AUDITORÍA GENERAL DE LA NACIÓN

GERENCIA DE PLANIFICACIÓN Y PROYECTOS ESPECIALES
Dr. Felipe Pizzuto

DEPARTAMENTO DE AUDITORÍA INFORMÁTICA
Ing. Ernesto Casin

Objeto de Auditoría: Evaluación de la Tecnología Informática en el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados, organismo autárquico en la órbita del Ministerio de Salud y Ambiente, con el objeto de determinar debilidades y fortalezas de la gestión informática en el Organismo.-

INFORME DE AUDITORÍA

A la Lic. María Graciela Ocaña.
Directora Ejecutiva
Instituto Nacional de Servicios Sociales para Jubilados y Pensionados.

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

1. -Objeto de la auditoría

Evaluación de la Tecnología Informática en el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados, organismo autárquico en la órbita del Ministerio de Salud y Ambiente, con el objeto de determinar debilidades y fortalezas de la gestión informática en el Organismo.-
Período auditado: Año 2004.

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 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 Instituto Nacional de Servicios Sociales para Jubilados y Pensionados, en base a la información obtenida de las siguientes fuentes:

- Entrevistas realizadas con las principales autoridades del Instituto.
- 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 del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados.-

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

Las tareas de campo abarcaron desde abril 2004 hasta noviembre 2004.-

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 del Instituto.
- Análisis de los informes de Auditoría Interna en temas informáticos.
- Entrevistas con los responsables de Gerencias del Instituto, en cuanto a la participación y experiencia propia y de su personal en el uso de la Tecnología de la Información.
- Entrevistas con los responsables del Área Informática del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados.-

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, realizadas 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.-

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

3.1.- Marco legal e institucional

3.1.1.- Antecedentes y Naturaleza Jurídica

El Instituto Nacional de Servicios Sociales para Jubilados y Pensionados fue creado por el Decreto Ley N° 19.032 del 13 de mayo de 1971 y reglamentado por el Decreto N° 1157/71 de igual fecha.

La ley en su primer artículo establece que funcionará como entidad de derecho público no estatal, con personalidad jurídica e individualidad financiera y administrativa.

El Instituto tiene como objeto otorgar —por sí o por terceros— a los jubilados y pensionados del Régimen Nacional de Previsión y del Sistema Integrado de Jubilaciones y Pensiones y a su grupo familiar primario, las prestaciones sanitarias y sociales, integrales, integradas y equitativas, tendientes a la promoción, prevención, protección, recuperación y rehabilitación de la salud.

Las prestaciones anteriormente mencionadas son consideradas servicios de interés público, siendo intangibles los recursos destinados a su financiamiento. Así lo establece la Ley N° 25.615 (B.O. 23/07/02) modificatoria del Decreto Ley N° 19.032.

La Ley N° 25.615 también rediseña el accionar del Instituto sobre la base de criterios y necesidades regionales, factores socio-demográficos, epidemiológicos, tasas de uso estimativas y costos de cada jurisdicción, coordinando su actividad con las autoridades sanitarias locales. En consonancia con ello, institucionaliza las Unidades de Gestión Local (UGL), haciéndolas partícipes en la responsabilidad de conducción, el control prestacional local y la administración de su padrón.

Actualmente el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados cuenta con 36 sucursales denominadas Unidades de Gestión Local (UGL), 291 agencias y 253 corresponsalías, distribuidas en todo el país. Tanto las agencias como las corresponsalías son dependientes de las UGL.

3.1.2.- Gobierno y Administración del Instituto.

El gobierno y administración del Instituto se encuentran establecidos por el Decreto N° 2 del año 2004, que establece que durante la etapa transicional que va desde el fin de la intervención hasta la sanción de la nueva norma que regulará su actividad por parte del Honorable Congreso de la Nación, se ejercen a través de un órgano Ejecutivo de Gobierno integrado por un Director Ejecutivo y un Subdirector Ejecutivo, designados por el Poder Ejecutivo Nacional.

3.1.3- Antecedentes.

La Ley N°19.032 ha sido modificada en distintas ocasiones en lo que a sus órganos de administración y control se refiere. Es necesario aclarar también que el Instituto ha sido intervenido en sucesivas oportunidades, por lo que los órganos de gobierno y administración no siempre han estado plenamente en funcionamiento. En el período comprendido entre los años 1991 y 2003 se designaron 9 interventores.

3.1.4.- Recursos del Instituto:

Los recursos del Instituto están formados de la siguiente manera: (Conforme lo prescripto por el artículo 8 de la Ley N° 19.032):

a) El aporte de los beneficiarios de la Administración Nacional de la Seguridad Social y del Sistema Integrado de Jubilaciones y Pensiones (SIJP), tengan o no grupo familiar, calculado sobre los haberes de las prestaciones incluido el haber complementario, equivalente al tres por ciento (3%) hasta el importe del haber mínimo y al seis por ciento (6%) sobre lo que excede dicho monto.

b) El aporte de los beneficiarios de la Administración Nacional de la Seguridad Social (Ex Caja de Jubilaciones para Trabajadores Autónomos), y Sistema Integrado de Jubilaciones y Pensiones (Ex Trabajadores Autónomos), tengan o no grupo familiar, del seis por ciento (6%) calculado sobre los haberes de las prestaciones, incluido el haber complementario.

c) El aporte de los trabajadores autónomos en actividad del cinco por ciento (5%) del monto que corresponda a su categoría conforme a las disposiciones de la Ley Nº 24.241.

d) El aporte del personal en actividad comprendido en el régimen nacional de jubilaciones y pensiones consistente en el tres por ciento (3%) de su remuneración conforme a las disposiciones de la Ley Nº 24.241.

e) La contribución de los empleadores comprendidos en el Régimen Nacional de Jubilaciones y Pensiones, consistente en el dos por ciento (2%) de las remuneraciones que deban abonar a sus trabajadores.

f) El aporte que el Poder Ejecutivo nacional fije para los afiliados a que se refiere el art. 4º de la presente ley, importe que no será inferior al promedio por cápita que el Instituto erogue por afiliado y familiares a cargo.

g) El producido de los aranceles que cobre por los servicios que preste.

h) Las donaciones, legados y subsidios que reciba.

i) Los intereses y las rentas de los bienes que integran ese patrimonio y el producido de la venta de esos bienes.

j) Todo otro ingreso compatible con su naturaleza y fines.

k) Los aportes del Tesoro que determina la Ley de Presupuesto Nacional por cada período anual.

Los recursos no invertidos en un ejercicio se transferirán al siguiente.

3.1.5.- Población Beneficiaria

Según la información proporcionada por el PAMI este cuenta con 3.083.258 de afiliados en todo el país, a enero de 2004.

Los destinatarios principales de los servicios del Instituto, son los jubilados y pensionados del Régimen Nacional de Previsión y su grupo familiar primario, así como los provenientes de regímenes especiales. De éstos, el 79,93 % son mayores de 60 años.

Personas que pueden ser afiliados al Instituto:

- Los poseedores titulares de un beneficio de jubilación o pensión en el orden nacional (afiliación definitiva).
- Los que han iniciado el trámite para acceder a un beneficio previsional de jubilación, retiro, pensión, etc. (Afiliación provisoria) y familiares a cargo (afiliación provisoria).

- Si se es familiar a cargo (cónyuge, hijos/as menores o separado/a por art. 67 bis) de un afiliado titular (afiliación definitiva).
- Los hijos incapacitados en forma definitiva o transitoria. Los hijos estudiantes hasta los 25 años de edad inclusive.
- Los concubinos que no posean beneficio alguno (afiliación definitiva).
- Menores bajo guarda o tutela (hasta cumplir la mayoría de edad) Personas sujetas a curatela.
- Padre, madre, abuelos del titular sin beneficio previsional.
- Personas mayores de 70 años sin beneficio ni cobertura de obra social (afiliación renovable anualmente).

4.- Comentarios y observaciones

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.-

Además, para cada uno de los objetivos de control se indica cuáles de los requerimientos de la información, detallados a continuación, son afectados:

*Eficacia***:** Se refiere a que la información sea relevante y pertinente para la misión del ente, así como a que su entrega sea oportuna, correcta, consistente y utilizable.

*Eficiencia***:** Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

*Confidencialidad***:** se refiere a la protección de información sensible contra divulgación no autorizada.

*Integridad***:** Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del organismo.

*Disponibilidad***:** Se refiere a la disponibilidad de la información cuando ésta es requerida por las misiones del organismo ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

Cumplimiento: Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el organismo está sujeto.

*Confiabilidad***:** Calidad de la información referida a la provisión de información apropiada a la administración para operar la entidad y para cumplir sus responsabilidades de generación de reportes financieros y de cumplimiento.

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 de la Información.

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia

y en forma secundaria:

- la eficiencia.

Nivel de madurez: Inicial / Ad Hoc. La gerencia de Tecnología de la Información reconoce la necesidad de una planificación estratégica de Tecnología de la Información, pero no hay un proceso de decisión estructurado. La planificación estratégica de Tecnología de la Información está determinada por necesidades puntuales, en respuesta a un requerimiento específico del organismo. Por lo tanto, los resultados no son uniformes. La planificación estratégica de Tecnología de la Información ocasionalmente se debate en reuniones de gestión de Tecnología de la Información, pero no en reuniones de la dirección del organismo. La alineación de los requerimientos del organismo, las aplicaciones y la tecnología se realiza en forma reactiva, generalmente a partir de propuestas de los proveedores, y no por una

estrategia para toda la organización. No se identifica la posición de riesgo estratégico de los proyectos.

Observaciones: El nivel de organización del Instituto es débil y la alta frecuencia de rotación de sus máximas autoridades dificulta la superación del problema. No existió en los últimos años un área dedicada al planeamiento y tampoco un plan estratégico del Instituto. Hoy existe la Gerencia de Tecnología y Planeamiento pero no ha conseguido definir el plan estratégico. No existe un comité de planificación de Tecnología Informática.

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

4.1.2. – Definición de la Arquitectura de la Información.

- **Objetivo de control:** La información debe mantenerse acorde con las necesidades y debe ser identificada, recopilada y comunicada en 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.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia

y en forma secundaria:

- la eficiencia
- la confidencialidad
- la integridad

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 reglas de sintaxis y diagramas de datos y documentación. Las definiciones se basan en los datos, en lugar de la información.

Hay una comunicación esporádica, no uniforme, de la necesidad de una arquitectura de la información.

Observaciones: Existe conciencia de la importancia de la arquitectura de la información pero no se ha avanzado en el tema y no existe un modelo al respecto. Del análisis de la base de datos de beneficiarios surgen serias deficiencias de calidad (Anexo I) imputables a este tema. Se ha detectado información específica almacenada en más de una base de datos con distinto formato lo cual dificulta, y en algunos casos imposibilita, los cruces de control (Anexo II).

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

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, servicios y mecanismos de entrega.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia

y en forma secundaria:

- la eficiencia

Nivel de madurez: Inicial / Ad Hoc. La alta gerencia reconoce la necesidad de la planificación de la infraestructura tecnológica, pero no ha formalizado ningún proceso o plan. El desarrollo de los componentes tecnológicos y la implementación de nuevas tecnologías son hechos ad hoc y aislados. El enfoque de la planificación es reactivo y se concentra en los aspectos operacionales. Las direcciones tecnológicas son manejadas por los planes de evolución de los proveedores de productos de hardware, software de sistemas y software de aplicaciones, a menudo contradictorios. No hay una comunicación normalizada del impacto potencial que podrían tener los cambios tecnológicos.

Observaciones: Se tiene conciencia de la importancia que la planificación de infraestructura tecnológica reviste para el organismo. Sin embargo a la fecha no se ha concretado esta

planificación. En la actualidad se informa que hace aproximadamente cinco años que no se actualiza dicha infraestructura. No se encuentra formalmente definida un área para la determinación de la dirección tecnológica que elabore y actualice periódicamente el plan de infraestructura. Sólo se conforma un grupo informal de trabajo en los casos en que sea necesario.

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

4.1.4. – Definición de la organización y las Relaciones de Tecnología de la Información.

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 y que facilite la estrategia y brinde una dirección eficaz y un control adecuado.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia

y en forma secundaria:

- la eficiencia

Nivel de madurez: No conforma. La estructura organizativa del organismo no está debidamente establecida para concretar el logro de sus objetivos.

Observaciones: Al no estar aprobada la planificación estratégica, no están oficialmente establecidos los objetivos de detalle del Instituto por lo que no se pueden adecuar los servicios de tecnología de la información a sus necesidades. En general los niveles gerenciales del Organismo tienen un alto grado de rotación. En particular cabe destacar que durante el trabajo de campo se trabajó con tres Gerentes de Tecnología y Planeamiento. Existe un organigrama con misiones y funciones aprobadas en 2003 que no se aplica estrictamente. La cantidad total de personal del organismo es de aproximadamente 11.000 agentes. En el sector de sistemas trabajan 106 personas de las cuales sesenta son personal técnico, mientras que el resto realiza tareas administrativas.

La dotación del área de Tecnología es reducida para el volumen de tareas que debería realizar el sector si asumiera la problemática de todo el organismo.

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

4.1.5. – Administración de la Inversión en Tecnología de Información.

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la confiabilidad

Nivel de madurez: Inicial / ad hoc. El organismo reconoce la necesidad de administrar la inversión en Tecnología de la Información, pero no hay una comunicación normalizada al respecto. No hay una asignación formal de la responsabilidad de la selección de inversiones y el desarrollo de presupuestos de Tecnología de la Información. En casos aislados se implementa la selección y presupuestación de inversiones de Tecnología de la Información, con documentación informal. La justificación de las inversiones de Tecnología de la Información es ad hoc. Se toman decisiones de presupuestación reactivas y concentradas en las operaciones.

