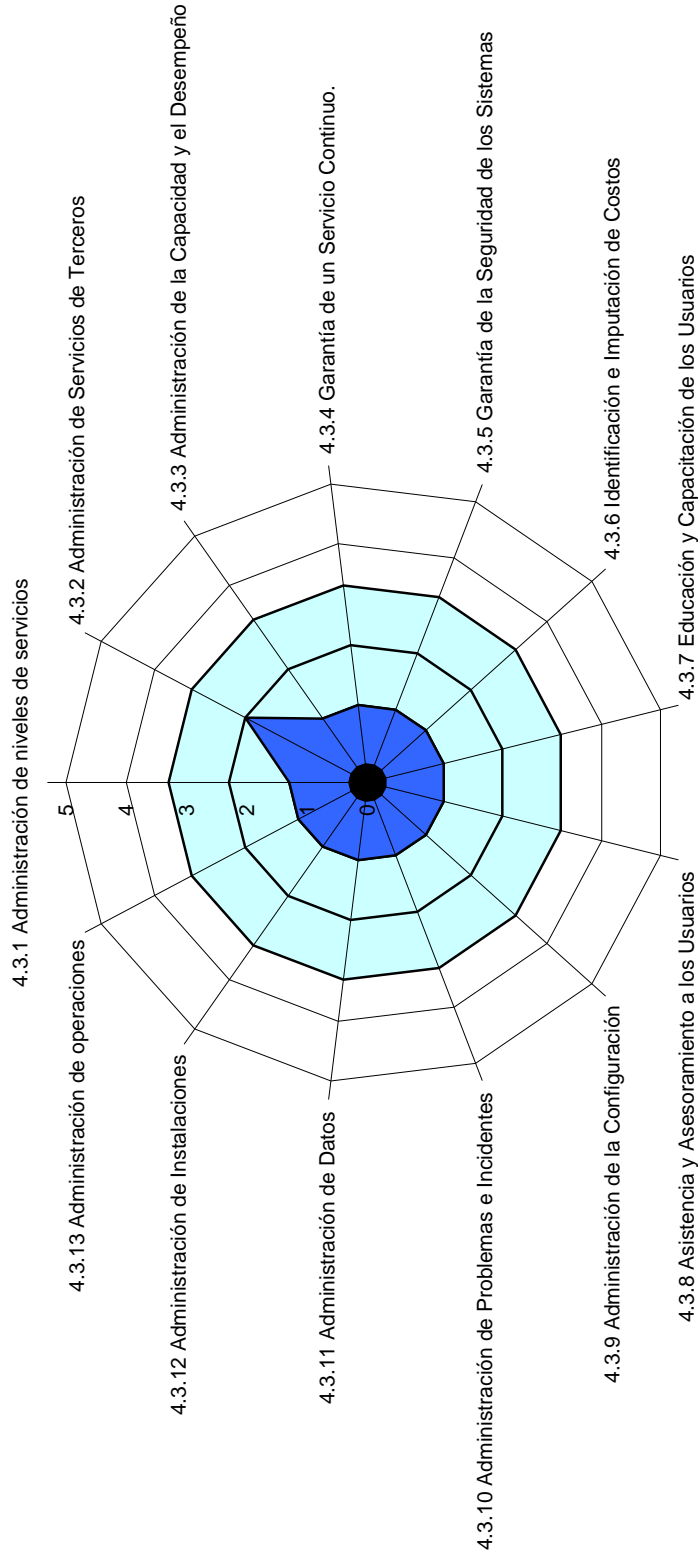
## Diagrama de brechas en Adquisición e Implementación y en Monitoreo





# Auditoría General de la Nación

## Diagrama de brechas en Entrega y Soporte



■ 3: Estandar aceptable    □ 2: Repetible    □ 1: Inicial    ■ Nivel de la organización



# Auditoría General de la Nación

## **Anexo II: Estimación de los Niveles de Riesgo para los requerimientos de la información según los procesos informáticos considerados**

La alta velocidad con la que se producen los cambios en la tecnología informática hace necesario optimizar la gestión de los riesgos relacionados con ella. Las misiones y funciones críticas de los organismos dependen en forma creciente de los sistemas de TI en un ambiente donde también aumentan las noticias sobre fraudes y desastres informáticos. En la actualidad se entiende que la gestión de riesgos relacionados con la TI es un elemento esencial de la administración del Estado Nacional.

En esta auditoría se trabajó sobre treinta y dos objetivos de control, cada uno de los cuales se corresponde con un proceso de tecnología informática.

Cada proceso hace a uno o más de los requerimientos que debe satisfacer la información dentro de un organismo para permitirle cumplir con sus misiones y funciones (ver Anexo V).

En los treinta y dos casos se indica dentro de las observaciones que requerimientos son afectados en forma primaria y secundaria por el objetivo de control (ver Tabla I).

El objeto de este Anexo es brindar parámetros cuantificables para establecer un Tablero de Control que posibilite conocer los problemas con mayor riesgo y al mismo tiempo controlar las mejoras que se produzcan en el futuro en forma explícita.

Se entiende como riesgo de un requerimiento a un valor que simboliza la probabilidad de que la información carezca del mencionado requisito. Este valor fluctúa entre cero y uno, siendo cero la situación más segura y uno la más insegura.

El proceso de cálculo parte de la base de que el riesgo es directamente proporcional al impacto definiendo como impacto el peligro de incumplimiento de las misiones y funciones del Organismo, para los procesos involucrados en el objetivo de control, y a la probabilidad de ocurrencia del evento.

Para cada uno de los procesos se definió el impacto como alto (99%), medio (66%) o bajo (33%).



## Auditoría General de la Nación

La probabilidad de ocurrencia está directamente vinculada a la calidad del control que se realiza, y éste es evaluado en el informe a través del nivel alcanzado según el modelo de madurez. A cada nivel se le asignó un coeficiente según el siguiente detalle:

<b>Nivel de Madurez</b>	<b>Coeficiente</b>
No conforma	1,00
Inicial	0,80
Repetible	0,50
Proceso Definido	0,30
Administrado	0,20
Optimizado	0,10



# Auditoría General de la Nación

Tabla I

Dominio	Proceso	Requerimiento de la información								
		eficacia	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	contabilidad		
Planeamiento y Organización	4.1.1	Definir un plan estratégico de sistemas	P	S						
	4.1.2	Definir la arquitectura de la información	P	S	S	S				
	4.1.3	Determinar la dirección tecnológica	P	S						
	4.1.4	Definir la organización y sus relaciones	P	S						
	4.1.5	Administrar las inversiones (en TI)	P	P						S
	4.1.6	Comunicar la dirección y objetivos de la gerencia	P						S	
	4.1.7	Administrar los recursos humanos	P	P						
	4.1.8	Garantizar el cumplimiento de los requisitos externos.	P		S				P	
	4.1.9	Evaluar riesgos	S	S	P	P	P	S	S	
	4.1.10	Administrar proyectos	P	P						
	4.1.11	Administrar calidad	P	P		P				S
Adquisición e Implementación	4.2.1	Identificar soluciones de automatización	P	S						
	4.2.2	Adquirir y mantener <i>software</i> de aplicación	P	P		S		S	S	
	4.2.3	Adquirir y mantener la arquitectura tecnológica	P	P		S				
	4.2.4	Desarrollar y mantener procedimientos	P	P		S		S	S	
	4.2.5	Instalar y acreditar sistemas de información	P			S	S			
	4.2.6	Administrar cambios	P	P		P	P			S
Entrega y Soporte de Servicios	4.3.1	Definir niveles de servicio	P	P	S	S	S	S	S	S
	4.3.2	Administrar servicios de terceros	P	P	S	S	S	S	S	S
	4.3.3	Administrar desempeño y capacidad	P	P			S			
	4.3.4	Asegurar continuidad de servicio	P	S			P			
	4.3.5	Garantizar la seguridad de sistemas			P	P	S	S	S	
	4.3.6	Identificar y asignar costos		P						P
	4.3.7	Educar y capacitar a usuarios	P	S						
	4.3.8	Apoyar y orientar a clientes	P							
	4.3.9	Administrar la configuración	P				S			S
	4.3.10	Administrar problemas e incidentes	P	P			S			
	4.3.11	Administrar la información				P				P
	4.3.12	Administrar las instalaciones				P	P			
	4.3.13	Administrar la operación	P	P		S	S			
Monitoreo	4.4.1	Monitorear el proceso	P	S	S	S	S	S	S	
	4.4.2	Evaluar idoneidad del monitoreo	P	P	S	S	S	S	S	



