# AUDITORÍA GENERAL DE LA NACIÓN

**GERENCIA DE PLANIFICACIÓN Y PROYECTOS ESPECIALES**
Dr. Felipe Pizzuto

**DEPARTAMENTO DE AUDITORÍA INFORMÁTICA Y SISTEMAS**
Ing. Ernesto Casin

**Objeto de Auditoría:** Evaluación de la Tecnología Informática en la Administración Federal de Ingresos Públicos, organismo autárquico en la órbita del Ministerio de Economía, con el objeto de determinar debilidades y fortalezas de la gestión informática unificada de la Dirección General Impositiva, la Dirección General de Aduana y la Dirección General de la Recaudación de la Seguridad Social y del proceso de transformación integral del área.

**INFORME DE AUDITORÍA**

Al Dr. Alberto R. Abad
Administrador Federal de Ingresos Públicos

En uso de las facultades conferidas por el artículo 118 de la Ley 24.156, la AUDITORÍA GENERAL DE LA NACIÓN procedió a efectuar un examen en el ámbito del Ministerio de Economía, con el objeto que se detalla en el apartado 1.-

**1. Objeto de la auditoría**

Evaluación de la Tecnología Informática en la Administración Federal de Ingresos Públicos, organismo autárquico en la órbita del Ministerio de Economía, con el objeto de determinar debilidades y fortalezas de la gestión informática unificada de la Dirección General Impositiva, la Dirección General de Aduana y la Dirección General de la Recaudación de la Seguridad Social y del proceso de transformación integral del área.-

**2. Alcance del examen**

2.1. El equipo de auditoría en la etapa de planificación identificó los temas de mayor exposición al riesgo y comprendió los siguientes ítems:

- 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 existencia de la documentación recomendada por la Secretaría de la Gestión Pública (SGP) y los estándares internacionales.
- Verificación de la adecuación de los sistemas y la infraestructura existentes y de la planificación a la misión y metas del Organismo y a 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.

- Relevamiento y Análisis del presupuesto operativo anual del área.
- Verificación del cumplimiento de la comunicación de los objetivos y las directivas de la Gerencia.
- Análisis de la administración de recursos humanos, 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 monitoreo de los procesos, la idoneidad del control interno y la existencia de auditoría interna.-

2.2. La tarea abarcó la Auditoría del estado de utilización de la Tecnología Informática en la Sede Central de la Administración Federal de Ingresos Públicos, en base a la información obtenida de las siguientes fuentes:

- Entrevistas realizadas con las principales autoridades de la Administración.
- Cuestionario para la determinación de las necesidades de análisis detallado.
- Cuestionarios para el análisis detallado de los temas que lo requerían.
- Manuales de Documentación de los Sistemas.
- Inspecciones directas efectuadas en el área de Sistemas de AFIP.-

2.3. Limitaciones: No formó parte de la presente Auditoría la evaluación del uso de la Tecnología Informática en las delegaciones del interior del país, ni en otras dependencias que no fuesen las instalaciones centrales.-

Las tareas de campo abarcaron desde junio 2002 hasta noviembre 2003.-

2.4. Metodología: La auditoría incluyó dos etapas: la primera de planificación del análisis detallado y la segunda de verificación del cumplimiento de lo informado en la primera etapa.

La etapa de planificación incluyó las siguientes actividades:

- Análisis del marco legal e institucional del funcionamiento de la Administración.
- Análisis de los informes de Auditoría Interna en temas informáticos.
- Entrevistas con los responsables de la Auditoría Interna y de cada una de las Direcciones de la Administración Federal, en cuanto a la participación y experiencia propia y de su personal en el uso de la Tecnología de la Información.
- Entrevistas con el responsable del Area Informática de la Administración Federal de Ingresos Públicos.-

En la etapa de análisis detallado se ejecutó:

- Análisis de las respuestas a los cuestionarios para determinación de las necesidades de análisis detallado.
- Determinación de las necesidades de verificación de las respuestas obtenidas.
- Verificación mediante inspecciones in situ y entrevistas con personal subalterno, realizada por especialistas en diversas ramas de la informática, a través del trabajo directo en el campo.-

En función de la información relevada y los niveles de riesgo estimados se definieron los trabajos de campo convenientes para realizar las verificaciones necesarias.-

Este informe es producto de la evaluación de la información recabada en las entrevistas mantenidas y de las observaciones realizadas en el trabajo de campo.-

Cabe destacar que se presentaron dificultades para realizar el relevamiento debido a la ausencia de una compilación ordenada de la normativa interna vigente, a las demoras en que incurrió la Administración Federal de Ingresos Públicos para la satisfacción de las solicitudes cursadas por esta Auditoría y a la falta de entrega de parte de la documentación solicitada.-

Por otra parte se realizó un análisis de los riesgos asociados a los Objetivos de Control definidos para cada uno de los procedimientos relevados.-

Se han encontrado observaciones que se detallan por separado.-

**3. Aclaraciones previas**

La Administración Federal de Ingresos Públicos fue creada por decreto 1.156 del 14 de octubre de 1.996, constituida por la fusión de la Administración General de Aduanas y la Dirección General Impositiva. Se trata de un ente autárquico en el ámbito del Ministerio de Economía de la Nación, (decreto 617/2.001).-

A través del decreto 217 del 17 de junio de 2003, conserva sus facultades en materia de Recursos de la Seguridad Social.-

El fundamento de su creación es el de asegurar que la función de recaudar se encuentre concentrada.-

Su misión es la de administrar con eficiencia y eficacia la aplicación, percepción y fiscalización de los tributos y las actividades relacionadas con el control del comercio exterior, brindando servicios de calidad y promoviendo el cumplimiento voluntario y oportuno de las obligaciones.-

Sus objetivos son:

Objetivo I. Incrementar la percepción de riesgo en la lucha contra la evasión y el fraude tributario y aduanero.-

Objetivo II. Mejorar la eficacia de los mecanismos de control y el aprovechamiento de la información disponible, para incentivar el cumplimiento voluntario.-

Objetivo III. Afianzar los principios de equidad y justicia en la aplicación de las normas tributarias y aduaneras y procurar su adecuación a las nuevas realidades del comercio exterior y a los desarrollos tecnológicos.-

Objetivo IV. Promover el compromiso de los sectores públicos y privados de brindar apoyo en la lucha contra la evasión y el contrabando y la comprensión del rol de la administración tributaria.-

Objetivo V. Brindar más y mejores servicios a los contribuyentes y usuarios del servicio aduanero para minimizar el costo del cumplimiento de las obligaciones.-

Objetivo VI. Promover el desarrollo personal, profesional y ético de los funcionarios asegurando el compromiso permanente con la misión y los objetivos de la organización.-

Objetivo VII. Mejorar los sistemas de control de gestión y procurar el uso eficiente de los

recursos financieros y materiales de la Administración.-

**4. Observaciones y Recomendaciones**

Se exponen a continuación las principales observaciones y comentarios surgidos del trabajo llevado a cabo por esta Auditoría.-

Para cada una de las observaciones detectadas se incluyen el nivel de madurez, conforme al Modelo de Madurez de la Capacidad de la Universidad Carnegie Melon enunciado más abajo, y las recomendaciones tendientes a mejorar el ambiente de control y reducir los riesgos identificados.-

Niveles del Modelo Genérico de Madurez:

- 0 – *No conforma*. Falta total de procesos reconocibles. La organización incluso no reconoce que existe un tema a ser tenido en cuenta.-
- 1 – *Inicial / Ad Hoc*. Hay evidencia de que la organización reconoce la existencia del tema y la necesidad de atenderlo. Sin embargo, no existen procesos estandarizados y en lugar de ellos existen aproximaciones ad-hoc que tienden a ser aplicadas sobre una base individual o caso por caso. La administración aparece como desorganizada.-
- 2 – *Repetible aunque Intuitivo.* 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 dejada a cada individuo. Hay un alto grado de confianza en el conocimiento de los individuos y los errores son probables.-
- 3 – *Proceso* D*efinido*. 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 tomar acción 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, basado en los resultados de la mejora continua y de la movilización 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 rápido a los cambios.-

A efectos de determinar el impacto de las observaciones detectadas, se clasificó a las mismas de acuerdo con el nivel de riesgo. Los niveles asignados son Alto, Medio y Bajo.-

**4.1 Planificación y Organización**

**4.1.1 - Definición de un Plan Estratégico de Tecnología Informática**

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

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* La planificación estratégica es comprendida por la gerencia de Tecnología Informática, pero no está documentada. La planificación estratégica está a cargo de la gerencia de Tecnología Informática, pero sólo se comparte con las autoridades del organismo en función de la necesidad. La actualización del plan estratégico de Tecnología Informática se produce sólo ante pedidos de la máxima autoridad y no hay un proceso proactivo para identificar las novedades de Tecnología Informática y del organismo que requieren actualizaciones al plan. Existe una estrategia global para la organización que no está fundamentada. Los riesgos y beneficios que las grandes decisiones estratégicas podrían tener para el usuario se reconocen, pero su definición es intuitiva.-

DESCRIPCIÓN: De la documentación obtenida se desprende que no existen procedimientos formales para la planificación estratégica de la tecnología de la información, que establezcan su relación con los objetivos estratégicos del organismo. Los planes generales de la Subdirección General definen metas concretas sin estimación de costos, ni plazos lo que dificulta su monitoreo y evaluación.-

RECOMENDACIÓN: La alta gerencia de la Organización es responsable de la

implementación y el desarrollo de planes a corto y largo plazo que cumplan la misión y las metas de la misma. En este aspecto, debe garantizar que:

- la tecnología de información forma parte del plan de la organización a corto y largo plazo,
- se elabora un Plan de Tecnología Informática a largo plazo,
- el enfoque y estructura de la planificación de Tecnología Informática a largo plazo se traducen en planes de mediano y corto plazo,
- se realizan los cambios del plan de Tecnología Informática a largo plazo,
- se elabora la planificación a corto plazo de la función de servicios de información,
- se comunican los planes de Tecnología Informática,
- se monitorea y evalúan los planes de Tecnología Informática,
- se evalúan los sistemas existentes.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**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 forma y tiempo tales que permitan a las personas cumplir sus responsabilidades de manera eficiente y oportuna. La función de servicios de información debe crear y mantener un modelo de arquitectura de información que incluya el modelo de datos del organismo y los sistemas de información relacionados. En este aspecto, la función de servicios de información debe garantizar:

- 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.-

NIVEL DE MADUREZ: *Inicial / Ad Hoc*. La alta gerencia reconoce la necesidad de una arquitectura de la información, pero no ha formalizado ni un proceso ni un plan para desarrollarla. Hay un desarrollo aislado y reactivo de los componentes de la arquitectura de la información. Existen implementaciones aisladas y parciales de diagramas de datos, documentación y reglas de sintaxis de datos. Las definiciones se basan en los datos, en lugar de la información. Hay conciencia de la necesidad de una arquitectura de la información, pero

no está desarrollada.-

DESCRIPCIÓN: No se recibió información normativa en el tema de arquitectura de la información. Existe un sistema denominado SUPA (Sistema Único de Parámetros de AFIP) que incluye el diseño de la mayoría de las tablas de Oracle. La intención es que cada tabla tenga un dueño responsable de la administración de sus campos. Se está trabajando en el tema sin asignarle un rol protagónico en la planificación informática. Genera confusión en el uso de la información, especialmente cuando se la trata con fines de control fiscal.-

RECOMENDACIÓN: La información debe mantenerse acorde con las necesidades y debe ser identificada, recopilada y comunicada en forma y tiempo tales que permita a las personas cumplir sus responsabilidades de manera eficiente y oportuna. La función de servicios de información debe crear y mantener un modelo de arquitectura de información que incluya el modelo de datos del organismo y los sistemas de información relacionados. En este aspecto, se debe garantizar:

- 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.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

### 4.1.3 - Determinación de la Dirección Tecnológica

OBJETIVO DE CONTROL: La función de servicios de información 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 y servicios.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Hay un entendimiento implícito de la necesidad e importancia de la planificación tecnológica. No obstante, la planificación es táctica y se concentra en la generación de soluciones técnicas a problemas técnicos, y no en el uso de la tecnología para satisfacer las necesidades de las actividades del organismo. La evaluación de los cambios tecnológicos se deja librada al criterio de distintas personas que siguen procesos intuitivos, aunque similares. No hay una actividad formal de capacitación y comunicación de los roles y responsabilidades. Aparecen técnicas y normas comunes para el

desarrollo de los componentes de la infraestructura.-

DESCRIPCIÓN: De la información recibida se desprende que no existen procedimientos formales para la confección de un plan de infraestructura tecnológica. Se han fijado rumbos, en materia de infraestructura, contenidos en el Plan General de Sistemas que se pueden compartir; sin embargo no están justificados ni evaluados. Se determinan temas estratégicos de alta significación económica para la Nación sin evaluación formal de impacto, riesgos y costos.-

RECOMENDACIÓN: La función de servicios de información debe crear y actualizar periódicamente un plan de infraestructura tecnológica. Dicho plan debe comprender aspectos tales como la arquitectura de los sistemas, la dirección tecnológica y las estrategias de información. En este aspecto, debe garantizar:

- la planificación de la infraestructura tecnológica,
- el monitoreo de las tendencias y reglamentaciones futuras,
- la evaluación de contingencias de la infraestructura tecnológica,
- planes de adquisición de hardware y software,
- la definición de normas de tecnología.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**4.1.4 - Definición de la Organización y las Relaciones de Tecnología Informática**

OBJETIVO DE CONTROL: La máxima autoridad debe establecer una estructura organizativa adecuada en términos de cantidad e idoneidad del personal, con roles y responsabilidades definidos y comunicados, alineada con la misión del organismo, que facilite la estrategia y brinde una dirección eficaz y un control adecuado.-

NIVEL DE MADUREZ: *Proceso Parcialmente Definido*. Existen roles y responsabilidades definidos para la organización de Tecnología Informática y los proveedores. La organización de Tecnología Informática está desarrollada, documentada, comunicada y alineada con la estrategia de Tecnología Informática. El diseño de la organización y el ambiente de control interno están definidos. Falta formalización de las relaciones con otras partes, tales como comités de dirección, auditoría interna y administración de proveedores. La organización de Tecnología Informática está funcionalmente completa, sin embargo, todavía se concentra más

en las soluciones técnicas que en el uso de la tecnología para resolver problemas de las actividades sustantivas del organismo. Hay definiciones de las funciones que debe desempeñar el personal de Tecnología Informática y de las que serán desempeñadas por los usuarios.-

DESCRIPCIÓN: De la documentación recibida se desprende que falta formalizar las relaciones con otras partes, tales como comités de dirección, auditoría interna y administración de proveedores. La organización no está funcionalmente completa. La alta gerencia del Organismo reconoce tener limitaciones por falta de nivel técnico del personal y por la inestabilidad del personal contratado, significativo en áreas de informática.-

RECOMENDACIÓN: Al ubicar la función de servicios de información dentro de la estructura del organismo, la alta gerencia debe garantizar autoridad, masa crítica e independencia de las áreas usuarias en la medida necesaria para garantizar soluciones de tecnología de información eficientes. En este aspecto, la máxima autoridad y la alta gerencia deben garantizar:

- la designación de un comité de planificación de Tecnología Informática,
- la ubicación de la función de servicios de información en el organismo,
- la revisión de los logros organizacionales,
- 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 Tecnología Informática,
- la separación de funciones,
- la competencia del personal de Tecnología Informática,
- las descripciones de los puestos del personal de Tecnología Informática,
- la identificación del personal clave de Tecnología Informática,
- las políticas y procedimientos relativos al personal contratado,
- las relaciones de coordinación, comunicación y enlace.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**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.-

NIVEL DE MADUREZ: *No Conforma*. No se ha tomado conciencia de la importancia de la selección y presupuesto de las inversiones de Tecnología Informática. No se hace un seguimiento o monitoreo de las inversiones y los gastos de Tecnología Informática.-

DESCRIPCIÓN: De la documentación recibida se desprende que no existen procedimientos formales que definan el mecanismo para la administración de la inversión. Los presupuestos anuales de tecnología informática recibidos son incompletos y no representativos. La inversión principal se realiza a través de organismos internacionales lo que dificulta tener una visión global del presupuesto y su ejecución.-

RECOMENDACIÓN: La alta gerencia es responsable de la implementación de un proceso de formulación presupuestaria que garantice el establecimiento de un presupuesto operativo anual de la función de servicios de información y su aprobación de conformidad con los planes a corto y largo plazo del organismo y de tecnología de información. En este aspecto, se debe garantizar:

- un presupuesto operativo anual de Tecnología Informática,
- el monitoreo de costos y beneficios,
- la justificación de costos y beneficios.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**4.1.6 - Comunicación de los Objetivos y Directivas de la Gerencia**

OBJETIVO DE CONTROL: La máxima autoridad debe impulsar la definición de políticas y su comunicación a la comunidad de usuarios. Además, es preciso que se establezcan normas a fin de traducir las opciones estratégicas en reglas prácticas y útiles.-

NIVEL DE MADUREZ: *Inicial / Ad Hoc*. La alta gerencia es reactiva en el abordaje de los requerimientos del ambiente de control de la información. Las políticas, procedimientos y normas se desarrollan y comunican en forma ad hoc, en función de las necesidades, impulsadas principalmente por problemas. Los procesos de desarrollo, comunicación y cumplimiento son informales y no siguen criterios uniformes.-

DESCRIPCIÓN: De la documentación recibida se desprende que no existen políticas formales para la comunicación de las decisiones y normativas del área y tampoco para el control de su cumplimiento.-

RECOMENDACIÓN: La máxima autoridad y la alta gerencia deben crear 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, deben garantizar:

- la responsabilidad de la alta gerencia sobre la formulación de las políticas,
- la comunicación de las políticas del organismo,
- los recursos para la implementación de políticas,
- el mantenimiento de políticas,
- el cumplimiento de las políticas, los procedimientos y las normas,
- el compromiso con la calidad,
- la política marco de seguridad y control interno,
- los derechos de propiedad intelectual,
- las políticas específicas,
- la comunicación de la concientización en materia de seguridad.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**4.1.7 - Administración de los Recursos Humanos**

OBJETIVO DE CONTROL: La máxima autoridad debe implementar prácticas de administración de personal sólidas, justas y transparentes en cuanto a selección, alineación, verificación de antecedentes, remuneración, capacitación, evaluación, promoción y despido.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Hay un entendimiento implícito de la necesidad de administración de los recursos humanos de Tecnología Informática. Hay un enfoque táctico de la contratación y administración del personal de Tecnología Informática, impulsado por necesidades específicas de proyectos, y no por una dirección tecnológica y un equilibrio bien entendido entre la disponibilidad interna y externa de personal capacitado. Se realiza una capacitación informal para los nuevos empleados, que luego son entrenados según

necesidades particulares.-

DESCRIPCIÓN: De la documentación recibida se desprende que no existen procedimientos formales para la selección, formación y promoción del personal. La dirección reconoce tener limitaciones por falta de nivel técnico del personal y por la inestabilidad del personal contratado, significativo en áreas de informática.-

RECOMENDACIÓN: La máxima autoridad y la alta gerencia deben implementar y evaluar periódicamente los procesos necesarios para selección y promoción del personal y debe procurar que el organismo cuente con una fuerza laboral que tenga las habilidades necesarias para lograr sus metas. En este aspecto, deben garantizar:

- 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 extinción de la relación laboral.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**4.1.8 - Garantía del Cumplimiento de los Requerimientos Externos**

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

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Se comprende y se comunica la necesidad de cumplir con los requerimientos externos. Cuando el cumplimiento se convierte en un requerimiento recurrente, como en las regulaciones administrativas o la legislación sobre la privacidad, se desarrollan procedimientos individuales, que se siguen año tras año. Sin embargo, no hay un esquema general que garantice el cumplimiento de todos los requerimientos. Por lo tanto, es probable que haya excepciones y que las necesidades de cumplimiento que van surgiendo sólo se aborden en forma reactiva. Se depende mucho del

conocimiento y la responsabilidad de ciertas personas y hay probabilidad de errores. Existe una capacitación informal sobre los requerimientos externos y las cuestiones relativas al cumplimiento.-

DESCRIPCIÓN: De la documentación recibida se desprende que no están establecidos procedimientos formales relativos al cumplimiento (identificación, análisis y adaptación) de los requerimientos externos.-

RECOMENDACIÓN: La máxima autoridad y la alta gerencia deben establecer y mantener procedimientos para la revisión de los requerimientos externos que permitan identificar los relacionados con las prácticas y controles de la tecnología de información. Además, se debe determinar en que medida es preciso que las estrategias de Tecnología Informática respalden los requerimientos de cualquier tercero relacionado. En este aspecto, 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 salud ocupacional (higiene del trabajo),
- la privacidad, propiedad intelectual y flujo de datos,
- el cumplimiento de la legislación en las actividades de comercio/gobierno electrónico,
- los cumplimientos de los contratos de seguro.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**4.1.9 - Evaluación 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 Informática y analizar su impacto, involucrando funciones multidisciplinarias y adoptando medidas eficaces en función de costos a fin de mitigar los riesgos.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Está empezando a entenderse que los riesgos de Tecnología Informática son importantes y deben ser tenidos en cuenta. Existe algún enfoque a la evaluación de riesgos, pero el proceso todavía es inmaduro y está desarrollándose. La evaluación en general se produce a un nivel muy general y se aplica sólo

a los grandes proyectos. La evaluación de las operaciones en marcha depende principalmente de que los gerentes de Tecnología Informática la planteen como un tema a tratar, lo cual a menudo sucede sólo cuando se producen problemas. La gerencia de Tecnología Informática no ha definido procedimientos o descripciones de puestos generales en el tema de la administración de riesgos.-