Observaciones: Al no existir aprobación oficial de las metas detalladas del organismo se imposibilita el logro del objetivo. Existen equipos ya adquiridos que no se utilizan por falta de contrataciones auxiliares que permitan su instrumentación. El presupuesto de Tecnología de Información asignado para el corriente año es del 0.8% del total de las erogaciones programadas del organismo. La no concreción de compras necesarias programadas lleva a la subejecución presupuestaria.

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

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.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia

y en forma secundaria:

- el cumplimiento

Nivel de madurez: Inicial / ad hoc. Las políticas, procedimientos y normas se desarrollan y comunican en forma ad hoc, en función de las necesidades, impulsadas principalmente por la aparición de problemas. Los procesos de desarrollo, comunicación y cumplimiento son informales y no siguen criterios uniformes.

Observaciones: De la información recibida no se pudo establecer la existencia de procedimientos orientados a establecer un ambiente positivo de control a través de la comunicación de reglas y normas que permitan el logro de las estrategias gerenciales.

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

4.1.7. – Administración de los Recursos Humanos.

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia
- la eficiencia

Nivel de madurez: Inicial / ad hoc. La alta gerencia reconoce la necesidad de la administración de los recursos humanos pero no ha formalizado ningún proceso o plan. El proceso de administración de los recursos humanos de Tecnología de la Información es informal y tiene un enfoque reactivo y centrado en las operaciones para la contratación y administración del personal. Hay escasa conciencia sobre el impacto que los rápidos cambios de las actividades sustantivas del organismo y la tecnología y las soluciones cada vez más complejas pueden tener en la necesidad de nuevos niveles de habilidades y competencias.

Observaciones: La información recibida no permite determinar que se hayan implementado los procesos necesarios para la administración eficiente de recursos humanos para la tecnología de la información. Las tareas mínimas para el funcionamiento del área de Tecnología de la Información, en algún caso, son ejecutadas por el personal sin que figuren en su misión y funciones debido a defectos formales en su confección. Los agentes de desarrollo de sistemas realizan tareas de actualización de bases de datos que no corresponden a su perfil ni a sus funciones. No existen definiciones de los puestos del personal de Tecnología Informática.

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

4.1.8. – 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 de la Información y analizar su impacto, involucrando funciones multidisciplinarias y adoptando medidas eficaces en función de costos a fin de mitigar los riesgos.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la confidencialidad
- la integridad
- la disponibilidad

y en forma secundaria:

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

Nivel de madurez: No conforma. No se realiza una evaluación de riesgos para los procesos y las decisiones de actividades sustantivas. El organismo no considera los impactos en la actividad relacionados con las vulnerabilidades de la seguridad y las incertidumbres de los proyectos de desarrollo. La administración de riesgos no se identificó como punto relevante en la adquisición de soluciones de Tecnología de la Información y la prestación de servicios de Tecnología de la Información.

Observaciones: De la información recibida se concluye que no existen políticas y procedimientos formales para la evaluación del riesgo tecnológico.

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

4.1.9. – Administración de Proyectos.

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia
- la eficiencia

Nivel de madurez: Inicial / ad hoc. El organismo tiene una noción de la necesidad de estructurar los proyectos y conoce los riesgos que se corren al tener proyectos mal administrados. El uso de técnicas y enfoques de administración de proyectos dentro de

Tecnología de la Información es una decisión que queda a criterio de cada uno de sus gerentes. Los proyectos en general están mal definidos y no incorporan los objetivos técnicos ni de la actividad del organismo ni de las partes interesadas. No hay una organización clara dentro de los proyectos de Tecnología de la Información y no se han definido formalmente roles ni responsabilidades. No hay una buena definición de los cronogramas y plazos. El tiempo y los gastos del personal asignado al proyecto no se rastrean ni cotejan con los presupuestos ni con las planificaciones que deberían existir.

Observaciones: Durante el período auditado la actividad de desarrollo de sistemas aplicativos se encuentra distribuida entre la Gerencia de Tecnología y Planeamiento y las Gerencias (que solamente deberían ser usuarias) y sin política uniforme. Los procedimientos para el desarrollo de sistemas son informales.

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

4.1.10. – 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 claves y responsabilidades explícitas.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia
- la eficiencia
- la integridad

y en forma secundaria:

- la confiabilidad

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 de la Información no reconocen la necesidad de un programa de calidad. Nunca se verifica la calidad de los proyectos y las operaciones.

Observaciones: La alta gerencia y el personal de Tecnología no establece un programa de control de calidad y éste no se verifica en los proyectos y las operaciones. No se aplica la metodología de ciclo de vida, no existe una planificación previa de los proyectos de desarrollo de sistemas ni un sistema formal para su seguimiento. Se han observado datos erróneos almacenados en las bases principales que los sistemas aplicativos no deberían admitir (Anexo I).

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

4.2. -Administración e implementación.

4.2.1. - Identificación de Soluciones Automatizadas

Objetivo de control: La máxima autoridad debe garantizar una identificación y un análisis claro y objetivo de las alternativas, medidas en comparación con los requerimientos del usuario.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia

y en forma secundaria:

- la eficiencia

Nivel de madurez: No conforma. El organismo no exige la identificación de requerimientos funcionales y operativos para el desarrollo, la implementación o modificación de las soluciones de sistemas, servicio, infraestructura, software y datos. El organismo no se mantiene informado de las soluciones tecnológicas disponibles que potencialmente pudieran ser relevantes para su actividad.

Observaciones: De la información recibida surge que:

- No se han documentado criterios para la consideración de las opciones de desarrollo interno, de terceros y soluciones compradas.
- No existe un método general de adquisición e implementación ni una metodología de ciclo de vida de desarrollo de sistemas que sea claro y este entendido y aceptado.

- No existe un proceso transparente, ágil y eficiente para la planificación, iniciación y aprobación de soluciones.
- No se implementó un proceso estructurado de análisis de requerimientos.
- No existen procedimientos formales para evaluar los requerimientos de seguridad y control desde el principio de los desarrollos.

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

4.2.2. - Adquisición y Mantenimiento del Software de Aplicación

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la integridad
- el cumplimiento
- la confiabilidad

Nivel de madurez: No conforma. No hay un proceso para diseñar y especificar aplicaciones. En general, las aplicaciones se obtienen sobre la base de ofrecimientos de los proveedores, reconocimiento de la marca o familiaridad del personal de Tecnología de la Información con productos específicos, mientras que los requerimientos reales prácticamente no se tienen en cuenta.

Observaciones: De la información recibida no surge la existencia de una metodología formal de adquisición, diseño, desarrollo e implementación aceptada, entendida y aplicada.

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

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 de los rendimientos, y la administración coherente de sistemas.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la integridad

Nivel de madurez: No conforma. No se reconoce la infraestructura tecnológica como un tema lo suficientemente importante a ser resuelto.

Observaciones: Se observó que la infraestructura informática del organismo es obsoleta e insuficiente para las tareas que se están desarrollando. Se han detectado procesos de contratación de duración superior a la razonable. Existen equipos recepcionados que no pudieron ser puestos en funcionamiento por demoras en la contratación de los servicios correspondientes. Se ha verificado la pérdida o desaparición de expedientes de contratación de lo que se deriva la falta de prácticas de adquisición adecuadas.

No está definida por la alta gerencia una estrategia de arquitectura de Tecnología de la Información y los requerimientos relacionados para el organismo.

No se cuenta con un inventario actualizado de la infraestructura de Tecnología de la Información (hardware y software). El inventario de hardware que se ha recibido es incompleto y no permite evaluar adecuadamente el estado de la infraestructura tecnológica, a pesar de lo cual se pudo inferir que equipamiento disponible es obsoleto e incompleto. No se ha recibido un inventario de las aplicaciones de base y de usuario.

De la información obtenida no surge que se hayan definido políticas para:

- Evaluar adecuadamente las opciones de desarrollo interno, por terceros y el aprovechamiento de infraestructuras externas.

- Manejar los casos en los que se depende de un proveedor de única fuente.
- La administración de cambios.
- El uso de una metodología de ciclo de vida bien definida para seleccionar, adquirir, mantener y quitar componentes de la infraestructura de Tecnología de la Información.
- Fundamentar las adquisiciones en los requerimientos de desempeño y capacidad mediante la integración con procesos de administración de los mismos.

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

4.2.4. - Desarrollo y Mantenimiento de Procedimientos

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la integridad
- el cumplimiento
- la confiabilidad

Nivel de madurez: No conforma. No hay un proceso para la producción de documentación del usuario, manuales de operaciones y material de capacitación. Los únicos materiales son los que vienen con los productos comprados.

Observaciones: De la información recibida no surge que:

- Existan acuerdos de nivel de servicio bien definidos, con vínculos con las normas de documentación.
- Se mantengan inventarios de programas y procedimientos del organismo ni de Tecnología de la Información utilizando herramientas automatizadas.

- El proceso de desarrollo asegure el uso de procedimientos operativos estándares y una apariencia estándar de las interfaces de usuario.
- La capacitación del usuario en la utilización de los procedimientos esté integrada con los planes de capacitación del organismo y de Tecnología de la Información.
- Exista un marco estándar, definido y monitoreado, para la documentación y la redacción de los procedimientos.
- Para desarrollar, distribuir y mantener los procedimientos se empleen técnicas de administración del conocimiento, de flujo de trabajo ni herramientas automatizadas.
- La infraestructura y estructura organizativa estén diseñadas para promover y compartir la documentación del usuario, los procedimientos técnicos y el material de capacitación entre los instructores, la mesa de ayuda y los grupos de usuarios.

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

4.2.5. - Instalación y acreditación de aplicativos.

Objetivo de control: La implementación de nuevos sistemas debe realizarse por medio de un plan bien formalizado de instalación, migración, conversión y aceptación.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia

y en forma secundaria:

- la integridad
- la disponibilidad

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

Observaciones: De la información disponible se deduce que:

- No existe una metodología documentada de adquisición e implementación que esté asentada y se aplique con criterios uniformes.
- No existe un mecanismo formal de realimentación implementado para optimizar y mejorar continuamente los procesos.
- No existen procedimientos documentados para la certificación y acreditación formal de sistemas de seguridad con una definición uniforme.
- Sólo se administran en la Gerencia de Tecnología y Planeamiento cuatro sistemas (Padrón General, Beneficiarios, Mesa de Entradas y SAP) mientras que el resto de las aplicaciones de uso en el Organismo son desarrollos informales de distintas Gerencias del Instituto.

Cabe destacar que el sistema SAP con el cual se realiza la gestión económica y financiera es alimentado por información proveniente de sistemas que no han sido aprobados formalmente y que consecuentemente no satisfacen requerimientos de confiabilidad e integridad.

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

4.2.6. - Administración de Cambios

Objetivo de control: Se debe implementar un sistema de administración de cambios que permita el análisis, la implementación y el seguimiento de todas las modificaciones solicitadas y realizadas en la infraestructura de Tecnología de la Información existente.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

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

y en forma secundaria:

- la confiabilidad

Nivel de madurez: Inicial / Ad Hoc. Se reconoce que los cambios deberían ser administrados y controlados, pero no hay un proceso uniforme que pueda seguirse. Las prácticas varían y es

factible que ocurran cambios no autorizados. La documentación de los cambios es escasa o nula, mientras que la documentación de la configuración es incompleta y poco confiable. Es probable que se produzcan errores e interrupciones en el ambiente de producción debido a una deficiente administración.

Observaciones: Del análisis de la información recibida surge que:

- No existen políticas de cambio claras y conocidas que se implementen en forma rigurosa y sistemática.
- La administración de cambios no está integrada con la administración de las versiones de software ni forma parte de la administración de la configuración.
- No existe un proceso rápido y eficiente de planificación, aprobación e iniciación que cubra la identificación, categorización, evaluación de impactos y fijación de prioridades para los cambios.
- No se cuenta con herramientas de proceso automatizadas para respaldar la definición de flujo de trabajo, planes de trabajo normados, plantillas de aprobación, pruebas, configuración y distribución.
- No hay un proceso formal definido para la transición del ambiente de desarrollo al de operaciones.
- No se analiza si los cambios tienen impacto en los requisitos de capacidad y desempeño.
- No se dispone de documentación de aplicaciones y configuración completa y actualizada.
- No hay un proceso implementado para administrar la coordinación entre los cambios que tenga en cuenta las interdependencias de los sistemas.

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

4.3. -Entrega y Soporte.

4.3.1.- Definición y Administración de los Niveles de Servicio.

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

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

Nivel de madurez: No conforma. La dirección no ha reconocido la necesidad de un proceso para la definición de niveles de servicio. La rendición de cuentas y las responsabilidades del monitoreo de dichos niveles no están asignadas.

Observaciones: De las reuniones mantenidas y de la documentación recibida surge que la organización no consideró en el período auditado la necesidad del establecimiento de un proceso para la definición de niveles de servicio ni de su gestión.

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

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.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la confidencialidad

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

Nivel de madurez: No conforma. Las responsabilidades y la rendición de cuentas no están definidas. No hay políticas y procedimientos formales para la contratación de terceros. Los servicios de terceros no son aprobados ni revisados por la dirección. No hay actividades de medición ni informes de los proveedores y en consecuencia la alta gerencia no está al tanto de la calidad del servicio prestado.