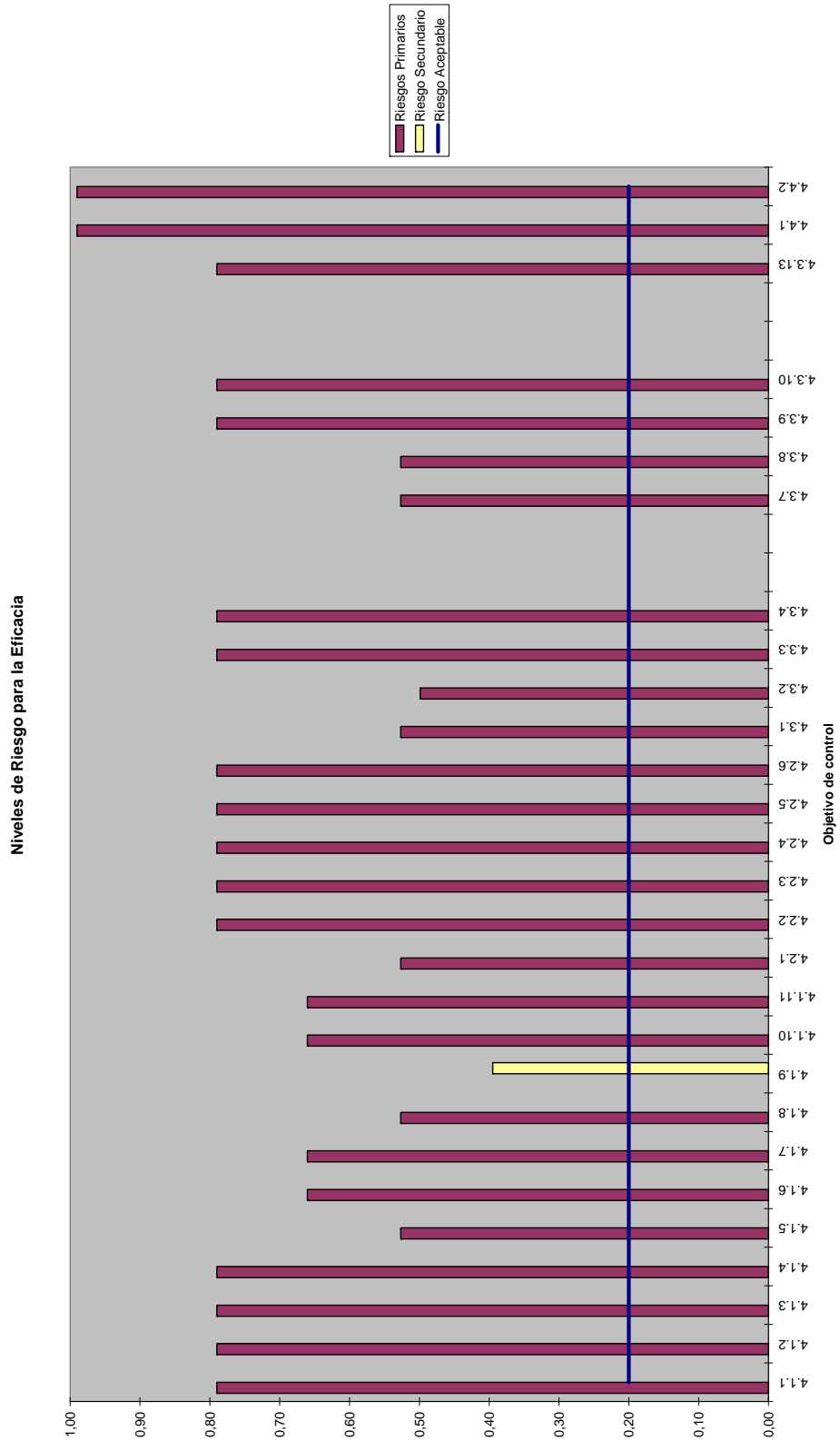
# Auditoría General de la Nación

## Anexo III

**Gráficos de los niveles de riesgo de cada uno de los requerimientos de la información para los 32 objetivos de control ponderados y su promedio general.**