DESCRIPCIÓN: De la documentación recibida se desprende que no existen procedimientos formales referentes a la administración de riesgos y tampoco una evaluación y un plan de acción de reducción de riesgos. Se desconoce el nivel de riesgo de la Tecnología Informática en la Administración.-

RECOMENDACIÓN: La alta gerencia es responsable de 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 como deben administrarse los riegos a un nivel aceptable. En este aspecto, debe garantizar:

- una evaluación de riesgos de la actividad,
- el enfoque de la evaluación de riesgos,
- la identificación de riesgos,
- la medición de riesgos,
- el plan de acción de reducción de riesgos,
- la aceptación de riesgos.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**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. Asimismo, el organismo debe adoptar y aplicar técnicas bien concebidas de administración de proyectos por cada proyecto que se inicie.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* La alta gerencia tomó conciencia de la necesidad de una administración de los proyectos de Tecnología Informática. El organismo está en el proceso de aprender y repetir ciertas técnicas y métodos de un proyecto a otro. Los

proyectos de Tecnología Informática tienen objetivos técnicos y de recaudación definidos informalmente. Hay una participación limitada de las partes interesadas en la administración de proyectos de Tecnología Informática. Se desarrollaron algunas pautas para la mayoría de los aspectos de la administración de proyectos, pero su aplicación queda a discreción de cada gerente de proyecto.-

DESCRIPCIÓN: Desde principios del año 2002 se está llevando a cabo la transformación del área de Tecnología de la Información de la Administración Federal de Ingresos Públicos. Esto abarca la totalidad de las incumbencias del sector y prácticamente la totalidad de su personal. El éxito del proyecto hace a la calidad y cantidad de la recaudación pública de la Nación. De la documentación recibida se desprende que no existe una metodología formalmente establecida en el Organismo para la administración de proyectos de esta naturaleza y tampoco se está utilizando alguna de las metodologías clásicas de programación por camino crítico. El tiempo y los gastos del personal asignado al proyecto no se presupuestan ni controlan. Las reprogramaciones, convertidas en Planes para cada año calendario, se realizan en forma reactiva de acuerdo con las necesidades y los atrasos que se generaron. Durante el año se han detectado modificaciones en las tareas programadas para el mismo que no se reflejaron en los documentos recibidos.-

RECOMENDACIÓN: La alta gerencia es responsable de 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. En este aspecto, debe garantizar que:

- aplica un marco de administración de proyectos,
- contempla la participación del departamento de usuarios en el inicio del proyecto,
- asigna miembros y responsabilidades del equipo del proyecto,
- realiza la definición del proyecto,
- aprueba las fases del proyecto,
- crea un plan maestro del proyecto,
- planifica el monitoreo y el control de avance,
- planifica la reprogramación permanente,
- prepara un plan de garantía de calidad del sistema,

- planifica métodos de garantía,
- implementa la administración formal de riesgos del proyecto,
- elabora un plan de pruebas, si corresponde,
- elabora un plan de capacitación,
- desarrolla un plan de revisión posterior a la implementación.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**4.1.11 - Administración de la Calidad**

OBJETIVO DE CONTROL: La alta gerencia debe desarrollar la planificación, implementación y el mantenimiento de normas y sistemas de administración de calidad del organismo, que proporcionen distintas fases de desarrollo, prestaciones clave y responsabilidades explícitas.-

NIVEL DE MADUREZ: *No Conforma*. El organismo carece de un proceso de planificación de garantía de calidad y una metodología de ciclo de vida de desarrollo de sistemas. La alta gerencia y el personal de Tecnología Informática no reconocen la necesidad de un programa de calidad. Nunca se verifica la calidad de los proyectos y las operaciones.-

DESCRIPCIÓN: En la documentación recibida no se detectan intentos por desarrollar un plan general de calidad.-

RECOMENDACIÓN: La alta gerencia es responsable de desarrollar y mantener periódicamente un plan general de calidad basado en los planes del organismo y de tecnología de información a largo plazo. Dicho marco debe promover la filosofa de mejora continua. En este aspecto, debe garantizar:

- un plan general de calidad,
- el enfoque de garantía de calidad,
- la planificación de garantía de calidad,
- la revisión de garantía de calidad de la observación de las normas y procedimientos de la función de servicios de información,
- 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 Tecnología Informática,
- un marco de adquisición y mantenimiento de la infraestructura tecnológica,
- las relaciones con terceros a cargo de la implementación,
- la observación de las normas de documentación de programas,
- el cumplimiento de las normas de prueba de programas,
- el cumplimiento de las normas de prueba de sistemas,
- la utilización de pruebas en paralelo/piloto,
- la documentación de pruebas de sistemas,
- la evaluación de la observación de las normas de desarrollo.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**4.2 Adquisición e Implementación**

**4.2.1 - Identificación de Soluciones Automatizadas**

OBJETIVO DE CONTROL: La máxima autoridad debe garantizar una identificación y análisis claro y objetivo de las oportunidades alternativas, medidas en comparación con los requerimientos del usuario.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* A pesar de no haber una metodología formalmente definida para la adquisición e implementación, los requerimientos tienden a ser definidos en forma similar, con las diferencias propias de los distintos orígenes de los sectores incluidos en la Administración, debido a prácticas comunes dentro de la función de Tecnología Informática. Las soluciones se identifican informalmente en función de la experiencia interna y el conocimiento de la función de Tecnología Informática. El éxito de cada proyecto depende de la pericia de unas pocas personas clave y la calidad de la documentación y la toma de decisiones puede variar considerablemente.-

DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido una metodología escrita de implementación de las soluciones de Tecnología Informática para satisfacer los requerimientos de AFIP. Cada una de las áreas que antes eran independientes (DGI, DGA, DGRSS) tiene sus propias características al respecto. No se realiza la consideración escrita de alternativas, evaluadas con respecto a los requerimientos

del usuario, oportunidades tecnológicas, factibilidad económica, evaluaciones de riesgos y otros factores. El proceso no se sigue por igual en todos los proyectos y depende de las decisiones tomadas por el personal involucrado y la dimensión y prioridad del requerimiento del problema original.-

RECOMENDACIÓN: La alta gerencia es responsable de establecer una metodología que requiera la especificación de los requerimientos funcionales y operativos de las soluciones, incluidos el rendimiento, la seguridad, contabilidad, compatibilidad y legislación. En este aspecto, la alta gerencia y el funcionario principal de servicios de información deben garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- definición de los requerimientos de información,
- formulación de cursos alternativos de acción,
- formulación de la estrategia de adquisición,
- requisitos de servicios prestados por terceros,
- estudio de factibilidad tecnológica,
- estudio de factibilidad económica,
- arquitectura de la información,
- informe de análisis de riesgos,
- controles de seguridad económicos,
- diseño de pistas de auditoría,
- ergonomía,
- selección del software de sistemas,
- control de compras,
- adquisición de productos de software,
- mantenimiento del software de terceros,
- programación contratada de aplicaciones,
- aceptación de las instalaciones,
- aceptación de la tecnología.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**4.2.2 - Adquisición y Mantenimiento del Software de Aplicación**

OBJETIVO DE CONTROL: La adquisición y mantenimiento del software de aplicación debe realizarse por medio de la definición específica de requerimientos funcionales y operativos, y una implementación por etapas con prestaciones claras.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Existen procedimientos similares para adquirir y mantener las aplicaciones, pero se basan en la pericia de la función de Tecnología Informática, no en un proceso documentado. La tasa de éxito de las aplicaciones depende en gran medida de las habilidades internas y la experiencia de la función de Tecnología Informática. El mantenimiento suele ser problemático y se ve perjudicado cuando por algún motivo se pierde conocimiento interno del organismo.-

DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido una metodología formal para definir las necesidades de nuevas aplicaciones y los requerimientos de sus actualizaciones y mantenimiento. En estos momentos no se están contratando servicios externos de provisión de soluciones; pero, si hubiera que hacerlo por razones de fuerza mayor, tampoco existen procedimientos para la adquisición y acreditación de aplicaciones provistas por terceros.-

RECOMENDACIÓN: La alta gerencia y el funcionario principal de la función de servicios de información son responsables de establecer procedimientos y técnicas adecuadas para la aplicación de la metodología del ciclo de vida de desarrollo de sistemas (CVDS) del organismo, que impliquen una coordinación estrecha con los usuarios de sistemas, para la creación de especificaciones de diseño para cada proyecto de desarrollo de un sistema nuevo y la verificación de dichas especificaciones. En este aspecto, se debe garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- métodos de diseño,
- cambios importantes de los sistemas existentes,
- aprobación del diseño,
- definición y documentación de los requerimientos de archivos,
- especificaciones de programas,
- diseño de la recopilación de datos fuente,

- definición y documentación de los requerimientos de entrada,
- definición de interfaces,
- interfaces usuario–máquina,
- definición y documentación de los requerimientos de procesamiento,
- definición y documentación de los requerimientos de salida,
- controlabilidad,
- disponibilidad como factor clave del diseño,
- especificaciones de integridad de tecnología de información en programas de aplicación,
- pruebas del software de aplicación,
- materiales de soporte y referencia del usuario,
- reevaluación del diseño de sistemas.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**4.2.3 - Adquisición y Mantenimiento de la Infraestructura Tecnológica**

OBJETIVO DE CONTROL: La gerencia de la función de servicios de información debe impulsar la adquisición criteriosa del software y el hardware, la estandarización del software, la evaluación del rendimiento del hardware y el software, y la administración coherente de sistemas.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Existe uniformidad entre los enfoques tácticos, cuando se trata de adquirir y mantener la infraestructura de Tecnología Informática. No obstante, se carece de un marco normativo explícito para la administración y de procedimientos formales de evaluación de rendimiento de equipos y sistemas.-

DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido un marco normativo formal referente a la adquisición y mantenimiento de la infraestructura tecnológica y de su integridad. No se evidencia capacidad de monitorear y medir el desempeño de la infraestructura existente con miras a la detección oportuna de problemas y el dimensionamiento de las ampliaciones. No se encontraron registros, tales como registros de fallas debidas a falta de mantenimiento o a cambio de hardware o software de sistemas y registros de costos de las grandes modificaciones de infraestructura, que garanticen la elaboración de índices de desempeño. El costo y el tiempo para llegar al nivel

deseable de escalabilidad, flexibilidad e integración no están determinados. Se debe sobredimensionar la infraestructura a fin de evitar limitaciones ante problemas de los cuales no existen registros históricos.-

RECOMENDACIÓN: La gerencia de la función de servicios de información es responsable por la evaluación, incorporación, instalación, mantenimiento y seguridad de la configuración de Tecnología Informática. En este aspecto, se debe garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- evaluación del hardware y el software nuevos,
- mantenimiento preventivo del hardware,
- seguridad del software del sistema,
- instalación del software del sistema,
- mantenimiento del software del sistema,
- controles de cambios del software del sistema.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**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.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Se toman enfoques similares con respecto a la producción de procedimientos y documentación, pero no están basados en un lineamiento o marco estructurado. Las guías de operación y del usuario existen pero se carece de un abordaje uniforme y, por lo tanto, su exactitud y disponibilidad dependen en gran medida de las personas, y no de un proceso formal. El material de capacitación tiende a ser producido individualmente y la calidad depende de las personas involucradas. Por consiguiente, el desarrollo de guías para usuarios y operadores y la calidad del soporte al usuario pueden variar de deficiente a muy satisfactorio, con poca uniformidad e integración en las distintas áreas del organismo.-

DESCRIPCIÓN: De la documentación recibida no se deduce que la Administración haya

establecido una metodología del ciclo de vida del desarrollo de sistemas. Los niveles de servicio acordados con los usuarios son no mensurables. No se tiene control del nivel de satisfacción de los usuarios con los manuales y materiales de capacitación. Esta situación deviene en perdida de eficacia y eficiencia.-

RECOMENDACIÓN: La metodología del ciclo de vida del desarrollo de sistemas (CVDS) del organismo debe garantizar la definición oportuna de los requerimientos operativos y niveles de servicio, la preparación de manuales de usuario y de operaciones y el desarrollo de materiales de capacitación. En este aspecto, se debe garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- requerimientos operativos y niveles de servicio,
- manuales de procedimientos del usuario,
- manual de operaciones,
- materiales de capacitación.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**4.2.5 - Instalación y Acreditación de Sistemas de Aplicación**

OBJETIVO DE CONTROL: La implementación de nuevos sistemas debe realizarse por medio de un plan bien formalizado de instalación, migración, conversión y aceptación.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Hay consistencia entre los enfoques de prueba y acreditación, pero no se basan en una metodología formal. Las áreas definidoras individuales son las que normalmente deciden el enfoque de prueba. Hay un procedimiento de aprobación no necesariamente basado en criterios estandarizados. La acreditación y aprobación formal se aplica ad hoc.-

DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido estándares formalmente definidos que comprendan la totalidad de las tareas requeridas para la implementación de los nuevos sistemas o modificaciones a los existentes. Esto puede generar deficiencias particulares en cada caso e impide la realización del control de cumplimiento e incertidumbre respecto a la calidad de la instrumentación realizada.-

RECOMENDACIÓN: Los funcionarios de las partes pertinentes y los funcionarios

responsables de la función de servicios de información deben preparar, revisar y aprobar un plan de implementación o modificación de los sistemas de aplicación. En este aspecto, se debe garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- capacitación de los usuarios y personal de servicios de información,
- dimensionamiento del desempeño del software de aplicación,
- plan de implementación,
- conversión de sistemas de aplicación,
- conversión de datos,
- estrategia y planes de prueba,
- prueba de cambios,
- criterios de ejecución de pruebas paralelas/piloto,
- prueba de aceptación final,
- pruebas de acreditación de seguridad,
- prueba de funcionamiento,
- transición a producción,
- evaluación del cumplimiento de los requerimientos del usuario,
- revisión de la gerencia posterior a la implementación.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**4.2.6 - Administración de Cambios**

OBJETIVO DE CONTROL: Se debe disponer de un sistema de administración de cambios que permita el análisis, la implementación y el seguimiento de todos los cambios solicitados y realizados en la infraestructura de Tecnología Informática existente.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Existe un proceso informal de administración de cambios, con un enfoque que se sigue para la mayoría de los casos. Sin embargo, este proceso no está estructurado. La documentación de la configuración no es precisa y sólo se hace una planificación y evaluación limitada del impacto antes del cambio.-

DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido un procedimiento formal de administración de cambios. Existe el riesgo de no

disponer de los cambios necesarios en el momento oportuno.-

RECOMENDACIÓN: La alta gerencia y el funcionario principal de la función de servicios de información deben implementar procedimientos específicos para tratar los pedidos de cambios, mantenimiento de sistema y mantenimiento del proveedor. En este aspecto, se debe garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- inicio y control de solicitudes de cambio,
- evaluación del impacto,
- control de cambios,
- cambios de emergencia,
- documentación y procedimientos,
- mantenimiento autorizado,
- política de versiones de software,
- distribución de software.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**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 que promueva el establecimiento de acuerdos de nivel de servicio que formalicen los criterios de desempeño en virtud de los cuales se medirá la cantidad y calidad del servicio.-

NIVEL DE MADUREZ: *Inicial / Ad Hoc*. 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.-

DESCRIPCIÓN: De la documentación recibida se deduce que los niveles de servicio comprometidos son genéricos y si bien demuestran la buena intención de las partes, no son mensurables y no garantizan la satisfacción de las necesidades del usuario.-

RECOMENDACIÓN: La alta gerencia es responsable de definir un marco dentro del cual

promueva la definición de acuerdos de nivel de servicio y defina los contenidos mínimos. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- marco de acuerdos de nivel de servicio,
- aspectos de los acuerdos de nivel de servicio,
- procedimientos de ejecución,
- monitoreo e informes,
- revisión de los contratos y acuerdos de nivel de servicio,
- ítems imputables,
- programa de mejora del servicio.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**4.3.2 - Administración de Servicios Prestados por Terceros**

OBJETIVO DE CONTROL: La máxima autoridad debe implementar medidas de control orientadas a la revisión y al monitoreo de los contratos y procedimientos existentes para garantizar su eficacia y el cumplimiento de la política del organismo.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* 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. Se toman mediciones, pero no son relevantes.-

DESCRIPCIÓN: No se obtuvo evidencia del registro de los servicios efectuados por mantenimiento de hardware informático. No existe control por parte de la gerencia de tecnología informática de las tareas de mantenimiento de infraestructura (aire acondicionado, sistemas de energía ininterrumpible, tableros de energía, sistemas de protección de incendio, sistemas de control de acceso y similares) que pueden afectar la continuidad de los servicios. El control de la prestación de los servicios de mantenimiento es responsabilidad del área de servicios generales. La delegación de la responsabilidad del monitoreo de la calidad del mantenimiento de los sistemas de infraestructura informática puede conducir a una situación de in operabilidad de los centros de cómputos. Ante la eventualidad de necesitar de servicios prestados por terceros, no existe un marco normativo adecuado.-

RECOMENDACIÓN: La máxima autoridad y la alta gerencia son responsables de que los servicios prestados por terceros se identifiquen de modo adecuado y que la interpelación técnica y funcional con los proveedores esté documentada. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- interpelación con proveedores de Tecnología Informática,
- asignar la responsabilidad por la 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.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**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, el análisis y los informes sobre el desempeño de los recursos de Tecnología Informática, la dimensión de los sistemas de aplicación y la demanda de cargas de trabajo.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* La máxima autoridad del organismo es consciente del impacto de no administrar la capacidad y el desempeño. En general, se satisfacen las necesidades de desempeño de las áreas críticas, en función de una evaluación de los sistemas individuales y del conocimiento de los equipos de soporte y de proyecto. Pueden usarse algunas herramientas aisladas para diagnosticar problemas de capacidad y desempeño, pero la uniformidad de los resultados depende de la pericia de personas clave. No hay una evaluación general del desempeño de la infraestructura de Tecnología Informática ni consideración de las situaciones de cargas pico en el peor de los casos. Es probable que surjan problemas de disponibilidad en forma inesperada y al azar, cuyo diagnóstico y corrección lleven un tiempo considerable.-

DESCRIPCIÓN: A pesar de la complejidad de los servicios informáticos que se prestan en la Administración, de la documentación recibida no se deduce que el organismo disponga de herramientas de modelado del desempeño de la infraestructura que permitan administrar adecuadamente la capacidad, la confiabilidad y la disponibilidad.-

RECOMENDACIÓN: La máxima autoridad y el funcionario principal de sistemas de información son responsables de identificar las necesidades de capacidad y desempeño de los servicios de información, y que se traduzcan en términos y requerimientos de disponibilidad. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- identificación de requerimientos de disponibilidad y desempeño,
- establecer un plan de disponibilidad,
- monitoreo e informes del desempeño de los recursos de Tecnología Informática,
- utilización de herramientas para la creación de modelos de desempeños,
- administración productiva del desempeño,
- pronósticos de la carga de trabajo,
- administración de la capacidad de los recursos,
- disponibilidad de recursos,
- planificación de recursos.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**4.3.4 - Garantía de un Servicio Continuo**

OBJETIVO DE CONTROL: La máxima autoridad debe implementar un plan de continuidad de tecnología de información probado y operativo que concuerde con el plan de continuidad general del organismo y sus requerimientos de actividad relacionados.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* La responsabilidad del servicio continuo ha sido asignada. Los enfoques al servicio continuo son fragmentados. Los informes de la disponibilidad de sistemas son incompletos y no tienen en cuenta el impacto en el organismo. No hay planes del usuario o de continuidad documentados, a pesar de que hay un compromiso con la disponibilidad de un servicio continuo y se conocen sus principios más importantes. Existe un inventario no confiable de los sistemas y componentes críticos. Está apareciendo

una estandarización de las prácticas de servicio continuo y monitoreo del proceso, pero su éxito depende de cada persona.-

DESCRIPCIÓN: De la documentación recibida se deduce que los planes para garantizar la continuidad del servicio están siendo redactados. Se está a la espera de la contratación de un aplicativo a usar como herramienta para la preparación de un plan de contingencia completo.-

RECOMENDACIÓN: El funcionario principal de la función de servicios de información es responsable de crear un marco de continuidad que defina los roles, responsabilidades, enfoque y las normas y estructuras para documentar el plan, como así también los procedimientos de aprobación. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- marco de continuidad de Tecnología Informática,
- estrategias y filosofía del plan de continuidad de Tecnología Informática,
- contenido del plan de continuidad de Tecnología Informática,
- reducción de los requerimientos de continuidad de Tecnología Informática,
- mantenimiento del plan de continuidad de Tecnología Informática,
- prueba del plan de continuidad de Tecnología Informática,
- capacitación en el plan de continuidad de Tecnología Informática,
- distribución del plan de continuidad de Tecnología Informática,
- procedimientos para el resguardo del procesamiento alternativo del usuario,
- identificar recursos críticos de Tecnología Informática,
- sitio y equipamiento alternativo,
- almacenamiento de resguardo en sitio alternativo,
- reevaluación periódica del plan.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**4.3.5 - Garantía de la Seguridad de los Sistemas**

OBJETIVO DE CONTROL: La máxima autoridad debe establecer y mantener un programa de seguridad de la información para implementar los controles de acceso lógico que garantizan que el acceso a los sistemas, datos y programas está limitado a los usuarios autorizados.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Las responsabilidades y la rendición de cuentas de la seguridad de Tecnología Informática están asignadas a un coordinador de Tecnología Informática que depende directamente de la Subdirección General. La concientización de la seguridad es fragmentada y limitada. Las soluciones de seguridad tienden a responder reactivamente a los incidentes de seguridad de Tecnología Informática. Se están desarrollando políticas de seguridad, pero todavía se usan habilidades y herramientas inadecuadas.-