Observaciones: De la información recibida surge que la mayoría de los servicios que se le prestan al Instituto no cuentan con contratos vigentes. Los servicios, en esos casos, son prestados efectivamente por terceros cuyos contratos han vencido y son pagados con la figura de legítimo abono.

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

4.3.3.- Administración de la Capacidad y el Desempeño.

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la disponibilidad

Nivel de madurez: No conforma. La alta gerencia no reconoció que las actividades sustantivas claves pueden requerir altos niveles de desempeño de Tecnología de la

Información y que la necesidad del organismo de tales servicios excede la capacidad instalada. No se cuenta con ningún proceso de planificación de la capacidad de procesamiento.

Observaciones: Según la información disponible no existen en el instituto políticas y procedimientos formales para la planificación de la capacidad. Si bien se realizan estimaciones basadas en las expectativas de cambio del modelo prestacional, la falta de definiciones al respecto dificulta la concreción y formalización de ampliaciones de una infraestructura que a la fecha es totalmente insuficiente, incluso para las aplicaciones en uso.

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

4.3.4. - Garantía de un Servicio Continuo.

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia
- la disponibilidad

y en forma secundaria:

- la eficiencia

Nivel de madurez: No conforma. No se comprenden los riesgos, las vulnerabilidades y las amenazas para las operaciones de Tecnología de la Información, ni el impacto que la pérdida de servicios de Tecnología de la Información puede tener en el organismo. No se considera que la continuidad del servicio requiera la atención de la máxima autoridad y la alta gerencia.

Observaciones: De la información recibida surge que no se ha formalizado un plan de continuidad del servicio. A pesar de que existe conciencia de los riesgos a los que está expuesto el Instituto, hasta la fecha no se tomaron las acciones requeridas para superarlos.

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

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 esta limitado a los usuarios autorizados.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la confidencialidad
- la integridad

y en forma secundaria:

- la disponibilidad
- el cumplimiento
- la confiabilidad

Nivel de madurez: Proceso parcialmente definido. La dirección tiene conciencia de la seguridad y la promueve. Se estandarizaron y formalizaron sesiones informativas sobre temas de seguridad. Los procedimientos de seguridad de Tecnología de la Información están parcialmente definidos e integrados en una estructura de políticas y procedimientos de seguridad. Las responsabilidades de la seguridad de Tecnología de la Información están asignadas, aunque no se observan en forma consistente. No existe un plan de seguridad de Tecnología de la Información con análisis de riesgos y soluciones de seguridad. El informe de la seguridad de Tecnología de la Información se concentra en la función de Tecnología de la Información y no en la misión del organismo. No se realizan pruebas de intrusión ad hoc.

Observaciones: El tema de seguridad de los sistemas recién comienza a manejarse formalmente en Octubre de 2.003, cuando se aprueba la política en la materia, la cual todavía se encuentra en proceso de instrumentación y no fue debidamente concientizada por los niveles gerenciales. Se constató en el campo el uso de utilitarios de mensajería instantánea, como el Microsoft Messenger, que implican una vulnerabilidad externa al habilitar entradas no protegidas a la red interna.

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

4.3.6. – Identificación e Imputación de Costos.

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficiencia
- la confiabilidad

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.

Observaciones: La máxima autoridad del área entiende que, dada la gravedad de los problemas que debe enfrentar, el análisis de la imputación de costos es secundario.

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

4.3.7. – Educación y Capacitación de los Usuarios.

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia

y en forma secundaria:

- la eficiencia

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. En ausencia de un programa organizado, los empleados identifican y asisten a cursos de capacitación por cuenta propia. Algunos de estos cursos tratan temas de conducta ética, concientización de seguridad de sistemas y prácticas de seguridad. 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.

Observaciones: De la información recibida no surge la existencia de procedimientos para identificar y documentar las necesidades de capacitación de todo el personal que utiliza servicios de información. No existen políticas y procedimientos aprobados para la identificación de las necesidades de capacitación y tampoco un plan de capacitación a usuarios. Para los sistemas corporativos el Departamento de Apoyo y Seguimiento Operativo realiza una capacitación informal. Lo mismo ocurre con la capacitación de los referentes informáticos del interior. La capacitación y concientización en los principios de seguridad se realiza sin políticas y procedimientos aprobados y con escaso éxito en el nivel gerencial. El área de recursos humanos capacita a los empleados en el uso de herramientas informáticas de oficina (Excel, Word, etc.).

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

4.3.8. – Asistencia y Asesoramiento a los Usuarios de Tecnología de la Información.

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia

Nivel de madurez: Repetible aunque intuitivo. El organismo tomó conciencia de la necesidad de contar con una función de mesa de ayuda. La asistencia está disponible informalmente, a través de una red de personas con conocimientos especializados. Estas personas cuentan con

algunas herramientas comunes para ayudar a resolver los problemas. No hay una capacitación ni comunicación formal sobre procedimientos estándares, y la responsabilidad queda librada a cada uno. Sin embargo, existe una comunicación uniforme sobre las cuestiones globales y la necesidad de abordarlas.

Observaciones: Existe una mesa de ayuda que atiende a los usuarios de los sistemas centralizados. No se dispone de documentación que formalice y estandarice los procedimientos.

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

4.3.9. – Administración de la Configuración.

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia

y en forma secundaria:

- la disponibilidad
- la confiabilidad

Nivel de madurez: Repetible aunque intuitivo. La alta gerencia reconoce los beneficios de controlar la configuración de Tecnología de la Información pero implícitamente se depende de los conocimientos y la experiencia del personal técnico. Se están empleando herramientas de administración de la configuración hasta cierto punto, pero difieren de una plataforma a otra. Más aun, no se han definido prácticas de trabajo estándares. El contenido de los datos de configuración es limitado y no es utilizado por procesos interrelacionados, como la administración de cambios y la administración de problemas.

Observaciones: De la documentación recibida se deduce que no existen procedimientos formales para la administración de la configuración. Los datos disponibles no son de calidad y difieren según la ubicación física del bien.

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

4.3.10. – Administración de Problemas e Incidentes.

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la disponibilidad

Nivel de madurez: Inicial / ad hoc. El organismo reconoce que hay una necesidad de resolver problemas y evaluar incidentes. Hay especialistas dentro del organismo que ayudan a resolver los problemas relacionados con su área de conocimiento y responsabilidad. La información no se comparte con otros y las soluciones varían de una persona de soporte a otra, con lo cual se crean problemas adicionales y se pierde tiempo productivo mientras se buscan las respuestas.

Observaciones: De la información recibida no surge que existan procedimientos formales para la administración de problemas e incidentes de seguridad y tampoco sistemas al efecto que permitan realizar el escalamiento y seguimiento de los problemas y pistas de auditoría. No se ha obtenido documentación referente a autorizaciones de emergencia, acceso temporario y prioridades de procesamiento en situaciones de indisponibilidad.

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

4.3.11. – Administración de Datos.

Objetivo de control: La máxima autoridad debe establecer y mantener una combinación eficaz de controles generales y de aplicación sobre las operaciones de Tecnología de la Información.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la integridad
- la confiabilidad

Nivel de madurez: No conforma. Los datos no están considerados como un recurso y un bien del organismo. No se asignó la responsabilidad sobre los datos ni rendición de cuentas individual por la integridad y confiabilidad de los datos. La calidad y seguridad de los datos es escasa o nula.

Observaciones: Si bien se asigna la responsabilidad sobre los datos a los departamentos, no existe control por oposición en la autorización de documentos fuente que luego son conservados por cortos lapsos (en Afiliaciones por 18 meses). No existen procedimientos para el monitoreo de exactitud, integridad y autorización. Los sistemas, en particular el SAP desde el cual se autorizan todas las erogaciones del Instituto (superiores a los $3.000.000.000 anuales), se alimentan con información generada en aplicaciones “ad hoc”, desarrolladas fuera del control del área de Tecnología Informática, y con utilitarios de oficina y, por lo tanto, sin satisfacer mínimamente normas de calidad y seguridad.

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

4.3.12. – Administración de Instalaciones.

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la integridad
- la disponibilidad

Nivel de madurez: No conforma. No se ha tomado conciencia de la necesidad de proteger las instalaciones o la inversión en recursos de computación. No hay control ni monitoreo de los factores ambientales, que incluyen protección contra incendio, polvo, alta tensión y excesivo calor y humedad.

Observaciones: La normativa de seguridad informática aprobada en octubre 2003 no incluye el tema de seguridad física de las instalaciones. No existe control del acceso a los edificios y tampoco a los centros de procesamiento. Las visitas ajenas a la organización transitan libremente sin que se registre su ingreso. Los equipos de alimentación de energía alternativa (fuentes de alimentación de energía ininterrumpible y motogenerador) se encuentran sin mantenimiento preventivo. El mantenimiento del edificio es mínimo, existen sectores con exceso de empleados por metro cuadrado y las instalaciones eléctricas y de comunicaciones no cumplen con las normas de seguridad de aplicación en la Ciudad de Buenos Aires.

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

4.3.13. – Administración de Operaciones

Objetivo de control: Se debe establecer de un cronograma de actividades de soporte que se registre y apruebe para el logro de todas las actividades.

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia
- la eficiencia

y en forma secundaria:

- la integridad
- la disponibilidad

Nivel de madurez: Inicial / ad hoc. El organismo reconoce la necesidad de estructurar las funciones de soporte de Tecnología de la Información. Sin embargo, no hay procedimientos estándares establecidos y las actividades son de tipo reactivo. La mayoría de las operaciones no están formalmente programadas y los pedidos de procesamiento se aceptan sin validación

previa. Las computadoras que dan soporte a los procesos con frecuencia tienen interrupciones y demoras. Los empleados pierden tiempo por tener que esperar los recursos. Los sistemas no son estables ni están disponibles.

Observaciones: De la información recibida no surge la existencia de procedimientos estándar documentados para las operaciones de tecnología de información. Tampoco se tuvo conocimiento de la existencia de manuales de instrucciones y procedimientos de operación, documentación del proceso de puesta en marcha y otras tareas, programas de trabajo y registro de operaciones.

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

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

Este objetivo de control afecta los siguientes requerimientos de la información necesaria para cumplir las misiones del organismo, primariamente:

- la eficacia

y en forma secundaria:

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

Nivel de madurez: No conforma. El organismo no tiene procesos de monitoreo implementados. La función de Tecnología de la Información 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.

Observaciones: De la información recibida se desprende que no se han establecido formalmente políticas, procedimientos, objetivos e indicadores de desempeño. Consecuentemente no se realiza el monitoreo continuo y sistemático de la actividad del área de tecnología de la información.

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

5.- Análisis de la Vista

Habiendo transcurrido un plazo prudencial desde la solicitud de prórroga por parte del Organismo y siguiendo con las instrucciones recibidas de la Comisión de Supervisión (Nota Nº 163/05-CSPyPEyCI, fs. 101 de la presente Actuación), se da por concluida la redacción del informe sin el correspondiente descargo del organismo.

6.- Recomendaciones

6.1.- Planificación y organización.

6.1.1.- Definición de un Plan estratégico de Tecnología de la Información: La alta gerencia debe implementar planes a corto y largo plazo que sean compatibles con la misión y las metas de la organización. En este aspecto, debe garantizar que:

- la tecnología de información forme parte del plan de la organización a corto y largo plazo
- se elabore un Plan de Tecnología de la Información a largo plazo
- se actualiza el enfoque y la estructura de la planificación de Tecnología de la Información a largo plazo
- se realicen los cambios del plan de Tecnología de la Información a largo plazo
- se elabore la planificación a corto plazo de la función de servicios de información
- se comuniquen los planes de Tecnología de la Información
- se controlen y evalúen los planes de Tecnología de la Información
- se evalúen los sistemas existentes

6.1.2. – Definición de la Arquitectura de la Información: La máxima autoridad debe impulsar la creación y el mantenimiento de un modelo que contemple lo siguiente:

- un modelo de arquitectura de la información
- el diccionario de datos del organismo y reglas de sintaxis de los datos
- un esquema de clasificación de los datos
- los niveles de seguridad.

6.1.3. – Determinación de la dirección Tecnológica: Se debe crear y actualizar periódicamente un plan de infraestructura tecnológica. Dicho plan debe comprender aspectos tales como la arquitectura de los sistemas, la dirección tecnológica y las estrategias de información.

6.1.4. – Definición de la organización y las Relaciones de Tecnología de la Información: 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 de usuarios en la medida necesaria para lograr soluciones de tecnología de información eficientes. En este aspecto se debe asegurar:

- la designación de un comité de planificación de Tecnología de la Información
- 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 de la Información
- la separación de funciones
- la competencia del personal de Tecnología de la Información
- las descripciones de los puestos del personal de Tecnología de la Información

- las políticas y procedimientos relativos al personal contratado
- las relaciones de coordinación, comunicación y enlace.

6.1.5. – Administración de la Inversión en Tecnología de Información: Debe implementarse un proceso de formulación presupuestaria que contemple lo siguiente:
- un presupuesto operativo anual de Tecnología de la Información
- el monitoreo de costos y beneficios
- la justificación de costos y beneficios.

6.1.6. – Comunicación de los Objetivos y Directivas de la Gerencia: Se debe implementar un marco y un programa de concientización que propicien un ambiente de control positivo en todo el organismo. Este marco debe abordar la integridad, los valores éticos, y la competencia de las personas, la filosofía de gestión, el estilo operativo y la rendición de cuentas. En este aspecto, la máxima autoridad y la alta gerencia deben garantizar:
- la responsabilidades sobre la formulación de las políticas
- la comunicación de las políticas del organismo
- la disponibilidad de los recursos para la implementación de políticas
- el mantenimiento de políticas
- el cumplimiento de las políticas, los procedimientos y las normas
- el compromiso con la calidad
- la política marco de seguridad y control interno
- la observancia de los derechos de propiedad intelectual
- la comunicación de la concientización en materia de seguridad.