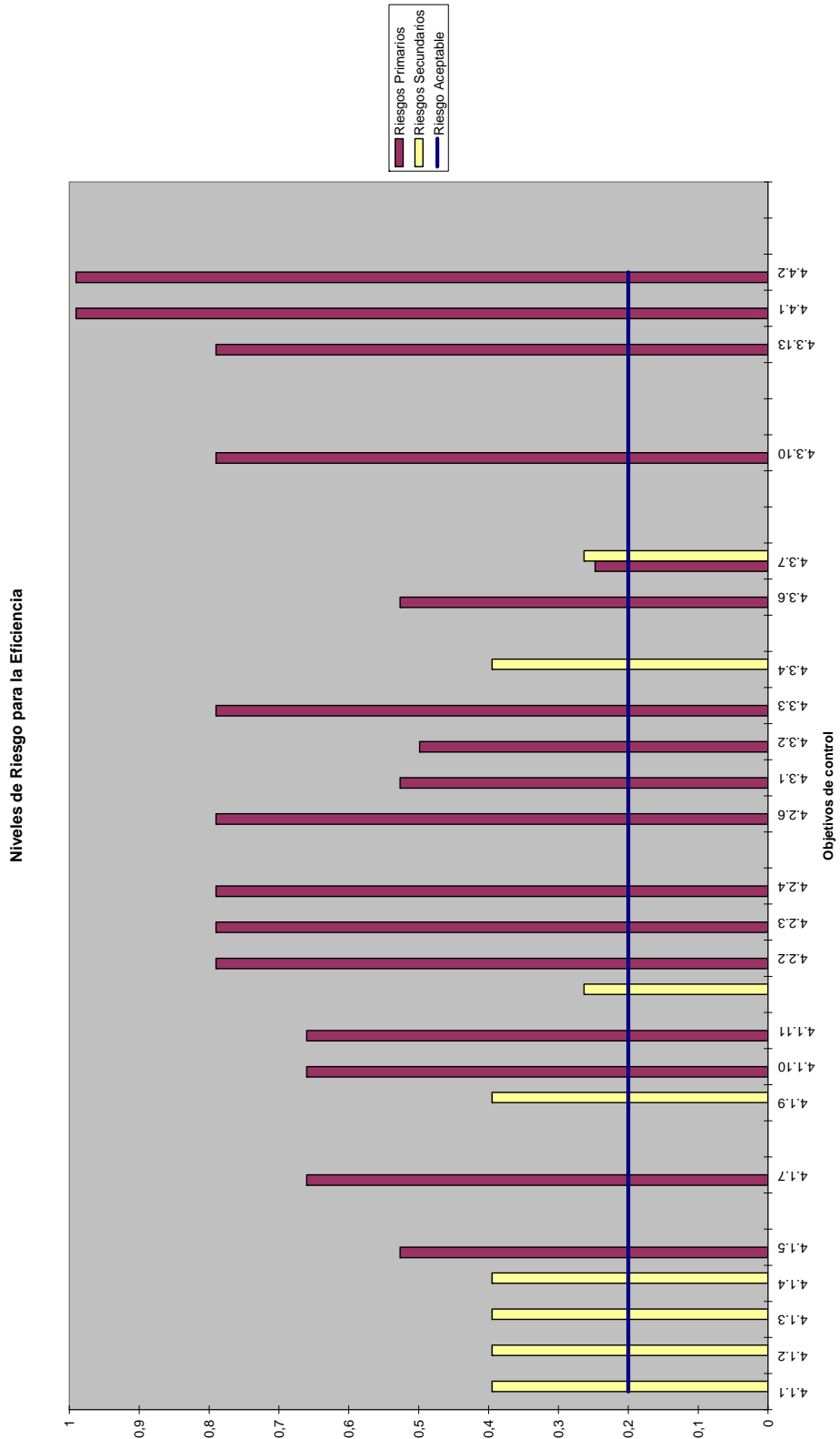


# Auditoría General de la Nación



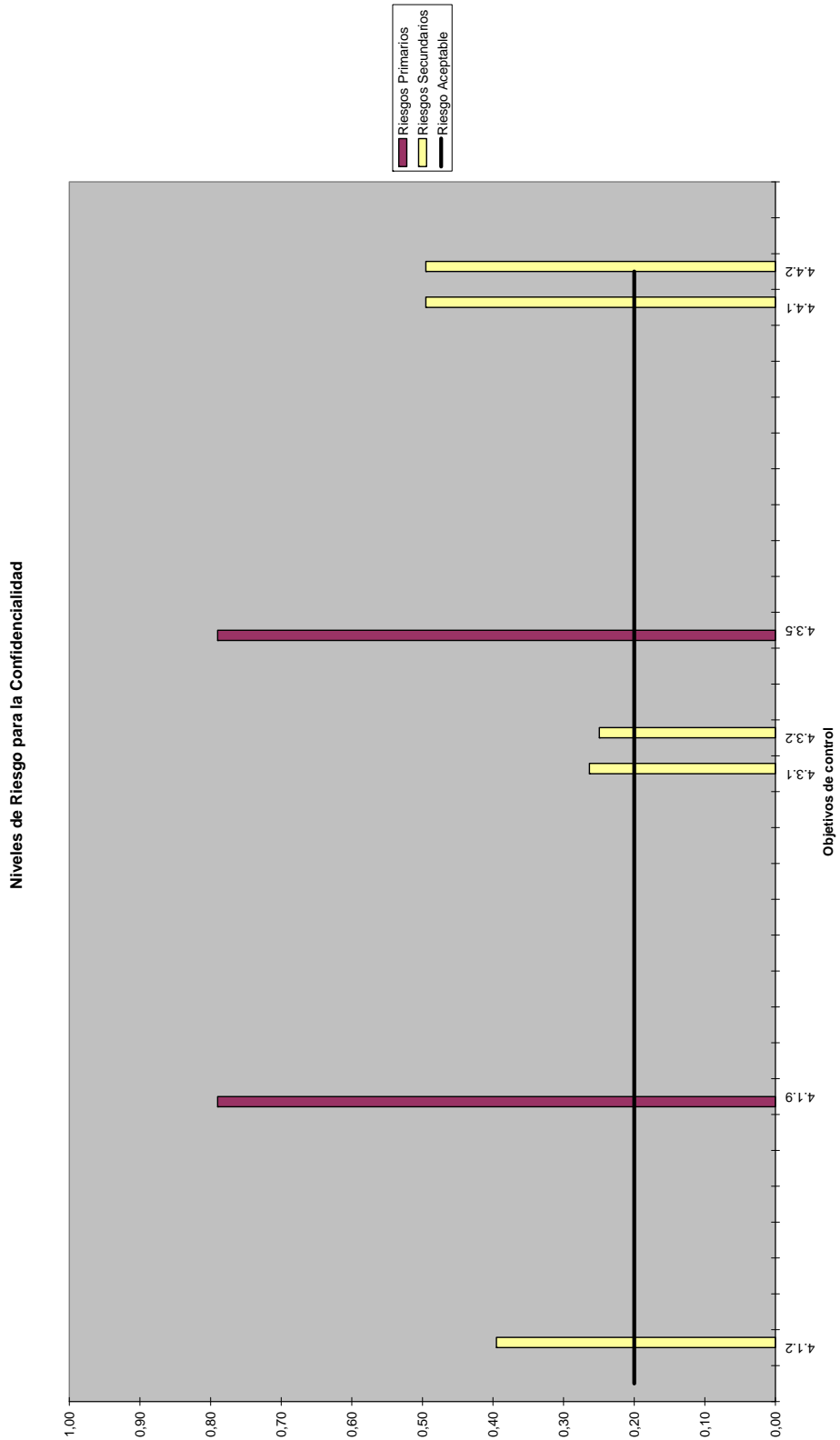


# Auditoría General de la Nación



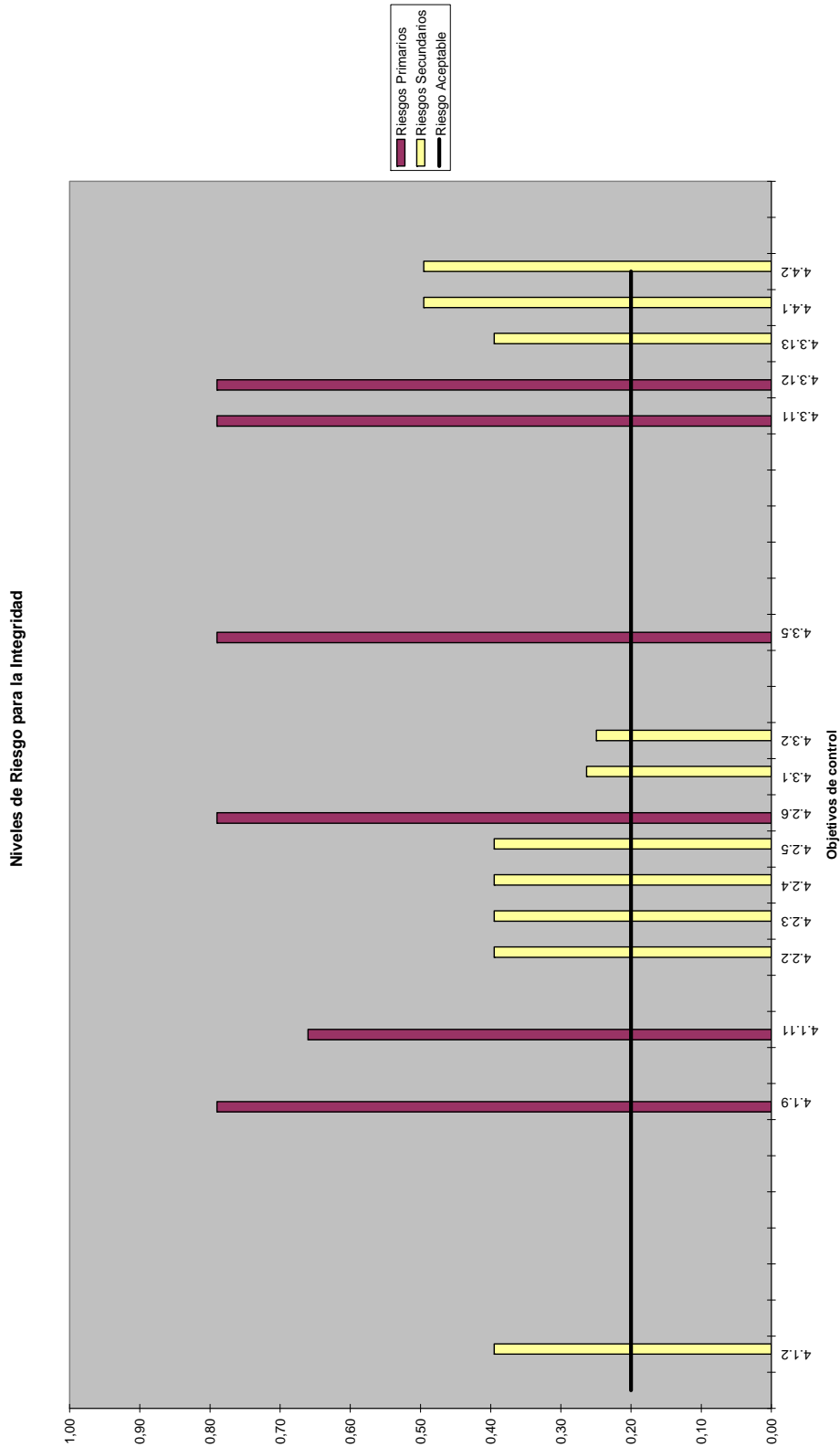


# Auditoría General de la Nación



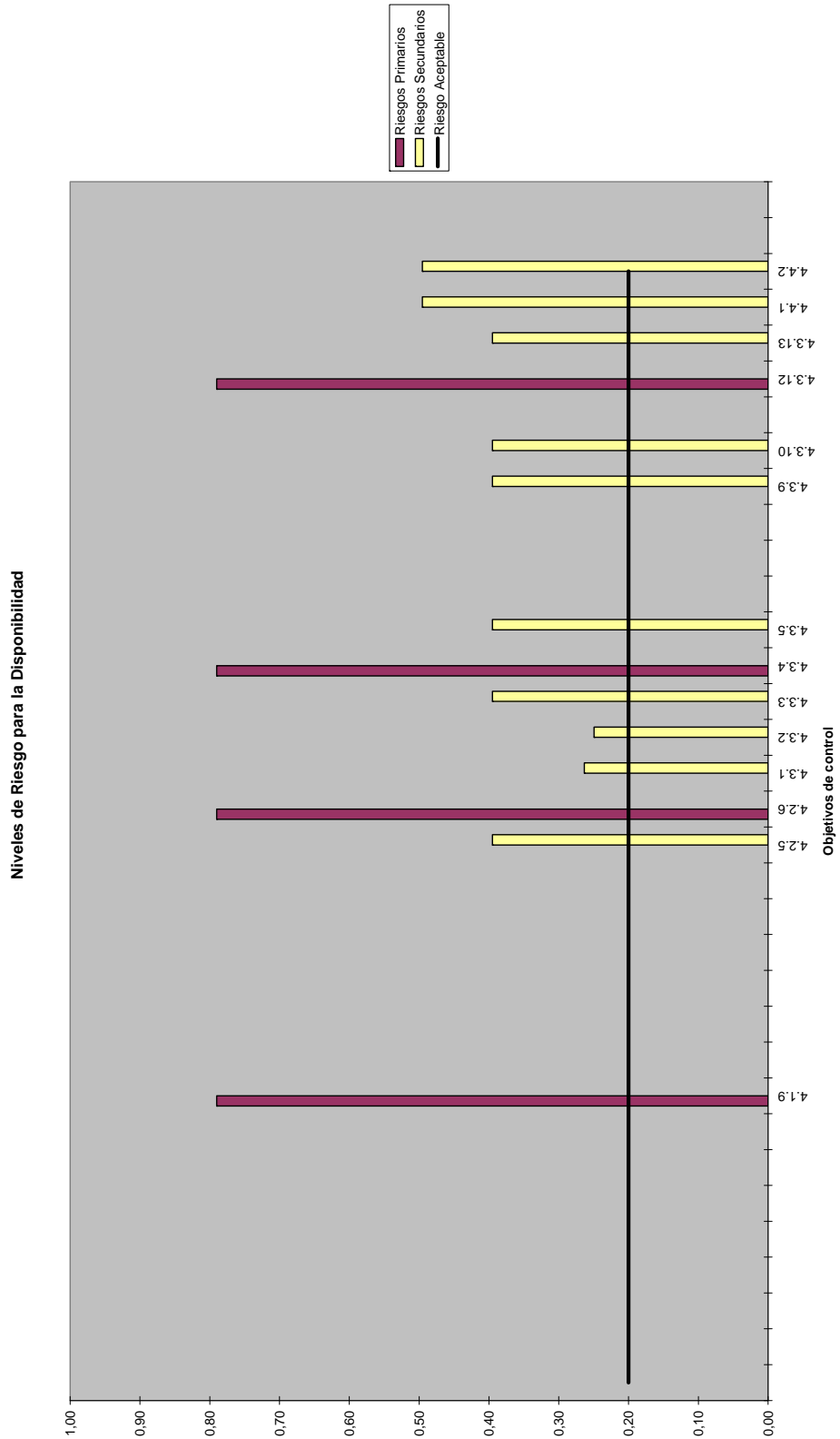


# Auditoría General de la Nación



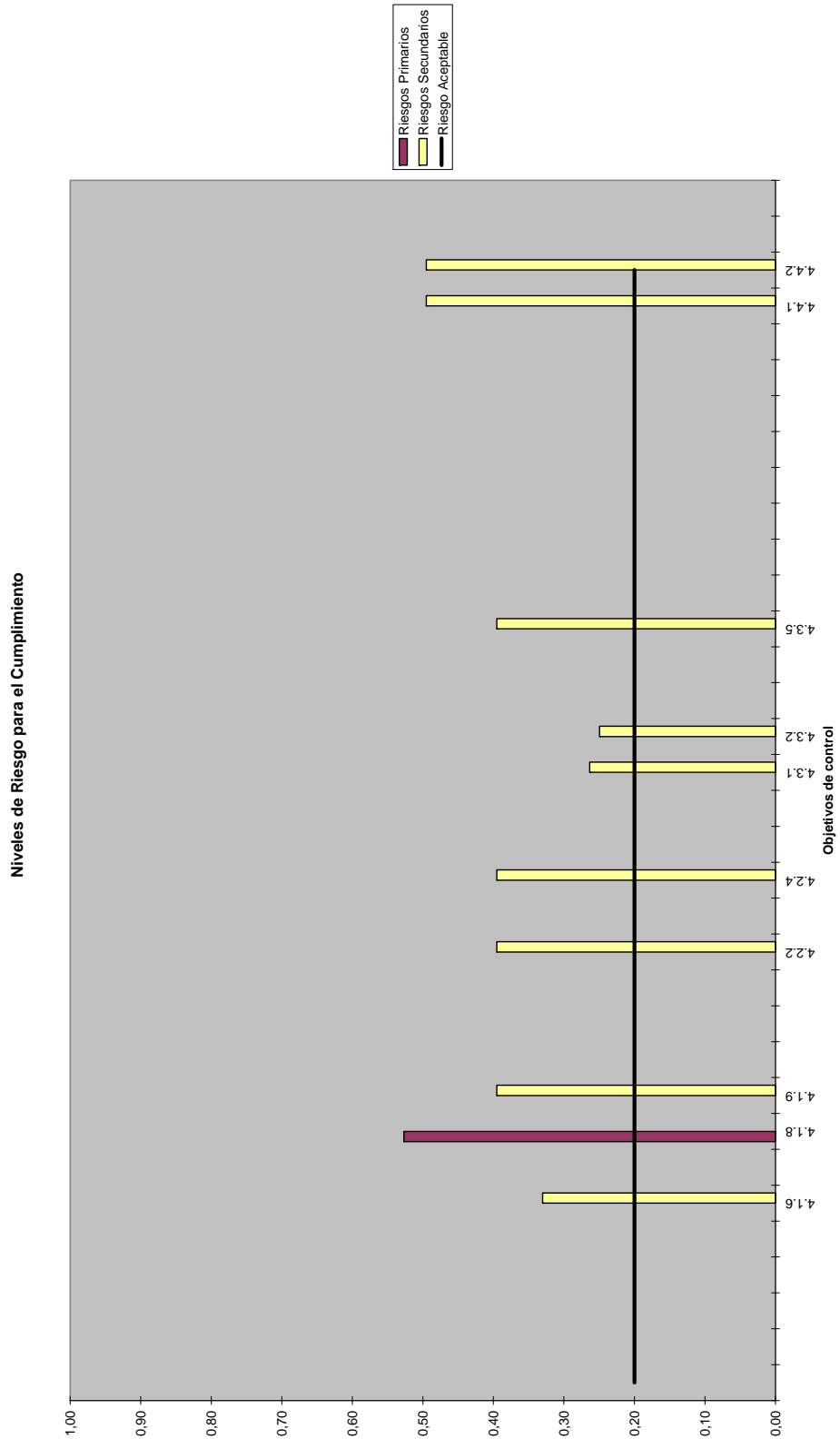


# Auditoría General de la Nación



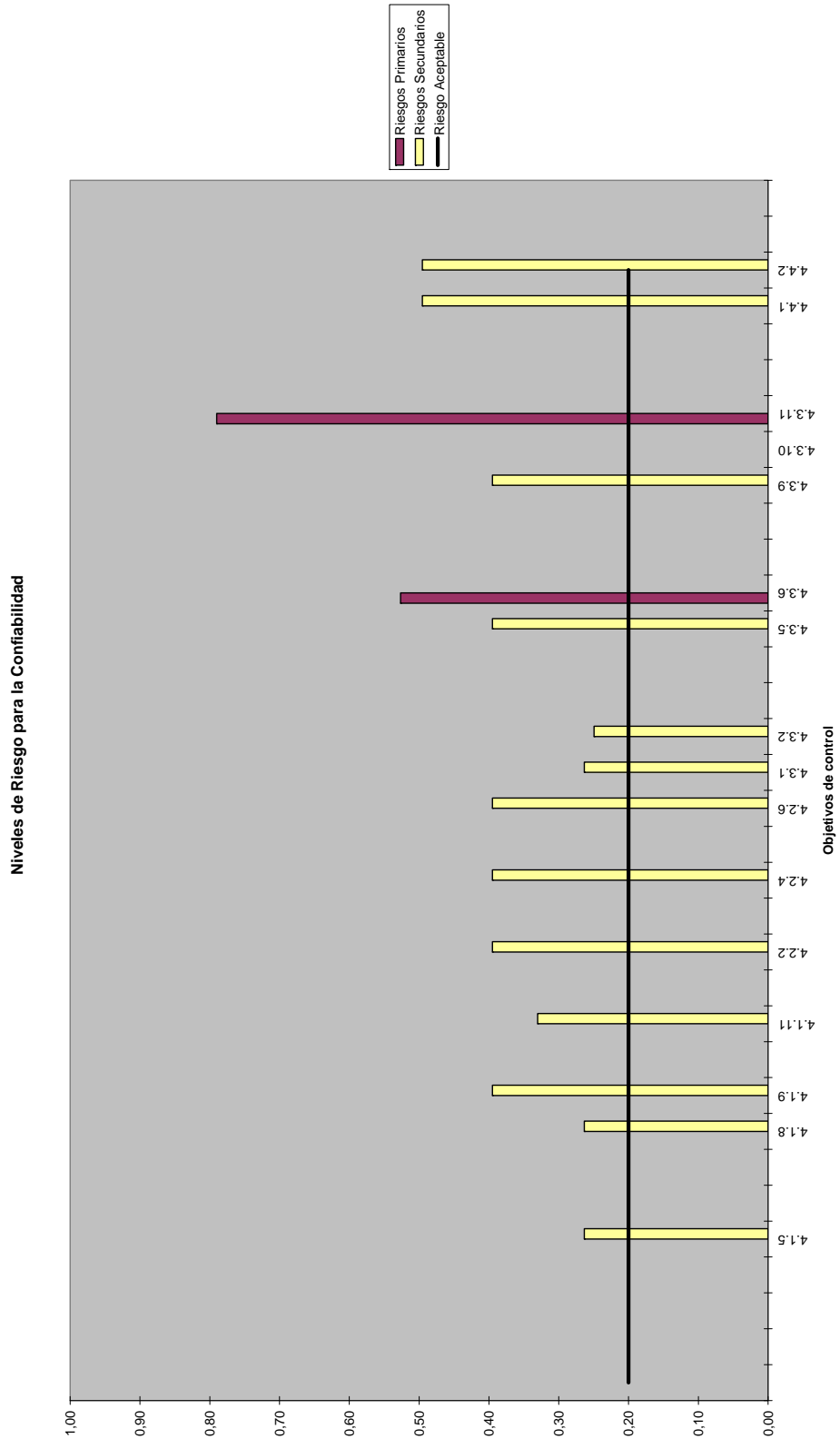


# Auditoría General de la Nación



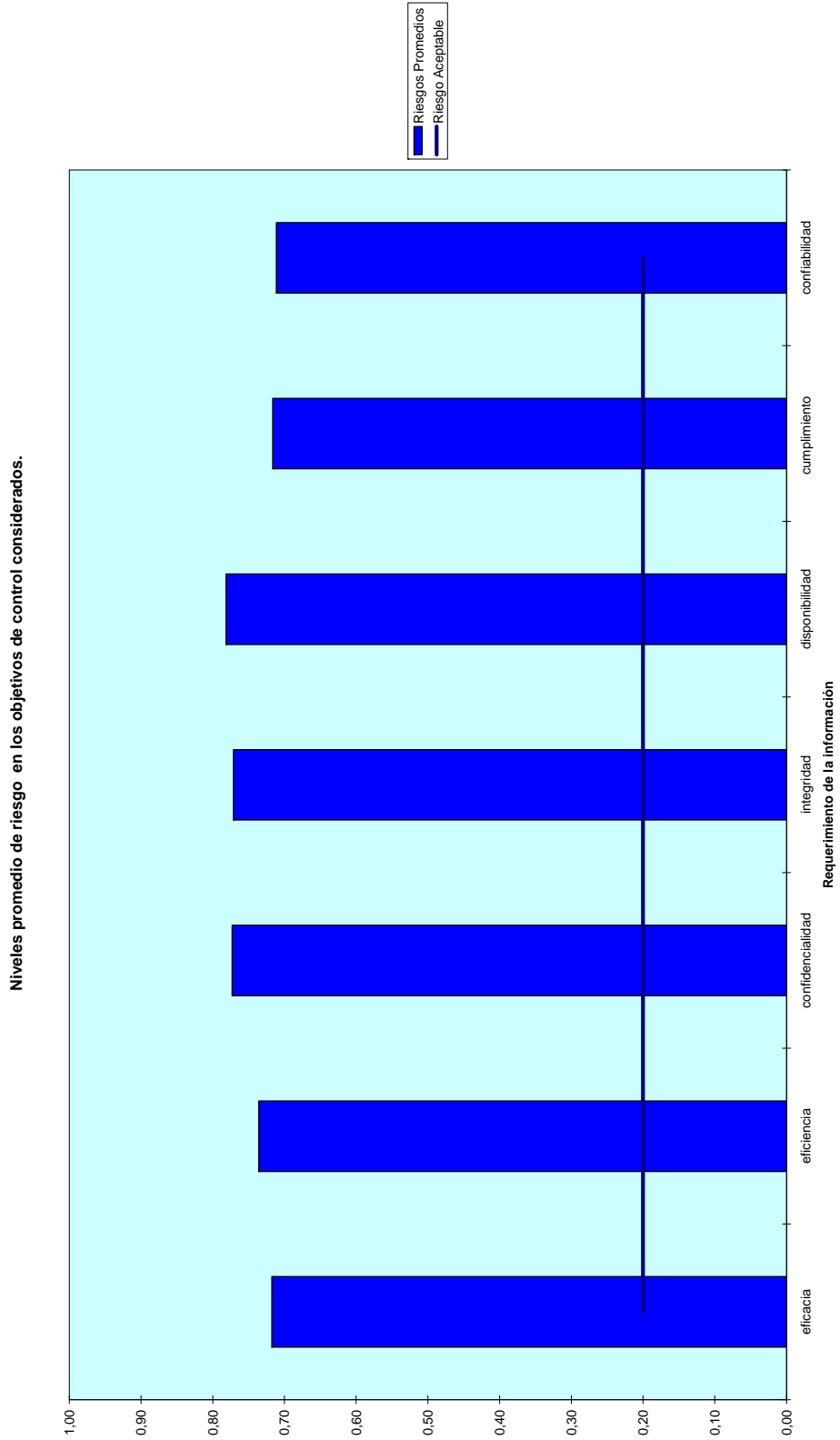


# Auditoría General de la Nación





# Auditoría General de la Nación





# Auditoría General de la Nación

## ANEXO IV

### Niveles del Modelo Genérico de Madurez

0 – *No conforma*. Falta total de procesos reconocibles. La organización no reconoce que existe un tema a ser tenido en cuenta.

1 – *Inicial*. La organización reconoce la existencia del tema y la necesidad de atenderlo. Sin embargo, no existen procesos estandarizados sino aproximaciones ad hoc que suelen ser aplicadas sobre una base individual o caso por caso. La administración aparece como desorganizada.