DESCRIPCIÓN: De la documentación recibida se deduce que la seguridad de acceso lógico está limitada a los servidores centrales de aplicaciones y datos excluyendo a la red de computadoras personales e impresoras de red del organismo. Se está trabajando para que el acceso a los datos lo maneje la base de datos y no cada uno de los aplicativos. Los usuarios no tienen control sobre el uso de sus propias cuentas.-

RECOMENDACIÓN: La alta gerencia es responsable de la gestión de la seguridad de la información de modo tal que las medidas de seguridad de Tecnología Informática concuerden con los requerimientos de la misión del organismo. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- administración de las medidas de seguridad,
- identificación, autenticación y acceso,
- seguridad del acceso en línea a los datos,
- administración de cuentas de usuarios,
- revisión por la gerencia de las cuentas de usuarios,
- control ejercido por el usuario en sus propias cuentas,
- supervisión de la seguridad,
- clasificación de los datos,
- administración centralizada de identificaciones y derechos de acceso,
- informes de violación y actividades de seguridad,
- manejo de incidentes,
- reacreditación,
- confianza en la contraparte,

- autorización de transacciones,
- imposibilidad de rechazo,
- ruta de acceso confiable,
- protección de las funciones de seguridad,
- administración de claves criptográficas,
- prevención, detección y corrección de software malicioso,
- arquitectura de firewalls y conexiones con redes públicas,
- protección de valores electrónicos.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**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 con la posibilidad de ofrecer el servicio adecuado.-

NIVEL DE MADUREZ: *Inicial / Ad Hoc*. 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.-

DESCRIPCIÓN: De la documentación recibida se deduce que si bien se tiene conciencia de la necesidad de un sistema de imputación, no existe por el momento ningún tipo de asignación de costos informáticos. En las conversaciones mantenidas se reconoce que algunas modificaciones de los sistemas existentes para adaptarlos a actos o decisiones emanados de otras autoridades (leyes, decretos, resoluciones, etc.), generan costos superiores a los beneficios que las disposiciones generan al fisco. No se puede evaluar la eficiencia del gasto del área de Tecnología Informática.-

RECOMENDACIÓN: El funcionario responsable de la función de servicios de información, con la orientación de la alta gerencia, debe definir e implementar procedimientos de determinación de costos para ofrecer información administrativa sobre los costos de la

prestación de los servicios de procesamiento de información. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- identificar ítems imputables,
- definir procedimientos de determinación de costos,
- utilizar procedimientos de cargos e imputación de costos al usuario.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**4.3.7 - Educación y Capacitación de los Usuarios**

OBJETIVO DE CONTROL: Se debe establecer y mantener un plan integral de capacitación y desarrollo.-

NIVEL DE MADUREZ: *Inicial / Ad Hoc*. Hay evidencia de que el organismo reconoció la necesidad de un programa de educación y capacitación, pero no hay procesos estandarizados. El enfoque global de la dirección carece de cohesión y la comunicación de los temas y abordajes de la educación y capacitación es sólo esporádica y poco coherente.-

DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido un programa organizado que origine que los empleados asistan a cursos de capacitación sobre temas de conducta ética, concientización de seguridad de sistemas y prácticas de seguridad. La alta gerencia de Tecnología Informática delega la planificación de la capacitación en el área de Recursos Humanos.-

RECOMENDACIÓN: La máxima autoridad es responsable de impulsar procedimientos para identificar y documentar las necesidades de capacitación de todo el personal que utiliza servicios de información. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- identificación de necesidades de capacitación,
- organización de sesiones de capacitación,
- capacitación y concientización en los principios de seguridad.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**4.3.8 - Asistencia y Asesoramiento a los Usuarios de Tecnología Informática**

OBJETIVO DE CONTROL: Se debe establecer una función de mesa de ayuda que brinde soporte y asesoramiento de primera línea.-

NIVEL DE MADUREZ: *Proceso Definido*. Hay una acabada comprensión de los beneficios que puede brindar una mesa de ayuda en todos los niveles del organismo, y dicha función se ha creado en unidades organizacionales apropiadas. Los procedimientos se estandarizaron y documentaron, y se está dictando una capacitación informal. Sin embargo, la capacitación y adhesión a las normas corre por cuenta de cada persona. Se desarrollaron preguntas frecuentes y pautas para el usuario, pero no están lo suficientemente accesibles y tal vez no siempre sean observadas. Se hace un seguimiento manual y un monitoreo individual de las consultas y los problemas, pero no existe un sistema formal de presentación de informes. Ha empezado a implementarse el escalamiento de problemas. La respuesta oportuna a las consultas y los problemas no se mide y puede haber problemas a los que no se dé solución.-

DESCRIPCIÓN: Se está utilizando un sistema de aplicación Mr. Sea que cuenta con pocas licencias y no incluye el módulo de gerenciamiento para efectuar el seguimiento de las tendencias y generar informes sobre las actividades de la mesa de ayuda. El personal disponible, 12 agentes, resulta escaso para los catorce mil usuarios internos de la Administración. Los usuarios externos (contribuyentes y otros) no acceden directamente a la mesa de ayuda del área de Tecnología Informática sino a la del área correspondiente a sus aportes. No está claro el procedimiento de escalamiento entre mesas de ayuda.-

RECOMENDACIÓN: El funcionario principal de servicios de información es responsable de establecer el soporte al usuario dentro de la función de mesa de ayuda. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- el soporte al usuario a través de la mesa de ayuda,
- registro de consultas de usuarios,
- escalamiento de consultas de usuarios,
- monitoreo de soluciones,
- análisis e informe de tendencias.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

### 4.3.9 - Administración de la Configuración

OBJETIVO DE CONTROL: Se deben implementar controles que identifiquen y registren todos los bienes de Tecnología Informática y su ubicación física, y un programa de verificación regular que confirme su existencia.-

NIVEL DE MADUREZ: *Inicial / Ad Hoc*. 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.-

DESCRIPCIÓN: No se recibió la documentación solicitada que hubiese permitido verificar la existencia de procedimientos que aseguren el registro e identificación en inventario de los bienes de Tecnología Informática. Tampoco se pudo determinar la existencia de procedimientos para la administración de los cambios en la configuración.-

RECOMENDACIÓN: El funcionario principal de la función de servicios de información es responsable de implementar procedimientos de control para identificar y registrar todos los bienes de Tecnología Informática y su ubicación física, y una rutina de verificación regular que confirme su existencia. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- registro de la configuración,
- nivel básico de configuración,
- registro del estado de la configuración,
- control de la configuración,
- detectar el software no autorizado,
- almacenamiento del software,
- procedimientos de administración de configuración,
- seguimiento y control de versiones de software.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

### 4.3.10 - Administración de Problemas e Incidentes

OBJETIVO DE CONTROL: Se debe implementar un sistema de administración de problemas que registre y dé respuesta a todos los incidentes.-

NIVEL DE MADUREZ: *Proceso Definido*. La necesidad de un sistema eficaz de administración de problemas es aceptada y evidenciada por la intención de contratación de una herramienta específica. Los procesos de solución de problemas, escalamiento y resolución están normados. Los usuarios recibieron comunicaciones sobre dónde y cómo informar problemas e incidentes. El registro y seguimiento de los problemas y su resolución está fragmentado dentro del equipo de respuesta, que utiliza las herramientas disponibles. Las desviaciones de las normas o los estándares establecidos probablemente pasen desapercibidas.-

DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido la política de registro y respuesta a incidentes incluyendo el escalamiento de problemas. Está prevista la adquisición de una herramienta que permita su administración eficaz y eficiente.-

RECOMENDACIÓN: El funcionario principal de la función de servicios de información es responsable de implementar un sistema de administración de problemas e incidentes de seguridad. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- sistema de administración de problemas,
- escalamiento de problemas,
- seguimiento de problemas y pistas de auditoría,
- autorizaciones de emergencia y acceso temporario,
- prioridades de procesamiento de emergencia.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**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 Informática para asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* En todo el organismo prevalece el reconocimiento de la necesidad de la exactitud de los datos y del mantenimiento de su

integridad. Se comienza a asignar responsabilidad sobre los datos. Las reglas y los requerimientos no son uniformes en todo el organismo y todas las plataformas. Los datos están en custodia de la función servicios de información y las reglas y definiciones son impulsadas por los requerimientos de Tecnología Informática. La seguridad e integridad de los datos entran principalmente dentro de las responsabilidades de la función de servicios de información.-

DESCRIPCIÓN: La captura de datos se encuentra automatizada en forma prácticamente total. Sin embargo se están programando tareas de reingeniería de los sistemas existentes (Vg. Sistema de Declaraciones Juradas) para adecuarlos a un ingreso remoto de los datos por parte del usuario final (contribuyente) sin generar puntos de falla en su ciclo de procesamiento. Las salidas impresas se han reducido significativamente y el volumen de impresión es bajo. La operación de resguardo de los datos no incluye la prueba periódica de restauración que garantice la eficacia de la copia.-

RECOMENDACIÓN: La alta gerencia y toda la organización son responsables de establecer procedimientos para garantizar la calidad de los datos. En este aspecto, se debe garantizar la eficacia de los procedimientos y prácticas formalmente establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- procedimientos de preparación de datos,
- procedimientos de autorización de documentos fuente,
- recopilación de datos de documentos fuente,
- manejo de errores de documentos fuente,
- conservación de documentos fuente,
- procedimientos de autorización de entrada de datos,
- verificación de exactitud, integridad y autorización,
- manejo de errores de entrada de datos,
- 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,
- períodos de conservación y condiciones de almacenamiento,
- sistema de administración de biblioteca de medios,
- responsabilidades de administración de la biblioteca de medios,
- procedimiento de resguardo y restauración,
- tareas de resguardo,
- almacenamiento de resguardos,
- archivos,
- protección de mensajes críticos,
- autenticación e integridad,

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**4.3.12 - Administración de Instalaciones**

OBJETIVO DE CONTROL: Se debe contar con controles ambientales y físicos adecuados cuya revisión se efectúe periódicamente a fin de determinar su correcto funcionamiento.-

NIVEL DE MADUREZ: *Inicial / Ad Hoc*. El organismo reconoce el requerimiento de la actividad de brindar un entorno físico adecuado que proteja los recursos y el personal contra los peligros generados por la naturaleza y el hombre. No existen procedimientos estándares y la administración de las instalaciones y los equipos dependen de la idoneidad y capacidad de ciertas personas clave. No se revisan las actividades de maestranza en las instalaciones y la gente se desplaza con restricciones relativas. La dirección no monitorea los controles ambientales de las instalaciones ni el movimiento del personal. Los procedimientos de mantenimiento de las instalaciones no están documentados y dependen de las mejores prácticas del personal de Servicios Generales. Las metas de la seguridad física no están basadas en ninguna norma formal y la gestión no garantiza que se cumplan los objetivos de

seguridad.

DESCRIPCIÓN: No se registran todos los accesos a los centros de cómputos. Se ha observado que, cuando existe un libro de registro de visitas, las entradas registradas en tres días sólo comprenden al personal de esta Auditoría y no figura el personal de proveedores que, simultáneamente, está realizando tareas de instalación. Se ha verificado in situ que existen sistemas de alarma de acceso físico cuyo uso es desconocido por el personal y que están prácticamente fuera de servicio.-

RECOMENDACIÓN: El funcionario principal de la función de servicios de información es responsable de implementar medidas de control de acceso y seguridad física adecuadas en las instalaciones de tecnología de información. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- seguridad física,
- discreción del sitio de tecnología de información,
- acompañamiento de visitas,
- salud y seguridad del personal,
- protección contra factores ambientales,
- fuente de alimentación de energía ininterrumpible y elementos alternativos que garanticen la continuidad del servicio.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

#### 4.3.12.1 Seguridad Física

OBJETIVO DE CONTROL: Deberán establecerse medidas apropiadas de seguridad física y control de acceso para las instalaciones de tecnología de información de acuerdo con la política de seguridad general, incluyendo el uso de dispositivos de información fuera de las instalaciones. El acceso deberá restringirse a las personas debidamente autorizadas.-

**A - Centro de Cómputos de los Edificios: Hipólito Yrigoyen y Paseo Colón**

DESCRIPCIÓN: No se obtuvo evidencia de normas y procedimientos para el control de entradas y salidas.-

RECOMENDACIÓN: Deben formalizarse normas y procedimientos para el control de

entradas y salidas al Centro de Cómputos.-
NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**4.3.12.2 Escolta de Visitantes**

OBJETIVO DE CONTROL: Deberán establecerse apropiados procedimientos que aseguren que las personas que no formen parte del grupo de operaciones de la función de servicios de información sean escoltadas por algún miembro de ese grupo cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes.-

**A - Centro de Cómputos de los Edificios: Hipólito Yrigoyen y Paseo Colón**

DESCRIPCIÓN: Las visitas que acceden a los Centros de Cómputos no se acreditan en los Accesos a los edificios del organismo. En la entrada al edificio no se solicita el documento de identidad ni se avisa telefónicamente a los Centros de Cómputos quien va a ingresar.-

RECOMENDACIÓN: Se deben formalizar procedimientos para acceder a los Centros de Cómputos desde el ingreso al Organismo. Un miembro del Centro de Cómputos debe escoltar a las visitas en los Centros de Cómputos.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**4.3.12.3 Salud y Seguridad del Personal**

OBJETIVO DE CONTROL: Deberán establecerse y mantenerse prácticas de salud y seguridad en línea con las leyes y regulaciones nacionales y locales.-

**A - Centro de Cómputos de los Edificios: Hipólito Yrigoyen y Paseo Colón**

DESCRIPCIÓN: No se obtuvo evidencia de las mediciones de los niveles de iluminación (Ley de Higiene y Seguridad / Ley de Riesgo del Trabajo), ni sobre los registros de inspección en instalaciones eléctricas, como así tampoco de los planes de inspección de los equipos.-

RECOMENDACIÓN: Se deben realizar las mediciones de los niveles de iluminación y, si corresponde, adecuarlos a la Legislación vigente.-

Se debe realizar una planificación sobre las inspecciones de los equipos, como así también efectuar los registros de inspección de las instalaciones eléctricas que se realizan.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**4.3.12.4 Protección contra Factores Ambientales**

OBJETIVO DE CONTROL: La gerencia de la función de servicios de información deberá asegurar que se establezcan y mantengan las suficientes medidas para la protección contra los factores ambientales (por ejemplo, fuego, polvo, electricidad, calor o humedad excesivos). Deberán instalarse equipo y dispositivos especializados para monitorear y controlar el ambiente.-

**A - Centro de Cómputos de los Edificios: Hipólito Yrigoyen y Paseo Colón**

DESCRIPCIÓN: No se ha obtenido evidencia formal con respecto a:

- la política en materia de Seguridad y Salud Ocupacional definida por las máximas autoridades del Organismo,
- los antecedentes y documentación de la obra, como así tampoco de los estudios de carga de fuego y las normas que se han tenido en cuenta en el diseño de los Centros de Cómputos desde el punto de vista de riesgo de incendios,
- evaluaciones de riesgo en caso de incendio con respecto a los locales linderos,
- la documentación probatoria correspondiente a los controles de los matafuegos,
- el procedimiento para realizar la limpieza de los Centros de Cómputos, como así tampoco de los registros donde se indique que el personal de limpieza tiene conocimiento del mismo,
- si se inspeccionan antes de retirarse de los locales de los Centros de Cómputos. Los recipientes de residuos no tienen tapa y las bolsas de residuos son negras (opacas),
- un procedimiento escrito indicando el destino de las cintas, cartuchos y toner de las impresoras usados,
- las evaluaciones y estudios en el sistema de ventilación cuando se cambian y/o ingresan equipos,
- los registros de los controles de variación de la temperatura,
- los registros de los controles de las luces de emergencia.
- las normas que indican con qué frecuencia se inspeccionan y se realiza la limpieza de piso técnico (Polvo, basuras, acumulación de cables que no se usan, etc.). Potencial riesgo de incendio,

- la capacitación del personal en el manejo de los matafuegos,
- instrucciones en los locales indicando cómo actuar en caso de incendio en el Centro de Cómputos. Impide actuar en forma rápida y eficaz,
- la ejecución de los simulacros de evacuación,
- la documentación y control de los Sistemas de Hidrantes,
- los registros de los Sistemas de Detección y Extinción de incendios,
- las instrucciones, ni los registros de controles sobre el gas extintor FM–200. Potenciales fallas en el funcionamiento del Sistema de Extinción durante un incendio.-

No existe un sistema de audio para usarlo en caso de emergencia.-

En algunos locales no se observan los carteles indicando “Prohibido Fumar”.-

Inexistencia de escaleras de emergencias.-

RECOMENDACIÓN: Fijar la política en materia de Seguridad y Salud Ocupacional.-

Disponer de los antecedentes y la documentación de la obra, estudios de carga de fuego y las normas que se han tenido en cuenta en los diseños de los Centro de Cómputos desde el punto de vista de riesgo de incendios.-

Realizar una evaluación sobre cómo afectaría al Centro de Cómputos un incendio en otras áreas.-

Obtener la documentación correspondiente a los controles que se realizan de los matafuegos.-

Asegurar la existencia de procedimientos para las tareas de limpieza y recolección de bolsas de residuos. Es conveniente que las bolsas de residuos sean transparentes. Todos los recipientes de residuos deben tener bolsas y ser resistentes al fuego.-

Asegurar la existencia de un procedimiento respecto al destino de elementos usados como las cintas, cartuchos y toner de impresoras.-

Realizar evaluaciones y estudios en el sistema de ventilación cuando se cambian y/o ingresan equipos.-

Obtener los registros de las variaciones de temperatura.-

Realizar un mantenimiento integral de las luces de emergencia con los correspondientes registros.-

Formalizar normas para la inspección y limpieza de los pisos falsos.-

Capacitar y entrenar en forma semestral al personal de los Centros de Cómputos en el manejo

de los matafuegos.-

Los locales deberían tener instrucciones indicando como actuar en caso de incendio.-

Realizar los simulacros de evacuación.-

Obtener la documentación y los controles de los Sistemas de Hidrantes. Riesgo: Potencial falta de respuesta ante un incendio.-

Construir una escalera de emergencia o conformar, si es posible “Caja de Escalera”.-

Efectuar el control de los Sistemas de Detección y Extinción y obtener los registros correspondientes.-

Colocar instrucciones sobre el sistema de extinción fijo y realizar los controles correspondientes.-

Instalar un sistema de audio para casos de emergencia.-

Colocar los carteles faltantes indicando “Prohibido Fumar”.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**B - Centro de Cómputos de los Edificios: Hipólito Yrigoyen**

DESCRIPCIÓN: El acceso de algunos matafuegos se encuentra obstruido. No se obtuvo evidencia sobre:

- los controles y registros de humedad,
- protección de los accesos contra el fuego en áreas externas al Centro de Cómputos,
- Plan de Emergencia y Evacuación.-

En los pisos de las áreas de ingreso al Centro de Cómputos se observan falta de revestimientos (cerámicas), cajas y otros elementos sobre el piso.-

Se fuma en los locales del Centro de Cómputos.-

El depósito de insumos del Centro de Cómputos no posee un sistema de detección y extinción.-

No se han observado en la puerta principal controles eléctricos de emergencia (llaves de corte de energía eléctrica usadas en casos de emergencia).-

La puerta de emergencia se abre frecuentemente.-

Es confusa la Señalización para acceder al Centro de Cómputos, se observa doble numeración en los locales. Los números indicados en los carteles generales no coinciden con los de las

oficinas pudiendo demorar la llegada de auxilio.-
RECOMENDACIÓN: Mantener libres los accesos a los matafuegos.-
Realizar el control de la humedad, como así también obtener los registros correspondientes.-
Proteger los locales contra posibles fuegos externos al Centro de Cómputos.-
Reparar los pisos y liberar las rutas de ingreso y egreso.-
Formalizar el Plan de Emergencia y Evacuación, aprobarlo y ejecutarlo.-
Prohibir fumar.-
Instalar un sistema de detección y extinción en el depósito de insumos.-
Instalar en las puertas controles eléctricos de emergencia accesibles al operador (llaves de corte de energía eléctrica usadas en casos de emergencia). Los mismos deberían estar protegidos contra potenciales sabotajes, etc. ocasionados por personal no autorizado.-
Realizar las modificaciones correspondientes a la señalización de las oficinas.-

**C - Centro de Cómputos de los Edificios: Paseo Colón – Primer Piso**
DESCRIPCIÓN: Los matafuegos no se encuentran ubicados correctamente.-
La instalación de algunos equipos permite que los cables provenientes del piso técnico queden a la vista.-
RECOMENDACIÓN: Mantener libres los accesos a los matafuegos.-
Instalar los equipos evitando que los cables provenientes del piso técnico queden a la vista.-

D - **Centro de Cómputos de los Edificios: Paseo Colón – Tercer Piso**
DESCRIPCIÓN: Algunos insumos están distribuidos sobre el piso del local.-
La instalación de algunos equipos permite que los cables provenientes del piso técnico queden a la vista.-
No se han observado en la puerta principal controles eléctricos de emergencia (llaves de corte de energía eléctrica usadas en casos de emergencia).-
RECOMENDACIÓN: Ordenar y retirar los elementos combustibles que se encuentran en los locales.-
Instalar los equipos evitando que los cables provenientes del piso técnico queden a la vista.-
Instalar en la puerta controles eléctricos de emergencia accesibles al operador (llaves de corte

de energía eléctrica usadas en casos de emergencia). Los mismos deberían estar protegidos contra potenciales sabotajes, etc. ocasionados por personal no autorizado.-

**4.3.13 - Administración de Operaciones**

OBJETIVO DE CONTROL: Se debe establecer un cronograma de actividades de soporte que registre todas las tareas a realizar y su oportunidad.-

NIVEL DE MADUREZ: *Proceso Definido*. La necesidad de administrar las operaciones de sistemas es comprendida y aceptada dentro del organismo. Se asignaron recursos y se brinda entrenamiento, no permanente, para el puesto de trabajo. Los eventos y resultados de las tareas completas se registran, pero no se guardan en el tiempo, los informes a la dirección son limitados. El uso de programación automatizada y otras herramientas se extiende y estandariza para limitar la intervención del operador. Otras actividades regulares de soporte de la tecnología informática también son identificadas y las tareas relacionadas están siendo definidas. Se ejercen controles para poner en operación los puestos nuevos. Los acuerdos de mantenimiento y servicio con proveedores son formales.-

DESCRIPCIÓN: De la información recibida no se deduce que las operaciones están respaldadas por presupuestos de recursos para gastos de capital y recursos humanos. La capacitación no está formalizada ni es continua. No resultó posible medir y monitorear las actividades diarias con acuerdos de desempeño estandarizados y niveles de servicio establecidos. No está establecida una política formal para reducir la cantidad de eventos no programados. Se entablan acuerdos formales de mantenimiento y servicio con los proveedores del mantenimiento de hardware y software.-

RECOMENDACIÓN: El funcionario principal de la función de servicios de información es responsable de establecer y documentar los procedimientos estándar para las operaciones de tecnología de información. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- manuales de instrucciones y procedimientos de las operaciones de procesamiento,
- documentación del proceso de puesta en marcha y otras operaciones,
- programas de trabajo,
- desviaciones de los programas estándares de trabajo,

- continuidad del procesamiento,
- registro de operaciones,
- salvaguardia de formularios especiales y dispositivos de salida,
- operaciones remotas.-

NIVEL DE RIESGO: [ ] Bajo [X] Medio [ ] Alto

**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 del desempeño y la acción inmediata en caso de desviaciones.-

NIVEL DE MADUREZ: *Inicial / Ad Hoc.* La dirección reconoce la necesidad de recopilar y evaluar información sobre los procesos de monitoreo. No se identificaron procesos estándares de recopilación y evaluación. El monitoreo en general se implementa en forma insuficiente para los requerimientos del organismo.