6.1.7. – Administración de los Recursos Humanos: El organismo debe contar con una fuerza laboral que tenga las habilidades necesarias para lograr sus metas. En este aspecto, la máxima autoridad y la alta gerencia deben garantizar que se realicen:
- la selección y promoción del personal
- la formación y experiencia del personal

- la definición de roles y responsabilidades
- la capacitación del personal
- la capacitación cruzada o personal de reemplazo
- los procedimientos de verificación de antecedentes del personal
- la evaluación del desempeño laboral
- el cambio de puestos y la seguridad en la extinción de la relación laboral.

6.1.8. – Evaluación de Riesgos: Se debe establecer un marco de evaluación sistemática de riesgos. Dicho marco debe incorporar una evaluación periódica de los riesgos de información relacionados con la consecución de los objetivos del organismo, que constituya una base para determinar cómo deben administrarse los riegos a un nivel aceptable. En este aspecto, la alta gerencia debe garantizar que se realice:
- una evaluación de riesgos de la actividad
- la identificación de riesgos
- la medición de riesgos
- un plan de acción de reducción de riesgos
- la aceptación de riesgos.

6.1.9. – Administración de Proyectos: Se debe establecer un marco de administración de proyectos que debe contemplar, como mínimo, la asignación de responsabilidades, división de tareas, presupuestación del tiempo y los recursos, plazos, puntos de verificación y aprobaciones. En este aspecto, la alta gerencia debe garantizar que:
- se aplique un marco de administración de proyectos
- se contemple la participación del departamento de usuarios en el inicio del proyecto
- se asignen miembros y responsabilidades del equipo del proyecto
- exista una definición del proyecto
- se aprueben las fases del proyecto
- exista un plan maestro del proyecto
- se defina un plan de garantía de calidad del sistema

- se implemente la administración formal de riesgos del proyecto
- se elabore un plan de pruebas
- se elabore un plan de capacitación
- se desarrolle un plan de revisión posterior a la implementación.

6.1.10. – Administración de la Calidad: Debe desarrollarse y mantenerse periódicamente un plan general de calidad basado en los planes del organismo y de tecnología de información a largo plazo. En este aspecto, la alta gerencia debe garantizar que exista:

- un plan general de calidad
- un enfoque de garantía de calidad
- una planificación de garantía de calidad
- la revisión de garantía de calidad 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 de la Información
- un marco de adquisición y mantenimiento de la infraestructura tecnológica
- un marco para las relaciones con terceros a cargo de la implementación
- la observación de las normas de documentación de programas verificando que:
    - se cumplan las normas de prueba de programas
    - se cumplan las normas de prueba de sistemas
    - se utilicen pruebas en paralelo/piloto
- la documentación de pruebas de sistemas

6.2.- Administración e implementación.

6.2.1. - Identificación de Soluciones Automatizadas

Recomendaciones: Se debe implementar una metodología del ciclo de vida de desarrollo de sistemas (CVDS) para el organismo con la especificación de los requerimientos funcionales y operativos de las soluciones, incluidos el rendimiento, la seguridad, confiabilidad, compatibilidad y legislación.

Además, la metodología del CVDS debe contemplar un plan de estrategias de adquisición de software y de evaluación de requerimientos y especificaciones para la contratación de terceros proveedores de servicios. En este aspecto, se debe garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:

- definición de los requerimientos de información
- formulación de cursos alternativos de acción
- formulación de la estrategia de adquisición
- formulación requisitos para servicios prestados por terceros
- estudio de factibilidad tecnológica
- estudio de factibilidad económica
- definición de la arquitectura de la información
- informe de análisis de riesgos
- controles de seguridad económicos
- diseño de pistas de auditoría
- adecuación ergonómica
- 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

6.2.2. - Adquisición y Mantenimiento del Software de Aplicación

Recomendaciones: Se deben 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, debe garantizarse la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:

- normalización de los métodos de diseño
- registración de los cambios importantes de los sistemas existentes
- aprobación del diseño
- definición y documentación de los requerimientos de archivos
- especificación de programas
- diseño de la recopilación de datos fuente
- definición y documentación de los requerimientos de entrada
- definición de interfaces
- normalización de la interfase usuario-máquina
- definición y documentación de los requerimientos de procesamiento
- definición y documentación de los requerimientos de salida
- normalización de la controlabilidad
- establecimiento de la disponibilidad como factor clave del diseño
- normalización de las especificaciones de integridad de tecnología de información en programas de aplicación
- realización de las pruebas del software de aplicación
- desarrollo de materiales de soporte y referencia del usuario
- reevaluación del diseño de sistemas

6.2.3. - Adquisición y Mantenimiento de la Infraestructura Tecnológica

Recomendaciones: Garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:

- evaluación del hardware y el software nuevos
- mantenimiento preventivo del hardware
- atender a la seguridad del software del sistema
- instalación del software del sistema
- mantenimiento del software del sistema
- realizar los controles de cambios del software del sistema

6.2.4. - Desarrollo y Mantenimiento de Procedimientos

Recomendaciones: Utilizar una metodología del ciclo de vida del desarrollo de sistemas (CVDS) del organismo de manera tal de garantizar la definición oportuna de los requerimientos operativos y niveles de servicio, la preparación de manuales de usuario y de operaciones y el desarrollo de materiales de capacitación. En este aspecto, la alta gerencia y el funcionario principal de la función de servicios de información deben verificar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:

- los requerimientos operativos y niveles de servicio
- la confección de manuales de procedimientos del usuario
- la confección del manual de operaciones
- la preparación de los materiales de capacitación

6.2.5. - instalación y Acreditación de Sistemas de aplicación

Recomendaciones: Se debe preparar, revisar y aprobar un plan de implementación o modificación de los sistemas de aplicación. En este aspecto, la alta gerencia y el funcionario principal de la función de servicios de información deben garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:

- capacitación de los usuarios y personal de servicios de información
- dimensionamiento del desempeño del software de aplicación
- desarrollar el plan de implementación

- conversión de sistemas de aplicación
- conversión de datos
- definir la estrategia y los planes de prueba
- realizar la prueba de cambios
- establecer criterios de ejecución de pruebas paralelas/piloto
- realizar la prueba de aceptación final
- realizar las pruebas de acreditación de seguridad
- realizar la prueba de funcionamiento
- transición a producción
- evaluación del cumplimiento de los requerimientos del usuario
- revisión de la gerencia posterior a la implementación

6.2.6. - Administración de Cambios

Recomendaciones: Implementar procedimientos específicos para tratar los pedidos de cambios, mantenimiento de sistemas y mantenimiento del proveedor. En este aspecto, la alta gerencia y el funcionario principal de la función de servicios de información deben garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:

- inicio y control de solicitudes de cambio
- evaluación del impacto
- control de cambios
- realizar los cambios de emergencia
- desarrollar documentación y procedimientos
- mantenimiento autorizado
- establecer políticas de versiones de software
- distribución de software

6.3. – Entrega y Soporte.

6.3.1. – Definición y Administración de los Niveles de Servicio: Garantizar la eficacia de las políticas y practicas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:

- establecer marco de acuerdos de nivel de servicio
- procedimientos de ejecución
- monitoreo e informes
- revisión de los contratos y acuerdos de nivel de servicio
- establecer un programa de mejora del servicio.

6.3.2. – Administración de Servicios Prestados por Terceros: Se debe verificar que los servicios prestados por terceros se identifiquen de modo adecuado y que la interrelación técnica y funcional con los proveedores esté documentada. En este aspecto, la máxima autoridad y la alta gerencia deben garantizar la eficacia de las políticas y practicas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:

- interrelación con proveedores de Tecnología de la Información
- asignar la responsabilidad por la relaciones
- formalización de contratos con terceros
- evaluación del conocimiento y la experiencia de terceros
- formalización de contratos de mercerización
- asegurar la continuidad de los servicios
- acordar las relaciones de seguridad
- monitoreo de la prestación del servicio.

6.3.3. – Administración de la Capacidad y el Desempeño: La máxima autoridad y la alta gerencia deben garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:

- identificación de requerimientos de disponibilidad y desempeño
- establecer un plan de disponibilidad
- monitoreo e informes del desempeño de los recursos de Tecnología de la Información

- utilización de herramientas para la creación de modelos
- administración proactiva del desempeño
- la realización de pronósticos de la carga de trabajo
- administración de la capacidad de los recursos
- establecer la disponibilidad de recursos
- planificación de recursos.

6.3.4. – Garantía de un Servicio Continuo: Se debe crear un marco de continuidad que defina los roles, responsabilidades, enfoque y las normas y estructuras para documentar un plan que garantice el servicio continuo. En este aspecto, la alta gerencia y el funcionario principal de la función de servicios de información deben garantizar la eficacia de las políticas y practicas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:

- un marco de continuidad de Tecnología de la Información
- definir estrategias y filosofía del plan de continuidad de Tecnología de la Información
- establecer contenido del plan de continuidad de Tecnología de la Información
- reducción de los requerimientos de continuidad de Tecnología de la Información
- mantenimiento del plan de continuidad de Tecnología de la Información
- realizar la prueba del plan de continuidad de Tecnología de la Información
- capacitación en el plan de continuidad de Tecnología de la Información
- distribución del plan de continuidad de Tecnología de la Información
- el resguardo del procesamiento alternativo del usuario
- identificar recursos críticos de Tecnología de la Información
- definir el sitio y equipamiento alternativos
- almacenamiento de resguardo en sitio alternativo
- reevaluación periódica del plan.

6.3.5. – Garantía de la Seguridad de los Sistemas: La alta gerencia y el funcionario principal de la función de servicios de información deben garantizar la eficacia de las políticas

y practicas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:

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

6.3.6. – Identificación e Implementación de Costos: La máxima autoridad y la alta gerencia deben garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:

- identificar ítems imputables
- definir procedimientos de determinación de costos

- utilizar procedimientos de cargos e imputación de costos al usuario.

6.3.7. – Educación y capacitación de los Usuarios: La máxima autoridad debe garantizar la eficacia de las políticas y practicas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:
- identificación de necesidades de capacitación
- organización de sesiones de capacitación
- capacitación y concientización en los principios de seguridad.

6.3.8. – Asistencia y Asesoramiento a los Usuarios de Tecnología de la Información: El funcionario principal de servicios de información debe garantizar la eficacia de las políticas y practicas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:
- 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.

6.3.9. – Administración de la Configuración: El funcionario principal de la función servicios de información debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:
- registro de la configuración
- establecer el nivel básico de configuración
- registro del estado de la configuración
- control de la configuración
- detectar el software no autorizado
- almacenamiento del software
- administración de configuración

- seguimiento y control de versiones de software.

6.3.10. – Administración de Problemas e Incidentes: El funcionario principal de la función de servicios de información debe garantizar la eficacia de las políticas y practicas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:
- sistema de administración de problemas
- escalamiento de problemas
- seguimiento de problemas y pistas de auditoría
- autorizaciones de emergencia y acceso temporario
- establecer las prioridades de procesamiento de emergencia.

6.3.11. – Administración de Datos: La alta gerencia, los responsables de programas y actividades y el funcionario principal de la función de servicios de información deben garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:
- preparación de datos
- autorización de documentos fuente
- recopilación de datos de documentos fuente
- manejo de errores de documentos fuente
- conservación de documentos fuente
- autorización de entrada de datos
- verificación de exactitud, integridad y autorización
- manejo de errores de entrada de datos
- asegurar la integridad del procesamiento de datos
- validación y edición del procesamiento de datos
- manejo de errores del procesamiento de datos
- manejo y conservación de salidas
- distribución de salidas de datos
- balanceo y conciliación de salidas de datos

- revisión y manejo de errores de salidas de datos
- seguridad de los informes de salida
- protección de información crítica durante la transmisión y el transporte
- protección de información crítica eliminada
- administración del almacenamiento
- establecer períodos de conservación y condiciones de almacenamiento
- establecer un sistema de administración de biblioteca de medios
- definir las responsabilidades de administración de la biblioteca de medios
- resguardo y restauración
- tareas de resguardo
- almacenamiento de resguardos
- administración de archivos
- protección de mensajes críticos
- autenticación e integridad.

6.3.12. – Administración de Instalaciones: El funcionario principal de la función de servicios de información debe garantizar la eficacia de las políticas y practicas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:
- seguridad física
- asegurar la discreción del sitio de tecnología de información
- acompañamiento de visitas
- salud y seguridad del personal
- protección contra factores ambientales
- disponibilidad de fuente de alimentación de energía ininterrumpible.

6.3.13. – Administración de Operaciones: El funcionario principal de la función de servicios de información debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de Tecnología de la Información:

- desarrollo de manuales de instrucciones y procedimientos de las operaciones de procesamiento
- documentación del proceso de puesta en marcha y otras operaciones
- fijación de programas de trabajo
- control de las desviaciones de los programas estándares de trabajo
- asegurar la continuidad del procesamiento
- registración de operaciones
- salvaguardia de formularios especiales y dispositivos de salida
- realización de operaciones remotas.

6.4. – Monitoreo.

6.4.1. – Monitoreo de los Procesos: La alta gerencia es responsable de garantizar que se:

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

7.- Conclusiones.