2 – *Repetible*. Los procesos han evolucionado hasta la etapa en la cual procedimientos similares son ejecutados por distintas personas que desarrollan las mismas tareas. No hay entrenamiento formal ni comunicación de procedimientos estándar y la responsabilidad es asumida por cada individuo. Hay un alto grado de confianza en el conocimiento de los individuos y los errores son probables.

3 – *Proceso Definido*. Los procedimientos han sido estandarizados, documentados y comunicados vía entrenamiento. Sin embargo, es responsabilidad de los individuos cumplir con estos procesos y es improbable que se detecten las desviaciones. Los procedimientos en sí mismos no son sofisticados pero son la formalización de prácticas existentes.

4 – *Administrado*. Es posible monitorear y medir el cumplimiento de los procedimientos y accionar cuando los procesos parecen no estar trabajando adecuadamente. Los procesos están bajo mejora constante y proveen una práctica correcta. El uso de herramientas y de automatización es limitado o fragmentario.

5 – *Optimizado*. Los procesos han sido corregidos al nivel de la mejor práctica, en base a los resultados de la mejora continua y de la comparación con otras organizaciones. La TI es usada de forma integrada para automatizar el flujo de trabajo, proveer herramientas para mejorar la calidad y la eficacia y hacer que la organización se adapte rápidamente a los cambios.



# Auditoría General de la Nación

## ANEXO V

### **Requerimientos de la información**

*Eficacia:* Que la información sea relevante y pertinente para la misión del ente, y que su entrega sea oportuna, correcta, consistente y utilizable.

*Eficiencia:* Que se provea información a través de la utilización óptima (más productiva y económica) de recursos.

*Confidencialidad:* Que se proteja la información sensible de la divulgación no autorizada.

*Integridad:* Que la información sea precisa y suficiente, y válida de acuerdo con los valores y expectativas del Organismo.

*Disponibilidad:* Que la información esté disponible cuando sea requerida por las misiones del Organismo, ahora y en el futuro. Que se salvaguarden los recursos necesarios y las capacidades asociadas.

*Cumplimiento:* Que se cumplan las leyes, regulaciones y acuerdos contractuales a que el Organismo está sujeto.

*Confiabilidad:* Que la información provista sea apropiada a la administración para operar la entidad y para elaborar informes financieros y de cumplimiento.