DESCRIPCIÓN: Se dificulta la evaluación de la gestión de la Tecnología Informática por falta de estadísticas confiables.-

RECOMENDACIÓN: La alta gerencia es responsable de que se definan los indicadores de desempeño pertinentes y que se recopilen datos para la elaboración de informes de gestión y 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, se debe garantizar que se:

- recopilan los datos de monitoreo,
- evalúa el desempeño en forma continua,
- evalúa la satisfacción del usuario,
- elaboran los informes de gestión.-

NIVEL DE RIESGO: [ ] Bajo [ ] Medio [X] Alto

**5. Comunicación del proyecto de informe y análisis de los descargos formulados por la Administración Federal de Ingresos Públicos**.

El proyecto de informe de auditoría fue enviado al organismo auditado para que formule las observaciones y/o comentarios que estime pertinentes, con fecha 21 de abril de 2004, por Nota AGN N° C.S. 80/2004 A02. Los mismos fueron remitidos por la Administración Federal de Ingresos Públicos, con fecha 4 de junio de 2004 a través de la Nota N° 13288-771-04-2

Como consecuencia del análisis del descargo presentado por el organismo auditado (que consta como Anexo), se ratifican las observaciones oportunamente formuladas.

**6. Conclusiones**

La situación de la Tecnología Informática en la Administración Federal de Ingresos Públicos, basándose en los procedimientos efectuados y la evidencia obtenida, merece las siguientes observaciones.-

- No existen procedimientos formales para la planificación estratégica de la tecnología de la información, que establezcan su relación con los objetivos estratégicos del organismo. Los planes generales de la Subdirección General definen metas concretas sin estimación de costos ni plazos, lo que dificulta su monitoreo y evaluación.-
- No se recibió información normativa en el tema de arquitectura de la información. Existe un sistema denominado SUPA (Sistema Único de Parámetros de AFIP) que incluye el diseño de la mayoría de las tablas de Oracle. La intención es que cada tabla tenga un dueño responsable de la administración de sus campos. Se está trabajando en el tema sin asignarle un rol protagónico en la planificación informática. Ello genera confusión en el uso de la información, especialmente cuando se la trata con fines de control fiscal.-
- No existen procedimientos formales para la confección de un plan de infraestructura tecnológica. Se han fijado rumbos, en esta materia, contenidos en el Plan General de Sistemas que se pueden compartir; sin embargo no están justificados ni evaluados. Se determinan temas estratégicos de alta significación económica para la Nación sin evaluación formal de impacto, riesgos y costos.-
- Faltan formalizar las relaciones con otras partes, tales como comités de dirección,

auditoría interna y administración de proveedores. La organización no está funcionalmente completa. La alta gerencia del Organismo reconoce tener limitaciones por falta de nivel técnico del personal y por la inestabilidad del personal contratado, significativo en áreas de informática.-

- No existen procedimientos formales que definan el mecanismo para la administración de la inversión. Los presupuestos anuales de tecnología informática recibidos son incompletos y no representativos. La inversión principal se realiza a través de organismos internacionales, lo que dificulta tener una visión global del presupuesto y su ejecución.-
- No existen políticas formales para la comunicación de las decisiones y normativas del área y tampoco para el control de su cumplimiento.-
- No existen procedimientos formales para la selección, formación y promoción del personal. Ello promueve las limitaciones mencionadas por la falta de nivel técnico del personal y por la inestabilidad del personal contratado.-
- No están establecidos procedimientos formales relativos al cumplimiento general de los requerimientos externos.-
- No existen procedimientos formales referentes a la administración de riesgos y tampoco una evaluación y un plan de acción de reducción de riesgos. Se desconoce el nivel de riesgo de la Tecnología Informática en la Administración.-
- Desde principios del año 2002 se está llevando a cabo la transformación del área de Tecnología de la Información de la Administración Federal de Ingresos Públicos. Esto abarca la totalidad de las incumbencias del sector y prácticamente la totalidad de su personal. El éxito del proyecto hace a la calidad y cantidad de la recaudación pública de la Nación. No existe una metodología formalmente establecida en el Organismo para la administración de proyectos de esta naturaleza, incluyendo a este proyecto, y tampoco se está utilizando alguna de las metodologías clásicas de programación por camino crítico. El tiempo y los gastos del personal asignado al proyecto no se presupuestan ni controlan. Las reprogramaciones plasmadas en Planes para cada año calendario se realizan de acuerdo con las necesidades que surgen y los atrasos que se generan. Durante el año se han detectado modificaciones en las tareas programadas que no se reflejaron en los documentos recibidos.-

- No se han detectado intentos por desarrollar un plan general de calidad.-
- El organismo no estableció una metodología escrita de implementación de las soluciones de Tecnología Informática para satisfacer los requerimientos de AFIP. Cada una de las áreas que antes eran independientes (DGI, DGA, DGRSS) tiene sus propias características al respecto. No se realiza la consideración escrita de alternativas, evaluadas con respecto a los requerimientos del usuario, oportunidades tecnológicas, factibilidad económica, evaluaciones de riesgos y otros factores. El proceso no se sigue por igual en todos los proyectos y depende de las decisiones tomadas por el personal involucrado y la dimensión y prioridad del requerimiento del problema original.-
- No existe una metodología formal para definir las necesidades de nuevas aplicaciones y los requerimientos de sus actualizaciones y mantenimiento. En estos momentos no se están contratando servicios externos de provisión de soluciones; pero, si hubiera que hacerlo por razones de fuerza mayor, tampoco existen procedimientos para la adquisición y acreditación de aplicaciones provistas por terceros.-
- No se ha encontrado un marco normativo formal referente a la adquisición y mantenimiento de la infraestructura tecnológica y de su integridad. No se evidencia capacidad de monitorear y medir el desempeño de la infraestructura existente con miras a la detección oportuna de problemas y el dimensionamiento de las ampliaciones. No se encontraron registros, tales como registros de fallas debidas a falta de mantenimiento o a cambio de hardware o software de sistemas y registros de costos de las grandes modificaciones de infraestructura, que garanticen la elaboración de índices de desempeño. El costo y el tiempo para llegar al nivel deseable de escalabilidad, flexibilidad e integración no están determinados. Se debe sobredimensionar la infraestructura a fin de evitar limitaciones ante problemas sobre los que no existen registros históricos.-
- No se ha definido en la Administración una metodología del ciclo de vida del desarrollo de sistemas. Los niveles de servicio acordados con los usuarios son no mensurables. No se tiene control del nivel de satisfacción de los usuarios con los manuales y materiales de capacitación. Esta situación deviene en pérdida de eficacia y eficiencia.-
- La ausencia de estándares formalmente definidos que comprendan la totalidad de las tareas requeridas para la implementación de los nuevos sistemas o modificaciones a los

existentes puede generar deficiencias particulares en cada caso e impide la realización de un control de cumplimiento e incertidumbre respecto a la calidad de la instrumentación realizada.-

- No se ha encontrado un procedimiento formal de administración de cambios. Existe el riesgo de no disponer de los cambios necesarios en el momento oportuno.-
- Los niveles de servicio comprometidos son genéricos y sólo demuestran la buena intención de las partes. No son mensurables. No garantizan la satisfacción de las necesidades del usuario.-
- No se obtuvo evidencia del registro de los servicios efectuados por mantenimiento de hardware informático. No existe control por parte de la gerencia de tecnología informática de las tareas de mantenimiento de infraestructura (aire acondicionado, sistemas de energía ininterrumpible, tableros de energía, sistemas de protección de incendio, sistemas de control de acceso y similares) que pueden afectar la continuidad de los servicios. El control de la prestación de los servicios de mantenimiento es responsabilidad del área de servicios generales. La delegación de la responsabilidad del monitoreo de la calidad del mantenimiento de los sistemas de infraestructura informática puede conducir a una situación de in operabilidad de los centros de cómputos.-
- A pesar de la complejidad de los servicios informáticos que se prestan en la Administración no se cuenta con herramientas de modelado del desempeño de la infraestructura que permitan administrar adecuadamente la capacidad, la confiabilidad y la disponibilidad.-
- Está pendiente la preparación de un plan de contingencia completo.-
- La seguridad de acceso lógico está limitada a los servidores centrales de aplicaciones y datos excluyendo a la red de computadoras personales e impresoras de red del organismo. Se está trabajando para que el acceso a los datos lo maneje la base de datos y no cada uno de los aplicativos. Los usuarios no tienen control sobre el uso de sus propias cuentas.-
- No existe ningún tipo de asignación de costos informáticos. En las conversaciones mantenidas se reconoce que algunas modificaciones de los sistemas existentes para adaptarlos a actos o decisiones emanados de otras autoridades (leyes, decretos, resoluciones, etc.), generan costos superiores a los beneficios que las disposiciones

generan al fisco. No se puede evaluar la eficiencia del gasto del área de Tecnología Informática.-

- En ausencia de un programa organizado los empleados no asisten a cursos de capacitación que traten temas de conducta ética, concientización de seguridad de sistemas y prácticas de seguridad. La alta gerencia de Tecnología Informática delega la planificación de la capacitación en el área de Recursos Humanos.-
- Se está utilizando un sistema de aplicación Mr. Sea que cuenta con pocas licencias y no incluye el módulo de gerenciamiento para efectuar el seguimiento de las tendencias y generar informes sobre las actividades de la mesa de ayuda. El personal disponible, doce agentes, resulta escaso para los catorce mil usuarios internos de la Administración. Los usuarios externos (contribuyentes y otros) no acceden directamente a la mesa de ayuda del área de Tecnología Informática sino a la del área correspondiente a sus aportes. No está claro el procedimiento de escalamiento entre mesas de ayuda.-
- No se recibió la documentación solicitada que hubiese permitido verificar la existencia de procedimientos que aseguren el registro e identificación en inventario de los bienes de Tecnología Informática. Tampoco se pudo determinar la existencia de procedimientos para la administración de los cambios en la configuración.-
- No se cuenta con una herramienta que permita la administración eficaz y eficiente de los incidentes registrados.-
- La captura de datos se encuentra automatizada en forma prácticamente total. Sin embargo se están programando tareas de reingeniería de los sistemas existentes (Vg. Sistema de Declaraciones Juradas) para adecuarlos a un ingreso remoto de los datos por parte del usuario final (contribuyente) sin generar puntos de falla en su ciclo de procesamiento. Las salidas impresas se han reducido significativamente y el volumen de impresión es bajo. La operación de resguardo de los datos no incluye la prueba periódica de restauración que garantice la eficacia de la copia.-
- No se registran todos los accesos a los centros de cómputos. Se ha observado que, cuando existe un libro de registro de visitas, las entradas registradas en tres días sólo comprenden al personal de esta Auditoría y no figura el personal de proveedores que, simultáneamente, está realizando tareas de instalación. Se ha verificado in situ que existen sistemas de

alarma de acceso físico cuyo uso es desconocido por el personal y que alguno no está siendo utilizado.-

- Las operaciones no están respaldadas por presupuestos de recursos para gastos de capital y recursos humanos. La capacitación no está formalizada ni es continua. No resultó posible medir y monitorear las actividades diarias con acuerdos de desempeño estandarizados y niveles de servicio establecidos. No está establecida una política formal para reducir la cantidad de eventos no programados. Se entablan acuerdos formales de mantenimiento y servicio con los proveedores del mantenimiento de hardware y software.-
- Se dificulta la evaluación de la gestión de la Tecnología Informática por falta de estadísticas confiables.-

Se recomienda generar políticas que aseguren:

- la implementación y el desarrollo de planes de tecnología informática a corto y largo plazo con estimación de recursos y plazos de ejecución que permitan su monitoreo,
- crear y mantener un modelo de arquitectura de información que incluya el modelo de datos del organismo y los sistemas de información relacionados,
- crear y actualizar periódicamente un plan de infraestructura tecnológica,
- el control de calidad,
- la competencia del personal de Tecnología Informática,
- la formulación presupuestaria que garantice el establecimiento de un presupuesto operativo anual de la función de servicios de información y su aprobación de conformidad con los planes a corto y largo plazo del organismo y de tecnología de información;
- 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;
- los procesos necesarios para selección y promoción del personal, procurando que el organismo cuente con una fuerza laboral que tenga las habilidades necesarias para lograr sus metas;
- el cumplimiento de la normativa en materia de seguridad y salud ocupacional (higiene del trabajo),
- la evaluación periódica de los riesgos de información relacionados con la consecución de

los objetivos del organismo,

- la adopción de herramientas para el control de proyectos,
- un plan general de calidad basado en los planes del organismo y de tecnología de información a largo plazo,
- una metodología que requiera la especificación de los requerimientos funcionales y operativos de las soluciones, incluidos el rendimiento, la seguridad, contabilidad, compatibilidad y legislación;
- la aplicación de la metodología del ciclo de vida de desarrollo de sistemas (CVDS) del organismo,
- la evaluación, incorporación, instalación, mantenimiento y seguridad de la configuración de Tecnología Informática,
- la definición oportuna de los requerimientos operativos y niveles de servicio, la preparación de manuales de usuario y de operaciones y el desarrollo de materiales de capacitación,
- una metodología formal de prueba y acreditación de sistemas,
- un procedimiento formal de administración de cambios,
- la definición de acuerdos de nivel de servicio concretos,
- el monitoreo de la calidad del mantenimiento de los sistemas de infraestructura informática,
- la identificación de requerimientos de disponibilidad y desempeño,
- el monitoreo e informes del desempeño de los recursos de Tecnología Informática,
- la utilización de herramientas para la creación de modelos de desempeños,
- un marco de continuidad que defina los roles, responsabilidades, enfoque y las normas y estructuras para documentar el plan, como así también los procedimientos de aprobación,
- la seguridad de todos los recursos de la red informática,
- los procedimientos de determinación de costos para ofrecer información administrativa sobre los costos de la prestación de los servicios de procesamiento de información,
- la identificación de necesidades de capacitación,
- la organización de sesiones de capacitación,
- la capacitación y concientización en los principios de seguridad,

- el soporte al usuario dentro de la función de mesa de ayuda, incluyendo el módulo de gerenciamiento que permita realizar estadísticas y análisis de tendencias;
- los procedimientos de control para identificar y registrar todos los bienes de Tecnología Informática y su ubicación física, y una rutina de verificación regular que confirme su existencia;
- la adquisición de una herramienta que permita la administración eficaz y eficiente de los problemas o incidentes,
- el manejo de errores de entrada de datos,
- las medidas de control de acceso y seguridad física adecuadas en las instalaciones de tecnología de información,
- las normas y los procedimientos para el control de entradas y salidas al Centro de Cómputos,
- el respaldo de la administración de operaciones en presupuestos de recursos, la formalización de la capacitación y su continuidad,
- la definición de los indicadores de desempeño pertinentes al monitoreo de la tecnología informática y la recopilación de datos para la elaboración continua de informes de gestión e informes de excepción con respecto a estos indicadores.-

Finalmente se evalúa que, de acuerdo con el Modelo Genérico de Madurez[*] y los niveles detectados durante el presente trabajo, la gestión de la tecnología informática en la Administración Federal de Ingresos Públicos se encuentra entre el nivel de madurez inicial y el de procesos repetibles aunque intuitivos. Dada la importancia del organismo dentro de la Administración Pública Nacional se recomienda:

1.- Tender a que la madurez de la calidad de la gestión se aproxime al nivel de procesos definidos.-

2.- Superar a la brevedad las limitaciones de aquellos procesos ponderados en niveles “No conforma” e “Inicial”.-

[*] Ver Modelo Genérico de Madurez en página 5.

**7.- LUGAR Y FECHA**

BUENOS AIRES, 23 de diciembre de 2003

**8.- FIRMA**

## ANEXO: ANALISIS DE LA VISTA ENVIADA AL ORGANISMO

### Observaciones al punto 4.1.1 - Definición de un Plan Estratégico de Tecnología Informática

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

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* La planificación estratégica es comprendida por la gerencia de Tecnología Informática, pero no está documentada. La planificación estratégica está a cargo de la gerencia de Tecnología Informática, pero sólo se comparte con las autoridades del organismo en función de la necesidad. La actualización del plan estratégico de Tecnología Informática se produce sólo ante pedidos de la máxima autoridad y no hay un proceso proactivo para identificar las novedades de Tecnología Informática y del organismo que requieren actualizaciones al plan. Existe una estrategia global para la organización que no está fundamentada. Los riesgos y beneficios que las grandes decisiones estratégicas podrían tener para el usuario se reconocen, pero su definición es intuitiva.-

DESCRIPCIÓN: De la documentación obtenida se desprende que no existen procedimientos formales para la planificación estratégica de la tecnología de la información, que establezcan su relación con los objetivos estratégicos del organismo. Los planes generales de la Subdirección General definen metas concretas sin estimación de costos, ni plazos lo que dificulta su monitoreo y evaluación.-

RECOMENDACIÓN: La alta gerencia de la Organización es responsable de la implementación y el desarrollo de planes a corto y largo plazo que cumplan la misión y las metas de la misma. En este aspecto, debe garantizar que:

- la tecnología de información forma parte del plan de la organización a corto y largo plazo,
- se elabora un Plan de Tecnología Informática a largo plazo,
- el enfoque y estructura de la planificación de Tecnología Informática a largo plazo se traducen en planes de mediano y corto plazo,

- se realizan los cambios del plan de Tecnología Informática a largo plazo,
- se elabora la planificación a corto plazo de la función de servicios de información,
- se comunican los planes de Tecnología Informática,
- se monitorean y evalúan los planes de Tecnología Informática,
- se evalúan los sistemas existentes.-

**Respuesta del organismo:**

*Tal como lo establece el Decreto Nº 1399/01, la AFIP produce anualmente sus planes de gestión, los que son conformados tanto por metas cuantitativas sobre los procesos a realizar como por iniciativas específicas, ambos alineados a la misión, visión y objetivos previamente definidos institucionalmente. Estos planes son validados y conformados por la Jefatura de Gabinete de Ministros.*

*El proceso de definición de los riesgos y oportunidades asociados a las grandes decisiones estratégicas vinculadas al área de Sistemas y Telecomunicaciones no difiere del utilizado por el resto de la organización, habiendo tomado conocimiento de acciones encaradas por la AFIP destinadas a mejorar las competencias existentes para la formulación del planeamiento.*

*Por su parte, en atención a la importancia que el tema informático reviste para la organización, mediante Disposición 159/01 (AFIP) se creó el "Comité de Coordinación y Control de Actividades Informáticas", con la función de evaluar los planes informáticos, asignar prioridades para los principales proyectos y actividades y la de evaluar de su ejecución. Asimismo, tiene la responsabilidad de garantizar la alineación de los mismos respecto a los objetivos estratégicos de la AFIP.*

*Cumplimentando el Decreto Nº 1399/01, la Subdirección General de Sistemas y Telecomunicaciones elabora sus planes estratégicos anuales y acordes a la normativa institucional.*

*Como se mencionó en el apartado Análisis de Situación de la SDG SIT debe destacarse que la estructura organizativa de la Subdirección General de Sistemas y Telecomunicaciones fue modificada durante el transcurso de la evaluación de referencia.*

**Comentario AGN:** La respuesta del organismo confirma que no existen procedimientos formales para la definición de planes estratégicos ni planes de Tecnología Informática de largo y mediano plazo aprobados por la alta gerencia.