La situación de la Tecnología Informática en el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados, basándose en los procedimientos efectuados y la evidencia obtenida, merece las siguientes observaciones:

En general los niveles gerenciales del Organismo tienen un alto grado de rotación. En particular cabe destacar que durante el trabajo de campo se trabajó con tres Gerentes de Tecnología y Planeamiento. Existe un organigrama con misiones y funciones aprobadas en 2003 que no se aplica estrictamente. La cantidad total de personal del organismo es de aproximadamente 11.000 agentes. En el sector de sistemas trabajan 106 personas de las cuales sesenta son personal técnico, mientras que el resto realiza tareas administrativas. La dotación del área de Tecnología es reducida para el volumen de tareas que debería realizar el sector si asumiera la problemática de todo el organismo.

Se han observado datos erróneos almacenados en las bases principales que los sistemas aplicativos no deberían admitir (Anexo I).
El sistema SAP con el cual se realiza la gestión económica y financiera es alimentado con información proveniente de sistemas que no han sido aprobados formalmente y que consecuentemente no satisfacen requerimientos de confiabilidad e integridad.
Del análisis del riesgo al que se encuentran sometidos los siete requerimientos (eficacia, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad) que debería satisfacer la información provista por el área de Tecnología de la Información se concluye (ver Anexo IV) que el riesgo promedio, teniendo en cuenta los treinta procesos considerados, se encuentra entre el 71% y el 82%.
Finalmente se evalúa que, de acuerdo con el Modelo Genérico de Madurez[*] y los niveles detectados durante el presente trabajo y representados gráficamente en el Anexo III, la gestión de la tecnología informática en el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados se encuentra, salvo excepción, entre el nivel de madurez "No conforma" y el "Inicial", poniendo en peligro la eficiencia en el cumplimiento de los objetivos del organismo e, incluso, la eficacia en su concreción.

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".-

A los efectos de superar las observaciones realizadas es imprescindible un fuerte compromiso de las máximas autoridades del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados, que deberán trasladar a las gerencias dependientes, con el objeto de lograr mejoras en los controles existentes e incorporar los controles aún no implementados.

[*] Ver Modelo Genérico de Madurez en página 7.

8.- LUGAR Y FECHA

BUENOS AIRES, DICIEMBRE DE 2005.

9.- FIRMA

Anexo I: Análisis de datos del Padrón Nacional de beneficiarios

Si bien la base de datos Padrón Nacional no era en sí mismo un objetivo de control, el análisis básico de la misma fue necesario a efectos de determinar el nivel de calidad de datos utilizados en el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados. De tal estudio, realizado sobre la copia de la base actualizada al 31 de agosto de 2004 y sus tablas asociadas, enviada a esta auditoría por la Gerencia de Tecnología y Planeamiento del Organismo, se observaron hechos significativos que hacen a la confiabilidad, la integridad, la eficacia y la eficiencia de la información.

Se encontró que los beneficiarios están registrados con distintos tipos de documentos. Esta situación dificulta el cruce de datos y los controles sobre la existencia de beneficiarios duplicados.

La cantidad de afiliados para cada tipo de documento es la siguiente:

LE	Libreta de Enrolamiento	426.638
LC	Libreta Cívica	991.089
CI	Cédula de Identidad	136.100
DNI	Documento Único	583.780
PAS	Pasaporte	64
LM	Libreta Masculina	366.988
LF	Libreta Femenina	578.690
SD	Sin Identificación	24
RN	Recién Nacido	21
CIC	Cédula de Identidad Chile	15
	TOTAL	3.083.609

- Para el caso de los beneficiarios registrados con tipo de documento Recién Nacido (RN) se pudo determinar que existen dos personas nacidas en los años 1931 y 1936
- Para el caso de los beneficiarios identificados con Pasaporte se detectaron cinco casos registrados con nacionalidad Argentina y otros cinco casos con nacionalidad Naturalizado.
- La discriminación por nacionalidad es la siguiente:

A	Argentina	2.801.510
E	Extranjero	257.649
M	A	94
X	No informado	168
N	Naturalizado	24.188
	TOTAL	3.083.609

Se destaca que para la nacionalidad registrada como “M” en la tabla asociada la descripción es la letra “A”. No se pudo obtener evidencia de su significado

- Del análisis de las fecha de nacimiento se obtuvo el siguiente detalle:
    - 2.819 casos con fecha de nacimiento anteriores a 1905 es decir más de 100 años, de los cuales 19 personas tienen más de 120 años. De la información proporcionada por el Instituto Nacional de Estadísticas y Censos en su página web se informa que para el año 2001 existen en todo el país 1855 personas mayores de 100 años.
    - 438 casos con fecha de nacimiento el 01/01/1901, 80 casos con fecha de nacimiento el 01/01/1900 y 11 casos con fecha de nacimiento el 01/01/1902.
    - 2.816 casos con fecha de nacimiento en cero
- El análisis por número de CUIL/CUIT. demuestra lo siguiente:
    - del total del padrón existen 829.715 casos con CUIL en cero
    - existen casos con CUIL/CUIT que no se corresponden con los datos registrados en AFIP ni en ANSeS, por ejemplo:
        - Un caso que se encuentra registrado en AFIP y ANSeS bajo el CUIL/CUIT 20-05746142-0, mientras que en el Padrón de Beneficiarios figura con el CUIT/CUIL 20-00000000-1.
    - 188.116 casos con CUIL/CUIT repetidos dentro de los cuales se destaca la existencia de:

      29 casos con CUIT 33-06379144-9 que para la AFIP se registra como Razón Social no disponible y

1673 casos con CUIT 33-63761744-9 registrado en la AFIP como perteneciente a la ANSeS.

- Del análisis por nombre y apellido se pudo determinar que:
    - 22 casos con apellido A
    - 1 caso con apellido que comienza con un signo suma
    - 1 caso con apellido que comienza con un numero
    - 526.046 registros con apellido y nombre duplicados, de los cuales se pudieron extractar 108 registros donde coinciden en 54 pares el nombre, el tipo y número de documento y la fecha de nacimiento. En uno de esos casos, coinciden todos los datos con excepción de la fecha de alta y del grado de parentesco, el cual en un registro corresponde a Esposa y en otro a Concubina.
- Del análisis por fecha de alta del beneficiario se encontró un caso con fecha de alta 11/10/1928, anterior al 13 de mayo de 1971 fecha de creación del INSSJP
- Del análisis por grado de parentesco se pudo determinar que:
    - existen 21 personas menores de 40 años identificadas con grado de parentesco Hijo/a Mayor de 60 años (código 41)
    - existen 15 beneficiarios identificados con el grado de parentesco Menores Bajo Guarda (códigos 90 al 95) con edades entre los 22 y 23 años
    - existen 36 personas registradas con el grado de parentesco Menores Bajo Guarda (código 40) con edades entre los 22 y 26 años
    - existe una afiliada registrada con el grado de parentesco Abuela/o (código 22) con 17 años de edad, registro número 44714.

Conclusiones:

Cabe destacar que la falta de datos confiables en el campo CUIL, conjuntamente con el inconveniente descrito en los tipos y números de documentos, hace dificultosa la realización de cruzamiento de datos con otras bases de datos del Estado como ser la base de la Administración Nacional de la Seguridad Social y contra si misma

Finalmente, de lo expuesto arriba, se infiere que en el software de aplicación para alta, baja y modificación del Padrón Nacional, no existen controles que impidan irregularidades, lo que torna a la información en poco confiable y con un alto grado de inseguridad.

Anexo II: Modelo de arquitectura de la información. Diccionario de datos corporativo y reglas de sintaxis de los datos.

Para verificar la definición de los datos se compararon, a modo de ejemplo, los diseños de registros de las base de datos de Padrón Nacional, utilizado para calcular los montos a abonar a los prestadores de servicios de salud y de la base de datos de Afiliados en Geriátricos, que permite establecer el valor de las retribuciones a abonar, obteniéndose para los datos más significativos el siguiente detalle:

- Número de afiliado al PAMI:
    - En el Padrón Nacional se usa el campo N_BENEFICIO (Número de beneficio) definido como numérico de 12 posiciones
    - En Geriátricos corresponde al campo NRO_DE_AFILIADO definido como alfabético de 14 posiciones.
- Número de documento de identidad:
    - En el Padrón se usa el campo N_DOCU (Número de documento) definido como numérico de 8 posiciones.
    - En la base de Geriátricos corresponde al campo NRO_DE_DOCUMENTO definido como alfabético de 11 posiciones.
- Tipo de documento de identidad:
    - En el Padrón se usa el campo T_DOCU (Tipo de documento) definido como alfabético de 3 posiciones.
    - En la base de Geriátricos corresponde al campo TIPO_DOCUMENTO definido como numérico de 8 posiciones.
- Clave Única de Identificación Tributaria:
    - En el Padrón se usa el campo N_CUIT (número de CUIT) definido como alfabético de 13 posiciones.
    - En la base de Geriátricos no se utiliza el CUIT.

Esta comparación permite verificar que no existe un modelo de arquitectura de la información, ni un diccionario de datos, ni reglas de sintaxis.

Anexo III

Gráficos de brecha para los niveles de madurez de los objetivos de control considerados.