# Auditoría General de la Nación

## ANEXO VI

### ANÁLISIS DE LA VISTA ENVIADA AL ORGANISMO

**Respuesta del organismo:** *Introducción: Cabe destacar a efectos de comprender el estado de madurez actual del área de Tecnología de la Información, el entorno y contexto institucional con relación a la TI de los años precedentes a la actual conducción. El INDEC desde el año 2003 ha ido sufriendo un alto nivel de desinversión en el área de Tecnología Informática, paralelamente se han abandonado prácticas desarrolladas para la planificación de la actividad desatendiéndose los planes, metodologías, procesos y normativas instaurados oportunamente. Desde el año 2008 se han encarado distintas acciones que conduzcan a la reorganización del área de Tecnología de Información, a la evaluación y adecuación de los aspectos de infraestructura, metodologías y formulación de los procesos relativos a la operatividad del área. Con el objeto de abordar estos objetivos a fines del año 2008 se ha encarado un análisis exhaustivo de la situación cuyo principal resultado fue obtener un diagnóstico de la misma. A partir de dicho diagnóstico se han encarado diferentes iniciativas tendientes a neutralizar los riesgos operativos y emprender una planificación y adecuación de los procesos operativos y de gestión del área de TI. No obstante estos emprendimientos se encuentran en una etapa inicial de transformación al momento en que se ha desarrollado esta auditoría, por lo cual muchas de las recomendaciones propuestas si bien pueden haber sido consideradas aún no cuentan con la formalización recomendada, careciendo de las normas y procedimientos a los cuales hace referencia el informe de auditoría.*

*Se adjuntan los comentarios y aclaraciones respecto del borrador del informe suministrado.*

*Comentarios y aclaraciones:*

#### *1. - Punto 3.1. Aclaración*

*Las Direcciones Nacionales y Direcciones simples de primer nivel enumeradas, dependen de la Dirección Técnica la que a su vez depende de la Dirección del INDEC.*



## Auditoría General de la Nación

**Comentario AGN:** Se tiene en cuenta la aclaración y se modifica la redacción correspondiente.

**Respuesta del organismo:** 2.- *Punto 4. Planificación y organización*

*a. Punto 4.1.1. Definición de un Plan Estratégico de TI*

*Con relación a este punto en lo que respecta al Plan Estratégico de TI, la Dirección ha solicitado el desarrollo de dicho Plan con alineación al Plan Estratégico del Organismo. Los lineamientos estratégicos de dicho Plan se adjuntan en el Anexo 1.*

*Anexo 1 - Lineamientos estratégicos para el Plan estratégico de la Tecnología de la Información*

*La tecnología de Información constituye actualmente un herramental fundamental para el desarrollo de las actividades del INDEC como así también para el desarrollo de sus actividades y la divulgación de la información generada por lo cual, resulta imprescindible considerar los aspectos estratégicos para contar con un marco actualizado y acorde a los requerimientos de información de la sociedad, ese marco se sustenta en los lineamientos estratégicos que deben adoptarse en el área de Tecnología de la Información, y que se detallan a continuación.*

*1.- Fortalecer la estructura tecnológica.*

*Completar la actualización y adecuación tecnológica de la infraestructura de servidores y demás equipamiento del centro de cómputos como así también del parque de computadores de los puestos de trabajo, iniciada en el presente año.*

*Actualmente existe una fragilidad operacional del Centro de Cómputos por la obsolescencia e insuficiente capacidad de los principales servidores de producción; así también, por lo inadecuado de las versiones de la mayoría de los sistemas operativos instalados en los mismos, lo que dificulta la administración de la seguridad y los servicios que soportan.*

*Acciones estratégicas*

- Implementar el reemplazo del servidor y el almacenamiento principal.*
- Reemplazar los servidores de servicios y aplicaciones.*
- Reemplazar el sistema de resguardo y recuperación de información para adecuarlo a*



## Auditoría General de la Nación

*las nuevas necesidades de información.*

- *Reemplazar equipamiento obsoleto de los puestos de trabajo.*
- *Efectuar la actualización de los sistemas operativos tanto de los servidores como de los puestos de trabajo con el objeto de permitir una eficiente administración de los recursos tecnológicos o de la seguridad de la información.*

### *2.- Fortalecer la Red Nacional de Comunicaciones del INDEC*

*La Red Nacional de informática fue creada en el año 1992 con el objeto de brindar a los programas de trabajo y a las Provincias, servicios de conectividad para facilitar el intercambio de información, y suministrar a las mismas, servicios de correo electrónico, intercambio de archivos, Intranet y acceso a base de datos institucionales. Adicionalmente, la Red presta servicio de acceso a Internet al personal del Indec.*

*La Red interna cuya situación resulta crítica, fundamentalmente por la falta de actualización desde su instalación (1993). La antigüedad y obsolescencia de los dispositivos activos y pasivos de la electrónica de red; y la falta de acompañamiento al crecimiento del número de puestos, con la correspondiente adecuación del tendido de la misma, han provocado la proliferación de instalaciones de hubs y switchs sueltos en un gran número de oficinas, incrementando las probabilidades de interrupción en los servicios que brinda.*

#### *Acciones estratégicas*

- *Reemplazar la lógica de Red con equipamiento de última generación que se adecue a las necesidades actuales de comunicación que plantean los nuevos desafíos institucionales. Asimismo, se deberá proceder al reemplazo de la totalidad del cableado estructurado para permitir nuevos servicios en la red y que permita a la misma adecuarse a la infraestructura edilicia del INDEC.*

### *3.- Desarrollar la Seguridad informática institucional*

*La seguridad informática si bien en parte existe, no se ha planteado en el marco de una política de seguridad orgánicamente estructurada, normalizada, documentada e implementada de acuerdo a las recomendaciones de la ONTI. En el presente año se ha realizado un diagnóstico de la situación y se han encarado diferentes iniciativas tendientes*



## Auditoría General de la Nación

*a poder obtener un marco normativo que garantice la implementación de políticas que contribuyan a mejorar la seguridad informática en todos los niveles.*

### *Acciones estratégicas*

*- Profundizar el marco normativo e incorporar herramientas de hardware y software que faciliten el cumplimiento de las normativas vigentes a nivel del Gobierno Nacional y de las recomendaciones internacionales en esta cuestión.*

### *4.- Sistemas de Información*

*Mejorar el desarrollo e implementación de aplicaciones y servicios de información a los distintos niveles de usuarios de información estadística de la sociedad.*

### *Acciones estratégicas*

- Implementar una metodología de sistemas adecuada a las tendencias actuales*
- Fortalecer el desarrollo de aplicaciones y servicios de Información mediante el uso de herramientas modernas para la captura, análisis, producción y divulgación de la información.*
- Capacitar los recursos humanos de tecnología de la Información en las nuevas herramientas de software.*
- Reemplazar la tecnología de software actualmente utilizada para el desarrollo de aplicaciones por herramientas moderna que facilitan el desarrollo de aplicaciones y la explotación de la Información.*

### *5.- Monitoreo de la gestión de TI*

*Es fundamental para el desarrollo y fortalecimiento de la Función de servicio de información contar los mecanismos necesarios que permitan monitorear la gestión de la Tecnología de la Información para poder dar cumplimiento eficiente a los objetivos y metas institucionales planteadas en el Plan estratégico.*

### *Acciones estratégicas*

- Desarrollar e implementar las normas y procedimientos que permitan obtener la información necesaria para el seguimiento de la evolución y evaluación de la Tecnología de la Información.*



## Auditoría General de la Nación

- *Instrumentar indicadores que permitan monitorear las distintas áreas y servicios relacionados con la Tecnología de la Información.*

**Comentario AGN:** El Organismo reconoce que no existe Plan Estratégico y anuncia los lineamientos para su concreción, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *b. Punto 4.1.2. Definición de la arquitectura de la Información.*

*Respecto al modelo de arquitectura y de datos la Dirección del INDEC ha impulsado el desarrollo de un proyecto integral de las estadísticas económicas. Este proyecto implica en una primera instancia la homogeneización de todas las variables de todos los operativos económicos; esta etapa (homogeneización de variables) está previsto finalizarla durante el primer trimestre de 2010. El resultado de esta etapa permitirá contar con la información necesaria para el desarrollo del modelo de datos de los operativos de estadísticas económicas.*

*Este proyecto cuenta con un sistema en el cual se tiene información de todas las variables y los operativos de encuestas vinculados a la actividad económica, asimismo cuenta para cada uno de ellos, con información de metadatos la cual permite fehacientemente conocer el propósito de dichas variables como la vinculación de las mismas con los diferentes operativos económicos.*

*Está previsto realizar un modelo similar con las variables de los operativos que se desarrollan para la obtención de las estadísticas sociales, permitiendo a su finalización conformar el modelo de datos y metadatos de las variables.*

**Comentario AGN:** El Organismo reconoce que no existe la Arquitectura de la Información e indica su próxima realización, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *c. Punto 4.1.3. Determinación de la Dirección Tecnológica*

*Si bien es cierto que no existe un Plan formalmente planteado con relación a la infraestructura tecnológica existen recomendaciones a adoptar en el diagnóstico entregado como así también planes y cronogramas de actividades tendientes a mejorar el*