**En consecuencia se mantiene la observación.**

**Observaciones al punto 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 forma y tiempo tales que permitan a las personas cumplir sus responsabilidades de manera eficiente y oportuna. La función de servicios de información debe crear y mantener un modelo de arquitectura de información que incluya el modelo de datos del organismo y los sistemas de información relacionados. En este aspecto, la función de servicios de información debe garantizar:

- 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.-

NIVEL DE MADUREZ: *Inicial / Ad Hoc*. La alta gerencia reconoce la necesidad de una arquitectura de la información, pero no ha formalizado ni un proceso ni un plan para desarrollarla. Hay un desarrollo aislado y reactivo de los componentes de la arquitectura de la información. Existen implementaciones aisladas y parciales de diagramas de datos, documentación y reglas de sintaxis de datos. Las definiciones se basan en los datos, en lugar de la información. Hay conciencia de la necesidad de una arquitectura de la información, pero no está desarrollada.-

DESCRIPCIÓN: No se recibió información normativa en el tema de arquitectura de la información. Existe un sistema denominado SUPA (Sistema Único de Parámetros de AFIP) que incluye el diseño de la mayoría de las tablas de Oracle. La intención es que cada tabla tenga un dueño responsable de la administración de sus campos. Se está trabajando en el tema sin asignarle un rol protagónico en la planificación informática. Genera confusión en el uso de la información, especialmente cuando se la trata con fines de control fiscal.-

RECOMENDACIÓN: La información debe mantenerse acorde con las necesidades y debe ser

identificada, recopilada y comunicada en forma y tiempo tales que permita a las personas cumplir sus responsabilidades de manera eficiente y oportuna. La función de servicios de información debe crear y mantener un modelo de arquitectura de información que incluya el modelo de datos del organismo y los sistemas de información relacionados. En este aspecto, se debe garantizar:

- 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.-

**Respuesta del organismo:**

*Dentro de cada área de negocio la arquitectura de la información es administrada y documentada con procesos repetibles. En los últimos años se ha avanzado significativamente en la utilización cruzada de datos entre las distintas áreas, fomentando de esta manera una tendencia hacia un reservorio institucional. El proyecto SUPA, mencionado en el informe, es un claro ejemplo de esta tendencia limitado exclusivamente a las tablas de parámetros.*

*Además, las pautas descritas en el apartado incluyen una serie de aspectos tendientes a aumentar la utilización cruzada de datos y evitar la redundancia como proceso sistemático y uniforme a todas las áreas definidoras y de desarrollo.*

*A modo de ejemplo, debe tenerse en cuenta la centralización de los padrones de contribuyentes en el Padrón Unificado de Contribuyentes de reciente implementación.*

*De acuerdo a los parámetros de autoevaluación del control utilizados por el área de TI, este proceso se encuentra en nivel 2.*

**Comentario AGN:** La respuesta del organismo confirma que no existe plan de desarrollo de la arquitectura de la información.

**En consecuencia se mantiene la observación.**

**Observaciones al punto 4.1.3 - Determinación de la Dirección Tecnológica**

OBJETIVO DE CONTROL: La función de servicios de información 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 y servicios.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Hay un entendimiento implícito de la necesidad e importancia de la planificación tecnológica. No obstante, la planificación es táctica y se concentra en la generación de soluciones técnicas a problemas técnicos, y no en el uso de la tecnología para satisfacer las necesidades de las actividades del organismo. La evaluación de los cambios tecnológicos se deja librada al criterio de distintas personas que siguen procesos intuitivos, aunque similares. No hay una actividad formal de capacitación y comunicación de los roles y responsabilidades. Aparecen técnicas y normas comunes para el desarrollo de los componentes de la infraestructura.-

DESCRIPCIÓN: De la información recibida se desprende que no existen procedimientos formales para la confección de un plan de infraestructura tecnológica. Se han fijado rumbos, en materia de infraestructura, contenidos en el Plan General de Sistemas que se pueden compartir; sin embargo no están justificados ni evaluados. Se determinan temas estratégicos de alta significación económica para la Nación sin evaluación formal de impacto, riesgos y costos.-

RECOMENDACIÓN: La función de servicios de información debe crear y actualizar periódicamente un plan de infraestructura tecnológica. Dicho plan debe comprender aspectos tales como la arquitectura de los sistemas, la dirección tecnológica y las estrategias de información. En este aspecto, debe garantizar:

- la planificación de la infraestructura tecnológica,
- el monitoreo de las tendencias y reglamentaciones futuras,
- la evaluación de contingencias de la infraestructura tecnológica,
- planes de adquisición de hardware y software,
- la definición de normas de tecnología.-

**Respuesta del organismo:**

*Los procesos de adquisición, ya sea los llevados adelante por el Proyecto BID o por la AFIP, contemplan la realización de especificaciones técnicas, comparaciones, evaluaciones y otras herramientas que sustentan las elecciones realizadas.*

*Otro tipo de decisiones estratégicas sobre la infraestructura informática son respaldadas por evaluaciones e investigaciones que se materializan en informes producidos por el Departamento de Tecnología e Ingeniería de Software, unidad orgánicamente responsable. La definición de normas tecnológicas, el monitoreo de tendencias y la edición de normas de tecnología son prácticas habituales en ese departamento, que incluso tiene por establecido difundir sus investigaciones a otras Instituciones de la Administración Pública Nacional.*
*Los condicionamientos normativos expuestos en el apartado en ocasiones producen distorsiones en la dirección tecnológica de la AFIP*

**Comentario AGN:** Según la información relevada no se evidencia la existencia de un plan de infraestructura tecnológica. La respuesta del organismo confirma que no existe justificación y evaluación documentada del rumbo tecnológico en infraestructura informática.
**En consecuencia se mantiene la observación**.

**Observaciones al punto 4.1.4 - Definición de la Organización y las Relaciones de Tecnología Informática**

OBJETIVO DE CONTROL: La máxima autoridad debe establecer una estructura organizativa adecuada en términos de cantidad e idoneidad del personal, con roles y responsabilidades definidos y comunicados, alineada con la misión del organismo, que facilite la estrategia y brinde una dirección eficaz y un control adecuado.-

NIVEL DE MADUREZ: *Proceso Parcialmente Definido*. Existen roles y responsabilidades definidos para la organización de Tecnología Informática y los proveedores. La organización de Tecnología Informática está desarrollada, documentada, comunicada y alineada con la estrategia de Tecnología Informática. El diseño de la organización y el ambiente de control interno están definidos. Falta formalización de las relaciones con otras partes, tales como comités de dirección, auditoría interna y administración de proveedores. La organización de Tecnología Informática está funcionalmente completa, sin embargo, todavía se concentra más en las soluciones técnicas que en el uso de la tecnología para resolver problemas de las actividades sustantivas del organismo. Hay definiciones de las funciones que debe desempeñar el personal de Tecnología Informática y de las que serán desempeñadas por los

usuarios.-

DESCRIPCIÓN: De la documentación recibida se desprende que falta formalizar las relaciones con otras partes, tales como comités de dirección, auditoría interna y administración de proveedores. La organización no está funcionalmente completa. La alta gerencia del Organismo reconoce tener limitaciones por falta de nivel técnico del personal y por la inestabilidad del personal contratado, significativo en áreas de informática.-

RECOMENDACIÓN: Al ubicar la función de servicios de información dentro de la estructura del organismo, la alta gerencia debe garantizar autoridad, masa crítica e independencia de las áreas usuarias en la medida necesaria para garantizar soluciones de tecnología de información eficientes. En este aspecto, la máxima autoridad y la alta gerencia deben garantizar:

- la designación de un comité de planificación de Tecnología Informática,
- la ubicación de la función de servicios de información en el organismo,
- la revisión de los logros organizacionales,
- 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 Tecnología Informática,
- la separación de funciones,
- la competencia del personal de Tecnología Informática,
- las descripciones de los puestos del personal de Tecnología Informática,
- la identificación del personal clave de Tecnología Informática,
- las políticas y procedimientos relativos al personal contratado,
- las relaciones de coordinación, comunicación y enlace.-

**Respuesta del organismo:**

*Se considera que las observaciones respectivas reflejan la realidad y se tomarán las acciones correspondientes para mejorar y formalizar los procesos.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 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.-

NIVEL DE MADUREZ: *No Conforma*. No se ha tomado conciencia de la importancia de la selección y presupuesto de las inversiones de Tecnología Informática. No se hace un seguimiento o monitoreo de las inversiones y los gastos de Tecnología Informática.-

DESCRIPCIÓN: De la documentación recibida se desprende que no existen procedimientos formales que definan el mecanismo para la administración de la inversión. Los presupuestos anuales de tecnología informática recibidos son incompletos y no representativos. La inversión principal se realiza a través de organismos internacionales lo que dificulta tener una visión global del presupuesto y su ejecución.-

RECOMENDACIÓN: La alta gerencia es responsable de la implementación de un proceso de formulación presupuestaria que garantice el establecimiento de un presupuesto operativo anual de la función de servicios de información y su aprobación de conformidad con los planes a corto y largo plazo del organismo y de tecnología de información. En este aspecto, se debe garantizar:

- un presupuesto operativo anual de Tecnología Informática,
- el monitoreo de costos y beneficios,
- la justificación de costos y beneficios.-

**Respuesta del organismo:**

*La Subdirección General de Sistemas y Telecomunicaciones, prepara las alternativas de tecnología informáticas y de comunicaciones, de acuerdo con las ofertas del mercado proveedor, seleccionando aquellas que resulten compatibles con las distintas aplicaciones que están implementadas en el organismo o las que se prevea su desarrollo. Las alternativas son discutidas y evaluadas con las máximas autoridades y, una vez finalizado el proceso, son aprobadas por la alta gerencia.*

*El organismo utiliza distintas fuentes de financiamiento (internas y externas) dependiendo en cada momento de los fondos que se encuentran disponibles y de los montos a invertir. Cuando el organismo utiliza fuentes de financiamiento externo, no prescinde de sus definiciones tecnológicas, ya que éstas deben ser cumplidas por los oferentes. Sin embargo, es importante tener en cuenta que la AFIP está obligada a comprar lo ofrecido por el mercado proveedor, habida cuenta que no es un organismo que desarrolle tecnología propia.*

*Si bien el presupuesto de inversiones en tecnología de información no se ha formalizado en un documento único, eso no indica que el mismo no exista. Hay documentación que permite inferir que los distintos tipos de requerimientos se efectúan de manera homogénea, tanto a las unidades de financiamiento externo (Programa PNUD con financiamiento BM y BID) como las que se afectan con recursos propios (Presupuesto AFIP).*

*Las compras que se derivan de ese presupuesto son controladas y auditadas por varios organismos. Hasta la fecha, no se han recibido observaciones desde el punto de vista de la coherencia de las decisiones informáticas, ni tampoco por los montos erogados, que en todos los casos se han considerado razonables y ajustados a los precios de mercado.*

*La gerencia de Tecnología de Información tiene muy en claro la importancia de la "opción tecnológica" habida cuenta que una vez tomada la decisión por una de las alternativas, ésta impacta en la organización durante muchos años.*

*Como consecuencia de ello, hay un permanente seguimiento de la oferta de los proveedores a nivel mundial, un análisis de las distintas tendencias en el desarrollo de hardware y software y un monitoreo de la compatibilidad de las definiciones tomadas desde distintos puntos de vista (técnico, económico, financiero, etc.)*

**Comentario AGN:** Esta auditoría no recibió documentación respaldatoria de lo enunciado por el organismo. En esta observación se cuestiona la falta de un presupuesto anual y por lo tanto la no existencia de monitoreo y justificación de gastos.

**En consecuencia se mantiene la observación.**

**Observaciones al punto 4.1.6 - Comunicación de los Objetivos y Directivas de la Gerencia**

OBJETIVO DE CONTROL: La máxima autoridad debe impulsar la definición de políticas y su comunicación a la comunidad de usuarios. Además, es preciso que se establezcan normas a fin de traducir las opciones estratégicas en reglas prácticas y útiles.-

NIVEL DE MADUREZ: *Inicial / Ad Hoc*. La alta gerencia es reactiva en el abordaje de los requerimientos del ambiente de control de la información. Las políticas, procedimientos y normas se desarrollan y comunican en forma ad hoc, en función de las necesidades, impulsadas principalmente por problemas. Los procesos de desarrollo, comunicación y cumplimiento son informales y no siguen criterios uniformes.-

DESCRIPCIÓN: De la documentación recibida se desprende que no existen políticas formales para la comunicación de las decisiones y normativas del área y tampoco para el control de su cumplimiento.-

RECOMENDACIÓN: La máxima autoridad y la alta gerencia deben crear 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, deben garantizar:

- la responsabilidad de la alta gerencia sobre la formulación de las políticas,
- la comunicación de las políticas del organismo,
- los recursos para la implementación de políticas,
- el mantenimiento de políticas,
- el cumplimiento de las políticas, los procedimientos y las normas,
- el compromiso con la calidad,
- la política marco de seguridad y control interno,
- los derechos de propiedad intelectual,
- las políticas específicas,
- la comunicación de la concientización en materia de seguridad.-

**Respuesta del organismo:**

*Además de los procedimientos formales de uso institucional que se implementan a través de Disposiciones, Instrucciones Generales, etc., la Subdirección General de Sistemas y*

*Telecomunicaciones ha ido incorporando desde el 2002 una serie de mecanismos de divulgación de decisiones y normativas internas del área.*
*Durante el 2003 se han implementado mecanismos regulares de comunicación, por ejemplo, reuniones semanales entre los responsables de las áreas que reportan al subdirector de tecnología, divulgación de información institucional por medio de correo electrónico y reuniones de presentación de temas específicos. Asimismo, cada cada una de las áreas de la subdirección utiliza las páginas publicadas en intranet como medio de comunicación institucional.*
*Para el 2004 se planificado un importante proceso de capacitación técnica para el personal del área de Tecnología de la Información. Está previsto además, avanzar en la producción de un boletín periódico de novedades y aspectos técnicos propios de la gestión informática*.

**Comentario AGN:** Esta auditoría no recibió documentación respaldatoria de lo enunciado por el organismo.
**En consecuencia se mantiene la observación**.

**Observaciones al punto 4.1.7 - Administración de los Recursos Humanos**
OBJETIVO DE CONTROL: La máxima autoridad debe implementar prácticas de administración de personal sólidas, justas y transparentes en cuanto a selección, alineación, verificación de antecedentes, remuneración, capacitación, evaluación, promoción y despido.-
NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Hay un entendimiento implícito de la necesidad de administración de los recursos humanos de Tecnología Informática. Hay un enfoque táctico de la contratación y administración del personal de Tecnología Informática, impulsado por necesidades específicas de proyectos, y no por una dirección tecnológica y un equilibrio bien entendido entre la disponibilidad interna y externa de personal capacitado. Se realiza una capacitación informal para los nuevos empleados, que luego son entrenados según necesidades particulares.-
DESCRIPCIÓN: De la documentación recibida se desprende que no existen procedimientos formales para la selección, formación y promoción del personal. La dirección reconoce tener limitaciones por falta de nivel técnico del personal y por la inestabilidad del personal

contratado, significativo en áreas de informática.-

RECOMENDACIÓN: La máxima autoridad y la alta gerencia deben implementar y evaluar periódicamente los procesos necesarios para selección y promoción del personal y debe procurar que el organismo cuente con una fuerza laboral que tenga las habilidades necesarias para lograr sus metas. En este aspecto, deben garantizar:

- 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 extinción de la relación laboral.-

**Respuesta del organismo:**

*En lo expresado en la observación general se manifiestan los esfuerzos permanentes que realiza la institución para procurar una fuerza laboral con las habilidades necesarias para la gestión informática.*

*Se considera que, dado el contexto de los últimos años y las acciones llevadas adelante, la institución manifiesta una clara tendencia por mejorar la gestión de sus recursos humanos.*

**Comentario AGN:** El organismo reconoce, en las observaciones generales de su respuesta a la vista [(1)] que en algunos aspectos el marco normativo no es el adecuado y la manifestación realizada sobre la tendencia a mejorar la gestión de recursos humanos confirma la necesidad de superarse en esta materia.

**En consecuencia se mantiene la observación.**

---

[(1)] Respuesta del Organismo, pág. 3, Observaciones Generales, La Gestión de RR HH en la AFIP: *Los requerimientos en materia de recursos humanos que enfrenta la Administración, en términos de reclutamiento, selección, desvinculación, promoción y remuneraciones, no encuentran en algunos aspectos, un marco adecuado en la normativa contenida en dichos Convenios. El problema se agrava cuando el tema se vincula con personal informático.*

**Observaciones al punto 4.1.8 - Garantía del Cumplimiento de los Requerimientos Externos**

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

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Se comprende y se comunica la necesidad de cumplir con los requerimientos externos. Cuando el cumplimiento se convierte en un requerimiento recurrente, como en las regulaciones administrativas o la legislación sobre la privacidad, se desarrollan procedimientos individuales, que se siguen año tras año. Sin embargo, no hay un esquema general que garantice el cumplimiento de todos los requerimientos. Por lo tanto, es probable que haya excepciones y que las necesidades de cumplimiento que van surgiendo sólo se aborden en forma reactiva. Se depende mucho del conocimiento y la responsabilidad de ciertas personas y hay probabilidad de errores. Existe una capacitación informal sobre los requerimientos externos y las cuestiones relativas al cumplimiento.-

DESCRIPCIÓN: De la documentación recibida se desprende que no están establecidos procedimientos formales relativos al cumplimiento (identificación, análisis y adaptación) de los requerimientos externos.-

RECOMENDACIÓN: La máxima autoridad y la alta gerencia deben establecer y mantener procedimientos para la revisión de los requerimientos externos que permitan identificar los relacionados con las prácticas y controles de la tecnología de información. Además, se debe determinar en que medida es preciso que las estrategias de Tecnología Informática respalden los requerimientos de cualquier tercero relacionado. En este aspecto, 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 salud ocupacional (higiene del trabajo),
- la privacidad, propiedad intelectual y flujo de datos,

- el cumplimiento de la legislación en las actividades de comercio/gobierno electrónico,
- los cumplimientos de los contratos de seguro.-

**Respuesta del organismo:**

*Como se ha explicado en la observación general desde principios del 2003 se está trabajando en la definición de pautas y procedimientos uniformes para el ciclo de vida de sistemas que incluyen la administración de requerimientos con impacto en tecnología de la información y el seguimiento de los mismos. Actualmente se están llevando adelante actividades de capacitación y selección de herramientas para impulsar la implantación efectiva de dichas pautas.*

*Actualmente, el Comité de Coordinación y Control de Actividades Informáticas es el que establece las prioridades en grandes términos de donde abocar los esfuerzos en Tecnología del la Información. La revisión de los requerimientos externos a la institución son administrados por esta vía y luego delegados al área responsable del desarrollo con el seguimiento de la Subdirección General de Sistemas y Telecomunicaciones.*

*Por lo tanto, se considera que en términos generales la observación es adecuada pero se deja constancia que existe normativa específica y que desde inicios del 2003 se están llevando adelante medidas para mejorar la situación.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 4.1.9 - Evaluación 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 Informática y analizar su impacto, involucrando funciones multidisciplinarias y adoptando medidas eficaces en función de costos a fin de mitigar los riesgos.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Está empezando a entenderse que los riesgos de Tecnología Informática son importantes y deben ser tenidos en cuenta. Existe algún enfoque a la evaluación de riesgos, pero el proceso todavía es inmaduro y está desarrollándose. La evaluación en general se produce a un nivel muy general y se aplica sólo

a los grandes proyectos. La evaluación de las operaciones en marcha depende principalmente de que los gerentes de Tecnología Informática la planteen como un tema a tratar, lo cual a menudo sucede sólo cuando se producen problemas. La gerencia de Tecnología Informática no ha definido procedimientos o descripciones de puestos generales en el tema de la administración de riesgos.-

DESCRIPCIÓN: De la documentación recibida se desprende que no existen procedimientos formales referentes a la administración de riesgos y tampoco una evaluación y un plan de acción de reducción de riesgos. Se desconoce el nivel de riesgo de la Tecnología Informática en la Administración.-

RECOMENDACIÓN: La alta gerencia es responsable de 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 como deben administrarse los riegos a un nivel aceptable. En este aspecto, debe garantizar:

- una evaluación de riesgos de la actividad,
- el enfoque de la evaluación de riesgos,
- la identificación de riesgos,
- la medición de riesgos,
- el plan de acción de reducción de riesgos,
- la aceptación de riesgos.-

**Respuesta del organismo:**

*En lo que respecta a riesgos asociados a la producción de software, como se ha explicado en la observación general desde principios del 2003 se está trabajando en la definición de pautas y procedimientos uniformes para el ciclo de vida de sistemas que definen un marco sistemático para evaluación de riesgos y mitigaciones asociados al ciclo de vida del software. Tanto en las etapas de diseño arquitectónico y funcional de sistemas como en la etapas propias del desarrollo y la puesta en funcionamiento está previsto realizar análisis específicos de riesgos y mitigaciones que deberán ser concertados multidisciplinariamente entre las distintas áreas intervinientes.*

*En lo que respecta a riesgos y mitigaciones asociados a la infraestructura tecnológica, las especificaciones para el nuevo edificio sede de Subdirección General de Sistemas y Telecomunicaciones -con centro de cómputos incluido- han sido desarrolladas teniendo en cuenta las consideraciones utilizadas internacionalmente para previsión y mitigación de desastres. Previamente a la explotación del nuevo edificio se deberán formalizar el marco de evaluación sistemática de riesgos.*
*Por lo tanto, se considera que en términos generales la observación es adecuada pero se deja constancia que, tanto para el desarrollo de software como para la disponibilidad de la infraestructura tecnológica se han tomado los recaudos pertinentes.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 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. Asimismo, el organismo debe adoptar y aplicar técnicas bien concebidas de administración de proyectos por cada proyecto que se inicie.-
NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* La alta gerencia tomó conciencia de la necesidad de una administración de los proyectos de Tecnología Informática. El organismo está en el proceso de aprender y repetir ciertas técnicas y métodos de un proyecto a otro. Los proyectos de Tecnología Informática tienen objetivos técnicos y de recaudación definidos informalmente. Hay una participación limitada de las partes interesadas en la administración de proyectos de Tecnología Informática. Se desarrollaron algunas pautas para la mayoría de los aspectos de la administración de proyectos, pero su aplicación queda a discreción de cada gerente de proyecto.-
DESCRIPCIÓN: Desde principios del año 2002 se está llevando a cabo la transformación del área de Tecnología de la Información de la Administración Federal de Ingresos Públicos. Esto abarca la totalidad de las incumbencias del sector y prácticamente la totalidad de su personal. El éxito del proyecto hace a la calidad y cantidad de la recaudación pública de la Nación. De la documentación recibida se desprende que no existe una metodología formalmente

establecida en el Organismo para la administración de proyectos de esta naturaleza y tampoco se está utilizando alguna de las metodologías clásicas de programación por camino crítico. El tiempo y los gastos del personal asignado al proyecto no se presupuestan ni controlan. Las reprogramaciones, convertidas en Planes para cada año calendario, se realizan en forma reactiva de acuerdo con las necesidades y los atrasos que se generaron. Durante el año se han detectado modificaciones en las tareas programadas para el mismo que no se reflejaron en los documentos recibidos.-