Diagrama de brechas
en Planificación y Organización

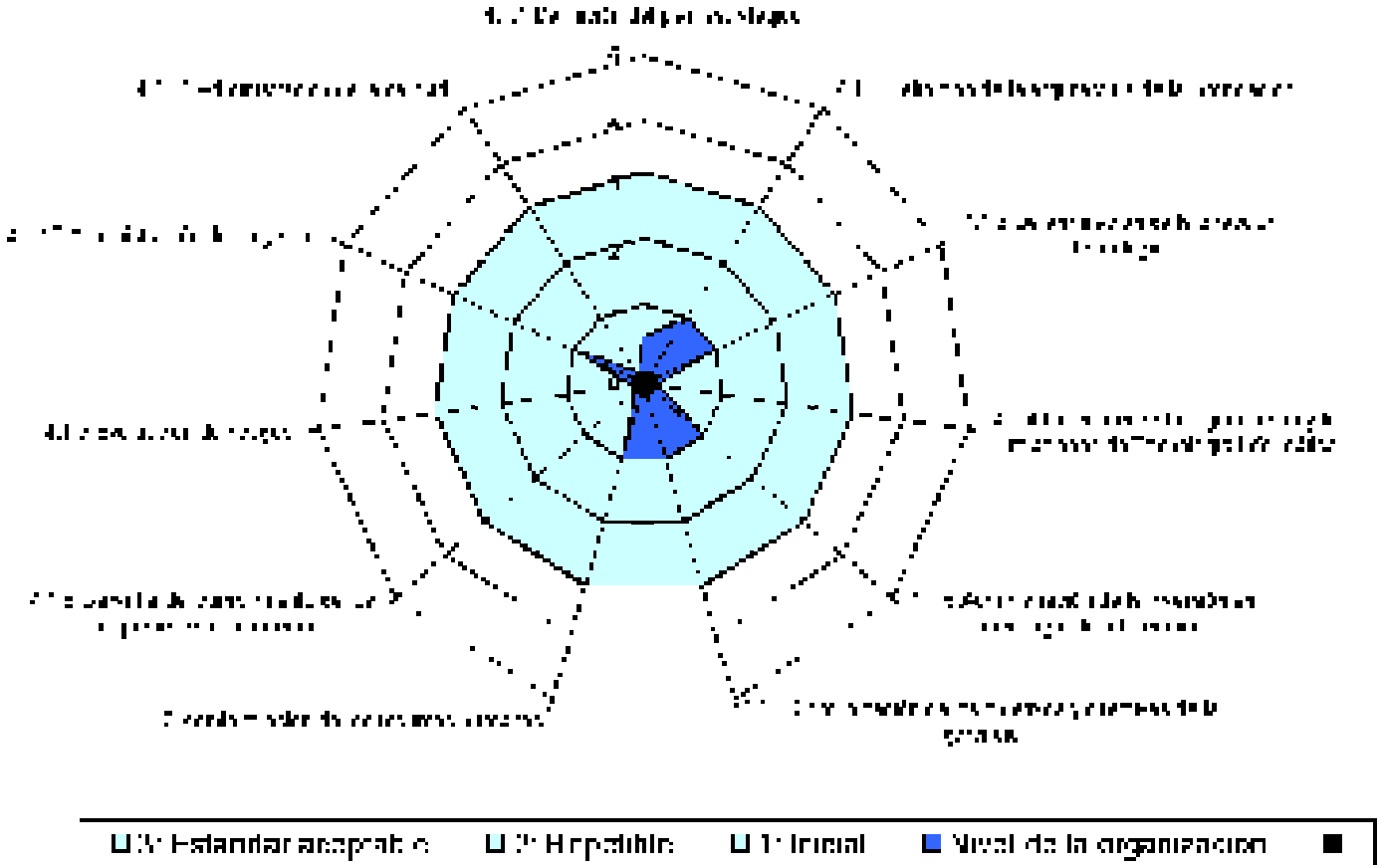


Diagrama de brechas en Adquisición e Implementación

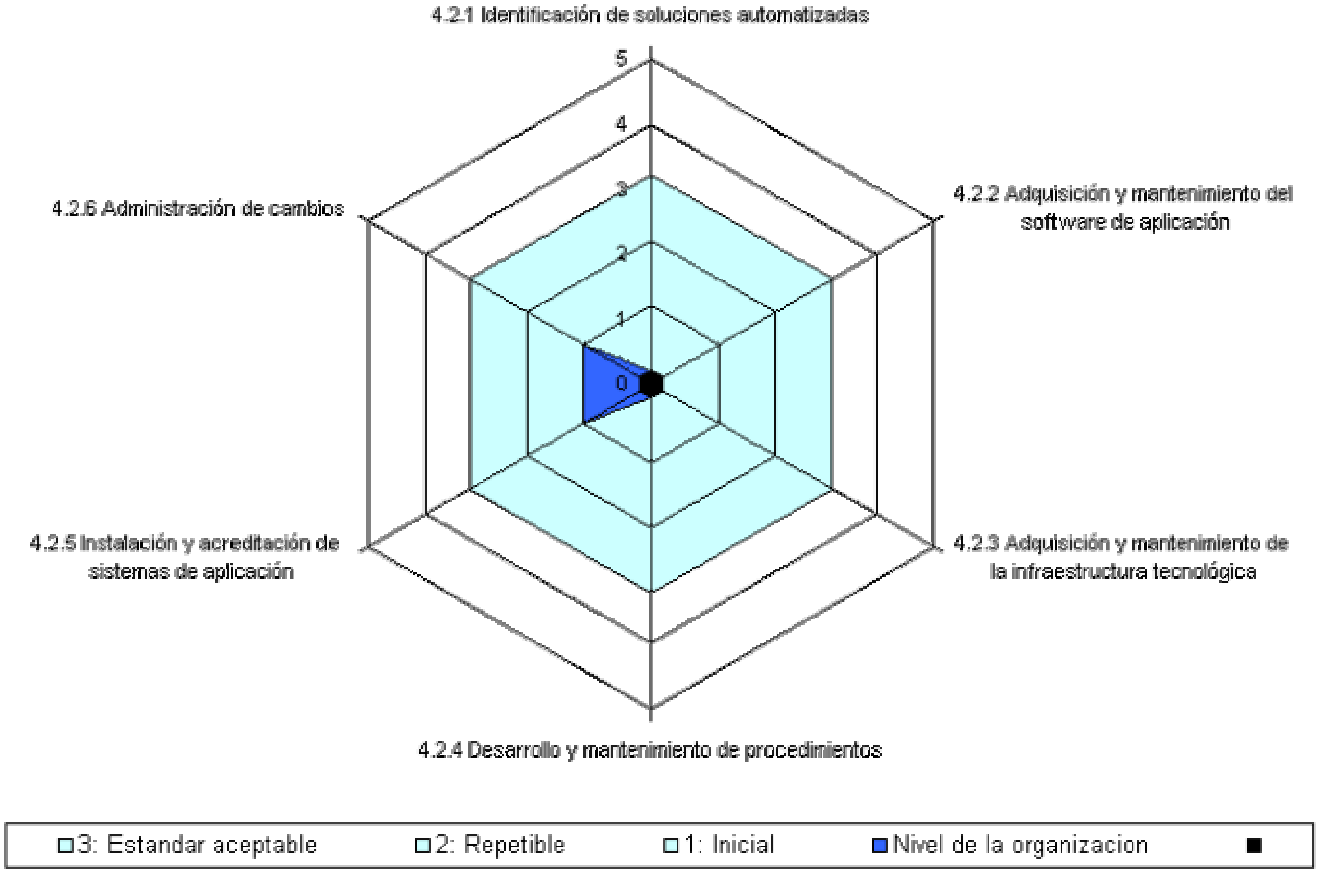
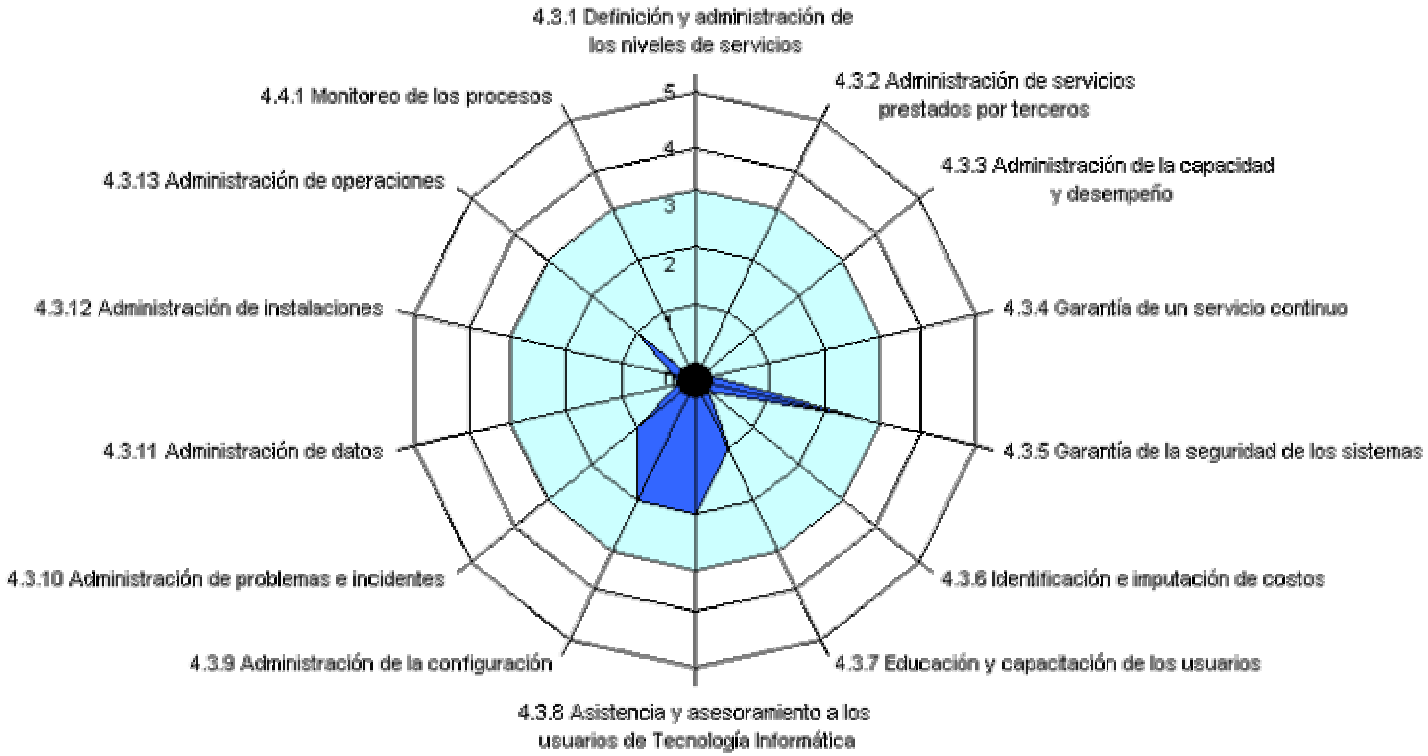


Diagrama de brechas
en Entrega y Soporte y en Monitoreo



Anexo IV: Estimación de los Niveles de Riesgo para los requerimientos de la información según los procesos informáticos considerados

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

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

Cada proceso hace a uno o más de los siguientes requerimientos que debe satisfacer la información dentro de un organismo para permitirle cumplir con sus misiones y funciones:

- *Eficacia***:** Se refiere a que la información sea relevante y pertinente para la misión del ente, así como a que su entrega sea oportuna, correcta, consistente y utilizable.
- *Eficiencia***:** Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
- *Confidencialidad***:** se refiere a la protección de información sensible contra divulgación no autorizada.
- *Integridad***:** Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del organismo.
- *Disponibilidad***:** Se refiere a la disponibilidad de la información cuando ésta es requerida para cumplir con las misiones del organismo, ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- *Cumplimiento*: Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el organismo está sujeto.
- *Confiabilidad***:** Se refiere a la provisión de información apropiada a la administración para operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

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

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

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

El proceso de cálculo parte de la base de que el riesgo es directamente proporcional al impacto definiendo como impacto el peligro de incumplimiento de las misiones y funciones del organismo, para los procesos involucrados en el objetivo de control, y a la probabilidad de ocurrencia del evento.
Para cada uno de los procesos se definió el impacto como alto (99%), medio (66%) o bajo (33%).
En cuanto a la probabilidad de ocurrencia se entiende que la misma está directamente vinculada a la calidad del control que se realiza y este es evaluado en el informe a través del nivel alcanzado según el modelo de madurez. A cada nivel se le asignó un coeficiente según el siguiente detalle:

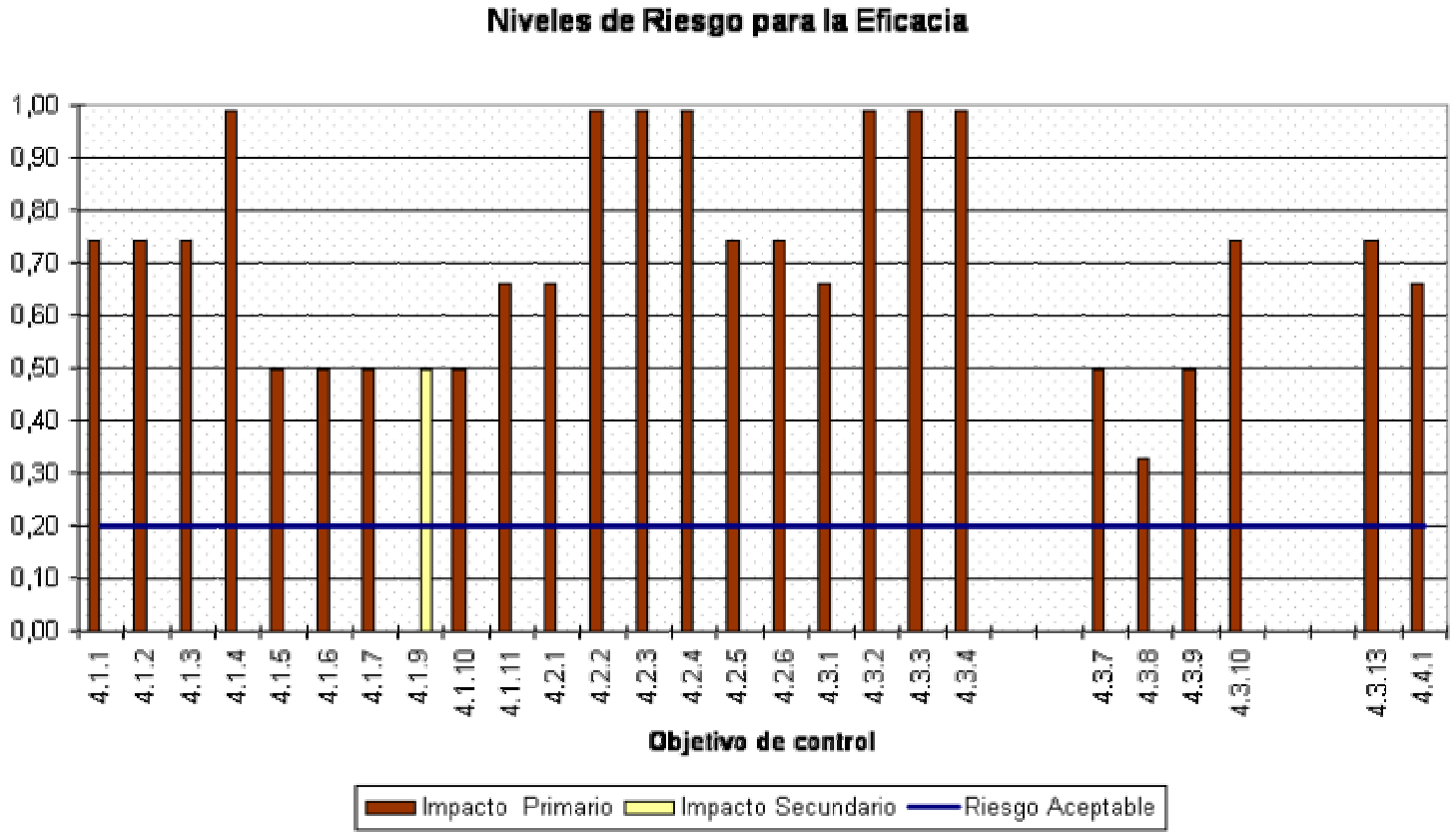
Nivel de Madurez	**Coeficiente**
No conforma	1,00
Inicial	0,75
Repetible aunque intuitivo	0,50
Proceso Definido	0,30
Administrado	0,20
Optimizado	0,10