## Auditoría General de la Nación

*uso y adecuación de dicha infraestructura, los mismos fueron suministrados oportunamente.*

*Con relación a las tendencias y la evaluación de nuevas tecnologías la misma no se lleva a cabo ad hoc sino con relación a las necesidades institucionales tanto actuales como futuras. Se tomarán en cuenta las recomendaciones respecto a formalizar los planes y a crear dentro de la Dirección de Informática un área encargada de estos aspectos.*

**Comentario AGN:** El Organismo reconoce que no existe un sector formal dedicado al tema y anuncia su próxima creación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *d. Punto 4.1.4. Definición de la organización y las relaciones de TI*

*El Comité de Sistemas de Información (Comité de Planificación de Servicios de Información) fue creado en diciembre del año 2002 y está integrado por la Dirección del INDEC y los Directores Nacionales o simples de primer nivel. El mismo dejó de funcionar durante el año 2004 y está prevista su restauración a partir del año 2010.*

**Comentario AGN:** El Organismo reconoce el no funcionamiento del Comité de Sistemas de Información y anuncia su próxima puesta en marcha, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *e. Punto 4.1.5. Administración de la inversión en Tecnología de Información*

*La Dirección de Informática prepara y suministra anualmente un presupuesto y plan anual de adquisiciones, el cual fue entregado oportunamente a la AGN.*

**Comentario AGN:** El Organismo presentó un presupuesto anual que incluye adquisiciones, sin embargo no existe una política formal ni un procedimiento de formulación presupuestaria que regulen su establecimiento y aprobación. Tampoco se hace un seguimiento o monitoreo de las inversiones y los gastos de TI.

**En consecuencia se mantiene la observación.**



## Auditoría General de la Nación

**Respuesta del organismo:** *f. Punto 4.1.6. Comunicación de los objetivos y directivas de la Gerencia*

*La comunicación es realizada mediante notas y documentos generados por la Gerencia.*

**Comentario AGN:** El Organismo no ha instaurado un conjunto uniforme de políticas, procedimientos y normas, junto con procesos de control de su cumplimiento, que garantice la satisfacción de los objetivos de su conducción.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *g. Punto 4.1.7. Administración de los recursos humanos de TI*

*Respecto a las observaciones planteadas cabe señalar:*

- *La administración de los recursos humanos de TI de la Dirección de Informática es responsabilidad del Director.*
- *Las funciones y responsabilidades de las áreas de la Dirección de Informática están definidas pese a no estar formalizadas mediante una descripción de puesto.*
- *El reclutamiento de personal de TI para la Dirección de Informática sigue los procedimientos establecidos por la Dirección Nacional de Recursos Humanos y Organización.*
- *El proceso de evaluación de desempeño y promoción está establecido por la normativa del SINEP.*

**Comentario AGN:** El Instituto carece de definiciones formales propias en esta materia que adapten la normativa vigente en la Administración Pública Nacional a su caso particular.

**En consecuencia se mantiene la observación, ajustando su redacción acorde a lo informado por el Organismo:**

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.

**Respuesta del organismo:** *h. Punto 4.1.8. Garantía de cumplimiento de los requisitos externos.*



## Auditoría General de la Nación

*Si bien no existen procedimientos escritos respecto al cumplimiento de la normativa de la Oficina Nacional de Tecnología de Información la misma está considerada, adoptada e implementada.*

*Respecto a las políticas de:*

- *seguridad e higiene, las mismas son instrumentadas por la Dirección de Administración de Recursos Humanos.*
- *cumplimiento de las exigencias de los contratos de seguros, son de responsabilidad de la Dirección General de Administración.*

**Comentario AGN:** El Instituto carece de definiciones formales propias en esta materia que adapten la normativa vigente en la ONTI y otras Direcciones a su caso particular, por otra parte acepta la indicación y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *i. Punto 4.1.9. Evaluación y administración de riesgos*  
*Se considerarán las observaciones planteadas para su implementación.*

**Comentario AGN:** El Organismo acepta la indicación.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *j. Punto 4.1.10. Administración de proyectos*

*Cabe mencionar que si bien no existen informes estadísticos continuos, práctica abandonada por la anterior conducción, se posee la información necesaria para desarrollar las mismas.*

**Comentario AGN:** El Instituto reconoce la inexistencia de normativas escritas y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *k. Punto 4.1.11. Administración de la calidad*

*Se recuerda que no solo se ha considerado la necesidad de implementar procesos de calidad sino que además se ha informado que se prevé para lo antes posible, incorporar dentro de la Dirección de Informática un área específica. A efectos de posibilitar la implementación de procesos calidad previamente deberá completarse el desarrollo del ciclo de vida y*



## Auditoría General de la Nación

*mantenimiento de los sistemas, la cual como se ha informado se encuentra en etapa de preparación.*

**Comentario AGN:** El Organismo no ha generado documentación que exprese la necesidad y la oportunidad de la instrumentación de los temas de calidad y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** 3.- Punto 4.2. Administración e implementación

*a. Punto 4.2.1. Identificación de soluciones automatizadas*

*Si bien no existen procedimientos escritos para el proceso de análisis de soluciones de sistemas de información, las soluciones que se adoptan no están limitadas a las propuestas de proveedores puesto que en general, el mercado de tecnología no dispone de soluciones específicas para las áreas temáticas de la estadística. Por otro lado, la elección de una solución de sistemas de información es contrastada por medio de la cooperación internacional, con soluciones emprendidas en otros Organismos Estadísticos.*

**Comentario AGN:** No existe un marco formal de administración de requerimientos de soluciones informáticas, entre cuyas etapas figure la posibilidad de tercerizar todo o parte del desarrollo de la solución.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *b. Punto 4.2.2. Adquisición y mantenimiento de software de aplicación*

*Cabe señalar que el desarrollo de sistemas de aplicaciones es interno y no se adquieren aplicaciones a terceros.*

**Comentario AGN:** Considerando que las acepciones de “adquirir” incluyen la de obtener con el propio esfuerzo, la respuesta del Instituto ignora las observaciones referentes a la inexistencia de metodologías adecuadas para el desarrollo interno y la falta de control sobre las tareas informáticas de tres de sus Direcciones.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *c. Punto 4.2.3. Adquisición y mantenimiento de la estructura tecnológica.*



## Auditoría General de la Nación

*Las políticas para la adquisición de tecnología cuentan con los procedimientos y normas que rigen a los procesos de adquisiciones para organismos de la Administración Pública Nacional.*

*Los cambios de infraestructura obedecen a los lineamientos estratégicos de la TI y no son producto de nuevas necesidades sino de un plan de infraestructura centralizada adoptado para el procesamiento de datos.*

*Respecto al plan de adquisiciones el mismo se realiza anualmente. En el se detallan las nuevas adquisiciones como así también los servicios requeridos dentro de los cuales se incluyen las contrataciones para el mantenimiento del hardware. Esta información ha sido suministrada oportunamente.*

**Comentario AGN:** No existe una política formal propia, ni normas y procedimientos, explícitos para las adquisiciones informáticas. Respecto del Plan de Adquisición y Mantenimiento de la Infraestructura Tecnológica, la auditoría lo solicitó durante el trabajo de campo y no fue entregado.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *d. Punto 4.2.4. Desarrollo y mantenimiento de procedimientos.*

*Al momento de la auditoría existía un grupo asignado a los efectos de instrumentar las normas y procedimientos operativos, el cual se encontraba elaborando el marco estándar para el desarrollo de normas y procedimientos operativos, su elaboración y difusión. Asimismo, al momento de la auditoría, se estaba implementando en carácter de prueba una aplicación web la cual, entre otras cosas, servirá como complemento a la comunicación de esas normas y procedimientos.*

**Comentario AGN:** El Organismo informa estar desarrollando una solución, la que será objeto de una próxima auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *e. Punto 4.2.5. Instalación y acreditación de aplicativos.*

*Se considerarán las observaciones planteadas para su implementación.*

**Comentario AGN:** El Organismo reconoce la necesidad y anuncia su próxima implementación, la que será objeto de una futura auditoría.