RECOMENDACIÓN: La alta gerencia es responsable de 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. En este aspecto, debe garantizar que:

- aplica un marco de administración de proyectos,
- contempla la participación del departamento de usuarios en el inicio del proyecto,
- asigna miembros y responsabilidades del equipo del proyecto,
- realiza la definición del proyecto,
- aprueba las fases del proyecto,
- crea un plan maestro del proyecto,
- planifica el monitoreo y el control de avance,
- planifica la reprogramación permanente,
- prepara un plan de garantía de calidad del sistema,
- planifica métodos de garantía,
- implementa la administración formal de riesgos del proyecto,
- elabora un plan de pruebas, si corresponde,
- elabora un plan de capacitación,
- desarrolla un plan de revisión posterior a la implementación.-

**Respuesta del organismo:**

*Como se ha explicado en la observación general desde principios del 2003 se está trabajando en la definición de pautas y procedimientos uniformes para el ciclo de vida de sistemas que incluyen un marco para la administración de proyectos. Este marco contempla*

*todas las características de buen uso internacional en esta temática pero adecuadas a las necesidades de la AFIP.*

*Dentro del proceso de formalización mencionado en el apartado  debe considerarse además el proyecto testigo descrito en el apartado  donde se están utilizando metodologías y herramientas específicas para la gestión del mismo.*

*A mediados de 2003 se llevó adelante la evaluación de herramientas de gestión de proyectos y ya se han iniciado los procesos de adquisición pertinentes.*

*Por lo tanto, se considera que en términos generales la observación es adecuada pero se deja constancia que existe normativa específica y que desde inicios del 2003 se están llevando adelante medidas para mejorar la situación.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 4.1.11 - Administración de la Calidad**

OBJETIVO DE CONTROL: La alta gerencia debe desarrollar la planificación, implementación y el mantenimiento de normas y sistemas de administración de calidad del organismo, que proporcionen distintas fases de desarrollo, prestaciones clave y responsabilidades explícitas.-

NIVEL DE MADUREZ: *No Conforma*. El organismo carece de un proceso de planificación de garantía de calidad y una metodología de ciclo de vida de desarrollo de sistemas. La alta gerencia y el personal de Tecnología Informática no reconocen la necesidad de un programa de calidad. Nunca se verifica la calidad de los proyectos y las operaciones.-

DESCRIPCIÓN: En la documentación recibida no se detectan intentos por desarrollar un plan general de calidad.-

RECOMENDACIÓN: La alta gerencia es responsable de desarrollar y mantener periódicamente un plan general de calidad basado en los planes del organismo y de tecnología de información a largo plazo. Dicho marco debe promover la filosofa de mejora continua. En este aspecto, debe garantizar:

- un plan general de calidad,
- el enfoque de garantía de calidad,

- la planificación de garantía de calidad,
- la revisión de garantía de calidad de la observación de las normas y procedimientos de la función de servicios de información,
- 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 Tecnología Informática,
- un marco de adquisición y mantenimiento de la infraestructura tecnológica,
- las relaciones con terceros a cargo de la implementación,
- la observación de las normas de documentación de programas,
- el cumplimiento de las normas de prueba de programas,
- el cumplimiento de las normas de prueba de sistemas,
- la utilización de pruebas en paralelo/piloto,
- la documentación de pruebas de sistemas,
- la evaluación de la observación de las normas de desarrollo.-

**Respuesta del organismo:**

*Desde el 2002 existen formalmente para cada una de las grandes áreas de desarrollo de sistemas, unidades de estructura de nivel de departamento específicas para el control de calidad del ciclo de vida de sistemas. Las funciones y responsabilidades de estas unidades han sido formalmente asignadas.*

*Se deja constancia además, que las pautas desarrolladas durante el 2003 descritas en la observación general ,contemplan procedimientos y producción de documentación uniformes en todas las áreas para la administración de la calidad.*

*De acuerdo a los parámetros de autoevaluación del control utilizados por el área de TI, este proceso se encuentra en nivel 2.*

Comentario AGN: El organismo indica, en las observaciones generales de su respuesta a la vista [2] que esta en proceso de aprobación una metodología de ciclo de vida de sistemas. Sin embargo la observación, recomendación, se refiere al tema de la administración de la calidad y la necesidad del organismo de contar con una adecuada planificación de garantía de calidad que debería abordar, entre otros, los siguientes puntos:

- en términos mensurables y no ambiguos, el nivel previsto de servicio a brindar a los usuarios internos y externos
- en términos mensurables y no ambiguos las interrupciones del servicio máximas previstas para cada sistema y plataforma
- las estadísticas de desempeño requeridas para monitorear los objetivos previstos de desempeño e interrupción de servicio incluyendo la forma en que se documentarán y a quienes se distribuiran los informes generados
- los procesos de monitoreo y revisión necesarios para garantizar que el desarrollo, la modificación o transición en el ambiente o infraestructura de la función seervicios de información identificados en los planes a corto y largo plazo de dicha función están bien planificados, son monitoreados correctamente, cuentan con los debidos recursos y son aprobados, documentados e implementados adecuadamente, incluyendo la capacitación pertinente
- los intervalos en que debe actualizarse el plan de calidad

**En consecuencia se mantiene la observación.**

[2] Respuesta del Organismo. pág 5 y 6, Oservaciones Generales, Normativa sobre el Control de Vida de Sistemas: *La Disposición 6/98 de la Subdirección General de Recaudación que determina la creación del "Comité de Sistemas de Recaudación" establece formalmente etapas, roles, responsabilidades y resultados entregables a ser cumplidos en todos proyectos de sistemas de la institución. Esta disposición está vigente y ha sido heredada por Subdirección General de Sistemas y Telecomunicaciones.*
*Con el objetivo de actualizar y adecuar la mencionada disposición a la nueva realidad de la AFIP, entre marzo y diciembre del 2003 el Departamento de Tecnología e Ingeniería de Software llevó adelante un proceso participativo y consensuado con representantes de las seis grandes áreas de desarrollo de software de Subdirección General de Sistemas y Telecomunicaciones. El resultado obtenido por este proceso consiste en un conjunto de pautas para el Ciclo de Vida de Sistemas que responden a los modelos internacionalmente utilizados en la temática. En estos momentos se encuentra en la etapa final de aprobación con formato de disposición para ser emitido formalmente y comenzar gradualmente su implementación.*

**Observaciones al punto 4.2.1 - Identificación de Soluciones Automatizadas**

OBJETIVO DE CONTROL: La máxima autoridad debe garantizar una identificación y análisis claro y objetivo de las oportunidades alternativas, medidas en comparación con los requerimientos del usuario.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* A pesar de no haber una metodología formalmente definida para la adquisición e implementación, los requerimientos tienden a ser definidos en forma similar, con las diferencias propias de los distintos orígenes de los sectores incluidos en la Administración, debido a prácticas comunes dentro de la función de Tecnología Informática. Las soluciones se identifican informalmente en función de la experiencia interna y el conocimiento de la función de Tecnología Informática. El éxito de cada proyecto depende de la pericia de unas pocas personas claves y la calidad de la documentación y la toma de decisiones puede variar considerablemente.-

DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido una metodología escrita de implementación de las soluciones de Tecnología Informática para satisfacer los requerimientos de AFIP. Cada una de las áreas que antes eran independientes (DGI, DGA, DGRSS) tiene sus propias características al respecto. No se realiza la consideración escrita de alternativas, evaluadas con respecto a los requerimientos del usuario, oportunidades tecnológicas, factibilidad económica, evaluaciones de riesgos y otros factores. El proceso no se sigue por igual en todos los proyectos y depende de las decisiones tomadas por el personal involucrado y la dimensión y prioridad del requerimiento del problema original.-

RECOMENDACIÓN: La alta gerencia es responsable de establecer una metodología que requiera la especificación de los requerimientos funcionales y operativos de las soluciones, incluidos el rendimiento, la seguridad, contabilidad, compatibilidad y legislación. En este aspecto, la alta gerencia y el funcionario principal de servicios de información deben garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- definición de los requerimientos de información,
- formulación de cursos alternativos de acción,
- formulación de la estrategia de adquisición,

- requisitos de servicios prestados por terceros,
- estudio de factibilidad tecnológica,
- estudio de factibilidad económica,
- arquitectura de la información,
- informe de análisis de riesgos,
- controles de seguridad económicos,
- diseño de pistas de auditoría,
- ergonomía,
- selección del software de sistemas,
- control de compras,
- adquisición de productos de software,
- mantenimiento del software de terceros,
- programación contratada de aplicaciones,
- aceptación de las instalaciones,
- aceptación de la tecnología.-

**Respuesta del organismo:**

*Como fue mencionado, en las pautas desarrolladas durante el 2003 descritas en la observación general, se establece una metodología para requerir la especificación de los requerimientos funcionales y operativos de las soluciones, incluidos el rendimiento, la seguridad, compatibilidad y legislación. Estas especificaciones contemplan todas las características de buen uso internacional en esta temática adecuadas a las necesidades de la AFIP.*

*Dentro de este proceso de formalización debe considerarse el proyecto testigo descrito en el apartado  donde se están utilizando metodologías y herramientas específicas para la gestión del mismo.*

*Por lo tanto, se considera que en términos generales la observación es adecuada pero se deja constancia que desde inicios del 2003 se están llevando adelante medidas para mejorar la situación.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 4.2.2 - Adquisición y Mantenimiento del Software de Aplicación**

OBJETIVO DE CONTROL: La adquisición y mantenimiento del software de aplicación debe realizarse por medio de la definición específica de requerimientos funcionales y operativos, y una implementación por etapas con prestaciones claras.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Existen procedimientos similares para adquirir y mantener las aplicaciones, pero se basan en la pericia de la función de Tecnología Informática, no en un proceso documentado. La tasa de éxito de las aplicaciones depende en gran medida de las habilidades internas y la experiencia de la función de Tecnología Informática. El mantenimiento suele ser problemático y se ve perjudicado cuando por algún motivo se pierde conocimiento interno del organismo.-

DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido una metodología formal para definir las necesidades de nuevas aplicaciones y los requerimientos de sus actualizaciones y mantenimiento. En estos momentos no se están contratando servicios externos de provisión de soluciones; pero, si hubiera que hacerlo por razones de fuerza mayor, tampoco existen procedimientos para la adquisición y acreditación de aplicaciones provistas por terceros.-

RECOMENDACIÓN: La alta gerencia y el funcionario principal de la función de servicios de información son responsables de establecer procedimientos y técnicas adecuadas para la aplicación de la metodología del ciclo de vida de desarrollo de sistemas (CVDS) del organismo, que impliquen una coordinación estrecha con los usuarios de sistemas, para la creación de especificaciones de diseño para cada proyecto de desarrollo de un sistema nuevo y la verificación de dichas especificaciones. En este aspecto, se debe garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- métodos de diseño,
- cambios importantes de los sistemas existentes,
- aprobación del diseño,

- definición y documentación de los requerimientos de archivos,
- especificaciones de programas,
- diseño de la recopilación de datos fuente,
- definición y documentación de los requerimientos de entrada,
- definición de interfaces,
- interfaces usuario–máquina,
- definición y documentación de los requerimientos de procesamiento,
- definición y documentación de los requerimientos de salida,
- controlabilidad,
- disponibilidad como factor clave del diseño,
- especificaciones de integridad de tecnología de información en programas de aplicación,
- pruebas del software de aplicación,
- materiales de soporte y referencia del usuario,
- reevaluación del diseño de sistemas.-

**Respuesta del organismo:**

*Como se ha explicado en la observación general, desde principios del 2003 se está trabajando en la definición de pautas y procedimientos uniformes para el ciclo de vida de sistemas que incluyen un marco para el desarrollo y mantenimiento de software de aplicación. Este marco contempla todas las características de buen uso internacional en esta temática pero adecuadas a las necesidades de la AFIP para los desarrollos de sistemas realizados institucionalmente.*

*La adquisición de software de aplicación de terceros se produce esporádicamente y en situaciones particulares. En estas situaciones, los procesos de adquisición se han llevado a cabo siguiendo estrictamente la normativa de la AFIP o del BID/PNUD según el caso. En ambos casos las especificaciones que determinan al producto que se desea adquirir, cumplen con todo el detalle y especificidad que indican las buenas prácticas.*

*Las adquisiciones realizadas por la AFIP se han concretado por medio de licitaciones públicas cuyos pliegos fueron escritos de manera repetitiva, consistente y uniforme y con*

*mejoras continuas gracias a la adquisición de experiencia del área involucrada en su elaboración.*

*Las adquisiciones realizadas por medio del Proyecto BID administrado por la unidad ejecutora del PNUD han sido elaborados cumpliendo toda la normativa y los controles correspondientes del caso.*

*Por lo tanto, se considera que en términos generales la observación es adecuada pero se deja constancia que existe un alto grado de formalidad en los procedimientos utilizados, como se ha descrito en el apartado.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 4.2.3 - Adquisición y Mantenimiento de la Infraestructura Tecnológica**

OBJETIVO DE CONTROL: La gerencia de la función de servicios de información debe impulsar la adquisición criteriosa del software y el hardware, la estandarización del software, la evaluación del rendimiento del hardware y el software, y la administración coherente de sistemas.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Existe uniformidad entre los enfoques tácticos, cuando se trata de adquirir y mantener la infraestructura de Tecnología Informática. No obstante, se carece de un marco normativo explícito para la administración y de procedimientos formales de evaluación de rendimiento de equipos y sistemas.-

DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido un marco normativo formal referente a la adquisición y mantenimiento de la infraestructura tecnológica y de su integridad. No se evidencia capacidad de monitorear y medir el desempeño de la infraestructura existente con miras a la detección oportuna de problemas y el dimensionamiento de las ampliaciones. No se encontraron registros, tales como registros de fallas debidas a falta de mantenimiento o a cambio de hardware o software de sistemas y registros de costos de las grandes modificaciones de infraestructura, que garanticen la elaboración de índices de desempeño. El costo y el tiempo para llegar al nivel

deseable de escalabilidad, flexibilidad e integración no están determinados. Se debe sobredimensionar la infraestructura a fin de evitar limitaciones ante problemas de los cuales no existen registros históricos.-

RECOMENDACIÓN: La gerencia de la función de servicios de información es responsable por la evaluación, incorporación, instalación, mantenimiento y seguridad de la configuración de Tecnología Informática. En este aspecto, se debe garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- evaluación del hardware y el software nuevos,
- mantenimiento preventivo del hardware,
- seguridad del software del sistema,
- instalación del software del sistema,
- mantenimiento del software del sistema,
- controles de cambios del software del sistema.-

**Respuesta del organismo:**

*Las adquisiciones realizadas por la AFIP se han realizado por medio de licitaciones públicas cuyos pliegos fueron escritos de manera repetitiva, consistente y uniforme y con mejoras continuas gracias a la adquisición de experiencia del área involucrada en su elaboración. Debe tenerse en cuenta en este aspecto en particular que los tiempos que requieren las adquisiciones por estas vías formales –que difícilmente son inferiores a 18 meses- afectan significativamente el diseño de los planes estratégicos.*

*Las adquisiciones realizadas por medio del Proyecto BID administrado por la unidad ejecutora del PNUD ha sido elaborados cumpliendo toda la normativa y los controles correspondientes del caso.*

*En lo referente al monitoreo de la infraestructura, durante el 2003 se llevó adelante el proceso licitatorio para la adquisición de un software específico para el monitoreo de la disponibilidad y rendimiento de la infraestructura tecnológica. Además, con el fin exclusivo de llevar adelante estas actividades para toda la infraestructura tecnológica, se creó en julio de 2003 una unidad de estructura específica dentro del Departamento de Operaciones.*

*De acuerdo a los parámetros de autoevaluación del control utilizados por el área de TI, este proceso se encuentra en nivel 3.*

**Comentario AGN:** De la documentación proporcionada por el organismo, no se constata la existencia de cálculos de niveles de procesamiento, capacidad de almacenamiento ni necesidades técnicas de los equipos a incorporar, lo que debería figurar como elemento indispensable del marco normativo propio. Tampoco se pudo verificar una adecuada capacidad de monitoreo

**En consecuencia se mantiene la observación.**

**Observaciones al punto 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.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Se toman enfoques similares con respecto a la producción de procedimientos y documentación, pero no están basados en un lineamiento o marco estructurado. Las guías de operación y del usuario existen pero se carece de un abordaje uniforme y, por lo tanto, su exactitud y disponibilidad dependen en gran medida de las personas, y no de un proceso formal. El material de capacitación tiende a ser producido individualmente y la calidad depende de las personas involucradas. Por consiguiente, el desarrollo de guías para usuarios y operadores y la calidad del soporte al usuario pueden variar de deficiente a muy satisfactorio, con poca uniformidad e integración en las distintas áreas del organismo.-

DESCRIPCIÓN: De la documentación recibida no se deduce que la Administración haya establecido una metodología del ciclo de vida del desarrollo de sistemas. Los niveles de servicio acordados con los usuarios son no mensurables. No se tiene control del nivel de satisfacción de los usuarios con los manuales y materiales de capacitación. Esta situación deviene en perdida de eficacia y eficiencia.-

RECOMENDACIÓN: La metodología del ciclo de vida del desarrollo de sistemas (CVDS) del organismo debe garantizar la definición oportuna de los requerimientos operativos y

niveles de servicio, la preparación de manuales de usuario y de operaciones y el desarrollo de materiales de capacitación. En este aspecto, se debe garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- requerimientos operativos y niveles de servicio,
- manuales de procedimientos del usuario,
- manual de operaciones,
- materiales de capacitación.-

**Respuesta del organismo:**

*Como fue mencionado, las pautas desarrolladas durante el 2003 descritas en la observación general , definen etapas, procesos y generación de documentos que debe ser cumplidos por todos los proyectos de desarrollo de sistemas informáticos. Este especificaciones contemplan todas las características de buen uso internacional en esta temática adecuadas a las necesidades de la AFIP.*

*Están todavía en elaboración las medidas a tomar en lo que hace a uniformidad de documentación, ayudas y características de "usabilidad" de los sistemas, especialmente para aquellos con acceso por usuarios externos a la institución.*

*Por lo tanto, se considera que en términos generales la observación es adecuada pero se deja constancia que desde inicios del 2003 se están llevando adelante medidas parciales para mejorar la situación y los responsables son conscientes de la necesidad de seguir avanzando en estos aspectos.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 4.2.5 - Instalación y Acreditación de Sistemas de Aplicación**

OBJETIVO DE CONTROL: La implementación de nuevos sistemas debe realizarse por medio de un plan bien formalizado de instalación, migración, conversión y aceptación.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Hay consistencia entre los enfoques de

prueba y acreditación, pero no se basan en una metodología formal. Las áreas definidoras individuales son las que normalmente deciden el enfoque de prueba. Hay un procedimiento de aprobación no necesariamente basado en criterios estandarizados. La acreditación y aprobación formal se aplica ad hoc.-

DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido estándares formalmente definidos que comprendan la totalidad de las tareas requeridas para la implementación de los nuevos sistemas o modificaciones a los existentes. Esto puede generar deficiencias particulares en cada caso e impide la realización del control de cumplimiento e incertidumbre respecto a la calidad de la instrumentación realizada.-

RECOMENDACIÓN: Los funcionarios de las partes pertinentes y los funcionarios responsables de la función de servicios de información deben preparar, revisar y aprobar un plan de implementación o modificación de los sistemas de aplicación. En este aspecto, se debe garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- capacitación de los usuarios y personal de servicios de información,
- dimensionamiento del desempeño del software de aplicación,
- plan de implementación,
- conversión de sistemas de aplicación,
- conversión de datos,
- estrategia y planes de prueba,
- prueba de cambios,
- criterios de ejecución de pruebas paralelas/piloto,
- prueba de aceptación final,
- pruebas de acreditación de seguridad,
- prueba de funcionamiento,
- transición a producción,
- evaluación del cumplimiento de los requerimientos del usuario,
- revisión de la gerencia posterior a la implementación.-

**Respuesta del organismo:**

*Como se ha explicado en la observación general , desde principios del 2003 se está trabajando en la definición de pautas y procedimientos uniformes para el ciclo de vida de sistemas que determinan la forma de realizar los planes de implementación o modificación de los sistemas de aplicación.*

*Por lo tanto, se considera que en términos generales la observación es adecuada pero se deja constancia que desde inicios del 2003 se están elaborando planes para mejorar la situación.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 4.2.6 - Administración de Cambios**

OBJETIVO DE CONTROL: Se debe disponer de un sistema de administración de cambios que permita el análisis, la implementación y el seguimiento de todos los cambios solicitados y realizados en la infraestructura de Tecnología Informática existente.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Existe un proceso informal de administración de cambios, con un enfoque que se sigue para la mayoría de los casos. Sin embargo, este proceso no está estructurado. La documentación de la configuración no es precisa y sólo se hace una planificación y evaluación limitada del impacto antes del cambio.-

DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido un procedimiento formal de administración de cambios. Existe el riesgo de no disponer de los cambios necesarios en el momento oportuno.-

RECOMENDACIÓN: La alta gerencia y el funcionario principal de la función de servicios de información deben implementar procedimientos específicos para tratar los pedidos de cambios, mantenimiento de sistema y mantenimiento del proveedor. En este aspecto, se debe garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- inicio y control de solicitudes de cambio,
- evaluación del impacto,
- control de cambios,

- cambios de emergencia,
- documentación y procedimientos,
- mantenimiento autorizado,
- política de versiones de software,
- distribución de software.-

**Respuesta del organismo:**

*Como se ha explicado en la observación desde principios del 2003 se está trabajando en la definición de pautas y procedimientos uniformes para el ciclo de vida de sistemas que determinan la forma administrar los requerimientos de cambios y mantenimiento de sistemas. Por lo tanto, se considera que en términos generales la observación es adecuada pero se deja constancia que desde inicios del 2003 se están llevando adelante medidas para mejorar la situación.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 4.3.1 - Definición y Administración de los Niveles de Servicio**

OBJETIVO DE CONTROL: La máxima autoridad debe definir un marco que promueva el establecimiento de acuerdos de nivel de servicio que formalicen los criterios de desempeño en virtud de los cuales se medirá la cantidad y calidad del servicio.-

NIVEL DE MADUREZ: *Inicial / Ad Hoc*. 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.-

DESCRIPCIÓN: De la documentación recibida se deduce que los niveles de servicio comprometidos son genéricos y si bien demuestran la buena intención de las partes, no son mensurables y no garantizan la satisfacción de las necesidades del usuario.-

RECOMENDACIÓN: La alta gerencia es responsable de definir un marco dentro del cual promueva la definición de acuerdos de nivel de servicio y defina los contenidos mínimos. En

este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- marco de acuerdos de nivel de servicio,
- aspectos de los acuerdos de nivel de servicio,
- procedimientos de ejecución,
- monitoreo e informes,
- revisión de los contratos y acuerdos de nivel de servicio,
- ítems imputables,
- programa de mejora del servicio.-

**Respuesta del organismo:**

*De acuerdo con las prácticas institucionales, los acuerdos de servicios con los usuarios internos no están formalizados. Sin embargo, se realizan acuerdos de sobre el nivel que tendrán los servicios ofrecidos por el área de Tecnología de la Información a las diferentes áreas de negocio de la AFIP.*

*Con respecto a los proveedores externos, en cada contrato se especifican los niveles de servicio que deben brindar. Por ejemplo, el nivel de acuerdo de servicios establecido para la prestación de telecomunicaciones está detallado en los documentos de licitación que conforman la contratación de servicios. En el servicio vigente se controla la disponibilidad de los principales vínculos y el incumplimiento lleva aparejado una penalidad de tipo económico que se corresponde al tipo del nodo involucrado y al tiempo de falta de servicio.*

*En la red que se encuentra en proceso de adquisición (la cual ya se encuentra adjudicada) está previsto controlar la disponibilidad de los enlaces principales, la calidad del servicio y la disponibilidad del esquema de back-up. Dado que el protocolo de transporte es "frame-relay", para el control de la calidad de las comunicaciones se procedió a confeccionar las especificaciones técnicas de un sistema de monitoreo específico capaz de detectar parámetros de dicho protocolo por umbrales de falla.*

*Además, se deja constancia que, luego del proceso licitatorio correspondiente, ya se encuentra disponible software específico para la gestión de niveles de acuerdo de servicio.*

*De acuerdo a los parámetros de autoevaluación del control utilizados por el área de TI, este proceso se encuentra en nivel 3.*

**Comentario AGN:** Los niveles de servicio ofrecidos a los usuarios presentan, según la documentación recibida oportunamente, las características señaladas en el párrafo DESCRIPCIÓN.
**En consecuencia se mantiene la observación.**

**Observaciones al punto 4.3.2 - Administración de Servicios Prestados por Terceros**
OBJETIVO DE CONTROL: La máxima autoridad debe implementar medidas de control orientadas a la revisión y al monitoreo de los contratos y procedimientos existentes para garantizar su eficacia y el cumplimiento de la política del organismo.-
NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* 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. Se toman mediciones, pero no son relevantes.-
DESCRIPCIÓN: No se obtuvo evidencia del registro de los servicios efectuados por mantenimiento de hardware informático. No existe control por parte de la gerencia de tecnología informática de las tareas de mantenimiento de infraestructura (aire acondicionado, sistemas de energía ininterrumpible, tableros de energía, sistemas de protección de incendio, sistemas de control de acceso y similares) que pueden afectar la continuidad de los servicios. El control de la prestación de los servicios de mantenimiento es responsabilidad del área de servicios generales. La delegación de la responsabilidad del monitoreo de la calidad del mantenimiento de los sistemas de infraestructura informática puede conducir a una situación de inoperabilidad de los centros de cómputos. Ante la eventualidad de necesitar de servicios prestados por terceros, no existe un marco normativo adecuado.-
RECOMENDACIÓN: La máxima autoridad y la alta gerencia son responsables de que los servicios prestados por terceros se identifiquen de modo adecuado y que la interpelación técnica y funcional con los proveedores esté documentada. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de

Tecnología Informática:
- interpelación con proveedores de Tecnología Informática,
- asignar la responsabilidad por la 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.-

**Respuesta del organismo:**

*Los contratos de servicios de infraestructura se monitorean permanentemente, a través del control de la ejecución de las respectivas ordenes de compra, dándose la conformidad o reparo según corresponda.*

*Para estos servicios, se utilizan contratos específicos (Pliego de especificaciones técnicas y Orden de Compra), producto de actos licitatorios de pública participación. Para cada servicio se determinan condiciones particulares en concordancia con el mismo.*

*La supervisión y el control de los servicios de infraestructura prestados por terceros son totalmente formales, con registros de lo actuado y en cumplimiento a lo establecido en las Ordenes de Compra respectivas. Se utiliza metodológicamente el control por oposición de intereses, atento que además del área de servicios, interviene la Comisión de Recepción Definitiva.*

*El control de la prestación de los servicios de infraestructura por acciones y tareas propias, está a cargo del área de servicios, existiendo como marco normativo el Régimen General de Contrataciones (Disposición N° 297/03, AFIP), las respectivas Ordenes de Compra y el reglamento de la Comisión de Recepción Definitiva.*

*Se ha acordado institucionalmente, de acuerdo a prácticas internacionales, que la administración de infraestructura informática para el nuevo edificio sede de la Subdirección General de Sistemas y Telecomunicaciones estará a cargo de la propia subdirección.*

*De acuerdo a los parámetros de autoevaluación del control utilizados por el área de TI, este proceso se encuentra en nivel 3.*

**Comentario AGN:** La Subdirección General de Sistemas y Telecomunicaciones no está a cargo de la administración de todos los servicios prestados por terceros, a pesar de que lo hará en el futuro.
**En consecuencia se mantiene la observación.**

**Observaciones al punto 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, el análisis y los informes sobre el desempeño de los recursos de Tecnología Informática, la dimensión de los sistemas de aplicación y la demanda de cargas de trabajo.-
NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* La máxima autoridad del organismo es consciente del impacto de no administrar la capacidad y el desempeño. En general, se satisfacen las necesidades de desempeño de las áreas críticas, en función de una evaluación de los sistemas individuales y del conocimiento de los equipos de soporte y de proyecto. Pueden usarse algunas herramientas aisladas para diagnosticar problemas de capacidad y desempeño, pero la uniformidad de los resultados depende de la pericia de personas clave. No hay una evaluación general del desempeño de la infraestructura de Tecnología Informática ni consideración de las situaciones de cargas pico en el peor de los casos. Es probable que surjan problemas de disponibilidad en forma inesperada y al azar, cuyo diagnóstico y corrección lleven un tiempo considerable.-
DESCRIPCIÓN: A pesar de la complejidad de los servicios informáticos que se prestan en la Administración, de la documentación recibida no se deduce que el organismo disponga de herramientas de modelado del desempeño de la infraestructura que permitan administrar adecuadamente la capacidad, la confiabilidad y la disponibilidad.-
RECOMENDACIÓN: La máxima autoridad y el funcionario principal de sistemas de información son responsables de identificar las necesidades de capacidad y desempeño de los servicios de información, y que se traduzcan en términos y requerimientos de disponibilidad.

En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:
- identificación de requerimientos de disponibilidad y desempeño,
- establecer un plan de disponibilidad,
- monitoreo e informes del desempeño de los recursos de Tecnología Informática,
- utilización de herramientas para la creación de modelos de desempeños,
- administración productiva del desempeño,
- pronósticos de la carga de trabajo,
- administración de la capacidad de los recursos,
- disponibilidad de recursos,
- planificación de recursos.-

**Respuesta del organismo:**
*Se considera que las observaciones respectivas reflejan la realidad y se tomarán las acciones correspondientes para mejorar y formalizar los procesos.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 4.3.4 - Garantía de un Servicio Continuo**
OBJETIVO DE CONTROL: La máxima autoridad debe implementar un plan de continuidad de tecnología de información probado y operativo que concuerde con el plan de continuidad general del organismo y sus requerimientos de actividad relacionados.-
NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* La responsabilidad del servicio continuo ha sido asignada. Los enfoques al servicio continuo son fragmentados. Los informes de la disponibilidad de sistemas son incompletos y no tienen en cuenta el impacto en el organismo. No hay planes del usuario o de continuidad documentados, a pesar de que hay un compromiso con la disponibilidad de un servicio continuo y se conocen sus principios más importantes. Existe un inventario no confiable de los sistemas y componentes críticos. Está apareciendo una estandarización de las prácticas de servicio continuo y monitoreo del proceso, pero su éxito depende de cada persona.-

DESCRIPCIÓN: De la documentación recibida se deduce que los planes para garantizar la continuidad del servicio están siendo redactados. Se está a la espera de la contratación de un aplicativo a usar como herramienta para la preparación de un plan de contingencia completo.-
RECOMENDACIÓN: El funcionario principal de la función de servicios de información es responsable de crear un marco de continuidad que defina los roles, responsabilidades, enfoque y las normas y estructuras para documentar el plan, como así también los procedimientos de aprobación. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:
- marco de continuidad de Tecnología Informática,
- estrategias y filosofía del plan de continuidad de Tecnología Informática,
- contenido del plan de continuidad de Tecnología Informática,
- reducción de los requerimientos de continuidad de Tecnología Informática,
- mantenimiento del plan de continuidad de Tecnología Informática,
- prueba del plan de continuidad de Tecnología Informática,
- capacitación en el plan de continuidad de Tecnología Informática,
- distribución del plan de continuidad de Tecnología Informática,
- procedimientos para el resguardo del procesamiento alternativo del usuario,
- identificar recursos críticos de Tecnología Informática,
- sitio y equipamiento alternativo,
- almacenamiento de resguardo en sitio alternativo,
- reevaluación periódica del plan.-

**Respuesta del organismo:**

*Actualmente existe medidas de aseguramiento de continuidad en los principales servicios de infraestructura que utiliza la Subdirección General de Sistemas y Telecomunicaciones.*

*En los aspectos inherentes a la infraestructura informática, como parcialidad de un plan de garantía de servicio continuo, en las especificaciones para el nuevo edificio sede de la Subdirección General de Sistemas y Telecomunicaciones se ha incluido la previsión de procesos y disponibilidad de sitios para la recuperación ante desastres.*

**Comentario AGN:** Tal como se indico en la descripción al presente no existen planes que garanticen la continuidad del servicio. Si bien el Plan de Sistemas correspondientes al nuevo edificio incorpora la disponibilidad de sitios para la recuperación ante desastres, al momento de realizarce esta auditoría no es posible verificar el cumplimiento de lo allí expresado.
**En consecuencia se mantiene la observación.**

**Observaciones al punto 4.3.5 - Garantía de la Seguridad de los Sistemas**
OBJETIVO DE CONTROL: La máxima autoridad debe establecer y mantener un programa de seguridad de la información para implementar los controles de acceso lógico que garantizan que el acceso a los sistemas, datos y programas está limitado a los usuarios autorizados.-
NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* Las responsabilidades y la rendición de cuentas de la seguridad de Tecnología Informática están asignadas a un coordinador de Tecnología Informática que depende directamente de la Subdirección General. La concientización de la seguridad es fragmentada y limitada. Las soluciones de seguridad tienden a responder reactivamente a los incidentes de seguridad de Tecnología Informática. Se están desarrollando políticas de seguridad, pero todavía se usan habilidades y herramientas inadecuadas.-
DESCRIPCIÓN: De la documentación recibida se deduce que la seguridad de acceso lógico está limitada a los servidores centrales de aplicaciones y datos excluyendo a la red de computadoras personales e impresoras de red del organismo. Se está trabajando para que el acceso a los datos lo maneje la base de datos y no cada uno de los aplicativos. Los usuarios no tienen control sobre el uso de sus propias cuentas.-
RECOMENDACIÓN: La alta gerencia es responsable de la gestión de la seguridad de la información de modo tal que las medidas de seguridad de Tecnología Informática concuerden con los requerimientos de la misión del organismo. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:
- administración de las medidas de seguridad,
- identificación, autenticación y acceso,

- seguridad del acceso en línea a los datos,
- administración de cuentas de usuarios,
- revisión por la gerencia de las cuentas de usuarios,
- control ejercido por el usuario en sus propias cuentas,
- supervisión de la seguridad,
- clasificación de los datos,
- administración centralizada de identificaciones y derechos de acceso,
- informes de violación y actividades de seguridad,
- manejo de incidentes,
- reacreditación,
- confianza en la contraparte,
- autorización de transacciones,
- imposibilidad de rechazo,
- ruta de acceso confiable,
- protección de las funciones de seguridad,
- administración de claves criptográficas,
- prevención, detección y corrección de software malicioso,
- arquitectura de firewalls y conexiones con redes públicas,
- protección de valores electrónicos.-

**Respuesta del organismo:**

*La seguridad de acceso lógico no está limitada únicamente a los servidores centrales de aplicaciones. Los servidores descentralizados (por ejemplo los 140 del Sistema Dosmil) cuentan con un sistema de seguridad propio. Se está trabajando para incorporar las computadoras personales conectadas a la red a un esquema de dominio mediante el cual se las podrá autenticar, para luego controlar el acceso a las aplicaciones y sistemas.*

**Comentario AGN:** tal como lo indica el índice de madurez asignado, las políticas se están desarrollando por lo que aún no pueden ser evaluadas.

**En consecuencia se mantiene la observación.**

**Observaciones al punto 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 con la posibilidad de ofrecer el servicio adecuado.-

NIVEL DE MADUREZ: *No Conforma*. Se carece totalmente de un proceso reconocible para identificar e imputar costos con respecto a los servicios de información prestados. El organismo ni siquiera ha reconocido que hay una cuestión que merece abordarse en cuanto a la contabilización de los costos y no hay comunicación al respecto. No hay un cálculo de costos por usuario, departamento, grupos de usuarios, funciones de servicio, proyectos o prestaciones. No hay monitoreo de costos. No hay proceso ni sistema de imputación a los usuarios de los costos incurridos en la prestación de servicios de información.-

DESCRIPCIÓN: De la documentación recibida se deduce que no existe ningún tipo de asignación de costos informáticos. En las conversaciones mantenidas se reconoce que algunas modificaciones de los sistemas existentes para adaptarlos a actos o decisiones emanados de otras autoridades (leyes, decretos, resoluciones, etc.), generan costos superiores a los beneficios que las disposiciones generan al fisco. No se puede evaluar la eficiencia del gasto del área de Tecnología Informática.-

RECOMENDACIÓN: El funcionario responsable de la función de servicios de información, con la orientación de la alta gerencia, debe definir e implementar procedimientos de determinación de costos para ofrecer información administrativa sobre los costos de la prestación de los servicios de procesamiento de información. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- identificar ítems imputables,
- definir procedimientos de determinación de costos,
- utilizar procedimientos de cargos e imputación de costos al usuario.-

**Respuesta del organismo:**

*La imputación de gastos por Centros de Costos tiene un desarrollo incipiente dentro del organismo, habiéndose comenzado a imputar costos por unidades presupuestariamente descentralizadas, por ser estas áreas las que tienen mejores posibilidades de medición.*
*Respecto de los costos de los servicios de información, existe un debate abierto sobre si debe ser atribuido a Dependencias o a Procesos. Con las limitaciones expuestas, habría posibilidades más o menos concretas para que, una vez adoptado un criterio funcionalmente medible, se llegue a distribuir costos por los servicios señalados, y comenzar a dar respuesta a la observación formulada.*
*En particular, el tema de los costos en organismos de Administración Tributaria, tiene algunos problemas de distribución que no han sido suficientemente esclarecidos. Sin embargo, es una preocupación de las autoridades de la AFIP de avanzar en ese sentido.*
*Se toma en cuenta la observación para que, juntamente con las dependencias con incumbencia en estos temas, se comience con la elaboración de indicadores que permitan iniciar un proceso en el sentido indicado.*
*De acuerdo a los parámetros de autoevaluación del control utilizados por el área de TI, este proceso se encuentra en nivel 1.*

**Comentario AGN:** Se acepta la sugerencia de elevar el índice de madurez al nivel I (Inicial / Ad Hoc)**,** tal como se autoevalúa el organismo**.**
**En consecuencia se mantiene la observación**.

**Observaciones al punto 4.3.7 - Educación y Capacitación de los Usuarios**
OBJETIVO DE CONTROL: Se debe establecer y mantener un plan integral de capacitación y desarrollo.-
NIVEL DE MADUREZ: *Inicial / Ad Hoc*. Hay evidencia de que el organismo reconoció la necesidad de un programa de educación y capacitación, pero no hay procesos estandarizados. El enfoque global de la dirección carece de cohesión y la comunicación de los temas y abordajes de la educación y capacitación es sólo esporádica y poco coherente.-
DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido un programa organizado que origine que los empleados asistan a cursos de

capacitación sobre temas de conducta ética, concientización de seguridad de sistemas y prácticas de seguridad. La alta gerencia de Tecnología Informática delega la planificación de la capacitación en el área de Recursos Humanos.-

RECOMENDACIÓN: La máxima autoridad es responsable de impulsar procedimientos para identificar y documentar las necesidades de capacitación de todo el personal que utiliza servicios de información. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- identificación de necesidades de capacitación,
- organización de sesiones de capacitación,
- capacitación y concientización en los principios de seguridad.-

**Respuesta del organismo:**

*Se considera que en términos generales la observación es adecuada y que ya se están elaborando planes para mejorar la situación.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 4.3.8 - Asistencia y Asesoramiento a los Usuarios de Tecnología Informática**

OBJETIVO DE CONTROL: Se debe establecer una función de mesa de ayuda que brinde soporte y asesoramiento de primera línea.-

NIVEL DE MADUREZ: *Proceso Definido*. Hay una acabada comprensión de los beneficios que puede brindar una mesa de ayuda en todos los niveles del organismo, y dicha función se ha creado en unidades organizacionales apropiadas. Los procedimientos se estandarizaron y documentaron, y se está dictando una capacitación informal. Sin embargo, la capacitación y adhesión a las normas corre por cuenta de cada persona. Se desarrollaron preguntas frecuentes y pautas para el usuario, pero no están lo suficientemente accesibles y tal vez no siempre sean observadas. Se hace un seguimiento manual y un monitoreo individual de las consultas y los problemas, pero no existe un sistema formal de presentación de informes. Ha empezado a

implementarse el escalamiento de problemas. La respuesta oportuna a las consultas y los problemas no se mide y puede haber problemas a los que no se dé solución.-

DESCRIPCIÓN: Se está utilizando un sistema de aplicación Mr. Sea que cuenta con pocas licencias y no incluye el módulo de gerenciamiento para efectuar el seguimiento de las tendencias y generar informes sobre las actividades de la mesa de ayuda. El personal disponible, 12 agentes, resulta escaso para los catorce mil usuarios internos de la Administración. Los usuarios externos (contribuyentes y otros) no acceden directamente a la mesa de ayuda del área de Tecnología Informática sino a la del área correspondiente a sus aportes. No está claro el procedimiento de escalamiento entre mesas de ayuda.-

RECOMENDACIÓN: El funcionario principal de servicios de información es responsable de establecer el soporte al usuario dentro de la función de mesa de ayuda. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- el soporte al usuario a través de la mesa de ayuda,
- registro de consultas de usuarios,
- escalamiento de consultas de usuarios,
- monitoreo de soluciones,
- análisis e informe de tendencias.-

**Respuesta del organismo:**

*Se considera que, en términos generales las observaciones son adecuadas y se seguirá trabajando para mejorar la asistencia a la usuarios de Tecnología Informática"*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 4.3.9 - Administración de la Configuración**

OBJETIVO DE CONTROL: Se deben implementar controles que identifiquen y registren todos los bienes de Tecnología Informática y su ubicación física, y un programa de verificación regular que confirme su existencia.-

NIVEL DE MADUREZ: *Inicial / Ad Hoc*. 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.-

DESCRIPCIÓN: No se recibió la documentación solicitada que hubiese permitido verificar la existencia de procedimientos que aseguren el registro e identificación en inventario de los bienes de Tecnología Informática. Tampoco se pudo determinar la existencia de procedimientos para la administración de los cambios en la configuración.-