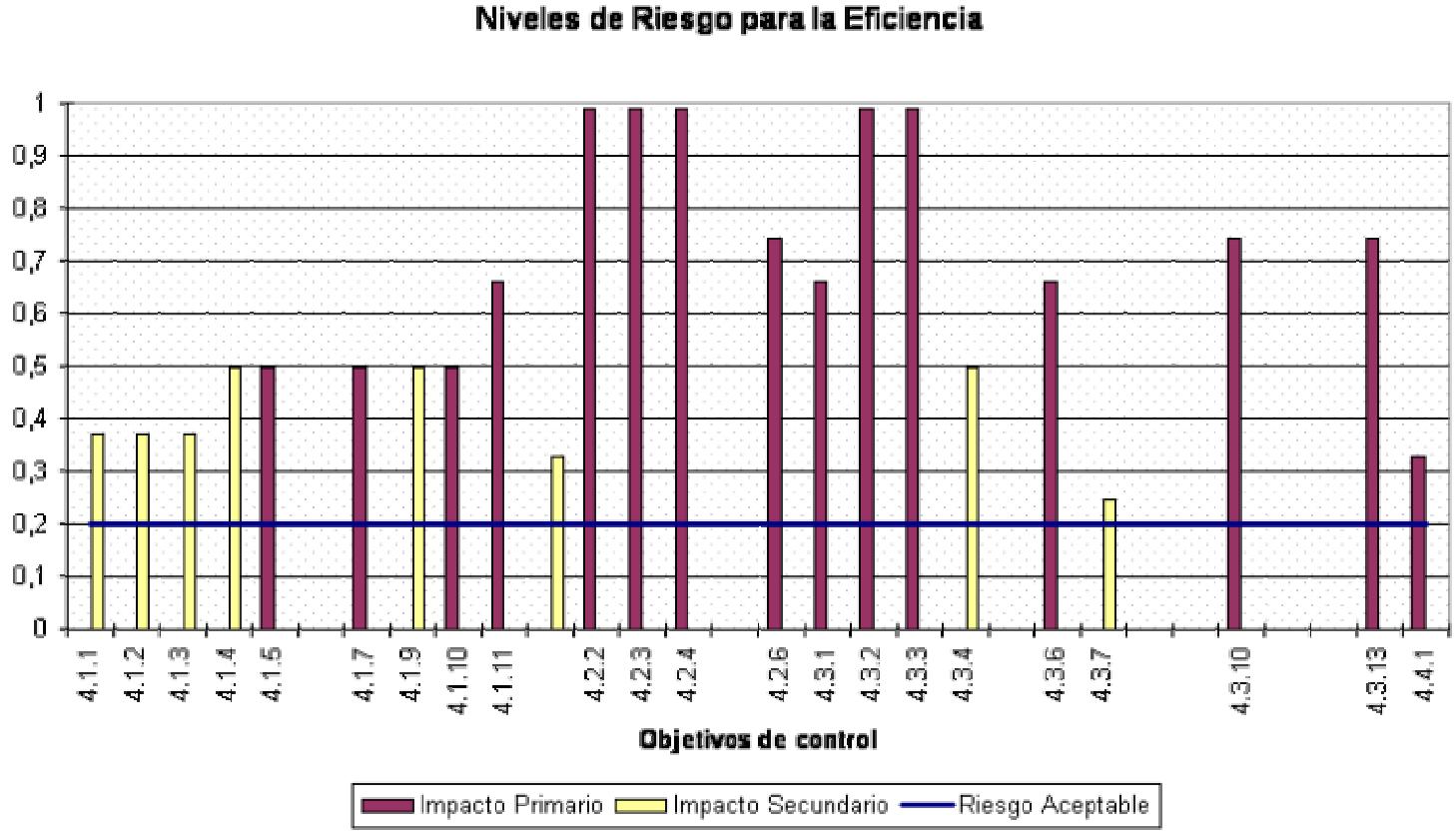
Tabla I

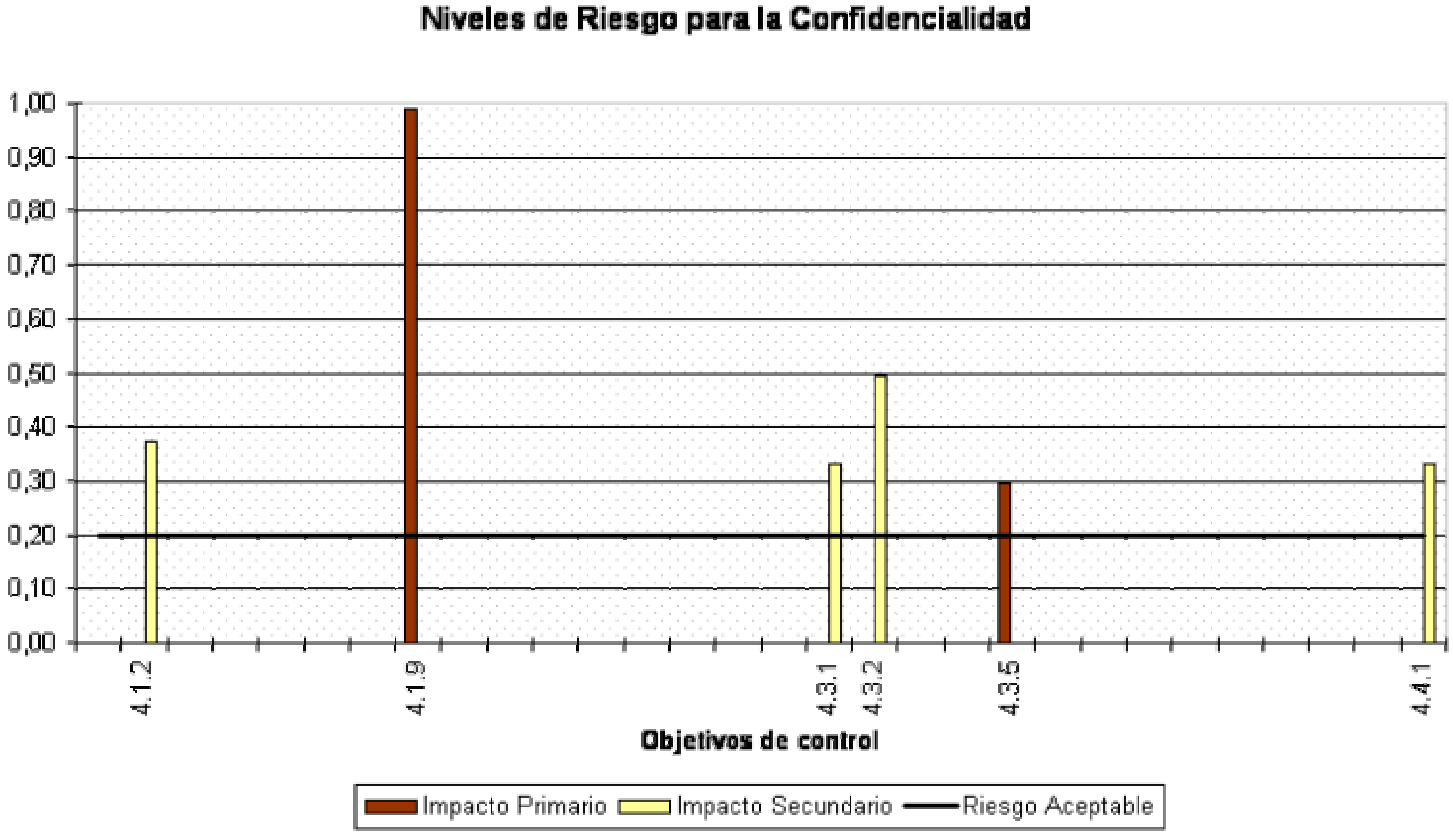
Dominio		Proceso	Requerimiento de la información						
			efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad
Planeamiento y Organización	4.1.1	Definir un plan estratégico de sistemas	P	S					
	4.1.2	Definir la arquitectura de la información	P	S	S	S			
	4.1.3	Determinar la dirección tecnológica	P	S					
	4.1.4	Definir la organización y sus relaciones	P	S					
	4.1.5	Administrar las inversiones (en TI)	P	P					S
	4.1.6	Comunicar la dirección y objetivos de la gerencia	P					S	
	4.1.7	Administrar los recursos humanos	P	P					
	4.1.8	Evaluar riesgos	S	S	P	P	P	S	S
	4.1.9	Administrar proyectos	P	P					
	4.1.10	Administrar calidad	P	P		P			S
Adquisición e Implementación	4,2,1	Identificar soluciones de automatización	P	S					
	4,2,2	Adquirir y mantener software de aplicación	P	P		S		S	S
	4,2,3	Adquirir y mantener la arquitectura tecnológica	P	P		S			
	4,2,4	Desarrollar y mantener procedimientos	P	P		S		S	S
	4,2,5	Instalar y acreditar sistemas de información	P			S	S		
	4,2,6	Administrar cambios	P	P		P	P		S
Entrega y Soporte de Servicios	4,3,1	Definir niveles de servicio	P	P	S	S	S	S	S
	4,3,2	Administrar servicios de terceros	P	P	S	S	S	S	S
	4,3,3	Administar desempeño y capacidad	P	P			S		
	4,3,4	Asegurar continuidad de servicio	P	S			P		
	4,3,5	Garantizar la seguridad de sistemas			P	P	S	S	S
	4,3,6	Identificar y asignar costos		P					P
	4,3,7	Educar y capacitar a usuarios	P	S					
	4,3,8	Apoyar y orientar a clientes	P						
	4,3,9	Administrar la configuración	P				S		S
	4,3,10	Administrar problemas e incidentes	P	P			S		
	4,3,11	Administrar la información				P			P
	4,3,12	Administrar las instalaciones				P	P		
	4,3,13	Administrar la operación	P	P		S	S		
Monitoreo	4,4,1	Monitorear el proceso	P	S	S	S	S	S	S