## Auditoría General de la Nación

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *f. Punto 4.2.6. Administración de cambios.*

*Se considerarán las observaciones planteadas para su implementación.*

**Comentario AGN:** El Organismo reconoce la necesidad y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *4. Punto 4.3 Entrega y soporte*

*a. Punto 4.3.1. Definición y administración de los niveles de servicio.*

*Se considerarán las observaciones planteadas para su implementación.*

**Comentario AGN:** El Organismo reconoce la necesidad y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *b. Punto 4.3.2. Administración de servicios prestados por terceros.*

*Cabe señalar que existen informes con relación al cumplimiento de los servicios contratados a terceros, estos informes forman parte de los expedientes de pago de cada uno de ellos. Dichos informes, denominados Informes Técnicos hacen referencia a como se han cumplimentado los servicios prestados para cada uno de los períodos de pago que se hayan establecido.*

**Comentario AGN:** Las órdenes de compra y los informes sobre el cumplimiento de las mismas fueron solicitados en reiteradas oportunidades y no se recibieron ni al momento de realizar los trabajos de campo ni en el descargo realizado por el Organismo.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *c. Punto 4.3.3. Administración de la capacidad y el desempeño.*

*Se considerarán las observaciones planteadas para su implementación.*

**Comentario AGN:** El Organismo acepta la indicación y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *d. Punto 4.3.4. Garantía de un servicio continuo*



## Auditoría General de la Nación

*Cabe señalar que el nivel de interrupciones en los servicios es mínimo. Las grandes interrupciones ocurridas se han debido a cortes de energía general, en estos el servicio de UPS del centro de cómputos se ha activado en forma automática permitiendo realizar el cierre y apagado de los servidores de la red sin pérdida de información alguna. Este servicio no alcanza a los usuarios en sus puestos de trabajo ni a las aplicaciones de uso local y almacenamiento local, por lo cual se está llevando a cabo un proceso de concienciar a los usuarios para que el almacenamiento de información se realice en los servidores y no en las PC' s. Ya son varias las Direcciones que han adoptado esta forma de trabajo. El Centro de Cómputos cuenta con servidores específicos para brindar el servicio de almacenamiento.*

*Con relación a las interrupciones para mantenimiento de la infraestructura, las mismas son planificadas en el Centro de Cómputos y se desarrollan fuera del horario normal de trabajo, estas interrupciones además son comunicadas con anterioridad a los usuarios.*

**Comentario AGN:** El nivel de interrupciones de servicio pretendido no fue documentado en la información recibida del Organismo. Por otra parte aún si fuera bajo no justificaría la carencia de un plan de contingencia formalmente definido.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** e. Punto 4.3.5. Garantía de la seguridad de los sistemas

*Cabe aclarar que los usuarios con permiso de de administrador para sus PC's no son la mayoría como se menciona sino una mínima porción que no supera el 5% de los usuarios. Por otro lado al momento de la auditoria se estaba realizando la planificación y el procedimiento a seguir para eliminar esta autorización.*

**Comentario AGN:** El Organismo durante los trabajos de auditoría no entregó la información solicitada en cuanto a la administración de equipos y reconoce que al presente existen usuarios con privilegio de administración y anuncia su próxima eliminación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación, ajustando la redacción del último párrafo acorde a la respuesta del Organismo:**



## Auditoría General de la Nación

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 sólo pone en riesgo la red de datos, sino que también deja al Organismo expuesto a sanciones judiciales.

**Respuesta del organismo:** *f. Punto 4.3.6. Identificación e imputación de costos*

*Se considerarán las observaciones planteadas para su implementación.*

**Comentario AGN:** El Organismo reconoce la necesidad y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *g. Punto 4.3.7. Educación y capacitación de los usuarios*

*Con relación a este punto cabe aclarar que:*

- *existen procesos de capacitación de usuarios respecto de las aplicaciones que se implementan.*
- *al momento de la auditoria se estaba llevando a cabo para personal de la Dirección de Informática un curso interno de programación orientada a objetos y otro interno en administración SQL Server.*
- *Además ya se había realizado un curso de introducción a PHP y estaba en preparación otro en Programación PHP, y otro de SQL para programadores.*
- *los cursos de SAS a los cuales se hace referencia fueron específicamente para personal de informática que luego trasladará sus conocimientos a los usuarios finales mediante cursos organizados por el INDEC.*
- *adicionalmente a la oferta de cursos del INAP existe la brindada por el INDEC y planificada por la Dirección de Desarrollo y Carrera del Personal.*

**Comentario AGN:** Los planes de capacitación, cursos realizados y el listado de agentes que concurren a los mismos, solicitados en reiteradas oportunidades, no fueron entregados ni al momento de realizar los trabajos de campo ni en el descargo realizado por el Organismo.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *h. Punto 4.3.8. Asistencia y asesoramiento a los usuarios de tecnología de la información*



## Auditoría General de la Nación

*Se considerarán las observaciones planteadas para su implementación.*

*Cabe mencionar que anteriormente existía una encuesta del nivel de satisfacción de la atención de los requerimientos de soporte la cual fue discontinuada por la gestión anterior y que será puesta en operación a la brevedad.*

**Comentario AGN:** El Organismo acepta la indicación y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *i. Punto 4.3.9. Administración de la configuración*

*Se considerarán las observaciones planteadas para su implementación.*

**Comentario AGN:** El Organismo acepta la indicación y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *j. Punto 4.3.10. Administración de problemas e incidentes*

*Cabe mencionar que si bien no existen informes estadísticos continuos, práctica abandonada por la anterior conducción, se posee la información necesaria para desarrollar las mismas.*

*Se considerarán las observaciones planteadas para su implementación.*

**Comentario AGN:** El Organismo acepta la indicación y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *k. Punto 4.3.11. Administración de datos*

*Todos los sistemas de información estadística desarrollados por la Dirección de Informática disponen de rutinas de validación de los datos que se ingresan, adicionalmente existe un análisis de congruencia de los datos en forma automatizada. En ninguna circunstancia la Dirección supone la precisión de los datos por el solo hecho de utilizar computadoras.*

*Los sistemas de información con relación a los datos suponen distintas instancias de validación de los mismos. Ellas son, la validación de los datos a su ingreso, la consistencia contra tablas en los casos que se dispongan y el análisis de congruencia entre variables. Además existen procesos de análisis utilizados para la imputación de los datos de acuerdo a*



## Auditoría General de la Nación

*las características de los procesos estadísticos de que se trate. Adicionalmente las salidas son analizadas en forma manual.*

*La función de administración existe pese a no estar formalizada en términos de descripción de la función. Esta función está centralizada en un pequeño grupo de personas dependientes del área de administración. En la gestión anterior esta función era desarrollada por personal externo al Organismo y dependía del área de desarrollo de sistemas.*

*Como se indica en el punto 2.b., a la finalización del proyecto previsto para el primer trimestre de 2010, se podrá disponer de los metadatos de todas las variables económicas, el mismo constituirá adicionalmente el diccionario de datos de las estadísticas económicas. Se prevé adoptar este modelo con las variables de las estadísticas sociales que realiza el INDEC.*

**Comentario AGN:** El Organismo no niega la observación y reconoce la necesidad del diccionario de datos y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** 1. Punto 4.3.12. Administración de instalaciones

*Se considerarán las observaciones planteadas para su implementación.*

*Al momento de la auditoría la Dirección de Informática ya había iniciado acciones para aislar totalmente los servidores dentro del Centro de Cómputos.*

**Comentario AGN:** El Organismo acepta la indicación y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** m. Punto 4.3.13. Administración de operaciones

*El Instituto cuenta con un sistema de resguardo robotizado centralizado para los sistemas de aplicaciones estadísticas. El informe hace referencia a los sistemas de resguardo de información no estadística que por falla de otros sistemas de resguardo, se ha debido adoptar métodos alternativos para el resguardar esa información. Pese a las limitaciones de este sistema se mantiene la integridad y resguardo de la información institucional. Además cabe señalar que al momento de la auditoría se había iniciado el proceso para el reemplazo*



## Auditoría General de la Nación

*del sistema de resguardo y recuperación de los datos almacenados en los distintos servidores.*

**Comentario AGN:** En su respuesta el Organismo no informa ni entrega datos sobre procedimientos formalmente definidos para operaciones de TI.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** 5.- Punto 4.4. Monitoreo

*a. Punto 4.4.1. Monitoreo de los procesos*

*El monitoreo de los proyectos se realiza mediante informes de avance no formalizados*

*Se considerarán las observaciones planteadas para su implementación.*

**Comentario AGN:** El Organismo acepta la indicación y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**

**Respuesta del organismo:** *b. Punto 4.4.2. Evaluación de la idoneidad del control interno*

*La Dirección de Informática es conciente de la necesidad de formalizar las actividades de control interno como así también disponer de indicadores para la gestión de la TI. En ese sentido se está trabajando para poder disponer nuevamente de la información requerida para la obtención de indicadores, los cuales fueron discontinuados por la anterior conducción.*

**Comentario AGN:** El Organismo acepta la indicación y anuncia su próxima implementación, la que será objeto de una futura auditoría.

**En consecuencia se mantiene la observación.**