RECOMENDACIÓN: El funcionario principal de la función de servicios de información es responsable de implementar procedimientos de control para identificar y registrar todos los bienes de Tecnología Informática y su ubicación física, y una rutina de verificación regular que confirme su existencia. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- registro de la configuración,
- nivel básico de configuración,
- registro del estado de la configuración,
- control de la configuración,
- detectar el software no autorizado,
- almacenamiento del software,
- procedimientos de administración de configuración,
- seguimiento y control de versiones de software.-

**Respuesta del organismo:**

*En lo que respecta a la configuración de los aplicativos en producción, cada área de negocio de la gerencia de Tecnología de la Información el control de la configuración de los aplicativos controlando los componentes de software, incluyendo el versionado correspondiente.*

*La adquisición, recepción y distribución del parque informático se realizan según procedimientos y utilizando sistemas informáticos específicos. El registro se lleva tanto para*

*los equipos asignados a los centros de cómputos como los que se distribuyen por los distintos edificios.*

*Se reconoce que es necesario ajustar y formalizar los mecanismos que permitan el mantenimiento de los registros de ubicación posteriormente a la distribución inicial y de la configuración de los equipos instalados fuera de los centros de cómputos.*

*La administración de las licencias de software se realiza de manera centralizada por medio de un sistema informatizado específico.*

*De acuerdo a los parámetros de autoevaluación del control utilizados por el área de TI, este proceso se encuentra en nivel 2.*

**Comentario AGN:** Tal como se indicó en la descripción, no se ha recibido la documentación que avale lo expresado en la respuesta del organismo**.**

**En consecuencia se mantiene la observación**.

**Observaciones al punto 4.3.10 - Administración de Problemas e Incidentes**

OBJETIVO DE CONTROL: Se debe implementar un sistema de administración de problemas que registre y dé respuesta a todos los incidentes.-

NIVEL DE MADUREZ: *Proceso Definido*. La necesidad de un sistema eficaz de administración de problemas es aceptada y evidenciada por la intención de contratación de una herramienta específica. Los procesos de solución de problemas, escalamiento y resolución están normados. Los usuarios recibieron comunicaciones sobre dónde y cómo informar problemas e incidentes. El registro y seguimiento de los problemas y su resolución está fragmentado dentro del equipo de respuesta, que utiliza las herramientas disponibles. Las desviaciones de las normas o los estándares establecidos probablemente pasen desapercibidos.-

DESCRIPCIÓN: De la documentación recibida no se deduce que el organismo haya establecido la política de registro y respuesta a incidentes incluyendo el escalamiento de problemas. Está prevista la adquisición de una herramienta que permita su administración eficaz y eficiente.-

RECOMENDACIÓN: El funcionario principal de la función de servicios de información es

responsable de implementar un sistema de administración de problemas e incidentes de seguridad. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- sistema de administración de problemas,
- escalamiento de problemas,
- seguimiento de problemas y pistas de auditoría,
- autorizaciones de emergencia y acceso temporario,
- prioridades de procesamiento de emergencia.-

**Respuesta del organismo:**

*Se consideran adecuadas las observaciones y recomendaciones y se continuarán mejorando los procesos asociados a la administración de problemas e incidentes y el respectivo seguimiento.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 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 Informática para asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento.-

NIVEL DE MADUREZ: *Repetible aunque Intuitivo.* En todo el organismo prevalece el reconocimiento de la necesidad de la exactitud de los datos y del mantenimiento de su integridad. Se comienza a asignar responsabilidad sobre los datos. Las reglas y los requerimientos no son uniformes en todo el organismo y todas las plataformas. Los datos están en custodia de la función servicios de información y las reglas y definiciones son impulsadas por los requerimientos de Tecnología Informática. La seguridad e integridad de los datos entran principalmente dentro de las responsabilidades de la función de servicios de información.-

DESCRIPCIÓN: La captura de datos se encuentra automatizada en forma prácticamente total.

Sin embargo se están programando tareas de reingeniería de los sistemas existentes (Vg. Sistema de Declaraciones Juradas) para adecuarlos a un ingreso remoto de los datos por parte del usuario final (contribuyente) sin generar puntos de falla en su ciclo de procesamiento. Las salidas impresas se han reducido significativamente y el volumen de impresión es bajo. La operación de resguardo de los datos no incluye la prueba periódica de restauración que garantice la eficacia de la copia.-

RECOMENDACIÓN: La alta gerencia y toda la organización son responsables de establecer procedimientos para garantizar la calidad de los datos. En este aspecto, se debe garantizar la eficacia de los procedimientos y prácticas formalmente establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- procedimientos de preparación de datos,
- procedimientos de autorización de documentos fuente,
- recopilación de datos de documentos fuente,
- manejo de errores de documentos fuente,
- conservación de documentos fuente,
- procedimientos de autorización de entrada de datos,
- verificación de exactitud, integridad y autorización,
- manejo de errores de entrada de datos,
- 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,
- períodos de conservación y condiciones de almacenamiento,

- sistema de administración de biblioteca de medios,
- responsabilidades de administración de la biblioteca de medios,
- procedimiento de resguardo y restauración,
- tareas de resguardo,
- almacenamiento de resguardos,
- archivos,
- protección de mensajes críticos,
- autenticación e integridad,

**Respuesta del organismo:**

*La administración de datos está altamente automatizada y monitoreada por procesos automáticos que permiten detectar problemas en flujo de transferencia y procesamiento. Estos procesos están siendo complementados actualmente gracias a la adquisición de un sistema de "Job Scheduling" (cuya proceso de adquisición fue elaborado en el 2003) que permitirá incrementar aun más el monitoreo de los procesos automáticos de datos.*

*Por lo tanto se considera que las recomendaciones son adecuadas y se continuará avanzado en la formalización y mejoramiento de los procesos correspondientes.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 4.3.12 - Administración de Instalaciones**

OBJETIVO DE CONTROL: Se debe contar con controles ambientales y físicos adecuados cuya revisión se efectúe periódicamente a fin de determinar su correcto funcionamiento.-

NIVEL DE MADUREZ: *Inicial / Ad Hoc*. El organismo reconoce el requerimiento de la actividad de brindar un entorno físico adecuado que proteja los recursos y el personal contra los peligros generados por la naturaleza y el hombre. No existen procedimientos estándares y la administración de las instalaciones y los equipos dependen de la idoneidad y capacidad de ciertas personas clave. No se revisan las actividades de maestranza en las instalaciones y la gente se desplaza con restricciones relativas. La dirección no monitorea los controles ambientales de las instalaciones ni el movimiento del personal. Los procedimientos de

mantenimiento de las instalaciones no están documentados y dependen de las mejores prácticas del personal de Servicios Generales. Las metas de la seguridad física no están basadas en ninguna norma formal y la gestión no garantiza que se cumplan los objetivos de seguridad.

DESCRIPCIÓN: No se registran todos los accesos a los centros de cómputos. Se ha observado que, cuando existe un libro de registro de visitas, las entradas registradas en tres días sólo comprenden al personal de esta Auditoría y no figura el personal de proveedores que, simultáneamente, está realizando tareas de instalación. Se ha verificado in situ que existen sistemas de alarma de acceso físico cuyo uso es desconocido por el personal y que están prácticamente fuera de servicio.-

RECOMENDACIÓN: El funcionario principal de la función de servicios de información es responsable de implementar medidas de control de acceso y seguridad física adecuadas en las instalaciones de tecnología de información. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:

- seguridad física,
- discreción del sitio de tecnología de información,
- acompañamiento de visitas,
- salud y seguridad del personal,
- protección contra factores ambientales,
- fuente de alimentación de energía ininterrumpible y elementos alternativos que garanticen la continuidad del servicio.-

**4.3.12.1 Seguridad Física**

OBJETIVO DE CONTROL: Deberán establecerse medidas apropiadas de seguridad física y control de acceso para las instalaciones de tecnología de información de acuerdo con la política de seguridad general, incluyendo el uso de dispositivos de información fuera de las instalaciones. El acceso deberá restringirse a las personas debidamente autorizadas.-

**A - Centro de Cómputos de los Edificios: Hipólito Yrigoyen y Paseo Colón**

DESCRIPCIÓN: No se obtuvo evidencia de normas y procedimientos para el control de entradas y salidas.-

RECOMENDACIÓN: Deben formalizarse normas y procedimientos para el control de entradas y salidas al Centro de Cómputos.-

**4.3.12.2 Escolta de Visitantes**

OBJETIVO DE CONTROL: Deberán establecerse apropiados procedimientos que aseguren que las personas que no formen parte del grupo de operaciones de la función de servicios de información sean escoltadas por algún miembro de ese grupo cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes.-

**A - Centro de Cómputos de los Edificios: Hipólito Yrigoyen y Paseo Colón**

DESCRIPCIÓN: Las visitas que acceden a los Centros de Cómputos no se acreditan en los Accesos a los edificios del organismo. En la entrada al edificio no se solicita el documento de identidad ni se avisa telefónicamente a los Centros de Cómputos quien va a ingresar.-

RECOMENDACIÓN: Se deben formalizar procedimientos para acceder a los Centros de Cómputos desde el ingreso al Organismo. Un miembro del Centro de Cómputos debe escoltar a las visitas en los Centros de Cómputos.-

**4.3.12.3 Salud y Seguridad del Personal**

OBJETIVO DE CONTROL: Deberán establecerse y mantenerse prácticas de salud y seguridad en línea con las leyes y regulaciones nacionales y locales.-

**A - Centro de Cómputos de los Edificios: Hipólito Yrigoyen y Paseo Colón**

DESCRIPCIÓN: No se obtuvo evidencia de las mediciones de los niveles de iluminación (Ley de Higiene y Seguridad / Ley de Riesgo del Trabajo), ni sobre los registros de inspección en instalaciones eléctricas, como así tampoco de los planes de inspección de los equipos.-

RECOMENDACIÓN: Se deben realizar las mediciones de los niveles de iluminación y, si corresponde, adecuarlos a la Legislación vigente.-

Se debe realizar una planificación sobre las inspecciones de los equipos, como así también efectuar los registros de inspección de las instalaciones eléctricas que se realizan.-

**4.3.12.4 Protección contra Factores Ambientales**

OBJETIVO DE CONTROL: La gerencia de la función de servicios de información deberá asegurar que se establezcan y mantengan las suficientes medidas para la protección contra los factores ambientales (por ejemplo, fuego, polvo, electricidad, calor o humedad excesivos). Deberán instalarse equipo y dispositivos especializados para monitorear y controlar el ambiente.-

**A - Centro de Cómputos de los Edificios: Hipólito Yrigoyen y Paseo Colón**

DESCRIPCIÓN: No se ha obtenido evidencia formal con respecto a:

- la política en materia de Seguridad y Salud Ocupacional definida por las máximas autoridades del Organismo,
- los antecedentes y documentación de la obra, como así tampoco de los estudios de carga de fuego y las normas que se han tenido en cuenta en el diseño de los Centros de Cómputos desde el punto de vista de riesgo de incendios,
- evaluaciones de riesgo en caso de incendio con respecto a los locales linderos,
- la documentación probatoria correspondiente a los controles de los matafuegos,
- el procedimiento para realizar la limpieza de los Centros de Cómputos, como así tampoco de los registros donde se indique que el personal de limpieza tiene conocimiento del mismo,
- si se inspeccionan antes de retirarse de los locales de los Centros de Cómputos. Los recipientes de residuos no tienen tapa y las bolsas de residuos son negras (opacas),
- un procedimiento escrito indicando el destino de las cintas, cartuchos y toner de las impresoras usados,
- las evaluaciones y estudios en el sistema de ventilación cuando se cambian y/o ingresan equipos,
- los registros de los controles de variación de la temperatura,
- los registros de los controles de las luces de emergencia.
- las normas que indican con qué frecuencia se inspeccionan y se realiza la limpieza de piso técnico (Polvo, basuras, acumulación de cables que no se usan, etc.). Potencial riesgo de incendio,
- la capacitación del personal en el manejo de los matafuegos,
- instrucciones en los locales indicando cómo actuar en caso de incendio en el Centro de Cómputos. Impide actuar en forma rápida y eficaz,
- la ejecución de los simulacros de evacuación,

- la documentación y control de los Sistemas de Hidrantes,
- los registros de los Sistemas de Detección y Extinción de incendios,
- las instrucciones, ni los registros de controles sobre el gas extintor FM–200. Potenciales fallas en el funcionamiento del Sistema de Extinción durante un incendio.-

No existe un sistema de audio para usarlo en caso de emergencia.-

En algunos locales no se observan los carteles indicando “Prohibido Fumar”.-

Inexistencia de escaleras de emergencias.-

RECOMENDACIÓN: Fijar la política en materia de Seguridad y Salud Ocupacional.-

Disponer de los antecedentes y la documentación de la obra, estudios de carga de fuego y las normas que se han tenido en cuenta en los diseños de los Centro de Cómputos desde el punto de vista de riesgo de incendios.-

Realizar una evaluación sobre cómo afectaría al Centro de Cómputos un incendio en otras áreas.-

Obtener la documentación correspondiente a los controles que se realizan de los matafuegos.-

Asegurar la existencia de procedimientos para las tareas de limpieza y recolección de bolsas de residuos. Es conveniente que las bolsas de residuos sean transparentes. Todos los recipientes de residuos deben tener bolsas y ser resistentes al fuego.-

Asegurar la existencia de un procedimiento respecto al destino de elementos usados como las cintas, cartuchos y toner de impresoras.-

Realizar evaluaciones y estudios en el sistema de ventilación cuando se cambian y/o ingresan equipos.-

Obtener los registros de las variaciones de temperatura.-

Realizar un mantenimiento integral de las luces de emergencia con los correspondientes registros.-

Formalizar normas para la inspección y limpieza de los pisos falsos.-

Capacitar y entrenar en forma semestral al personal de los Centros de Cómputos en el manejo de los matafuegos.-

Los locales deberían tener instrucciones indicando como actuar en caso de incendio.-

Realizar los simulacros de evacuación.-

Obtener la documentación y los controles de los Sistemas de Hidrantes. Riesgo: Potencial

falta de respuesta ante un incendio.-

Construir una escalera de emergencia o conformar, si es posible “Caja de Escalera”.-

Efectuar el control de los Sistemas de Detección y Extinción y obtener los registros correspondientes.-

Colocar instrucciones sobre el sistema de extinción fijo y realizar los controles correspondientes.-

Instalar un sistema de audio para casos de emergencia.-

Colocar los carteles faltantes indicando “Prohibido Fumar”.-

**B - Centro de Cómputos de los Edificios: Hipólito Yrigoyen**

DESCRIPCIÓN: El acceso de algunos matafuegos se encuentra obstruido. No se obtuvo evidencia sobre:

- los controles y registros de humedad,
- protección de los accesos contra el fuego en áreas externas al Centro de Cómputos,
- Plan de Emergencia y Evacuación.-

En los pisos de las áreas de ingreso al Centro de Cómputos se observan falta de revestimientos (cerámicas), cajas y otros elementos sobre el piso.-

Se fuma en los locales del Centro de Cómputos.-

El depósito de insumos del Centro de Cómputos no posee un sistema de detección y extinción.-

No se han observado en la puerta principal controles eléctricos de emergencia (llaves de corte de energía eléctrica usadas en casos de emergencia).-

La puerta de emergencia se abre frecuentemente.-

Es confusa la Señalización para acceder al Centro de Cómputos, se observa doble numeración en los locales. Los números indicados en los carteles generales no coinciden con los de las oficinas pudiendo demorar la llegada de auxilio.-

RECOMENDACIÓN: Mantener libres los accesos a los matafuegos.-

Realizar el control de la humedad, como así también obtener los registros correspondientes.-

Proteger los locales contra posibles fuegos externos al Centro de Cómputos.-

Reparar los pisos y liberar las rutas de ingreso y egreso.-

Formalizar el Plan de Emergencia y Evacuación, aprobarlo y ejecutarlo.-

Prohibir fumar.-

Instalar un sistema de detección y extinción en el depósito de insumos.-

Instalar en las puertas controles eléctricos de emergencia accesibles al operador (llaves de corte de energía eléctrica usadas en casos de emergencia). Los mismos deberían estar protegidos contra potenciales sabotajes, etc. ocasionados por personal no autorizado.-

Realizar las modificaciones correspondientes a la señalización de las oficinas.-

**C - Centro de Cómputos de los Edificios: Paseo Colón – Primer Piso**

DESCRIPCIÓN: Los matafuegos no se encuentran ubicados correctamente.-

La instalación de algunos equipos permite que los cables provenientes del piso técnico queden a la vista.-

RECOMENDACIÓN: Mantener libres los accesos a los matafuegos.-

Instalar los equipos evitando que los cables provenientes del piso técnico queden a la vista.-

D - **Centro de Cómputos de los Edificios: Paseo Colón – Tercer Piso**

DESCRIPCIÓN: Algunos insumos están distribuidos sobre el piso del local.-

La instalación de algunos equipos permite que los cables provenientes del piso técnico queden a la vista.-

No se han observado en la puerta principal controles eléctricos de emergencia (llaves de corte de energía eléctrica usadas en casos de emergencia).-

RECOMENDACIÓN: Ordenar y retirar los elementos combustibles que se encuentran en los locales.-

Instalar los equipos evitando que los cables provenientes del piso técnico queden a la vista.-

Instalar en la puerta controles eléctricos de emergencia accesibles al operador (llaves de corte de energía eléctrica usadas en casos de emergencia). Los mismos deberían estar protegidos contra potenciales sabotajes, etc. ocasionados por personal no autorizado.-

**Respuesta del organismo:**

*Se han elaborado pliegos relacionados con la administración de las instalaciones para cubrir las necesidades que se mencionan a continuación:*

1. *Instalación de un ambiente de alta seguridad para el Centro de Cómputos de la AFIP (Sala Cofre)*
2. *Control de accesos al edificio donde reside el Centro de Cómputos*
3. *Instalación de Sistema de Detección y Alerta de incendios en dicho edificio*
4. *Adquisición de un sistema ininterrumpible de energía*
5. *Adquisición de un grupo electrógeno para todo el inmueble.*

*Se considera que las observaciones son adecuadas y se continuará tomando medidas para salvarlas.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 4.3.13 - Administración de Operaciones**

OBJETIVO DE CONTROL: Se debe establecer un cronograma de actividades de soporte que registre todas las tareas a realizar y su oportunidad.-

NIVEL DE MADUREZ: *Proceso Definido*. La necesidad de administrar las operaciones de sistemas es comprendida y aceptada dentro del organismo. Se asignaron recursos y se brinda entrenamiento, no permanente, para el puesto de trabajo. Los eventos y resultados de las tareas completas se registran, pero no se guardan en el tiempo, los informes a la dirección son limitados. El uso de programación automatizada y otras herramientas se extiende y estandariza para limitar la intervención del operador. Otras actividades regulares de soporte de la tecnología informática también son identificadas y las tareas relacionadas están siendo definidas. Se ejercen controles para poner en operación los puestos nuevos. Los acuerdos de mantenimiento y servicio con proveedores son formales.-

DESCRIPCIÓN: De la información recibida no se deduce que las operaciones están respaldadas por presupuestos de recursos para gastos de capital y recursos humanos. La capacitación no está formalizada ni es continua. No resultó posible medir y monitorear las actividades diarias con acuerdos de desempeño estandarizados y niveles de servicio establecidos. No está establecida una política formal para reducir la cantidad de eventos no programados. Se entablan acuerdos formales de mantenimiento y servicio con los proveedores del mantenimiento de hardware y software.-

RECOMENDACIÓN: El funcionario principal de la función de servicios de información es responsable de establecer y documentar los procedimientos estándar para las operaciones de tecnología de información. En este aspecto, se debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología Informática:
- manuales de instrucciones y procedimientos de las operaciones de procesamiento,
- documentación del proceso de puesta en marcha y otras operaciones,
- programas de trabajo,
- desviaciones de los programas estándares de trabajo,
- continuidad del procesamiento,
- registro de operaciones,
- salvaguardia de formularios especiales y dispositivos de salida,
- operaciones remotas.-

**Respuesta del organismo:**

*Se considera que las recomendaciones son adecuadas y se continuará avanzado en la formalización y mejoramiento de los procesos correspondientes.*

**Comentario AGN: En consecuencia se mantiene la observación.**

**Observaciones al punto 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 del desempeño y la acción inmediata en caso de desviaciones.-

NIVEL DE MADUREZ: *No Conforma*. El organismo no tiene procesos formales de monitoreo implementado. La función de Tecnología Informática 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 objetivos de proceso claramente entendidos.-

DESCRIPCIÓN: Se dificulta la evaluación de la gestión de la Tecnología Informática por falta de estadísticas confiables.-

RECOMENDACIÓN: La alta gerencia es responsable de que se definan los indicadores de

desempeño pertinentes y que se recopilen datos para la elaboración de informes de gestión y 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, se debe garantizar que se:

- recopilan los datos de monitoreo,
- evalúa el desempeño en forma continua,
- evalúa la satisfacción del usuario,
- elaboran los informes de gestión.-

**Respuesta del organismo:**

*Desde el 2002, existen tres Divisiones formalmente definidas en las estructuras de las áreas de Seguridad, Operaciones y Comunicaciones que tienen como misión principal efectuar el monitoreo de los procesos que se lleven a cabo en sus áreas de incumbencia. Para el desarrollo de estas actividades, las áreas cuentan con un conjunto de herramientas de software específicas que está siendo ampliado mediante procesos de adquisición en curso.*

*Ya se han cumplido las etapas de adquisición y se encuentra en etapa de pre-implantación el software para Balance Scorecard con el objetivo de integrar las mediciones de desempeño de Tecnología de la Información.*

*De acuerdo a los parámetros de autoevaluación del control utilizados por el área de TI, este proceso se encuentra en nivel 1*.

**Comentario AGN:** Se acepta la sugerencia de elevar el índice de madurez al nivel I (Inicial / Ad Hoc)

**En consecuencia se mantiene la observación**.