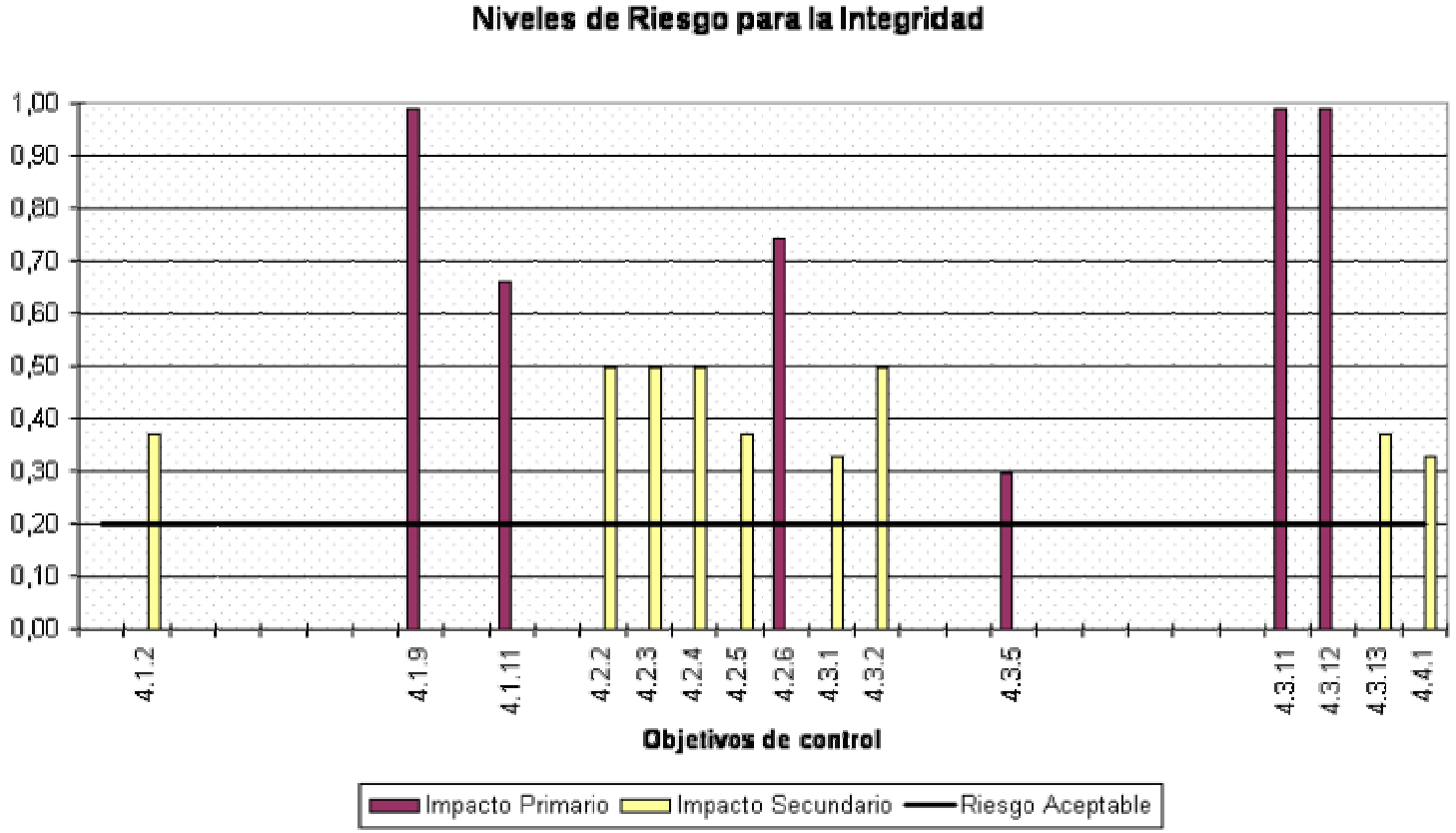
Anexo V

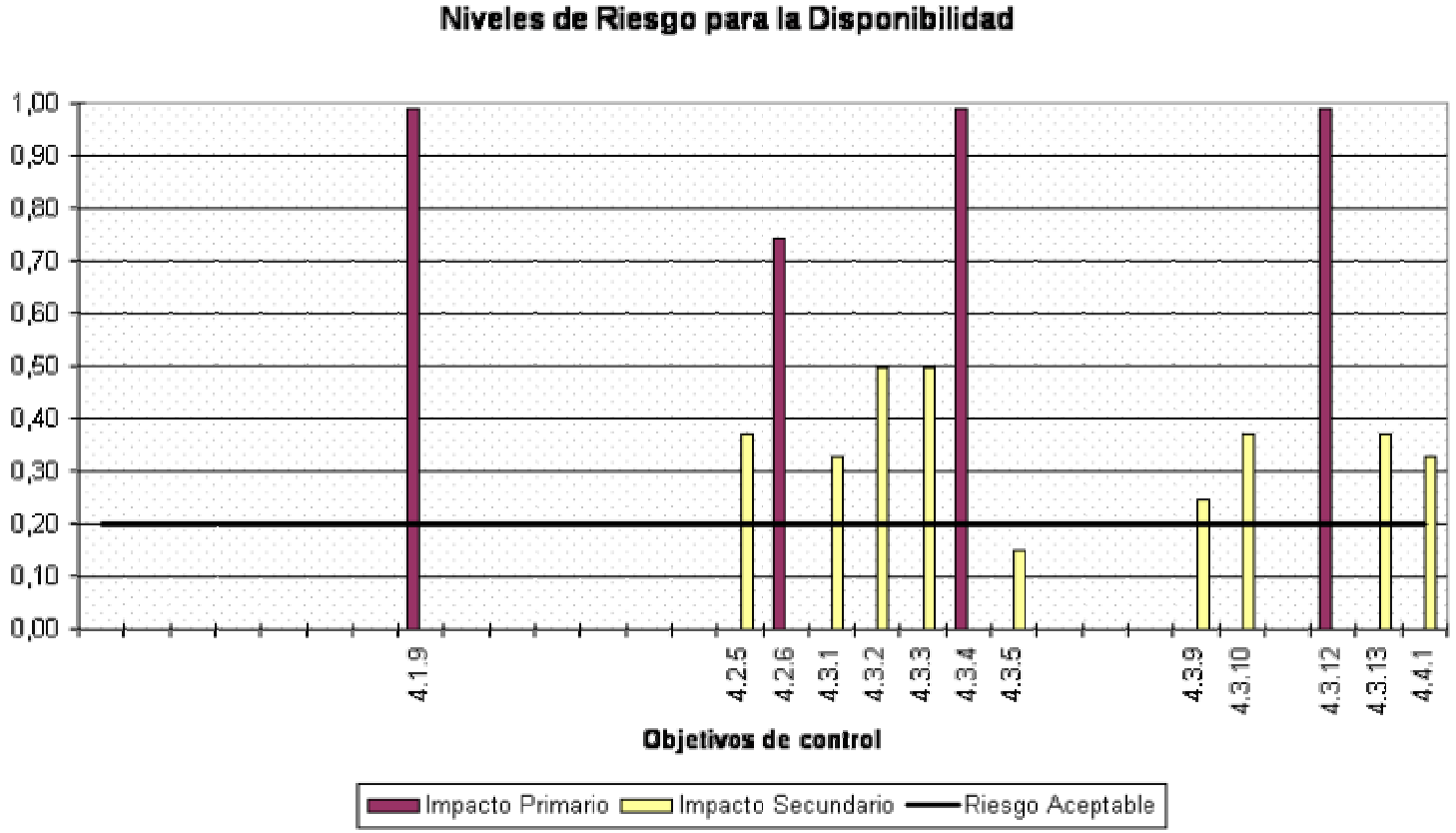
Gráficos de los niveles de riesgos para cada uno de los requerimientos de la información para cada uno de los treinta objetivos de control considerados y el promedio general.

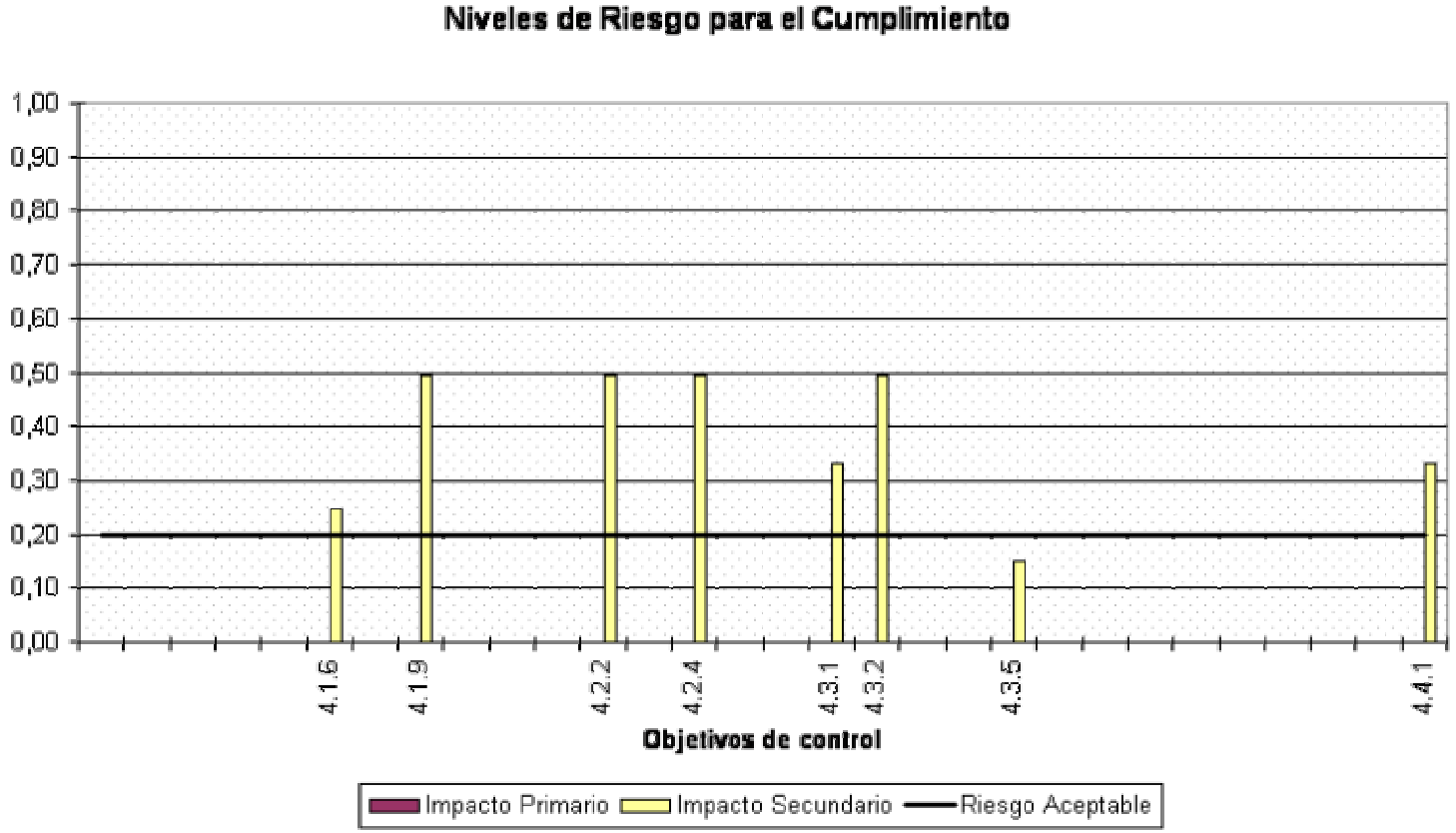

Niveles de Riesgo para la Eficacia
1,00
0,90
0,80
0,70
0,60
0,50
0,40
0,30
0,20
0,10
0,00
4.1.1
4.1.2
4.1.3
4.1.4
4.1.5
4.1.6
4.1.7
4.1.9
4.1.10
4.1.11
4.2.1
4.2.2
4.2.3
4.2.4
4.2.5
4.2.6
4.3.1
4.3.2
4.3.3
4.3.4
4.3.7
4.3.8
4.3.9
4.3.10
4.3.13
4.4.1
Objetivo de control
Impacto Primario
Impacto Secundario
Riesgo Aceptable

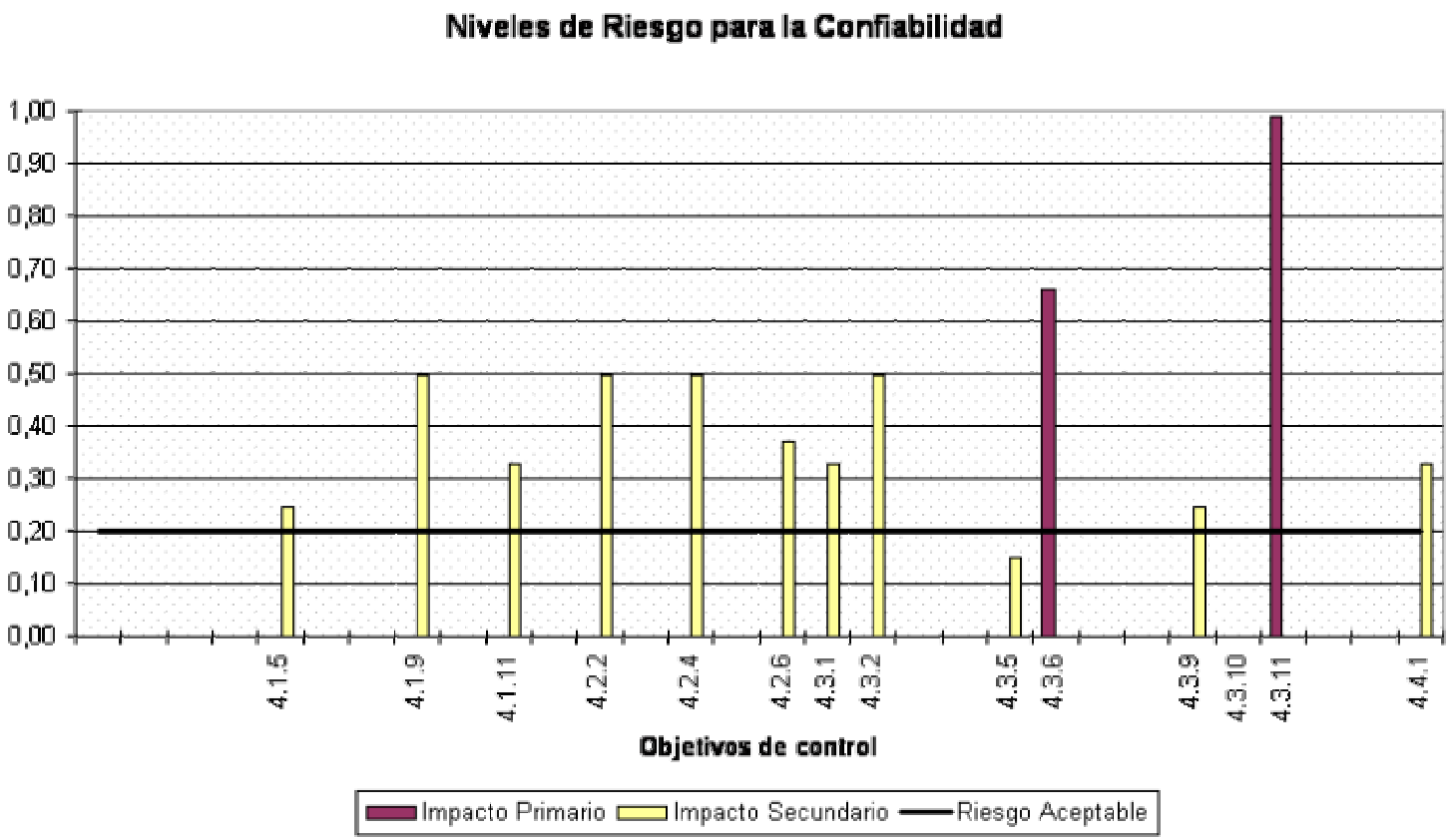

Niveles de Riesgo para la Eficiencia
1
0,9
0,8
0,7
0,6
0,5
0,4
0,3
0,2
0,1
0
4.1.1
4.1.2
4.1.3
4.1.4
4.1.5
4.1.7
4.1.9
4.1.10
4.1.11
4.2.2
4.2.3
4.2.4
4.2.6
4.3.1
4.3.2
4.3.3
4.3.4
4.3.6
4.3.7
4.3.10
4.3.13
4.4.1
Objetivos de control
Impacto Primario
Impacto Secundario
Riesgo Aceptable


Niveles de Riesgo para la Confidencialidad
1,00
0,90
0,80
0,70
0,60
0,50
0,40
0,30
0,20
0,10
0,00
4.1.2
4.1.9
4.3.1
4.3.2
4.3.5
4.4.1
Objetivos de control
Impacto Primario
Impacto Secundario
Riesgo Aceptable


Niveles de Riesgo para la Integridad
1,00
0,90
0,80
0,70
0,60
0,50
0,40
0,30
0,20
0,10
0,00
4.1.2
4.1.9
4.1.11
4.2.2
4.2.3
4.2.4
4.2.5
4.2.6
4.3.1
4.3.2
4.3.5
4.3.11
4.3.12
4.3.13
4.4.1
Objetivos de control
Impacto Primario
Impacto Secundario
Riesgo Aceptable


Niveles de Riesgo para la Disponibilidad
1,00
0,90
0,80
0,70
0,60
0,50
0,40
0,30
0,20
0,10
0,00
4.1.9
4.2.5
4.2.6
4.3.1
4.3.2
4.3.3
4.3.4
4.3.5
4.3.9
4.3.10
4.3.12
4.3.13
4.4.1
Objetivos de control
Impacto Primario
Impacto Secundario
Riesgo Aceptable


Niveles de Riesgo para el Cumplimiento
1,00
0,90
0,80
0,70
0,60
0,50
0,40
0,30
0,20
0,10
0,00
4.1.6
4.1.9
4.2.2
4.2.4
4.3.1
4.3.2
4.3.5
4.4.1
Objetivos de control
Impacto Primario
Impacto Secundario
Riesgo Aceptable


Niveles de Riesgo para la Confiabilidad
1,00
0,90
0,80
0,70
0,60
0,50
0,40
0,30
0,20
0,10
0,00
4.1.5
4.1.9
4.1.11
4.2.2
4.2.4
4.2.6
4.3.1
4.3.2
4.3.5
4.3.6
4.3.9
4.3.10
4.3.11
4.4.1
Objetivos de control
Impacto Primario
Impacto Secundario
Riesgo Aceptable

Niveles promedio de riesgo en los objetivos de control considerados.